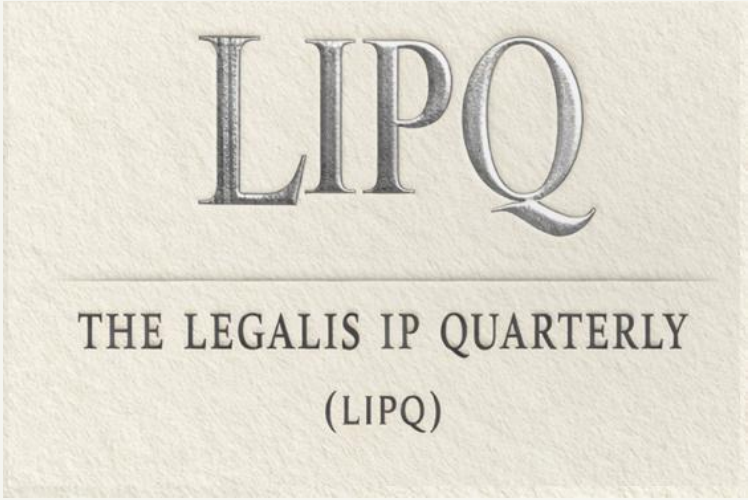
LEGALIS IP

A Specialist Discourse Platform on Law



The Legalis IP Quarterly

VOLUME I | ISSUE I

APRIL 2026

EDITORIAL MASTHEAD

Volume I | Issue I | 2026

Contents

Foreword

The legal landscape of the twenty-first century is no longer defined solely by the boundaries of physical territory or the ink of traditional statutes. We find ourselves at a critical juncture where the rapid development of technologies, particularly artificial intelligence and decentralised digital economies, has moved beyond the established pace of judicial precedent. In this period of relative uncertainty, the requirement for rigorous and interdisciplinary scholarship has become essential.

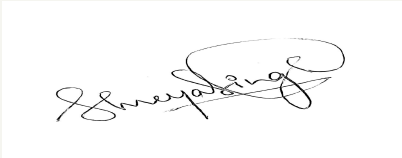
It is with a clear sense of purpose that we present the inaugural issue of *The Legalis IP Quarterly*.

Legalis IP was established on the principle that Intellectual Property law cannot be viewed in isolation. It serves as the vital link between technical innovation and ethical standards, and between private commercial incentives and broader public policy. As we operate in an environment where digital code increasingly dictates legal outcomes, our mission is to provide a specialised platform for discourse that remains technically accurate and legally sound.

This first issue demonstrates the range of our academic interests. Our contributors address the regulatory gaps in space medicine and astronaut protection, the evolving frameworks of copyright in the age of generative machine learning, and the legal integrity of borderless digital realities such as the metaverse. These articles offer more than a simple analysis of existing law. They challenge fundamental assumptions regarding authorship, platform liability, and even the application of international humanitarian law in modern asymmetric conflicts.

The publication of this journal is the result of the consistent effort of our Editorial Board and the leadership of our founder-President, Om Dwivedi. I must express my gratitude to our Senior Editors, Hari S. Nayar, Dr Rick Maity, and Thushara Kottieth. furthermore, special recognition is due to Dhruv Aditya for his leadership of the Junior Editorial team. His oversight of the technical review process ensured that this volume maintains the highest standards of academic quality.

As you read these contributions, we invite you to consider this publication as the beginning of a broader conversation. The future of law and technology remains a subject of active debate. We trust that *The Legalis IP Quarterly* will provide the forum where that future is examined and protected.



SHREYA SINGH
Editor-in-Chief
The Legalis IP Quarterly
April 2026

CLOSING REGULATORY GAPS IN SPACE LAW: A FRAMEWORK FOR ASTRONAUT HEALTH PROTECTION

By Divya Dattatraya Dhayagude

VOLUME I | ISSUE I | ARTICLE I

APRIL 2026

The Legalis IP Quarterly

Abstract

Deep-space exploration is the branch of astronomy, astronautics and space technology for exploration of distant regions of outer space. It consists of missions beyond Earth's atmosphere to deepen our understanding of the universe. These missions are beneficial in a wide range of areas monitoring security, health and many more involving both human spaceflight missions and robotic missions. The long-duration journeys away from earth orbit subject astronauts to considerable long-term health threats such as increased cancer risk from galactic cosmic radiation and solar particle interactions, cardiovascular deterioration, muscle and bone loss, neuro-ocular syndrome, and various physiological and psychological impacts resulting from extended periods of microgravity and isolation.

Existing regulatory frameworks do not sufficiently provide physiological and psychological health related protection to astronauts, they primarily focus on immediate damages, state accountability and liability for direct, acute harm resulting from space activities. They give limited or no specific guidelines for chronic, latent or delayed health issues that could emerge years or even decades after the mission. This results in substantial gaps in astronaut protection and legal accountability.

This paper is divided into three parts. The first part deals with analysis of existing legal frameworks and their limitations regarding long-term health protection. The second part discusses identification and examination of legal gaps including telemedicine licensing, cross-jurisdictional medical practice regulations for multinational crews, unclear

mechanisms for attributing medical responsibility and liability in collaborative missions involving state and private actors, lack of standardised insurance models or compensation frameworks capable of addressing post-mission health claims, including long-latency diseases. The third part of this paper analyses emerging challenges in multinational and commercial deep space missions and areas that need to reform for enhancing accountability, ensure equitable risk distribution, and facilitate sustainable human space exploration. As per the analysis, there is a need for rules to ensure health protection of spacecraft personnel along with existing rules.

Keywords: Astronaut Health; Space Law; Telemedicine; Legal Liability; Space Governance; Health Insurance; Human Spaceflight

---

I. INTRODUCTION

Space Medicine is a branch of medical science that deals with medical problems encountered beyond the earth's atmosphere. Space medicine evolved from aerospace medicine.[1] Hubertus Strughold introduced the term “space medicine” in 1948, nine years before Sputnik I’s launch, during a panel organised by Col. Harry G. Armstrong on the aeromedical challenges of space travel.[2] This emerging field has focused on the physiological and psychological challenges of spaceflight.

Gradually, space medicine has evolved from monitoring astronaut health to conducting research to researching counter-measures and systems that enable humans to survive and function safely in space’s extreme environments, such as microgravity and high radiation. It addresses vital issues such as microgravity induced bone and muscle loss, cardiovascular damage, cancer risk (radiation carcinogenesis), central nervous system (CNS) degeneration which causes cognitive impairment or accelerated neurodegenerative diseases. It also includes isolation related psychological effects, and behavioural health issues due to long duration missions.[3]

[1] Britannica, *Aerospace Medicine*, (Apr 8, 2019), https://www.britannica.com/science/aerospace-medicine.

[2] Lily Srivastava, *Space Medicine and the Law*, in *Current Developments in Air and Space Law* 284, 284 (Ranbir Singh, Sanat Kaul & Srikrishna Deva Rao eds., 2012).

[3] Britannica, *supra* note 1.

The World Health Organisation defines health as "a state of complete physical, mental, and social well-being and not merely the absence of disease or infirmity." This definition also applies to astronauts, whose well-being is necessary for mission success and safe return[4]. Even if the manned space exploration is limited and only achieved independently by only a few nations, these missions have provided important data on space travel's impacts on the human body, informing possible countermeasures, biomedical support systems, telemedicine and crew health protocols.

II. Existing International and Indian Frameworks for Astronaut Health Protection

Over time, India's space activities have progressed through various phases from conceptual, experimental, operation commercial and further expansion phases. With each stage, the demand for space systems, applications, and services to meet national priorities and global opportunities has grown rapidly[5] resulting in increased involvement of Indian industry and service providers, who play a more important role in diverse space initiatives under the technical guidance and authorisation of the Department of Space[6]. In India, the growing space program, like the Gaganyaan human spaceflight mission, international collaborations such as Indian astronaut Shubhanshu Shukla's participation in Axiom Mission 4 and ambitions for sustained exploration has increased the relevance of space medicine.

India has advanced space medicine through institutions like the Institute of Aerospace Medicine (IAM) under the Indian Air Force in coordination with ISRO, which conducts astronaut selection, training, physiological studies and research. Recent collaborations, such as ISRO's framework agreement with the Sree Chitra Tirunal Institute for Medical Science and Technology (under the department of Science and Technology), focus on human physiological and behavioural health studies, radiation biology, countermeasures, telemedicine and crew medical kits increasing academia-industry partnerships in medical device development and space health research[7]. It will form the opportunity in enhancing the

[4] Reddy Sai Spandana, *Space Medicine and Law: Emerging Trends and Challenges*, 3 Int'l J. Legal Sci. & Innovation 223, 224.
[5] Draft Space Activities Bill, 2017, Bill No. 2 of 2017 (India).
[6] Draft Space Activities Bill, 2017, Bill No. 2 of 2017, cl. 3 (India).
[7] Indian Space Research Organisation (ISRO), Department of Space (DoS) & Sree Chitra Tirunal Institute for Medical Sciences & Technology., Department of Science and Technology., *Framework Memorandum of Understanding on Cooperation in Space Medicine* (Apr. 25, 2025).

study of space medicine and at the same time it points towards the need for a strong framework for long term health protection of astronauts.

India is a part of major international space treaties, including the Outer Space Treaty (1967)[8], the Agreement on the Rescue of Astronauts (1968)[9], Liability Convention[10] and Registration Convention[11]. Article V of the Outer Space Treaty obligates assistance and safe return of astronauts in distress regardless of nationality.[12] Under the Outer space Treaty, states are required to authorise and exercise continuing supervision over activities of non-governmental entities in outer space, including the Moon and other celestial bodies, adhering to treaty's provisions. The responsibility of all national space activities, whether conducted by government agencies or private actors, is carried by states according to it.[13]

In India, however, there is still no comprehensive national legislation specifically regulating space activities. The current framework relies on constitutional provisions that allow for the implementation of international treaties along with policies such as the Satellite Communications Policy, 2000[14] and the Revised Remote Sensing Data Policy, 2011. While other space faring nations have built legal frameworks to look after and regulate their national programs[15], Indian Space Policy 2023 and IN-SPACe guidelines guide space activities as only a framework[16], and not as a legislation or a statute.

The Indian government has recognised this gap previously and considered the need for a law to regulate and support the country's expanding space activities. In November 2017, it released a draft Space Activities Bill[17] for public consultation to invite feedback from stakeholders, but lapsed without introduction in Parliament. Section 5(j) of the bill mandates "safety requirements and safety measures in relation to any space activity," and Section

[8] Treaty on Principles Governing the Activities on States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, Jan. 27, 1967, 18 U.S.T. 2410, 610 U.N.T.S. 205.
[9] Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space, Apr. 22, 1968, 19 U.S.T. 7570, 672 U.N.T.S. 119.
[10] Convention on International Liability for Damage Caused by Space Objects, Mar. 29, 1972, 24 U.S.T. 2389, 961 U.N.T.S. 187.
[11] Convention on Registration of Objects Launched into Outer Space, Jan. 14, 1975, 28 U.S.T. 695, 1023 U.N.T.S. 15.
[12] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies Art. V, Jan. 27, 1967, 18 U.S.T. 2410, 610 U.N.T.S. 205.
[13] Outer Space Treaty, *supra* note 13, art. VI.
[14] Department of Space, *Norms, Guidelines and Procedures for Implementation of the Policy Framework for Satellite Communications in India.*
[15] Rima Hore, *A Critique of the Draft Space Activities Bill, 2017*, at 87.
[16] Department of Space, Government of India, *Indian Space Policy 2023*, at 11 (2023)
[17] Department of Space, Government of India, *Draft Space Activities Bill,* (2017).

7(2)(a) makes sure activities "do not jeopardise public health or the safety of individuals or property[18]," but these are general and do not talk about radiation exposure, microgravity effects, psychological well-being, or occupational health for space personnel.

Reform efforts have been initiated through the creation of IN-SPACe's[19] and the Indian Space Policy 2023[20]. These policies promised to make new laws but prioritised guidelines such as NGP 2024 for private sector[21]. As the government develops sector specific standards for e.g. safety catalogues first such policies remain pending. These bills aimed at increasing innovation and entrepreneurship within the space industry and focused on licensing commercial space activities, safety requirements for operations like preventing public health risks or environmental damage from launches and conformity with international treaties. The specific provisions for astronaut health standards, psychological well-being, ethical protocols for long duration flights or dedicated occupational health frameworks do not exist.

Space missions such as Gaganyaan, are being carried out under the authority of executive decisions and policies made by the government. With the rapid development of space programs, and milestones like the Gaganyaan, human spaceflight mission, ambitions for long-term exploration highlights the importance of space medicine along with space health. While India has made progress in space medicine research and training through institutions like the Institute of Aerospace Medicine (IAM) under the Indian Air Force, and collaborations with ISRO, there is currently no space health law or specific statutory framework in India that fully regulates astronaut health standards, medical protocols, radiation limits, ethical concerns for long-duration flights or liability in health-related incidents during space activities. The absence of a dedicated legal framework for astronaut health in India must also be understood in relation to the broader global landscape of human spaceflight, where participation itself remains highly restricted. Manned-space exploration is also limited, only three countries so far have succeeded in man space missions. These missions have helped space scientists, doctors and surgeons observe, analyse and establish certain psychological and physiological impacts space travel has had on human body[22].

[18] *Indian Space Policy 2023*, *supra* note 17, §§ 5(j), 7(2)(a).
[19] Indian National Space Promotion & Authorization Centre (IN-SPACe), Department of Space, Government of India, IN-SPACe.
[20] *Indian Space Policy 2023*, *supra* note 17.
[21] Indian National Space Promotion & Authorization Centre (IN-SPACe), Department of Space, Government of India, *Norms, Guidelines and Procedures for Implementation of Indian Space Policy 2023 in Respect of Authorization of Space Activities (NGP)* (May 2024).
[22] Spandana, *supra* note 4, at 228.

III. Core Legal Gaps in Astronaut Health Regulation

Institute of Aerospace Medicine IAF Bangalore has defined areas of work including Isolation and Psychological Management, Microgravity research, Clinical Space Medical and Surgical Management, Radiation Protection, and Operational Space Medicine to support the Human Space Programme (HSP) of ISRO[23]. As pointed out by Prof. K. Kasturirangan, "In a space environment, human beings face micro-gravity conditions, which alter the flow, quantity, and distribution of body fluids, being free of the gravitational effect." It underlines the emerging field of space medicine, which tries to solve physiological challenges which are very different from extraterrestrial environments. The legal frameworks governing space activities remain underdeveloped while medical science begins to adapt these conditions, leaving gaps in regulation, liability and ethical concerns[24].

The evolution in human spaceflight has been seen from the short-duration missions on the International Space Station (ISS) which spanned to months with a stable multinational crew under unified command to the long-duration, deep-space multinational operations. Programs such as NASA's Artemis program, Mars analog simulations, and emerging private orbital stations such as Axiom Space or Starlab introduce extended exposure to microgravity, radiation, psychological stressors, and isolation, compounded by diverse crews from state agencies and private entities operating across jurisdictions. These changes increase the complexities of medical care delivery, demanding a review of existing legal frameworks[25]. These limitations reveal four core gaps, examined next.

A. Telemedicine and Licensing Deficiencies

Telemedicine is a field in which telecommunication technologies and medicine interact to allow for the provisions of health care remotely. It can be used for remote consultation between physicians or between physicians and patients regardless of geographic distance[26].

NASA has prioritised telemedicine, first using it to monitor astronauts' health through data transmission and remote communication and has now grown into something much more advanced.[27] Today's smart medical systems are being developed that not only track and

[23] Srivastava, *supra* note 2, at 286.
[24] Srivastava, *supra* note 2, at 286.
[25] Justin Zadorsky, *Western Researchers Call for Better Physician Licensing System to Address Medical Care in Space* (Feb. 28, 2023.)
[26] Britannica, *Telemedicine,* https://www.britannica.com/science/telemedicine (last visited Mar.1, 2026).
[27] Andrew T. Simpson, Charles R. Doarn & Stephen J. Garber, A Brief History of NASA's Contributions to Telemedicine (Mar. 26, 2020).

diagnose health conditions in space but also allow doctors on Earth to provide limited treatments from afar. It also enables physicians on Earth to remotely deliver limited treatments. This blending of communication functions and therapy marks a step forward for the future of human spaceflight, and it also has huge potential for emergency care in remote regions on Earth.

India's telemedicine journey started in the late 1970s with the Satellite Instructional Television Experiment, using NASA's Application Technology Satellite (ATS-F) the program connected over 2,000 villages across the country. It wasn't only limited to medicine, it brought education to rural communities, covering a wide range of topics like health, hygiene, adult learning and rural development. This helped to create the base for India's future in telemedicine and digital healthcare[28].

Astronauts on the International Space Station (ISS) stay connected with doctors on Earth by the communication systems that allow telemedicine. Living in space for long periods has a major impact on the body. It affects cardiovascular, vestibular, and musculoskeletal systems. Bones get weaker, losing about 1 to 3% of their strength each month, and muscles shrink by around 5% each month. After just a few weeks, the body also uses about 25% less oxygen than it normally would on Earth[29].

The partner space agencies on the International Space Station (ISS) such as National Aeronautics and Space Administration (NASA), European Space Agency (ESA), Canadian Space Agency (CSA), Russian Federal Space Agency (Roscosmos), and Japan Aerospace Exploration Agency (JAXA) have agreed on basic health rules such as ISS legal framework, International Space Station Intergovernmental Agreement, Memorandums of understandings and bilateral arrangements between partner agencies. These rules are based on international agreements and a shared Code of Conduct, setting minimum standards for crew health and safety. Countries also have their own programs, like the U.S. TREAT Astronauts Act or Canada's Health Beyond Initiative, and efforts to modernise astronaut medical records. These national initiatives help to tackle health challenges astronauts face in deep space, but they only apply within each country's system and don't extend internationally[30].

[28] Bhaskarnarayana, L.S. Satyamurthy & Murthy L.N. Remilla, Indian Space Research Organization and Telemedicine in India, Vol. 15, No.6, https://doi.org/10.1089/tmj.2009.0060 (Aug. 1, 2009).
[29] K. Ganapahty, Space Medicine: The Ultimate in Remote Healthcare, Telehealth & Med. Today, at 3, Space Medicine: The Ultimate in Remote Healthcare | Telehealth and Medicine Today (2020).
[30] Abeer Malik, *Housten, Do We Have a Lawyer? The Legal Black Hole of Astronaut Health Care,* Houston, Do We Have a Lawyer? The Legal Black Hole of Astronaut Health Care - Petrie-Flom Center (Apr. 3, 2025).

The International Space Station shows that countries can work together on space medicine, but the system is still not fully developed. Each space agency still follows its own rules, which means protections for astronauts and responsibility if something goes wrong are scattered across different national policies. Researchers point out that while countries like the U.S. and Russia have strong laws to safeguard astronaut's health and mental wellbeing, these protections don't line up internationally[31]. These measures lack international cohesion, therefore problematic for multinational crew missions or missions beyond ISS. There is a regulatory void leaving both astronauts and doctors at risk as no Earth- based medical licence explicitly covers deep space. Terrestrial telemedicine laws are limited to national borders and there is no clarity of legal jurisdiction.[32]

Telemedicine rules for space missions are built on Earth's patchwork of national systems, and that leaves a huge gap. In the U.S., doctors are licensed state by state. The Interstate Medical Licensure Compact[33] makes it easier to work across states, but physicians still need separate fees, background checks, and approvals especially for telehealth. In Europe, doctors are licensed nationally too, with some coordination through EU directives[34]. But differences between countries remain, and strict privacy laws like General Data Protection Regulation (GDPR) create extra hurdles, much like Health Insurance Portability and Accountability Act (HIPAA) does in the U.S. None of these systems even consider medical care beyond earth[35]. Right now, no medical licence on Earth officially covers deep space, unlike aviation medicine where countries recognise each other's standards through International Civil Aviation Organisation (ICAO).[36] There is no global agreement for "space medicine." This becomes an issue for deep-space telemedicine. Realtime consultations become impossible because communication delays to Mars range from 4 to 24 minutes one way [37]. Astronauts will have to rely on delayed instructions, onboard medical autonomy, and flight surgeons whose licences don't legally extend into space. That leaves unanswered questions about which laws apply,

[31] Holm, *Legal Protections for the Health of Astronauts: An Analysis* 98 (Inst. of Air & Space Law, McGill Univ. Faculty of Law, 2020).
[32] Zadorsky, *supra* note 25.
[33] Interstate Med. Licensure Compact, *States Information* States Information | Interstate Medical Licensure Compact, (2021).
[34] Vera Lúcia Raposo, *Telemedicine: The Legal Framework (or the Lack of It) in Europe*, GMS Health Tech. Assessment, https://pmc.ncbi.nlm.nih.gov/articles/PMC4987488/ (Aug. 16, 2016).
[35] Robb Taylor-Hiscock, *HIPAA vs. GDPR Compliance: What's the Difference?* (Sept. 21, 2022).
[36] International Civil Aviation Organisation, (ICAO), International Civil Aviation Organization (last visited Apr. 4,2026).
[37] Madison Diamond; Gloria R. Leon; Pablo de León, *Mars Mission Communication Delays and Impact on Mission Controller Performance, Workload, and Stress*, 96 Aerospace Medicine & Human Performance (2025).

who is responsible, and how accountability works when multinational crews face medical emergencies far from Earth.

India is uniquely positioned and needs to close this gap with a national telemedicine licensing framework for deep-space missions. India has already built a foundation to take telemedicine in space The Indian Space Research Organisation has been working on telemedicine using satellites since 2001, and in 2020 the National Medical Commission has given clear Telemedicine Practice Guidelines. The country has already developed the technical infrastructure via INSAT and GSAT satellite networks and a mature regulatory framework[38]India is well prepared to increase these capabilities beyond low-Earth orbit. A dedicated licensing system for space medicine would do several things including giving Indian doctors and flight surgeons clear legal authority to treat astronauts in space without worrying about jurisdiction issues. Build in training and protections for unique risks like communication delays, radiation and microgravity. It will help India in future bilateral and multilateral deep- space ventures accelerating innovation in space-health technologies, and will ensure that Indian astronauts and collaborating international crew members receive legally strong support.

B. Cross-Jurisdictional Practice Barriers

Today's space missions majorly bring together astronauts from many countries, all living and working inside the same spacecraft. Crew members from the NASA, Roscosmos, ESA, JAXA, and CSA share one home in orbit on ISS, even if each still follows their own nation's medical rules[39]. Things get more complicated with the joining of new private players like SpaceX, Axiom, and private astronauts. Physicians, flight surgeons, and medical officers trained under different national protocols are carried by a single spacecraft, yet all are required to respond instantly to the same microgravity emergency, radiation event, or psychological crisis[40].

The absence of a unified extraterritorial medical regulatory regime is a major regulatory gap behind this operational unity. The 1998 ISS Intergovernmental Agreement (IGA) and its supporting Memoranda of Understanding and multilateral Code of Conduct includes

[38] Utkarsha Mahajan, *India in Space for Health: A Case of Tele-Medicine and Tele-Health* India in Space for Health: A Case of Tele-Medicine and Tele-Health (Aug. 2, 2021).
[39] Malik, *supra* note 30.
[40] Adam Mann, *Human Spaceflight's New Era Is Fraught with Medical and Ethical Questions* Human spaceflight's new era is fraught with medical and ethical questions (June 11, 2024).

operational coordination, safety baselines, and jurisdiction rules. The right of Jurisdiction and control of each partner state over the elements it registers and over its own nationals aboard the station is granted by Article 5 of the IGA[41]. But the agreement defers medical standards of care, licensing, data privacy, informed consent and record-keeping to each national space agency. There is absence of code or treaty implying a common standard of care once the isolation begins[42].

Handling of astronaut health and research varies by space agencies. In the U.S. laws like the Privacy Act of 1974 make medical records very private. NASA has treated astronaut health information as highly sensitive, and historically produced under-reporting of clinical signs and symptoms. A 2001 National Academics report even noted that astronauts felt pressure not to disclose health issues worrying it will lead to disqualification from future flights[43]. In contrast, Russian protocols adopt broader psychophysical ideas such as "asthenia"[44] (a kind of fatigue or weakness) and sets different standards for when mental health care or research involvement is needed. For Europe's astronauts, ESA crew medical officers operate under the EU's Personal Data Protection framework[45]. These differences also show up in research ethics. American astronauts may refuse to take part in studies during missions, while in other agencies, being part of such studies is often seen as their duty.

During missions, these differences in medical privacy and research ethics may present serious difficulties. The U.S. medical programs and Russian protocols might be different towards approaches to prevention, treatment, and participation in research[46]. Consent in medical conditions also becomes tricky when experimental treatments are suggested, astronauts from different countries may disagree because their cultures and laws define personal choice and autonomy differently. In psychological cases, depression caused due to isolation or

[41] Agreement Among the Government of Canada, Governments of Member States of the European Space Agency, The Government of Japan, The Government of the Russian Federation, and the Government of the United States of America Concerning Cooperation on the Civil International Space Station, Jan. 29, 1998, T.I.A.S. No. 12927, at 5.
[42] Charles R. Doarn et al., A Framework for Multinational Medical Support for the International Space Station: A Model for Exploration, 92 Aerospace Medicine & Human Performance, (2021).
[43] National Academies of Sciences, Engineering, and Medicine, *Safe Passage: Astronaut Care for Exploration Missions* 174 (2001).
[44] NASA, *Human Health and Performance Risks of Space Exploration Missions: Evidence Reviewed by the NASA Human Research Program* 8, NASA SP-2009-3405.
[45] European Space Agency (ESA), *Highlights of ESA Rules and Regulations*, ESA - Highlights of ESA rules and regulations.
[46] Institute of Medicine, *Astronaut Care for Exploration Missions* (John R. Ball & Charles H. Evans, Jr. eds., 2001).

interpersonal conflict can trigger grounding recommendations under one nation's mental-health standards while another might not see it as serious enough. Problems continue after missions too, sharing medical data for research like studying bone loss, vision changes or psychological health is often blocked by national privacy rules.

The main space treaties like the 1967 Outer Space Treaty, The Rescue Agreement and the Liability Convention address the state responsibility for "activities" in outer space only in the broadest terms. They have no particular regulations pertaining to extraterritorial licence of medical practice[47]. The Artemis Accords, joined by India in 2023, support the emergency assistance requirements and promote safety zones but say nothing about medical jurisdiction, standards of care, or cross-national physician licensing. Things get even more complicated with private companies joining space missions. Their astronauts may fall under even less harmonised corporate medical oversight.

The consequences are serious and immediate. If crew members lose trust or unity in a stressful, isolated environment of space their performance and safety can suffer. Real time decision making in medical emergencies becomes slower and more controversial when flight surgeons have to deal with conflicting national guidelines. This cross-jurisdictional ambiguity also raises the question about who ultimately bears the medical responsibility and liability when multiple state and private actors collaborate.

India is still new to human spaceflight, with its Gaganyaan program aiming to send three astronauts on its first independent mission[48], with no multinational crew, medical oversight falling under Indian authority. The Institute of Aerospace Medicine (IAM) under the Indian Air Force in close collaboration with ISRO's Human Space Flight Centre looks after astronaut selection, physiological training, real-time health monitoring through telemedicine and bio-vests, radiation protection, emergency protocols, and crew healthcare systems[49]. India is also building its own expertise in space medicine, Recent collaboration of ISRO with Sree Chitra Tirunal Institute for Medical Sciences & Technology (SCTIMST) focuses on research into human physiology, behavioural health, radiation biology, microgravity effects and biomedical support according to India's needs and priorities. India depends a lot on partnerships with other countries to cover medical rules rather than setting rules by itself. By signing the

[47] Malik, *supra* note 30.
[48] ISRO, *Gaganyaan* (Nov. 23, 2022).
[49] Institute of Aerospace Medicine, *supra* note 7.

Artemis Accords in 2023[50], India agreed to principles of safe and transparent exploration, but the Accords don't cover medical rules or liability issues in multinational missions[51].

India adopts a pragmatic approach abroad by collaborating with different partners based on particular needs through targeted cooperation, examples of this include NASA's assistance with astronaut training[52], space medicine cooperation with France's CNES[53], previous training ties with Russia's Roscosmos and even Australian Space Agency in recovery planning[54]. This represents India's broader strategic stance, keeping its strategic autonomy[55], bilateral arrangements over multilateral regimes, and inclusive policies. But India hasn't yet adopted foreign medical standards into its own system. India hasn't taken any stance on whether there should be a single global medical system for space missions, but its emerging role positions it uniquely. With plans for the Bhartiya Antariksh Station (BAS) starting module launches around 2028 and full operations by the mid 2030's, India sees BAS as a national but also an open platform for microgravity research in life sciences and medicine[56]. This could give India the chance to set common medical protocols if it invites global partners, helping bridge the gaps between Western, Russian and emerging standards. India is handling the cross-jurisdictional challenges carefully, prioritising sovereign control over its crews and missions while drawing on international expertise to increase capability-building faster. As Gaganyaan mission moves forward and the Bhartiya Antariskh Station (BAS) takes shape, India can potentially propose medical harmonisation initiatives that help to build cross-jurisdictional medical practice regulations for multinational crews.

C. Liability and Attribution Ambiguities in Collaborative Missions Involving State and Private Actors

Human space travel is shifting from being run majorly by governments to missions where public agencies and private companies work together. In this new setup, figuring out who is responsible in case of medical problems arise has become a big challenge, mistakes in telemedicine, late diagnoses, or treatment decisions made during the mission don't have clear

[50] Claire A. O'Shea, *NASA Welcomes India as 27th Artemis Accords Signatory* (June 23, 2023).
[51] Malik, *supra* note 30.
[52] Simon Mansfield, *India's Gaganyatris Complete Initial Astronaut Training for ISRO-NASA Mission to ISS* (Dec. 2, 2024).
[53] *India-France Sign Agreement for Cooperation on Gaganyaan Mission*, The Hindu (Apr. 15, 2021)
[54] ISRO & ASA, *Implementing Arrangement for Gaganyaan.*
[55] Dimitrios Stroikos, *India's Space Policy: Between Strategic Autonomy and Alignment with the United States* (June 2, 2025).
[56] Sibu Kumar Tripathi, *First Pictures of ISRO's Bhartiya Antariksh Station Module Is Here* (Aug. 22, 2025).

rules about accountability[57]. Current international and national laws mainly deal with launch-related damage or agreements between parties, but they don't provide specific guidance for medical liability in these joint missions. India may face the problem of liability for acts not prohibited by international law as it does not have a domestic law to handle the consequences of its international and domestic obligations[58].

The 1967 Outer Space Treaty and the Liability Convention of 1972 (Liability Convention on International Liability for Damage Caused by Space Objects) still stand today as important international agreements. The State Parties "shall bear international responsibility for national activities in outer space, whether such activities are carried on by governmental agencies or by non-governmental agencies," according to Article VI of the Outer Space Treaty[59], which demands for the approval and ongoing oversight of private actors. Article VII[60] considers each launching state internationally liable for damage caused by its space object or component parts to another State party or its natural or juridical persons, on Earth, in the air, or in outer space. The Liability Convention elaborates these rules, Article II[61] imposes absolute liability for damage on Earth's surface or to aircraft in flight, while Article III[62] applies fault-based liability for damage elsewhere including to persons or property on board another space object. "Damage" is defined in Article I(a)[63] to include loss of life, personal injury or other impairment of health as well as property loss. These provisions were intended to govern state-to-state claims arising from collisions or re-entry incidents, rather than internal medical decisions made during flight.

The International Space Station (ISS) Intergovernmental Agreement (IGA) of 1998 provides a detailed operational model. Article 16[64] gives a cross-waiver of liability among partner states, United States, Russia, ESA member states, Japan and Canada and their related entities defined to include contractors, subcontractors, users, and customers at all tiers. Each Partner assumes

[57] Malik, *supra* note 30.
[58] C. Jayaraj, *India's Space Policy and Institutions, in Proceedings: United Nations/Republic of Korea Workshop on Space Law- United Nations Treaties on Outer Space: Actions at the National Level* 106.
[59] Outer Space Treaty, *supra* note 13, art. VI.
[60] Outer Space Treaty, *supra* note 13, art VII.
[61] Convention on International Liability for Damage Caused by Space Objects art. II, Mar. 29, 1972, 24 U.N.T.S. 187.
[62] *Id*. art. III.
[63] *Id*. art. I(a).
[64] Agreement Among the Government of Canada, Governments of Member States of the European Space Agency, the Government of Japan, the Government of the Russian Federation, and the Government of the United States of America Concerning Cooperation on the Civil International Space Station art. 16, Jan. 29, 1998, T.I.A.S. No. 12927.

risks coming in ISS activities and agrees not to bring claims against other Partners or related entities for damage arising from "Protected Space Operations." The waiver is interpreted broadly and explicitly includes claims that might otherwise arise under the Liability Convention. Article 17[65] keeps the Liability Convention obligations in place, except where the cross-waiver changes them. Additional Memoranda of Understanding between space agencies help put these rules into practice. However, the Intergovernmental Agreement is specific to the ISS, focuses mainly on government-led missions and does not account for private medical service providers working outside the Partner chain[66].

Collaborative situations make the problem worse. For example, a private company could, for instance, send NASA or ESA astronauts with paying customers and give them telemedicine or medical kits. A government surgeon giving advice across different agencies, or a private doctor in charge of radiation exposure, creates overlapping responsibilities with no clear rules about who is to blame. These hypothetical situations show that there aren't any clear answers. Consider a hypothetical scenario, where a private lunar mission with people from all over the world, like the ones planned under the Artemis program. If there's a medical mistake, an onboard medical malpractice event, such as failure to treat decompression sickness properly, someone may file a claim. But who is responsible, the person running the mission, the company that made the medical software, or the country's space agency that provided guidance?

The gap of lack of proper legal provisions guiding space medicine persists because the core treaties were formed during the Cold War era. At that time the space activities were assumed to be exclusively state-driven. The commercial boom has arrived since 2010s seen by SpaceX's first crewed flights in 2020 and subsequent Axiom private missions to the ISS[67]. The Artemis Accords (2020) is a non-binding political understanding signed by over 50 nations. They differ questions of liability to future bilateral agreements (Section 2)[68], which must include provisions on liability but do not address medical issues specifically. These

[65] *Id*. art. 17.
[66] Agreement Among the Government of Canada, Governments of Member States of the European Space Agency, the Government of Japan, the Government of the Russian Federation, and the Government of the United States of America Concerning Cooperation on the Civil International Space Station art. 16, Jan. 29, 1998, T.I.A.S. No. 12927, at 7.
[67] *Ethical Considerations for the Age of Non-Governmental Space Exploration* (June 11, 2024).
[68] The Artemis Accords: Principles for Cooperation in the Civil Exploration and Use of the Moon, Mars, Comets, and Asteroids for Peaceful Purposes § 2 (Oct. 13, 2020).

accords affirm compliance with the Outer Space Treaty and Liability Convention yet provide no harmonised rules for hybrid medical responsibility.

The Gaganyaan human spaceflight program, run by ISRO, is working with partners like the Sree Chitra Tirunal Institute for Medical Sciences & Technology on space medicine research covering telemedicine, radiation biology, and astronaut health systems. Indian astronauts have also trained through private U.S missions such as Axiom-4 on SpaceX vehicles. But if a medical error happens, for example a misdiagnosis during telemedicine in microgravity by a private consultant or an international partner advising an Indian crew member it's unclear who would be held responsible. Private providers are covered by normal medical licensing and tort laws on Earth, but laws in space are not settled. Current liability waivers or cross-agreements are patchy[69], usually limited to launch phases or specific contracts, and don't clearly medical malpractice. Unlike ISS Agreement, which has broad liability, sharing rules, India's frameworks don't yet provide mission-specific protections for medical issues in mixed state- private crews.

India's lack of a full national space law has created gaps in handling medical liability[70]. Although the 2023 Space Policy and National Space Promotion and Authorisation Centre (NGP)[71] encourage private sector involvement and align with international treaty obligations, they don't clearly explain who is responsible in medical situations. The proposed Space Activities Bill is expected to bring clarity on liability, insurance, and private regulation but for now India relies only on guidelines, which leave many uncertainties. This makes private medical companies hesitant to join missions, exposes India to international claims under the Liability Convention since the launching state carries the main responsibility, and could lead to lawsuits being filed in different countries[72]. It also means protections are uneven. Government astronauts may be covered by their agencies, while private participants or partners face weaker safeguards. As India moves forward with Gaganyaan and aims to grow its share of the global space economy, the lack of clear medical liability rules in joint missions' risks crew safety, international cooperation, and private sector growth. India urgently needs bilateral agreements or domestic reforms that specifically address medical responsibility in space.

[69] Malik, *supra* note 30.
[70] Shrawani Shagun, *Why India Needs a National Space Law Urgently*, The Hindu (Aug. 21, 2025).
[71] Department of Space, Government of India, *Indian Space Policy 2023* (Apr. 20, 2023)
[72] Jayaraj, *supra* note 60.

D. Gaps in Insurance Coverage for Hidden Health Issues.

One of the biggest gaps in space governance is the lack of strong, standardised insurance or compensation systems for astronaut health after missions. The immediate mission safety protocols receive attention at the same time long term impacts including on health and related financial costs remain ignored[73]. The long-term human and financial costs of space travel, particularly latent diseases, may appear years or decades later. This leaves astronauts carrying personal risks without proper protection. It threatens the future of human space exploration by weakening trust, people hesitate to get involved, and both space agencies and private companies are left facing unclear responsibilities and risks.

Current rules for astronaut health are scattered and limited. In the United States, NASA's TREAT Astronauts Act (2017)[74] allows the agency to monitor, diagnose and treat medical and psychological conditions linked to spaceflight for former government astronauts and payload specialists. This builds on the Lifetime Surveillance of Astronaut Health (LSAH)[75] program at Johnson Space Centre, which already tracks astronaut health over time. The Act expands this into full medical services, annual exams, screenings, and treatment without astronauts having to share costs. LSAH itself works like an occupational health system, collecting long-term data on illness, death and risks from space exposure. This information helps guide astronaut care, develop countermeasures, and set standards for future missions.

On Earth, there are various similar models, like worker's compensation for radiation workers or health protections for pilots. But these don't fully capture the substantial risks of space[76], in which astronauts face multiple hazards at once. For private astronauts and commercial crews, protections are even weaker. In U.S. Companies usually require participants to sign liability waivers or cross-waivers under FAA rules, meaning they agree not to sue each other if

[73] Marcia Smith, *Witnesses Argue Government Has Ethical Obligation for Lifetime Astronaut Medical Care- And Needs Data, Too* (June 15, 2016).
[74] NASA, *TREAT Astronauts Act.*
[75] *The Lifetime Surveillance of Astronaut Health*, [NLSP] NLSP (last visited Apr. 12, 2026).
[76] NASA Transition Authorization Act of 2017, Pub. L. NO. 115-10, § 442(a)(1), 131 Stat. 14, (2017).

something goes wrong[77]. While personal or group insurance policies often rely on employer-provided coverage that excludes commercial spaceflight[78].

The absence of an international or standardised compensation model for post mission claims, particularly those involving long-latency conditions, is a major gap. Commercial space insurance markets exclude or severely limit "space risks", including radiation-induced illnesses that may manifest 10-20 years or more after exposure. International crew members on joint missions often fall between national systems, with coverage depending on the sponsoring agency rather than a unified framework. This leaves commercial participants, former astronauts from non-NASA programs, and crews from emerging spacefaring nations without reliable recourse.

Long-latency diseases take years to show up and are challenging for space travel. NASA's Human Research Program (HRP) reports points to galactic cosmic rays (GCR) high energy, high-linear energy transfer particles as a primary driver of degenerative effects beyond low-Earth orbit. These can cause long-term health problems. These can increase lifetime cancer risk (radiation carcinogenesis), central nervous system (CNS) degeneration leading to cognitive impairment or accelerated neurodegenerative disease, cardiovascular damage, and even speed up aging[79]. Living in microgravity worsens health with conditions like Spaceflight-Associated Neuro-ocular Syndrome (SANS)[80], ongoing heart and circulation problems, and muscle and bone changes whose long-term effects are still being studied. The 2014 report by the Institute of Medicine (IOM), Health Standards for Long Duration and Exploration Spaceflight, warned that these risks are not well understood and stressed that chronic, low-dose exposure to GCR in space is very different from radiation exposure on Earth[81].

Real world cases show the weakness of protections. In 2014, the Institute of Medicine (IOM) called for NASA that it has an ethical duty to provide with lifetime health care and monitoring

[77] 14 C.F. R. pt. 440 (2025).
[78] *Space Tourism and Denied Life Insurance Claims*, Space Tourism and Space Related Life Insurance Claims (Jan.5, 2025).
[79] Nathan Cranford & Jennifer Turner, *The Human Body in Space* (Feb. 2, 2021).
[80] NASA, *Risk of Spaceflight Associated Neuro-ocular Syndrome (SANS)*, Risk of Spaceflight Associated Neuro-ocular Syndrome (SANS) - NASA (last updated Mar. 16, 2025).
[81] Institute Of Medicine Report, *Health Standards for Long Duration and Exploration Spaceflight: Ethics Principles, Responsibilities, and Decision Framework*, Institute of Medicine Report: "Health Standards for Long Duration and Exploration Spaceflight: Ethics Principles, Responsibilities, and Decision Framework" and OCHMO Implementation Plan (Apr. 7, 2015).

to astronauts, since they take extraordinary risks[82]. But NASA's TREAT Act only covers U.S. government astronauts, leaving commercial participants and international partners without similar guarantees[83]. Insurance problems add another layer as life and health policies often exclude hazardous activities like space travel, and proving that radiation exposure caused cancer decades later is extremely difficult[84]. Without clear frameworks, claims could easily be rejected. Because of exclusions in insurance contracts, time limits on filing cases, or the challenge of linking a disease directly to spaceflight[85]. This leaves astronauts vulnerable and highlights the urgent need for dedicated rules to ensure fair coverage and accountability for everyone involved in human space missions.

These gaps exist because space law has stayed silent on astronaut health[86]. The 1967 Outer Space Treaty only talks about helping and returning astronauts right after missions, but says nothing about long-term care or compensation. The 1972 Liability Convention makes countries strictly liable for damage caused by space objects like harm to people or property on Earth or in aircraft. But it doesn't cover crew health problems from space exposure. Unlike the nuclear sector's Price Anderson Act[87] or international conventions, or aviation's Montreal Convention with its structured passenger liability regimes[88] space law lacks any dedicated compensation convention for latent astronaut injuries. Treaties prioritise state liability for hardware-related damage over individual occupational health protections, and no multilateral body has filled the void despite decades of calls from ethics experts and scientists, no international body has stepped in to create clear rules or compensation systems for astronaut medical issues[89].

IV. Pathways for Reform: Towards a Comprehensive Indian Space Health Law

India's Gaganyaan mission, led by ISRO, is designed for short trips in low-Earth orbit about three days at 400 km altitude with a crew of three. The focus so far has been on keeping

[82] *Health Standards for Long Duration and Exploration Spaceflight: Ethics Principles, Responsibilities, and Decision Framework* (Apr. 2014).
[83] Robert E. Lewis, *FAQs for the TREAT Astronauts Act* (Mar. 16, 2023).
[84] *Cosmic Radiation Deaths: Can Life Insurance Deny Space Claims?* (Aug. 17, 2025).
[85] *Cosmic Radiation Deaths*, *supra* note 86.
[86] Malik, *supra* note 30.
[87] Price-Anderson Act: Nuclear Power Industry Liability Limits and Compensation to the Public After Radioactive Releases, Price-Anderson Act: Nuclear Power Industry Liability Limits and Compensation to the Public After Radioactive Releases | Congress.gov | Library of Congress, (last visited Apr. 12, 2026).
[88] International Civil Aviation Organisation (ICAO), *International Air Travel Liability Limits Set to Increase, Enhancing Customer Compensation.*
[89] Malik, *supra* note 30.

astronauts safe during the mission. This includes health monitoring systems, life support, radiation protection (developed with DRDO), emergency medical kits, and recovery plans. ISRO is also working with institutions like the Institute of Aerospace Medicine and has signed new agreements to strengthen space medicine research. These efforts address immediate risks such as bone and muscle loss from microgravity, fluid shifts in the body, and short-term radiation exposure. However, there are still no clear public plans for dealing with long-term health problems after missions. Issues like radiation-induced cancer, heart disease, nervous system damage, or faster aging conditions that may appear years later remain underdeveloped or missing from India's current frameworks.

Astronaut protections in India appear ad hoc and mission specific. For example, when Indian astronaut, Shubhanshu Shukla. joined the Axiom-4 mission to the ISS, a commercial multilateral flight, he was covered by a very high-value accident insurance coverage potentially upwards of ₹200 crore as a part of ~$60 million package, covering training, launch, and immediate risks[90]. Similar policies, ranging from ₹40 to160 crore per person, have been mentioned for other high-risk space activities[91]. These policies mainly cover accidents during training, launch, and immediate mission risks. They are arranged by the government or through global insurers, but they usually don't cover long-term health problems like radiation-related cancers, which may appear decades later and are hard to prove. In India, commercial space insurance is still new, costly, and focused mostly on satellites and launch risks, such as liability for debris or failures. Experts point out that India lacks structured systems for risk-sharing, long-term coverage, or clear rules for astronaut health claims after missions. Private companies are advised to get insurance, but there is no standard model for protecting astronauts against long- term medical issues.

Implementing these would not only fulfil ethical responsibilities but strengthen India's position as a responsible spacefaring nation, attract skilled talent, encourage private companies to join, and protect the long-term health of astronauts who take these risks. As Gaganyaan and formation of a national space station marks deeper exploration, closing this gap is essential to ensure human costs do not outpace technological gains.

[90] Diksha Modi, *Shubhanshu Shukla's Space Insurance Could Be the Costliest in the World. Here's What It Covers,* News18 (July 2, 2025).
[91] Modi, *supra* note 90.

V. Conclusion

Current international frameworks, such as the Outer Space Treaty and Liability Convention, prioritise state responsibility for acute harms but neglect chronic astronaut health risks like radiation-induced carcinogenesis and microgravity-related degeneration. India's reliance on policies like the Indian Space Policy 2023 and lapsed Draft Space Activities Bill exacerbates four interlinked gaps: telemedicine licensing, cross-jurisdictional medical practice, liability attribution in state-private collaborations, and insurance for latent post-mission conditions.

Collectively, these discrepancies reveal a major disconnect between outdated space agreements and present-day circumstances. The treaties created during the Cold War, assumed short missions run only by states. But modern spaceflight involves private companies, multinational crews, and deep-space missions with long communication delays, challenges the current laws don’t address. The resulting legal gaps threatens mission safety, deters participation, hampers international cooperation under instruments like the expanding Artemis Accords, and risks losing critical long-term health data essential for both space sustainability and terrestrial medical benefits. Closing these gaps is essential if human expansion beyond Earth is to be fair, safe, and sustainable.

India can draw from global models: the ISS Intergovernmental Agreement's cross-waivers offer a blueprint for hybrid liability; Canada's Health Beyond Initiative demonstrates post-mission surveillance; and EU GDPR-aligned ESA protocols ensure data harmonisation. Unlike these, India lacks statutory equivalents, leaving Gaganyaan and Bharatiya Antariksh Station (BAS) vulnerable.

India must enact a Space Health Act to:(i) establish extraterritorial telemedicine licences via ISRO and National Medical Commission integration; (ii) mandate unified medical standards for multinational crews, aligned with Artemis Accords; (iii) clarify liability through mandatory insurance pools for latency diseases; and (iv) create an Astronaut Health Authority under IN-SPACe for oversight. These measures would safeguard strategic autonomy, foster academia-industry ties (e.g., IAM-SCTIMST), and position India as a leader in equitable deep-space exploration.

In conclusion, bridging these gaps transforms space medicine from an operational afterthought to a robust legal pillar, ensuring mission success, astronaut well-being, and sustainable human expansion beyond Earth orbit.

DIGITAL INTELLECTUAL PROPERTY ENFORCEMENT IN PAKISTAN'S E-COMMERCE LANDSCAPE:

THE CASE FOR PLATFORM LIABILITY AND NOTICE-AND-TAKEDOWN REFORM

By Alina Haider

VOLUME I | ISSUE I | ARTICLE II

APRIL 2026

The Legalis IP Quarterly

ABSTRACT

Pakistan's digital economy has expanded rapidly over the last five years, yet its intellectual property enforcement framework remains anchored in pre-digital assumptions. This paper examines the structural inadequacy of existing trademark and copyright law in addressing online infringement on Pakistani e-commerce platforms, with particular focus on marketplace giants such as Daraz and OLX. Drawing on a comparative analysis of India's Information Technology Act, the European Union's Digital Services Act, and the United States' Digital Millennium Copyright Act, this paper argues that Pakistan must adopt a formalised notice-and-takedown regime for online platforms and reinterpret Section 156 of the Trademarks Ordinance 2001 to require platform-level enforcement. The paper further contends that stronger penalties alone are insufficient; what is needed are enforcement mechanisms calibrated to the operational realities of digital commerce, including a streamlined dispute resolution modelled on the Uniform Domain-Name Dispute-Resolution Policy (UDRP). The paper also engages with Pakistan's Copyright Amendment Bill 2024 and recent IP tribunal jurisprudence to demonstrate that reform is not merely desirable but legally tractable.

Keywords: *Intellectual property, e-commerce, platform liability, notice-and-takedown, Trademarks Ordinance 2001, Pakistan, Digital Services Act, DMCA, counterfeit goods, digital enforcement.*

I. INTRODUCTION

Pakistan's e-commerce sector has undergone a remarkable transformation. Between 2019 and 2024, the number of online shoppers in Pakistan grew from an estimated 20 million to over 50 million, driven by smartphone penetration, mobile banking expansion, and the maturation of domestic platforms such as Daraz, OLX, and Rozee.pk.[1] This explosion in digital commerce has not, however, been matched by a corresponding evolution in the legal architecture governing intellectual property rights. This mismatch has created a widening enforcement gap, leaving rights-holders, particularly SMEs, exposed to significant economic harm.

The problem is not merely one of scale; it is structural. Pakistan's primary IP instruments, such as the Trademarks Ordinance 2001, the Copyright Ordinance 1962 (as amended), and the Patents Ordinance 2000, were designed for a world in which infringement was tangible and traceable. Traditional enforcement mechanisms presupposed a physically identifiable infringer at a fixed commercial location. That model has been rendered functionally obsolete by the anonymity of online selling accounts, the ephemeral nature of infringing product listings, and the jurisdictional complexity of platform-mediated commerce.

According to the 2024 Overseas Investors Chamber of Commerce and Industry (OICCI) report, Pakistani businesses are losing approximately twenty per cent of their annual revenues to counterfeit goods, with a substantial and growing proportion of that loss attributable to digital channels.[2] IP tribunals in Pakistan have so far lacked clear procedural frameworks for handling such online infringement. Courts have applied existing doctrine inconsistently, with some treating e-commerce platforms as analogous to physical bazaars and others treating them as passive, neutral intermediaries insulated from liability.

This paper makes three central arguments. First, Pakistan's existing IP laws are structurally ill-suited to digital enforcement and require targeted legislative reform. Second, that Section 156 of the Trademarks Ordinance 2001, which permits courts to grant "any other relief", is capable of being interpreted to mandate platform-level takedown obligations upon receipt of adequate notice, and that IP tribunals should adopt this interpretation pending legislative action. Third,

[1] State Bank of Pakistan, *E-Commerce in Pakistan: Sector Profile and Outlook* 3–5 (Working Paper, 2024) (on file with author).
[2] Overseas Invs. Chamber of Com. & Indus. (OICCI), *Annual Business Confidence Survey 2024* 27 (2024).

Pakistan should adopt a formal notice-and-takedown regime analogous to those in India, the EU, and the US, and supplement this with streamlined arbitral dispute resolution for online IP disputes modelled on the UDRP framework.

This paper proceeds in six parts. Part II examines the digital intellectual property enforcement crisis in Pakistan through empirical material on online counterfeiting. Part III analyses the existing legal framework and identifies its principal deficiencies. Part IV compares the approaches adopted in India, the European Union, and the United States. Part V advances the article's central normative case for reform. Part VI considers the Copyright Amendment Bill 2024 and its implications. Part VII concludes with policy recommendations.

II. THE DIGITAL COUNTERFEITING CRISIS IN PAKISTAN

A. Scale and Economic Impact

The counterfeiting of goods, defined broadly as the sale of products bearing unauthorised marks or reproductions of protected works, is not a novel challenge for Pakistan. The country has featured on the United States Trade Representative's 'Special 301' Priority Watch List for several years running, reflecting persistent concerns about IP enforcement across multiple sectors, including pharmaceuticals, textiles, and software.[3] What is novel is the migration of this challenge to digital platforms at a pace that has outstripped regulatory responses.

The OICCI's 2024 report quantified the economic toll with a degree of precision uncommon in commercial surveys: businesses surveyed reported losing an average of 19.7 per cent of revenues to counterfeit competition, with e-commerce channels identified as the fastest-growing vector for such infringement.[4] This figure aligns with broader regional trends. The Asian Development Bank's 2023 Regional Economic Outlook noted that counterfeit goods now constitute between fifteen and twenty per cent of total online retail volume in several South Asian economies, including Pakistan, India, and Bangladesh.[5]

[3] Office of the U.S. Trade Representative, 2024 Special 301 Report 48-51 (2024).

[4] OICCI, *supra* note 2, at 29.

[5] Asian Development Bank [ADB], *Asian Development Outlook: South Asia 2023* 863591 (April, 2023), www.adb.org/sites/default/files/publication/863591/asian-development-outlook-april-2023.pdf

The sectors most affected by infringement in Pakistan's digital marketplace appear to be consumer electronics, apparel and fashion accessories, cosmetics, and automotive parts. Available platform-level evidence points to a substantial volume of complaints. Daraz, the country's largest e-commerce marketplace and a company within the Alibaba Group, reportedly received tens of thousands of intellectual property-related complaints in 2023, although it has not disclosed detailed enforcement figures.[6] Public-sector data point in the same direction. Reports issued by the customs intelligence directorate of the Federal Board of Revenue indicate that counterfeit goods with an estimated retail value exceeding PKR 12 billion were seized at Pakistani ports between 2022 and 2024. Investigators further observed that a large proportion of those consignments were associated with online orders.[7]

B. The Platform Dynamics of Online Counterfeiting

It is essential to understand the structural dynamics of online counterfeiting to design effective legal responses. It is unlike physical market counterfeiting, where the locus of infringement is geographically fixed, and enforcement requires physical intervention. Digital counterfeiting, instead, is characterised by several features that frustrate traditional enforcement tools.

First, sellers on online marketplaces routinely operate through pseudonymous or fictitiously registered accounts, making identification and prosecution difficult. A brand owner who successfully identifies an infringing seller on Daraz may find that the seller dissolves their account and relists under a new identity within hours.[8] Second, the speed of online commerce means that infringing listings may generate substantial sales before any enforcement mechanism can be activated. An online listing, unlike a physical shop, does not have a fixed address or set operating hours. It can attract orders at any time and from any location. Third, and perhaps most significantly, the intermediary role of platforms creates a layer of legal ambiguity. When a consumer purchases a counterfeit item from a third-party seller on Daraz, is Daraz itself liable, and if so, under what conditions? These questions remain inadequately resolved in Pakistani law, generating uncertainty for rights-holders, platforms, and consumers alike.

[6] Daraz Grp. & Alibaba Grp., Transparency Report 2023 (2024) (on file with author) (noting significant IP-related takedown activity).

[7] Fed. Bd. of Revenue, Customs Intelligence Annual Report 2024 34 (2024).

[8] Int'l Trademark Ass'n, Online Counterfeiting Landscape Report (2023) (noting that re-listing after takedown is a near-universal phenomenon across major marketplace platforms).

III. THE EXISTING LEGAL FRAMEWORK AND ITS DEFICIENCIES

A. The Trademarks Ordinance 2001

The Trademarks Ordinance 2001 (TO 2001) is the principal legislative instrument governing trademark protection in Pakistan. Enacted to bring Pakistan's trademark law into conformity with the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), the TO 2001 provides for trademark registration, establishes civil and criminal remedies for infringement, and creates a system of specialised IP tribunals with exclusive jurisdiction over trademark disputes.[9]

Section 46 of the TO 2001 defines trademark infringement in terms of the use of an identical or similar mark in the course of trade in relation to goods or services identical with or similar to those for which the trademark is registered, where such use is likely to cause confusion on the part of the public.[10] Section 79 empowers IP tribunals to grant injunctions, including interim injunctions, in trademark infringement proceedings.[11] Section 156 provides a catch-all relief provision, permitting tribunals to 'pass such other orders as it deems fit in the circumstances of the case.'[12]

A central weakness of these provisions, when applied to online infringement, lies in their premise that the infringer is a specific and identifiable actor with a discernible physical presence. TO 2001 does not address the position of intermediaries that host, enable, or facilitate infringing transactions without directly engaging in the infringing act. It contains no equivalent either to Section 230 of the US Communications Decency Act, which limits intermediary liability for third-party content, or to the notice-and-takedown framework associated with the Digital Millennium Copyright Act. Pakistani law neither immunises platforms nor imposes clear duties upon them.

B. The Copyright Ordinance 1962 and the Amendment Bill 2024

The Copyright Ordinance 1962 (as amended through the Copyright (Amendment) Act 1992 and subsequent modifications) governs copyright protection in Pakistan.[13] Similar to the TO 2001, it

[9] Trademarks Ordinance, 2001 (Ordinance No. XIX of 2001) (Pak.), § 2(1)(s).
[10] Trademarks Ordinance, 2001 (Pak.), § 46.
[11] Trademarks Ordinance, 2001 (Pak.), § 79.
[12] Trademarks Ordinance, 2001 (Pak.), § 156.
[13] The Copyright Ordinance, 1962 (Pak.), as amended by Copyright (Amendment) Act, 1992.

was designed for a pre-digital environment and does not contain provisions specifically addressing online infringement, platform liability, or notice-and-takedown obligations.

The Copyright Amendment Bill 2024, which was tabled before the National Assembly in the second quarter of 2024, represents the most significant proposed update to Pakistan's copyright framework in three decades.[14] The Bill proposes, *inter alia*, the introduction of technological protection measures (TPMs), the criminalisation of circumvention of TPMs, and the creation of a digital rights management framework. The Bill, however, has been criticised by IP law practitioners and academics for its failure to address online platform liability and its silence on notice-and-takedown procedures.[15] The Bill's emphasis on criminalisation over civil remedies has also been questioned as counterproductive, insofar as criminal proceedings are slower, more resource-intensive, and less suited to the commercially driven nature of online IP disputes.[16]

C. The Prevention of Electronic Crimes Act 2016

The Prevention of Electronic Crimes Act 2016 (PECA) is Pakistan's primary cybercrime statute. It criminalises a range of online conduct, including the unauthorised access to computer systems, cyberstalking, online harassment, and the dissemination of certain categories of illegal content. PECA does establish a mechanism—administered by the Pakistan Telecommunication Authority (PTA)—for blocking online content, and this mechanism has been used on occasion to block websites hosting pirated content.

The Prevention of Electronic Crimes Act 2016 (PECA) serves as Pakistan's principal cybercrime statute. It criminalises a range of online conduct, including unauthorised access to computer systems, cyberstalking, online harassment, and the dissemination of certain forms of unlawful content.[17] The statute also creates a framework for the blocking of online material through the Pakistan Telecommunication Authority (PTA). That framework is not directed specifically at intellectual property enforcement, yet it has, on occasion, been invoked to restrict access to websites alleged to host pirated content. [18]

[14] Copyright Amendment Bill, 2024, cl. 1 (Pak. Nat'l Assembly, tabled Mar. 2024).
[15] *See, e.g.*, Pak. Bar Council Intell. Prop. Comm., Memorandum on the Copyright Amendment Bill (2024).
[16] Bashir Ahmed Khilji, *Intellectual Property Law in Pakistan: Current Challenges and Reform Imperatives*, 34 Pak. L. Rev. 45, 62 (2022).
[17] The Prevention of Electronic Crimes Act, No. XL of 2016, Pak. Code §§ 3–44.
[18] Pak. Telecom Auth., Annual Report 2023 45 (2024) (noting the blocking of thousands of websites for various categories of prohibited content).

However, PECA's utility as an IP enforcement tool is severely limited. The PTA blocking mechanism is blunt: it operates at the level of entire websites or URLs rather than specific infringing listings, and it does not provide for the targeted removal of individual infringing product listings on e-commerce platforms. Moreover, PECA does not create civil liability for platforms that fail to act on infringement complaints, nor does it establish any procedural mechanism by which rights-holders can compel platforms to remove infringing content within defined timeframes.[19]

The resulting legal position leaves rights holders with two imperfect options: protracted and costly civil proceedings before intellectual property tribunals, which may take years to resolve, or reliance on voluntary platform compliance policies, whose consistency and rigour remain uneven and are not formally required.

IV. COMPARATIVE ANALYSIS: INDIA, THE EUROPEAN UNION, AND THE UNITED STATES

A. India: The Information Technology Act and Intermediary Guidelines

India's approach to online intellectual property enforcement has developed substantially since the enactment of the Information Technology Act 2000. Section 79 of that statute grants safe-harbour protection to intermediaries, a term defined broadly enough to encompass e-commerce platforms. Indian courts have interpreted the provision in a manner that creates tangible incentives for platforms to address rights-holder complaints with reasonable promptness and procedural seriousness.[20]

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 give institutional effect to these incentives. Platforms with more than 50 lakh registered users in India, classified as significant social media intermediaries, must appoint a grievance officer, acknowledge complaints within twenty-four hours, and dispose of them within fifteen days under the regulatory framework now in force.[21] For IP infringement complaints specifically, the platform is required to act on notice from the rights-holder or from a court order.

[19] *Id.*; *see also* Khilji, *supra* note 16, at 58–60.
[20] Information Technology Act, 2000, § 79(1) (India).
[21] Information Technology (Intermediary Guidelines & Digit. Media Ethics Code) Rules, 2021, rr. 3(2)(a), 4(1)(b) (India).

Critically, a platform loses its safe harbour protection under Section 79 if it has actual knowledge of infringing content and fails to expeditiously remove it.[22]

The Indian Supreme Court's decision in *Shreya Singhal v. Union of India (2015)* significantly shaped the contours of intermediary liability in India, striking down a broadly-worded criminal provision but affirming the constitutional validity of court-order-based content removal obligations.[23] Subsequent decisions, including the Delhi High Court's orders in *Christian Louboutin SAS v. Nakul Bajaj & Ors (2018),* have clarified that Indian courts are willing to issue dynamic injunctions requiring e-commerce platforms to proactively block infringing listings even before specific listings are identified.[24]

Pakistan and India share a common legal inheritance rooted in the common law tradition introduced during British colonial rule. Their e-commerce markets also display a similar structure, marked by the prominence of large third-party marketplace platforms. The Indian framework therefore offers a particularly relevant reference point for reform in Pakistan.

B. The European Union: The Digital Services Act

The EU's Digital Services Act 2022 (DSA) represents the most comprehensive legislative response to platform intermediary liability yet enacted in any jurisdiction.[25] The DSA, which entered into full application in February 2024, creates a tiered regulatory framework based on platform size and risk profile, with more onerous obligations imposed on 'very large online platforms' (VLOPs) and 'very large online search engines' (VLOSEs) with more than 45 million monthly active users in the EU.

For IP enforcement purposes, the most significant provisions of the DSA are those relating to notice-and-action mechanisms (Articles 16-17) and the management of illegal content.[26] Article 16 requires online platforms to implement 'easily accessible and user-friendly' mechanisms allowing any person to report alleged illegal content, including IP-infringing listings. Article 17 requires platforms to notify the notifying party of the decision taken on the

[22] Information Technology Act, 2000, § 79(3)(b) (India).
[23] Shreya Singhal v. Union of India*,* 5 SCC 1 (India).
[24] Christian Louboutin SAS v. Nakul Bajaj, 2018 SCC OnLine Del 12215, ¶¶ 82–95 (High Court of Delhi).
[25] Regulation (EU) 2022/2065, of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act), art. 1, 2022 O.J. (L 277) 1.
[26] *Id.* arts. 16–17.

report and to provide reasons for that decision.[27] Platforms that repeatedly fail to act on valid notices risk losing their conditional liability exemptions under Article 6 of the DSA.

The DSA also contains provisions directed specifically at online marketplaces in Articles 30 to 32. These provisions require platforms to obtain, verify, and make public basic information concerning commercial sellers who use their services. Such "Know Your Business Customer" obligations reduce the anonymity that often enables online counterfeiting.[28] This emphasis on traceability is especially pertinent to Pakistan, where anonymous seller accounts remain a facilitator of online IP infringement.

C. The United States: The DMCA Safe Harbour and Notice-and-Takedown

The Digital Millennium Copyright Act 1998 (DMCA) established the foundational legal architecture for online intermediary liability in the United States, and its safe harbour provisions under 17 U.S.C. § 512 remain the most-studied and most-emulated model in the world.[29] Under Section 512, online service providers benefit from safe harbour protection from copyright liability for third-party content if, *inter alia*, they do not have actual knowledge of infringing material, they do not receive a financial benefit directly attributable to the infringing activity, and they expeditiously remove infringing material upon receipt of a compliant takedown notice from a rights-holder.[30]

The DMCA notice-and-takedown system has been criticised for facilitating abuse by both rights-holders (who may issue overbroad notices) and infringers (who can restore content by filing counter-notifications, potentially without consequence).[31] Nevertheless, the system provides a legally certain procedural framework that gives rights-holders a meaningful remedy against infringing online content without requiring full civil litigation. For smaller rights-holders with limited enforcement budgets, the ability to compel a platform to remove an infringing listing within days by filing a standardised notice is enormously valuable.

[27] *Id.* art. 17(1).
[28] *Id.* art. 30.
[29] 17 U.S.C. § 512.
[30] 17 U.S.C. § 512(c)(1).
[31] Niva Elkin-Koren, After Twenty Years: Revisiting Copyright Liability of Online Intermediaries, in The Evolution and Equilibrium of Copyright in the Digital Age 23–26 (Susy Frankel & Daniel Gervais eds., Cambridge University Press 2014).

The Trademark context in the US is governed differently: unlike copyright, there is no statutory safe harbour for trademark infringement under the DMCA, and courts have developed a complex body of common law addressing contributory and vicarious trademark liability for online platforms. The landmark decisions in *Tiffany (NJ) Inc. v. eBay Inc.* (2010) and the more recent Second Circuit decisions on platform liability illustrate the fact-intensive analysis required in this area.[32] This common law approach, while flexible, generates significant uncertainty and litigation costs, suggesting that a legislative solution—as pursued in the EU—is preferable.

D. Synthesis: Lessons for Pakistan

The comparative survey yields several clear lessons for Pakistani reform. First, legal certainty is essential: platforms operate at scale and require clear, predictable rules governing their obligations when notified of infringing content. Second, notice-and-takedown works best when it is legislatively mandated, procedurally specific, and subject to proportionate consequences for non-compliance. Third, traceability of sellers—through identity verification and public disclosure—is a structurally important complement to takedown mechanisms. Fourth, streamlined dispute resolution that bypasses the ordinary civil courts is necessary for rights-holders who cannot afford protracted litigation.

V. THE CASE FOR REFORM: PLATFORM LIABILITY AND NOTICE-AND-TAKEDOWN IN PAKISTAN

A. Reinterpreting Section 156 of the Trademarks Ordinance 2001

In the absence of legislative action, Pakistani IP tribunals have a significant role to play in developing the law to address digital infringement. This paper argues that Section 156 of the TO 2001—which permits tribunals to ‘pass such other orders as it deems fit’—is broad enough to support platform takedown orders when a rights-holder provides adequate notice of infringing content.

This interpretation is supported by several considerations. First, the section’s text is deliberately open-ended, conferring broad equitable jurisdiction on IP tribunals. Second, Pakistani courts have, in other contexts, demonstrated willingness to issue novel injunctive relief

[32] *Tiffany (NJ) Inc. v. eBay Inc.*, 600 F.3d 93 (2d Cir. 2010).

against intermediaries: the Lahore High Court's willingness to issue website blocking orders in entertainment piracy cases demonstrates an awareness that the practical effectiveness of IP rights may require orders directed at third parties who are not themselves infringers but who control the channels through which infringement occurs.[33] Third, such an interpretation is consistent with the TRIPS Agreement's requirement that member states make available effective and proportionate remedies for IP infringement.[34]

A tribunal order requiring a platform to remove a specifically identified infringing listing—issued on the application of a rights-holder and after giving the platform an opportunity to respond—would not impose an unreasonable burden on platforms, would be proportionate to the harm suffered by rights-holders, and would be consistent with the constitutional protections for property rights contained in Article 23 of the Constitution of Pakistan.[35] The 'any other relief' language of Section 156 provides the necessary statutory hook for such relief, and the courts should not hesitate to use it.

B. The Case for a Legislative Notice-and-Takedown Regime

While creative statutory interpretation can provide interim relief, the long-term solution lies in legislation. This paper advocates for the enactment of a dedicated e-commerce IP enforcement statute or, alternatively, the amendment of the TO 2001 and Copyright Ordinance 1962 to incorporate a notice-and-takedown framework with the following essential components.

First, the framework should define the categories of online platform subject to the regime. This should include all operators of online marketplaces through which third-party sellers offer goods to Pakistani consumers, regardless of the platform's geographic location. The precedent of the IT Rules 2021 in India and the DSA in the EU for assertions of extraterritorial jurisdiction over large foreign platforms is relevant here.

Second, the framework should impose an obligation on platforms to designate a registered agent to receive IP infringement notices, and to process compliant notices within a defined timeframe—ideally 48 to 72 hours for initial takedown, with a longer period for final

[33] *See, e.g.,* PAK. TELECOMM. AUTH., ANNUAL REPORT 2023 (2024) (referencing blocking activity against online piracy).
[34] Agreement on Trade-Related Aspects of Intellectual Property Rights art. 41(1), Apr. 15, 1994, 1869 U.N.T.S. 299.
[35] PAK CONST. arts. 23–24.

determination of disputes. The Indian and DMCA models suggest that 15 days for final resolution is a workable benchmark.

Third, the framework should specify the contents of a valid notice, including identification of the rights-holder and the claimed right, a description of the allegedly infringing listing sufficient to locate it, and a declaration of good faith belief. A counter-notification procedure, allowing sellers to contest takedowns that they believe to be wrongful, should also be established.

Fourth, the framework should establish consequences for non-compliance: platforms that repeatedly fail to act on valid notices, or that fail to implement seller identity verification protocols, should lose any immunity from secondary liability they might otherwise enjoy under general tort principles.

Fifth, the framework should include "Know Your Seller" obligations analogous to the DSA's Article 30, requiring platforms to obtain and retain verified identity information for commercial sellers. This would address the fundamental problem of seller anonymity that currently frustrates enforcement.

C. Streamlined Dispute Resolution: A UDRP-Style Framework

Beyond the notice-and-takedown mechanism, this paper argues that Pakistan should develop a streamlined alternative dispute resolution system for online IP disputes, modelled on the Uniform Domain-Name Dispute-Resolution Policy (UDRP) administered by ICANN-accredited dispute resolution providers such as WIPO's Arbitration and Mediation Center.[36]

The UDRP demonstrates that online intellectual property disputes can be resolved through a specialised process that is relatively swift, inexpensive, and accessible. Proceedings are ordinarily concluded within a short period, filing costs are substantially lower than those associated with civil litigation, and the process is conducted online. The system has also produced a substantial body of decisions applying broadly consistent standards across a large number of cases. A comparable mechanism for e-commerce-related intellectual property disputes

[36] World Intell. Prop. Org. Arb. & Mediation Ctr., WIPO Overview of WIPO Panel Views on Selected UDRP Questions, 1–5 (3rd ed. 2017).

in Pakistan, administered either through an expanded intellectual property tribunal framework or through a designated arbitral or ADR institution, could offer rights holders a more effective and accessible alternative to conventional civil proceedings.

Such a system could handle disputes about infringing seller accounts, infringing product listings, and online trademark misuse, with remedies including account suspension, listing removal, and injunctive relief enforceable against platforms operating in the Pakistani market. The speed and accessibility of such a system would be particularly valuable for the large number of small and medium-sized Pakistani enterprises who currently lack the resources to litigate IP claims in the ordinary courts.

VI. THE COPYRIGHT AMENDMENT BILL 2024: AN ASSESSMENT

The Copyright Amendment Bill 2024 (CAB 2024) represents a meaningful, if incomplete, step towards modernising Pakistan's copyright framework. Its introduction of technological protection measures and digital rights management reflects a welcome acknowledgment that copyright enforcement in the digital environment requires new tools. The Bill's provisions on collective management organisations (CMOs) also represent a positive development, providing a more structured framework for licensing and remuneration for copyright owners in the digital ecosystem.[37]

However, the CAB 2024's most significant omission is its failure to address online platform liability and notice-and-takedown. This omission is not merely a drafting oversight; it reflects a broader conceptual gap in the Bill's approach, which remains focused on the creation and protection of rights rather than their digital enforcement. The Bill's emphasis on criminal penalties—including proposed increases in maximum custodial sentences for copyright piracy—reflects a traditional enforcement paradigm that is poorly suited to the scale and speed of online infringement.

Criminal prosecution is, in practice, a selective and resource-intensive tool: it cannot address the tens of thousands of infringing listings that appear on Pakistani e-commerce platforms daily, and it provides no mechanism for the rapid removal of infringing content.

[37] The Copyright (Amendment) Bill, 2026, cls. 14–22 (Pak. Nat'l Assembly).

Rights-holders—particularly individual creators whose copyrights are infringed in the digital environment—need swift, accessible civil remedies, not the prospect of criminal prosecutions that may never materialise.

Parliament's consideration of the CAB 2024 presents an important opportunity to remedy these deficiencies through amendment. The insertion of a Part covering online service provider liability—modelled on the IT Act Section 79 or the DMCA Section 512 framework—would transform the Bill from a limited measure into a genuinely comprehensive digital copyright statute. This paper urges the standing committee considering the Bill to recommend the inclusion of such provisions.

VII. CONCLUSIONS AND POLICY RECOMMENDATIONS

The structural inadequacy of Pakistan's digital IP enforcement framework has led to there being a genuine and growing crisis. The migration of commerce to online platforms has exposed the structural inadequacy of an IP legal framework designed for the physical world. Rights-holders are losing substantial revenues to online counterfeiting, enforcement mechanisms are slow and ill-suited to the digital environment, and Pakistani e-commerce platforms operate in a legal vacuum regarding their obligations when notified of infringing content.

This paper has argued that the solution lies in three complementary reforms. First, Pakistani IP tribunals should adopt a proactive interpretation of Section 156 of the Trademarks Ordinance 2001 to issue platform takedown orders as part of their equitable jurisdiction, pending legislative reform. This interpretation is consistent with the text of the statute, with Pakistan's TRIPS obligations, and with the constitutional protection of IP rights. Second, Parliament should enact a dedicated e-commerce IP enforcement framework—or amend existing IP statutes—to establish a mandatory notice-and-takedown regime with clear procedural requirements, defined timeframes, seller identity verification obligations, and proportionate consequences for non-compliance. Third, a UDRP-style streamlined arbitral mechanism for online IP disputes should be developed to provide rights-holders with fast, accessible, and cost-effective alternatives to civil court litigation.

The comparative evidence is clear: jurisdictions that have adopted legislative notice-and-takedown frameworks—India, the EU, and the US—have succeeded in creating meaningful, if imperfect, incentives for platform cooperation in IP enforcement. Pakistan's failure to do the same imposes real economic costs on rights-holders, undermines investor confidence in the protection of IP assets, and harms consumers who are misled by counterfeit goods. Stronger penalties alone will not solve this problem; what is needed are enforcement mechanisms built for the way online commerce actually works. The digital economy will continue to expand; accordingly, the need for reform has become both immediate and imperative.

DIGITAL PIRACY IN THE ERA OF ARTIFICIAL INTELLIGENCE AND CHALLENGES TO COPYRIGHT GOVERNANCE IN INDIA: AN ANALYTICAL STUDY OF THE ENTERTAINMENT SECTOR

By Gagandeep Singh

VOLUME I | ISSUE I | ARTICLE III

APRIL 2026

The Legalis IP Quarterly

ABSTRACT

The rapid expansion of digital platforms has fundamentally reshaped the entertainment industry in India, accompanied by a significant rise in digital piracy. The emergence of Artificial Intelligence (AI)-enabled technologies has further intensified this issue by enabling swift and automated duplication, modification, and large-scale dissemination of protected content. This development poses serious challenges to traditional copyright enforcement mechanisms, which were not designed to operate within an AI-driven digital ecosystem. Despite the presence of a comprehensive copyright framework in India, digital piracy continues to persist, raising concerns about the effectiveness of existing copyright governance. The rise of AI-driven piracy, combined with the role of online intermediaries and the cross-border flow of digital content, exposes critical gaps in enforcement strategies and regulatory frameworks. This study adopts a doctrinal research methodology, analysing relevant provisions of the Copyright Act, 1957 and the Information Technology Act, 2000, along with applicable case laws and regulatory mechanisms governing digital intermediaries and online platforms. It argues that digital piracy in the AI era is not merely a technological concern but reflects deeper governance challenges within India's copyright regime. AI-driven automation amplifies the scale, speed, and anonymity of infringement, while enforcement mechanisms and intermediary liability frameworks remain largely reactive. Consequently, the current legal framework struggles to balance

technological innovation, platform accountability, and the protection of creative rights. The paper concludes that there is an urgent need to re-evaluate copyright governance in India, emphasising stronger intermediary accountability, clearer regulatory obligations, and adaptive legal strategies to effectively combat digital piracy while accommodating ongoing technological advancements in the entertainment sector.

This paper argues that Indian copyright law, designed for human-scale infringement, is structurally incapable of addressing AI-enabled digital piracy, necessitating a shift towards platform-centric liability and regulatory oversight.

Keywords: *AI-enabled digital piracy; copyright governance in India; intermediary liability; platform-centric liability; copyright enforcement; digital entertainment sector; online platform regulation; cross-border digital infringement; regulatory accountability; adaptive legal strategies; Copyright Act, 1957; Information Technology Act, 2000.*

I. INTRODUCTION

A. The Rise of AI-enabled Digital Piracy as a Systemic Threat

The pace of technological innovation has significantly outstripped the issue-identification capacity and legislative responsiveness of the Indian Parliament.[1] Among the most pressing challenges emerging from this regulatory lag is the rise of AI-enabled digital piracy, which represents not merely a continuation of conventional copyright infringement but an evolved, systemic threat amplified by artificial intelligence tools.

In contrast to earlier forms of piracy, which were constrained by human effort and limitations in physical and digital distribution, contemporary artificial intelligence technologies have substantially reduced barriers to entry while vastly expanding the scale of infringement. AI-assisted content replication, deepfake dubbing, real-time subtitle generation, and algorithmically driven redistribution networks now facilitate the reproduction, localisation, and dissemination of infringing content with unprecedented speed and volume. As a result, digital piracy is no longer adequately understood as an isolated act of infringement; rather, it has evolved into a structural distortion of lawful markets.

The entertainment sector is particularly vulnerable to this shift, especially in economic terms. Revenue streams dependent on licensing, theatrical releases, streaming subscriptions, and territorial exclusivity are systematically undermined when AI tools enable near-instantaneous global circulation of pirated content, for emerging markets such as India, where monetisation already operates on thin margins, AI-driven piracy threatens the sustainability of creative industries by eroding incentives for investment, reducing employment opportunities, and destabilising legitimate distribution ecosystems.[2]

Crucially, existing copyright enforcement mechanisms, which are designed for human-scale infringement, are ill-equipped to address algorithmic piracy that operates across jurisdictions, platforms, and anonymised networks. The resulting enforcement asymmetry allows infringing actors to innovate faster than regulatory frameworks can adapt, thereby widening the gap between technological capability and legal control.

---

[1] Rohit Singh, *India Not Planning Separate AI Law; Digital India Act Remains Stalled*, MediaNama (Dec. 17, 2025), https://www.medianama.com/2025/12/223-india-ai-law-digital-india-act-stalled/. [https://perma.cc/GX8J-HE6T]

[2] John McLellan, *AI Piracy Is a Threat to Our Creative Industries,* THE TIMES (Feb. 24, 2025 at 14:45 GMT).

In this context, AI-enabled digital piracy must be understood not merely as a copyright violation but as a systemic economic and governance challenge, necessitating a re-examination of legislative strategy, enforcement architecture, and international cooperation in the digital age.

B. Why traditional copyright enforcement is failing

India's copyright framework was enacted in a vastly different historical and economic context. The Copyright Act, 1957, is a post-colonial statute drafted for a creative ecosystem centred on human authorship, identifiable infringers, and physical modes of distribution. Its underlying assumptions reflected a pre-digital economy, where creation and infringement were linear, traceable, and territorially confined.[3]

The emergence of artificial intelligence has disrupted these foundational assumptions. AI-enabled systems can now generate, replicate, modify, and distribute content at scale, often without clear attribution or direct human involvement. As a result, traditional enforcement tools—such as establishing authorship, originality, and liability—have become increasingly difficult to apply in practice.[4]

This structural mismatch has weakened the effectiveness of existing copyright enforcement mechanisms. Incremental judicial interpretation alone is insufficient to address algorithmic creation and AI-driven piracy. There is therefore a pressing need for targeted amendments to the Copyright Act and the development of AI-specific legislative frameworks suited to Indian market realities, aimed at balancing creators' rights with broader societal interests.

II. CONCEPTUAL FRAMEWORK: DIGITAL PIRACY AND COPYRIGHT

A. Copyright protection in the digital environment

The shift from physical copies to digital storage and online transmission has fundamentally changed copyright enforcement. Unlike tangible works, digital content can be copied,

[3] The Copyright Act, 1957 (India).
[4] Al-Busaidi et al., *supra* note 2, at 100640.

modified, and shared instantly at almost no cost.[5] Traditional copyright law was designed for a system where infringement occurred through identifiable physical reproduction. In the digital environment, however, copying happens rapidly and across borders, making detection and control significantly more difficult.

The internet has intensified this problem by enabling global access to copyrighted works such as books, films, music, software, and images. These works circulate through decentralised networks, often anonymously. As a result, tracing the source of infringement and establishing liability becomes complex. The issue is not merely unauthorised copying, but the scale, speed, and anonymity with which digital piracy operates.

A common misconception is that material available online is free for public use. In reality, availability does not mean absence of copyright. Unless a work has entered the public domain, been licensed, or falls within statutory exceptions, it remains protected. The digital environment, therefore, creates a tension between easy access and continued legal protection.

In India, the Copyright Act, 1957, does not clearly address intermediary liability in digital contexts. Instead, Section 79 of the Information Technology Act, 2000 grants safe harbour protection to intermediaries, provided they comply with due diligence requirements. While this provision aims to balance technological growth with legal accountability, it also limits the effectiveness of copyright enforcement in cases of large-scale digital piracy.

Thus, the challenge posed by digital technologies is not only technical but doctrinal. The foundations of copyright law, identifiable authors, physical copies, and centralised distribution are increasingly strained in the digital era.

B. Evolution of digital piracy in India

Digital piracy in India has evolved from physical VCD/DVD copying in the 1990s and peer-to-peer torrent sharing (2000s-2010s) to sophisticated, real-time illegal streaming, Telegram sharing, and IPTV, driven by high-speed internet and smartphone adoption.

[5] World Intellectual Property Organization, *Understanding Copyright and Related Rights 8–10* (2d ed. 2016); Organisation for Economic Co-operation and Development, OECD Digital Economy Outlook 2015 60–65 (2015).

Piracy rates in India reached 62% during the pandemic, causing massive financial losses, with social media and apps replacing torrents as primary distribution channels. [6]

The trajectory of digital piracy in India reflects a clear technological progression, closely aligned with changes in media consumption patterns and internet penetration. In the physical era (1980s–1990s**)**, piracy was primarily facilitated through analogue technologies such as VCRs and later VCD/DVD formats, enabling the unauthorised reproduction and circulation of cinematographic works from theatres to private viewing spaces. This phase was largely localised and dependent on physical distribution networks. The subsequent torrent and peer-to-peer (P2P) era (2000s–2010s) marked a significant shift toward digital decentralisation, wherein platforms such as The Pirate Bay enabled large-scale dissemination of copyrighted content, including films, music, and software, through file-sharing protocols that minimised reliance on central servers.

With the advent of affordable high-speed internet, particularly following the market disruption caused by Reliance Jio, India entered the streaming and social media era (2015–present). During this phase, piracy transitioned from download-based models to instantaneous streaming, with illegal websites, IPTV services, and encrypted platforms such as Telegram channels—often colloquially described as the "new Palika Bazaar"—emerging as dominant vectors. Concurrently, there has been a notable **shift toward mobile applications**, wherein unregulated and fraudulent apps provide direct access to pirated OTT content and even recently released theatrical films. Empirical observations indicate that torrent-based piracy has significantly declined, accounting for only a marginal proportion (approximately 6%) of total piracy consumption.

The economic and regulatory implications of this evolution are substantial. Industry estimates suggest that digital piracy has resulted in losses of approximately USD 2.8 billion to the Indian media and entertainment sector, with consequential impacts on employment and revenue generation. In response, the government introduced legislative reforms, most notably through the Cinematograph (Amendment) Act, 2019, aimed at strengthening anti-piracy enforcement. Additionally, Indian courts have increasingly adopted the mechanism of dynamic injunctions, enabling real-time blocking of mirror and proxy websites to curb recurring infringements. Despite these measures, enforcement

[6] Gunjan Chawla & Nidhi Hriday Buch*, Impact of Online Digital Piracy on the Indian Film Industry: An Empirical Investigation,* J. INTELL. PROP. RTS., January, 2023, at 21, 23.

challenges persist due to the transnational, encrypted, and rapidly adaptive nature of modern piracy networks. Furthermore, emerging trends indicate that approximately 10% of pirated content is now disseminated via social media platforms, particularly in the context of live sports streaming.

Overall, the evolution of digital piracy in India demonstrates a transition **from** physically distributed and decentralised file-sharing systems to highly centralised, encrypted, and instantaneous streaming ecosystems, thereby complicating traditional enforcement mechanisms and necessitating more adaptive, technology-driven regulatory responses.

C. Limits of author-centric enforcement

Indian copyright law is structurally premised upon identifiable human authorship and traceable acts of infringement. The Copyright Act, 1957, defines an "author" in relation to different categories of works under Section 2(d), and vests first ownership in such author under Section 17.[7] The statutory framework, therefore, assumes that creative expression originates from a natural person whose intellectual effort can be legally recognised and protected. This author-centric orientation extends to the threshold requirement of originality under section 13, which protects only those works that embody a degree of skill, labour, and judgment attributable to a human creator.[8]

The Supreme Court's decision in Eastern Book Company v. D.B. Modak clarified that Indian copyright law adopts a "modicum of creativity" standard, requiring the exercise of skill and judgment beyond mere mechanical labour.[9] This formulation, while modernised, remains fundamentally anchored in human intellectual contribution. Artificial intelligence systems, however, complicate this doctrinal foundation. Where AI tools autonomously generate derivative content, perform automated scraping, or remix existing works without direct human intervention, the nexus between authorship and creative control becomes attenuated. The law's insistence on human agency struggles to accommodate algorithmic production that operates without conventional intentionality.

[7] The Copyright Act, 1957, §§ 2(d), (India).

[8] Id. at § 13.

[9] *Eastern Book Co. v. D.B. Modak*, (2008) 1 SCC 1.

The enforcement model under section 51 of the Copyright Act further reflects this author-centric architecture. Infringement is framed as an act committed by a person who reproduces, distributes, or communicates a work to the public.[10] Liability presupposes identifiable agency and demonstrable causal participation. AI-enabled piracy, by contrast, often functions through distributed bot networks, automated content extraction, and algorithmic dissemination across multiple jurisdictions. In such contexts, locating a singular infringer or establishing direct intention becomes increasingly difficult.

The rise of intermediary-based enforcement mechanisms illustrates an attempt to adapt to digital realities. Section 79 of the Information Technology Act, 2000, grants conditional safe-harbour protection to intermediaries, provided they comply with due diligence and remove unlawful content upon actual knowledge.[11] In *Shreya Singhal v. Union of India*, the Supreme Court interpreted "actual knowledge" to require either a court order or a government notification before liability may attach.[12] While this interpretation protects free expression, it reinforces a reactive notice-and-takedown model that is ill-suited to algorithmic piracy operating at scale.

Judicial innovations such as "dynamic injunctions," recognised in UTV Software Communication Ltd. v. 1337X.to,[13] attempt to block mirror websites in real time. Yet these measures remain remedial rather than preventive, addressing symptoms rather than structural causation. They do not confront the core difficulty: the displacement of identifiable human infringers by automated systems and decentralised technological infrastructures.

Comparative scholarship has long recognised the strain that computer-generated works place on traditional authorship doctrines.[14] The challenge posed by AI-enabled piracy, therefore, lies not merely in enforcement logistics but in the conceptual architecture of

[10] The Copyright Act, 1957, § 51 (India).

[11]The Information Technology Act, 2000, § 79, (India).
[12] Shreya Singhal v. Union of India, (2015) 5 SCC 1.
[13] UTV Software Communication Ltd. & Ors. v. 1337X.to & Ors., 2019 SCC OnLine Del 8002 (High Court of Delhi).
[14] Pamela Samuelson, *Allocating Ownership Rights in Computer-Generated Works,* 47 U. PITT. L. REV. 1185 (1986).

copyright itself. An enforcement regime centred on identifiable human agency is increasingly inadequate in an environment where algorithmic processes replicate, transform, and distribute content at speed and scale beyond human control. The limits of author-centric enforcement thus reveal a deeper governance gap—one that necessitates reconsideration of liability models in the age of artificial intelligence.

III. JUDICIAL AND LEGISLATIVE RESPONSE IN INDIA

A. Key Judicial Approaches to Online Piracy

Indian courts have responded to the proliferation of online piracy through a combination of injunctive innovation and intermediary-based enforcement. The judiciary's primary strategy has been to adapt traditional copyright remedies to digital environments rather than reconceptualising liability structures.[15]

One of the most significant doctrinal developments has been the recognition of "dynamic injunctions." In *UTV Software Communication Ltd. v. 1337X.to*, the Delhi High Court acknowledged that rogue websites repeatedly evade blocking orders by creating mirror or redirect sites.[16] The Court, therefore, permitted plaintiffs to seek extension of blocking orders against newly emerging domains without initiating fresh litigation. This innovation reflects judicial awareness of the fluid architecture of digital piracy.

However, dynamic injunctions remain fundamentally reactive. They address specific infringing domains after harm has occurred and rely heavily on court-supervised enforcement. They do not impose systemic obligations on platforms or technological intermediaries to prevent recurrence.

Courts have also engaged with intermediary liability under Section 79 of the Information Technology Act, 2000. In *MySpace Inc. v. Super Cassettes Industries Ltd.*, the Delhi High Court examined the scope of safe harbour protection and emphasised that intermediaries must exercise due diligence and remove infringing content upon acquiring knowledge.[17] Subsequently, in Shreya Singhal v. Union of India, the Supreme Court clarified that "actual knowledge" under Section 79 requires a court order or government notification, thereby narrowing intermediary exposure to liability.[18]

[15] UTV Software Commc'ns Ltd., 2019 SCC OnLine Del 8002.
[16] UTV Software Commc'ns Ltd., 2019 SCC OnLine Del 8002, 45.
[17] MySpace Inc. v. Super Cassettes Indus. Ltd., 2016 SCC OnLine Del 6382 (High Ct. Del.).
[18] Shreya Singhal, (2015) 5 SCC 1 at 117.

While these decisions protect free speech and technological innovation, they reinforce a notice-and-takedown model that presumes identifiable content and traceable infringement. In an AI-driven ecosystem where automated systems replicate and redistribute content instantaneously, this reactive framework struggles to contain infringement at scale.

B. Inconsistencies and Enforcement Gaps

Despite judicial activism, enforcement outcomes remain uneven. Indian courts have adopted varying standards in assessing intermediary responsibility, often oscillating between strict oversight and deference to platform neutrality. The absence of uniform criteria for determining "knowledge," "control," and "due diligence" has generated doctrinal ambiguity.

The reliance on blocking orders illustrates another structural weakness. Website blocking is territorially limited and technologically circumventable through VPNs, mirror domains, and encrypted networks. Each successive injunction treats piracy as a discrete event rather than a systemic infrastructure problem. Consequently, enforcement becomes episodic rather than preventative.

Moreover, the infringement framework under Section 51 of the Copyright Act continues to assume direct or authorisable human conduct.[19] AI-enabled scraping tools, automated content cloning, and algorithmic redistribution networks complicate attribution. Where infringing acts are executed autonomously or through distributed networks, proving intention, authorisation, or direct participation becomes legally complex.

Enforcement asymmetry therefore persists: infringing actors exploit automation and decentralisation, while regulatory institutions rely on litigation-intensive, domain-specific remedies. This imbalance undermines deterrence and increases enforcement costs for rights holders.

C. Absence of AI-Specific Regulatory Vision

A significant gap in India's copyright governance is the absence of a coherent AI-specific regulatory framework. Neither the Copyright Act, 1957, nor the Information Technology

[19] The Copyright Act, 1957, § 51 (India).

Act, 2000, expressly addresses AI-generated infringement, automated content extraction, or algorithmic dissemination.

Recent legislative reforms, including amendments to the Cinematograph Act, aim to strengthen anti-camcording provisions and penalties for unauthorised recording in theatres.[20] However, such reforms remain oriented toward traditional forms of infringement and do not confront AI-enabled piracy operating through data scraping, machine translation, synthetic dubbing (use of AI voice technology to replace or generate dialogue in a different language or voice without traditional human dubbing artists recording every line) or automated content aggregation.

Similarly, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 impose due diligence obligations on intermediaries, including takedown requirements and grievance redressal mechanisms.[21] Yet these rules do not impose proactive monitoring duties specific to AI-driven replication, nor do they address algorithmic amplification of infringing material.

The absence of an AI-responsive regulatory architecture reflects a broader legislative hesitation. While policy discussions on artificial intelligence governance have intensified in India, copyright reform has not kept pace with technological acceleration. The current framework, therefore, remains reactive, platform-dependent, and case-specific ill-equipped to manage infringement systems powered by machine automation.

In sum, judicial innovation has mitigated certain operational challenges of online piracy, but it has not resolved the structural mismatch between author-centric copyright doctrine and algorithmic infringement ecosystems. The legislative response, similarly, remains fragmented and incremental. This convergence of judicial pragmatism and legislative inertia underscores the need for a reimagined governance model capable of addressing AI-enabled piracy at scale.

IV. AI-enabled Digital Piracy and the Structural Limits of Copyright Enforcement

A. Automation and Scale of Infringement

[20] The Cinematograph (Amendment) Bill 2019 (India).
[21] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) (India).

Artificial intelligence has fundamentally altered the operational architecture of digital piracy. Unlike earlier forms of infringement that required human effort and coordination, AI-enabled tools facilitate automated scraping, duplication, re-encoding, and redistribution of copyrighted content at scale. Algorithmic systems can extract audiovisual material, generate subtitles or dub versions, and disseminate infringing copies across multiple platforms within minutes of release. This automation significantly lowers entry barriers, reduces dependence on skilled infringers, and transforms piracy from discrete individual acts into systemic, technology-driven processes. The cross-border nature of digital networks further amplifies this scale, allowing infringing content to circulate globally with minimal friction.

B. Erosion of Legal Accountability

The expansion of AI-driven systems destabilises traditional principles of legal accountability. Copyright enforcement relies upon identifiable human agency and demonstrable intent. However, automated systems complicate the attribution of mens rea, particularly where infringement is executed through bots, algorithmic aggregation, or machine-generated replication. Authorship and originality standards anchored in human skill and judgment are blurred when AI modifies or reconstructs protected works. Additionally, traceability becomes technologically evasive in distributed digital ecosystems, making it increasingly difficult to distinguish between primary infringers and intermediaries. As agency becomes diffused across technological infrastructures, conventional liability models struggle to maintain doctrinal coherence.

C. Limits of Reactive Enforcement Models

Indian enforcement strategies largely remain reactive. The notice-and-takedown framework under intermediary regulation presupposes identifiable infringing content and responsive removal. In an AI-driven environment characterised by real-time replication, this model proves inadequate. Judicial reliance on blocking orders and dynamic injunctions addresses specific infringing domains but does not prevent automated re-emergence through mirror sites, encrypted platforms, or algorithmic redistribution. Safe harbour protections further reinforce platform neutrality, limiting proactive monitoring obligations. Consequently, litigation-centric remedies operate at a slower pace than automated infringement systems, resulting in persistent enforcement asymmetry.

D. Governance Gap in the Age of AI

The current statutory framework does not meaningfully engage with AI-enabled infringement. The absence of AI-specific copyright provisions reflects a broader regulatory lag in responding to technological acceleration. Human-centric doctrinal assumptions premised on identifiable authors and traceable acts are increasingly misaligned with algorithmic systems capable of autonomous replication and distribution. This structural gap underscores the need for a shift toward platform-centric and preventive governance models that integrate AI accountability mechanisms within copyright enforcement architecture.

V. CONCLUSION

Indian copyright law remains anchored in an author-centric and human-scale enforcement framework. The rise of AI-enabled piracy exposes structural weaknesses in attribution, liability, and deterrence, and highlights the limits of reactive judicial remedies. As automated systems accelerate infringement beyond traditional enforcement capacities, incremental adaptation is no longer sufficient.

To respond effectively, there is a need to move towards a more proactive and technology-aware system of copyright governance supported by clear reforms. First, the legislature should impose specific statutory obligations on digital intermediaries and AI platforms to actively prevent the misuse of copyrighted content. This should include mandatory deployment of advanced content recognition technologies capable of detecting copyrighted material at the stage of upload, as well as during dissemination. Platforms should also be required to maintain detailed audit logs of AI-generated outputs and user activity, enabling traceability in cases where infringing content is created or circulated through automated systems. In addition, periodic compliance audits and transparency reports should be mandated to ensure that platforms are not passively facilitating large-scale infringement.

Second, the law should establish a robust framework for attribution and traceability of AI-generated and AI-assisted content. This may include compulsory digital watermarking, embedded metadata standards, or unique content identifiers that remain attached to works even after modification. Such a system would make it significantly harder to circulate infringing content anonymously and would assist rights holders and enforcement authorities in identifying the source and chain of distribution of pirated material.

Third, India should introduce a specialised liability regime for AI systems that distinguishes between passive intermediaries and actively generative technologies. Where AI tools are designed or deployed in a manner that enables or encourages infringement, developers and deployers should be subject to a higher standard of responsibility, including potential contributory liability. This could be coupled with clear safe harbour conditions that are conditional upon demonstrable efforts to prevent misuse, thereby incentivising responsible innovation while discouraging negligent or exploitative deployment of AI systems.

Finally, enforcement mechanisms must be strengthened to match the speed and scale of AI-driven infringement. This can be achieved by formally recognising dynamic injunctions in statutory law and by establishing fast-track digital enforcement procedures, including dedicated tribunals or specialised benches for technology-related copyright disputes. Real-time blocking measures and coordinated action with internet service providers can further ensure that infringing content is taken down swiftly before it proliferates widely.

These reforms would help shift copyright enforcement from a reactive approach to a more preventive and technologically aligned system, ensuring that creative incentives are protected while effectively addressing the challenges posed by AI-driven piracy.

TRANSITIONING FROM PASSIVE SAFE HARBOURS TO ACTIVE SENTINELS: A CRITICAL INFORMATION TECHNOLOGY (INTERMEDIARY GUIDELINES AND DIGITAL MEDIA ETHICS CODE) AMENDMENT RULES, 2026.

By Padmini Majhi

VOLUME I | ISSUE I | ARTICLE IV

APRIL 2026

The Legalis IP Quarterly

Abstract

The proliferation of high-fidelity synthetic media in India presents unprecedented social, economic, and psychological risks to its 850 million internet users. Initially, an artistic medium, the malicious application of generative AI has facilitated identity manipulation, misinformation, and fraud, challenging existing regulatory frameworks spreading misinformation, and facilitating fraudulent activities, which have exposed serious regulatory and legal challenges. Currently, the Indian judicial system still relies on "technologically neutral" provisions, specifically Section 66C (Identity theft) and Section 66D (Cheating by personation) of the Information Technology Act 2000, and Sections 319 and 353 of the Bharatiya Nyaya Sanhita, 2023. While these laws are bailable and cognisable offences, they fail to address the technical aspects and forensic challenges of synthetic media. This paper focuses on the doctrinal and comparative methodology where a strategic realignment in Indian jurisprudence is introduced by the IT (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2026, where for the first time deepfake has been statutorily recognised as Synthetically Generated Information (SGI), which mandates watermarking and labelling mandates and Rule 4(1A), which requires platforms to verify user declarations through appropriate technical measures, while comparatively examining the IT Amendment

Rules 2026 against the EU AI Act's value-chain transparency model and the United States TAKE IT DOWN Act's harm-specific targeting approach. This research paper argues whether the current legislative pivot imposes an undue burden onto the digital intermediaries by transitioning them from "Passive Safe Harbours to Active Sentinels". Furthermore, forensic targeting of individual creators is often technically infeasible and shifts the liability to platforms, creating a de facto censorship regime. Such a shift risks undermining the legal protections and procedural due process established in the Shreya Singhal v. Union of India judgment. This interrogation evaluates the 2026 Rules through the lens of constitutional proportionality.

Keywords: *Deepfakes, Synthetically Generated Information (SGI), IT Amendment Rules 2026, Intermediary Liability, Safe Harbour, Shreya Singhal, EU AI Act, TAKE IT DOWN Act, Article 19, Digital Censorship, Generative AI Regulation*

I. INTRODUCTION

The Election Commission of India issued an advisory directing political parties to label AI-generated or synthetic content used in their social media campaigns.[1] The urgency of such measures became evident when, in late November 2025, a deepfake video circulated widely depicting Chief Election Commissioner Gyanesh Kumar bowing before Home Minister Amit Shah.[2] A similar incident had emerged in late November 2023, when actress Rashmika Mandanna's face was superimposed onto a video of British-Indian influencer Zara Patel. These incidents illustrate that, although India's existing legal framework addresses certain forms of cybercrime, it still lacks a targeted statutory regime capable of addressing the specific harms posed by synthetic media.

[1] *EC Directs All AI-Generated Poll Ads to Be Labelled as Such*, *Times of India* (Oct. 25, 2025), https://timesofindia.indiatimes.com/india/ec-directs-all-ai-generated-poll-ads-to-be-labelled-as-such/articleshow/124798284.cms

[2] *'Potential to Mislead': FIR Registered Against X for AI Video on PM Modi, ECI Chief Gyanesh Kumar*, *Times of India*(Mar. 26, 2026), https://timesofindia.indiatimes.com/india/potential-to-mislead-fir-registered-against-x-for-ai-video-on-pm-modi-eci-chief-gyanesh-kumar/articleshow/129817472.cms

The Indian judicial system still relies on "technologically neutral" provisions, specifically Section 66C (Identity theft) and Section 66D (Cheating by personation) of the Information Technology (IT) Act 2000, and Sections 319 and 353 of the Bharatiya Nyaya Sanhita (BNS) 2023.[3] Although these laws are non-bailable and cognisable offences, they fail to address the technical aspects and forensic challenges of synthetic media. Despite the significance of this regulatory shift, no comprehensive scholarly analysis has examined the constitutional validity of the 2026 Rules against the guardrails established in *Shreya Singhal v. Union of India* or evaluated India's approach with EU and US models. The Government of India notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 (the "2026 Rules"), mandating a watermarking and labelling mandate and Rule 4(1A) mandating platforms to verify user declaration through technical measures burdening the social Media Intermediaries while transitioning them from passive safe harbours to active sentinels. This transition challenges the constitutional guardrails established in *Shreya Singhal*, which protects citizens freedom of speech and expression under Article 19(1)(a).

This paper argues that the 2026 Rules, while pursuing a legitimate aim, are constitutionally suspect, failing the proportionality test under Article 19(1)(a), replicating none of Section 69A's procedural safeguards, and structurally producing a de facto regime through safe harbour conditionality.

Part II examines the anatomy of deepfakes and the failure of existing Indian laws to address them. Part III analyses the pre-amendment intermediary liability regime and the constitutional guardrails of *Shreya Singhal*. Part IV examines the architecture of the 2026 Rules. Part V undertakes a comparative analysis of the EU and US frameworks. Part VI critically interrogates the constitutional validity of the 2026 Rules. Part VII proposes recommendations. Part VIII concludes.

[3] Information Technology Act, No. 21 of 2000, §§ 66C–66D (India); Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 319, 353 (India).

II. THE ANATOMY OF DEEPFAKES: TECHNOLOGY, HARM, AND THE LIMITS OF EXISTING INDIAN LAW

A. How Deepfakes Work: A Legal-Technical Primer

Deepfakes are synthetic media content produced through artificial intelligence techniques primarily Generative Adversarial Networks and diffusion models, capable of creating realistic audio, video and audio-visual content depicting real life individuals or events in a situation that never occurred. Unlike earlier forms of digital manipulation, deepfakes are capable of generating content indistinguishable from original media even to trained observers. Current AI-based detection tools maintain an accuracy rate of 65% to 70%, rendering them insufficient for the conclusive forensic identification required by judicial standards.

B. Harm Taxonomy: Identity Fraud, NCII, Electoral Manipulation, and Reputational Injury

The range of harms caused by deepfake technology breaks down into five different types, each requiring a specific regulatory response.

In the domain of identity fraud and financial crime, AI-generated videos of N.R. Narayana Murthy served as a bait to trick victims into a fake trading platform operated by Lakhani, while similar deepfake videos of Mukesh Ambani and Murthy cheated several victims of around ₹95 lakh in late 2024.[4]

In the sphere of non-consensual porn, for instance, on Oct 13th 2023, the face of Rashmika Mandanna was taken as a deepfake and digitally imposed on the body of British Indian

[4] HT News Desk, *Two Bengaluru people fell prey to Narayana Murthy and Mukesh Ambani deep fake videos, loses close to ₹90L, Hindustan Times (Nov 4, 2024),* https://www.hindustantimes.com/cities/bengaluru-news/two-bengaluru-people-fell-prey-to-narayana-murthy-and-mukesh-ambani-deep-fake-videos-loses-close-to-rs-90l-report-101730688063694.html *[https://perma.cc/2UG5-8Q3J].*

Influencer Zara Patel in the case below, clearly shows that synthetic media can destroy an individual's dignity with the help of a proper legislative framework.[5]

The electoral application of deepfake mischief was pushed to the foreground by none other than India during general elections of 2024 with an important observation: last year there was a surge in deepfakes, which include fake videos of political figures and celebrities that endorse a candidate who they never even met, therefore, harm impact democratic society directly.

Judicial interventions have been the consequence of harm to the reputation of public figures. Towards the end of 2025, Salman Khan, Kumar Sanu, Nagarjuna, Aishwarya Rai Bachchan and other celebrities approached the Delhi High Court against unauthorised use of their personas in AI-generated works.[6] Similarly, in *Anil Kapoor v. Simply Life India & Ors.*, the Delhi High Court granted an injunction which cements protection for personality rights from AI misuse.[7]

Apart from the politicians and other public figures, ordinary individuals too become victims of deep fakes in psychological and social fronts, an injury that has no sufficient legal redress since it is still less reported due to ignorance and stigma.

C. Why Technologically Neutral Provisions Fail: Section 66C, 66D, and the BNS 2023

Section 66C and Section 66D of the IT Act, governing identity theft and cheating by personation respectively, were designed to address password theft and impersonation fraud in financial transactions, not for the forensic and epistemic complexities of synthetically generated media.[8] Both provisions require proof of dishonest intent and an actual fraudulent

[5] Arvind Ojha, *Rashmika Mandanna deepfake video: Delhi Police registers case, India Today* (Nov 10, 2023), https://www.indiatoday.in/india/story/rashmika-mandanna-deepfake-video-delhi-police-case-registered-2461547-2023-11-10 [https://perma.cc/RN5R-4Y56].
[6] TOI Entertainment Desk, *After Aishwarya Rai Bachchan, Kumar Sanu and Nagarjuna, Salman Khan moves to Delhi High Court seeking protection of personality, publicity rights, Times of India (Dec 13, 2025), https://timesofindia.indiatimes.com/entertainment/hindi/bollywood/news/after-aishwarya-rai-bachchan-kumar-sanu-and-nagarjuna-salman-khan-moves-delhi-high-court-seeking-protection-of-personality-publicity-rights/articleshow/125897674.cms [https://perma.cc/F5WJ-BQCL].*
[7] *Anil Kapoor v. Simply Life India*, CS(COMM) 652/2023 (High Court of Delhi 2023).
[8] Information Technology Act, 2000, §§ 66C, 66D (India).

transaction, elements that are structurally inapplicable in the case of AI, synthetically generated content and digital forgery as there are no such fraudulent transactions in the deepfakes crime.[9]

Section 319 (Cheating by Personation) and Section 353 (Public Mischief) were designed to combat misinformation and deception, and suffers from the same structural inadequacy to deal with deepfakes.[10] Neither provision mentions forensic evidence required to prove the involvement of deepfakes or AI based crimes. Furthermore, a deepfake electoral misinformation video does not fit into this provision.[11]

Both IT Act provisions and BNS provisions are bailable offences, meaning the accused person can secure bail easily, that is inadequate to a category of harm causing an irreversible and psychological damage to the victims within hours of publication. Moreover, neither framework set down any forensic evidentiary standard to address the technical and forensic aspects in respect to synthetic media, leaving courts without any legal basis to evaluate deepfake evidence.[12] The legislative vacuum left by both acts necessitated the 2026 Rules, where the architecture and constitutional implications of which are examined in Parts III and IV.[13]

III. THE PRE-AMENDMENT INTERMEDIARY LIABILITY REGIME

A. Section 79 and the Safe Harbour Architecture

Section 79 of the IT Act establishes the foundational safe harbour architecture for the "Social Media Intermediaries" (such as Google, Instagram, Facebook) from liability for third party content hosted on their platforms.[14] The architecture ensures the platforms provide a neutral ground of communication rather than being an active participant in content creation or

[9] *Id.*
[10] Bharatiya Nyaya Sanhita, 2023, §§ 319, 353 (India).
[11] *Id.*
[12] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, rule 2(1)(wa) [hereinafter 2026 Rules].
[13] Information Technology Act, 2000, § 79.
[14] *Id.*

dissemination. For the intermediaries to be exempted from the liabilities, Section 79(2) states[15] that the intermediaries' role must be limited to provide a communication system, where third-party information is sent, hosted, and received. The intermediaries must not initiate or select the receiver of the transmission, or select or modify the information, it must also follow guidelines prescribed by the Central Government. Intermediaries lose the safe harbour protection upon proof of conspiracy, abetment, or inducement of an unlawful act, abetted, aided or induced for committing the unlawful act. Furthermore, if it fails to expeditiously remove or disable access to the information after receiving the actual knowledge or being notified by the government.

Section 79 imposes liabilities on intermediaries for committing an unlawful act but also exempts them from liability for the independent actions of their users.

B. The IT (Intermediary Guidelines) Rules, 2021

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (subsequently amended in 2022, 2023, and 2026),[16] under which the concept establishes Safe Harbour protection for intermediaries. Rule 7 is the "enforcement" clause[17] of the guidelines the Rules explicitly state the intermediary fails to observe the due diligence that is outlined, the intermediaries would be held responsible for the unlawful act and Section 79(1) shall not apply. Rule 3 requires intermediaries[18] to periodically inform users of their own rules, privacy policies and user agreements in English or in any language mentioned in the Eighth Schedule of the Indian Constitution. Rule 3(1)(b)[19] states to make reasonable efforts that users should not host content that contains obscene, pornographic, invading another's privacy, gender biased, infringing patents and property rights, misinformation, threatening the sovereignty, integrity or security of India. Once the intermediaries are notified the content must be removed or disabled no later than 36 hours.[20] Rule 3(1)(d) states[21] that

[15] *Id.* § 79(2).
[16] 2026 Rules, *supra* note 9, rule 7.
[17] 2026 Rules, *supra* note 9, rule 7.
[18] 2026 Rules, *supra* note 9, rule 3.
[19] 2026 Rules, *supra* note 9, rule 3(1)(b).
[20] 2026 Rules, *supra* note 9, rule 3(1)(b).
[21] 2026 Rules, *supra* note 9, rule 3(1)(d).

after removal of the content, the intermediaries must keep the information and associated records for 180 days for investigation purposes. Rule 4 prescribes heightened compliance obligations for Significant Social Media Intermediaries (SSMI)[22]. It requires such intermediaries to appoint a Chief Compliance Officer resident in India, who bears personal liability for any failure to observe due diligence requirements; to publish monthly compliance reports, including details of links removed through proactive monitoring; and to designate a nodal contact person for round-the-clock coordination with law enforcement agencies. For serious offences involving threats to State security or public order, Rule 4 requires SSMI to identify the first originator of the information pursuant to a judicial order. It also mandates the appointment of a grievance redressal officer under Rule 3(2), who must acknowledge complaints within 24 hours and resolve them within 15 days. A user dissatisfied with the decision of the grievance redressal officer may prefer an appeal before the Grievance Appellate Committee (GAC).[23]

These provisions not only act as an active obligation but also give a clear understanding where the Intermediaries may be liable and for what.

C. *Shreya Singhal v. Union of India*: Constitutional Guardrails on Intermediary Liability

In the landmark case of *Shreya Singhal vs Union of India (2015)*,[24] the Supreme Court delivered a foundational judgment to protect the fundamental right to free speech and expression under Article 19(1)(a),[25] and clarified how intermediaries are held liable for third-party content. Under Section 79(3)(b) of the IT Act,[26] an intermediary loses its "Safe Harbour Immunity" if it fails to remove the unlawful content after receiving the "actual knowledge" which is only triggered by a court order or a notification from the appropriate government. After striking down Section 66A[27], the Supreme Court clarified that intermediaries may, consistently with Article 19(2)[28], block or remove content only on

[22] 2026 Rules, *supra* note 9, rule 4.
[23] 2026 Rules, *supra* note 9, rule 3(2).
[24] *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
[25] India Const. art. 19, cl. 1(a).
[26] Information Technology Act, 2000, § 79(3)(b) (India).
[27] *Shreya Singhal,* (2015) 5 SCC 1, 93.
[28] India Const. art. 19, cl. (2).

constitutionally recognised grounds, including the sovereignty and integrity of India, the security of the State, public order, and incitement to an offence. The Court held that mere discussion or even advocacy of an unpopular cause remains protected under Article 19(1)(a), and that speech may be curtailed only when it crosses the threshold of incitement or otherwise threatens public order or State security. While upholding Section 69A[29], the Court stressed that blocking orders must be reasoned and remain open to judicial challenge. It further required that both the originator and the intermediary be given an opportunity to be heard, and that a review committee examine the legality of blocking directions at least once every two months. The judgment also reaffirmed the void-for-vagueness doctrine[30], holding that a law is unconstitutional where an ordinary citizen cannot reasonably understand what conduct it prohibits.

However, none of these constitutional safeguards find any equivalent in the IT Amendment Rules 2026,[31] which conspicuously fails to define with sufficient clarity what synthetic content is prohibited and on what grounds.

IV. The IT Amendment Rules 2026: Architecture and Obligations

A. Synthetically Generated Information: The New Definitional Framework

The IT Amendment Rules 2026, introduce for the first time a statutory definition of Synthetically Generated Information ("SGI").[32] According to the Rules, SGI refers to audio, visual or audio-visual information, which can be artificially or algorithmically created and later generated, modified or altered using a computer equipment in such a way where the information appears to be real, original, authentic and depict any individual or event in a manner that is likely to be perceived as indistinguishable from a natural person or a real world event.[33] The rules clarify that not all AI-generated content qualifies as SGI-exceptions

[29] *Shreya Singhal*, (2015) 5 SCC 1, 112.
[30] *Id.* 93.
[31] 2026 Rules, *supra* note 9, rule 2(1)(wa).
[32] 2026 Rules, *supra* note 9, rule 2(1)(wa).
[33] *Id.*

include noise reduction, colour correction or compression that does not misrepresent the content.[34] The Rules further exclude creation of standard educational materials such as PDFs, presentations that do not constitute false electronic records.[35] It also excludes AI tools that are used as accessibility tools for the purpose of translation, subtitles, refining or improving content material.[36]

B. The Watermarking and Labelling Mandate

Rule 3(3) imposes an "ex-ante" obligation for the intermediaries that facilitate the creation or sharing of SGI.[37] Under this rule, the intermediaries must deploy automated tools to prohibit users from creating or sharing unlawful SGI such as child sexual abuse material ("CSAM"), non-consensual intimate imagery ("NCII"), forged documents or impersonation as public figures.[38] The Rules further mandate that visual SGI content be prominently labelled, while audio content requires a prefixed audio disclosure. Intermediaries must also embed permanent metadata and a unique identifier into the SGI to track the source of the information.[39] Modification, suppression or removal of these labels or identifiers is strictly prohibited for users.[40] Rule 3(1)(d) reduces the takedown timeline from 36 hours to 3 hours for content identified by court order or government notification,[41] while Rule 3(2)(b) mandates removal within 2 hours for complaints involving morphed intimate imagery.[42]

C. Rule 4(1A): Platform Verification and the Constructive Knowledge Problem

An additional responsibility is imposed on the Significant Social Media Intermediaries under the Rule 4(1A).[43] This rule makes it mandatory for the SGI to be published with more stringent requirements where users should confirm and declare that such content is

[34] 2026 Rules, *supra* note 9, rule 2(1)(wa)(i).
[35] 2026 Rules, *supra* note 9, rule 2(1)(wa)(ii).
[36] 2026 Rules, *supra* note 9, rule 2(1)(wa)(iii).
[37] 2026 Rules, *supra* note 9, rule 3(3).
[38] *Id.*
[39] *Id.*
[40] *Id.*
[41] 2026 Rules, *supra* note 9, rule 3(1)(d).
[42] 2026 Rules, *supra* note 9, rule 3(2)(b).
[43] 2026 Rules, *supra* note 9, rule 4(1A).

synthetically generated using automated tools or technical measures as provided by the SSMIs. An SSMI which permits, promotes or fails to act upon violating SGI will be regarded as failing to exercise due diligence obligations.[44] The "deemed failure" provision effectively imposes a constructive knowledge standard that compels intermediaries to pre-screen content, in clear departure from the "actual knowledge" standard affirmed in *Shreya Singhal*. The constitutional implications of this shift are examined in Part VI.

D. Safe Harbour Conditionality and the Chilling Effect on Intermediaries

The IT Amendment Rules 2026 under Section 79 of the IT Act make safe harbour protection expressly conditional on compliance with SGI obligations.[45] The Rule 7 states that if an intermediary fails to observe the process of due diligence, they lose their immunity and become liable for punishment under the IT Act 2000 and the Bharatiya Nyaya Sanhita, 2023.[46] However, Rule 1B (Protection for Removal)[47] clarifies that if an intermediary removes SGI to comply with these IT Act guidelines (including using automated tools), this action does not constitute a violation of the Rules and preserves the intermediary's safe harbour status. The conditionality of safe harbour creates a structural incentive for platforms to over-remove borderline content rather than risk losing Section 79 protection entirely, producing precisely the chilling effect on legitimate expression that *Shreya Singhal* warned against.[48]

V. COMPARATIVE ANALYSIS: THE EUROPEAN UNION AND THE UNITED STATES

A. The European Union: Article 50, EU AI Act and the Value-Chain Transparency

[44] *Id.*
[45] 2026 Rules, *supra* note 9, rule 7.
[46] *Id.*
[47] 2026 Rules, *supra* note 9, rule 1B.
[48] *Shreya Singhal, (2015) 5 SCC 1*.

Article 50 of the EU AI Act, which comes into force in August 2026, establishes transparency obligations for AI-generated synthetic content across the AI value chain addressing deepfakes specifically through a risk-tiered, expression-preserving framework that contrasts sharply with India's broad SGI regime.[49]

Under Article 50 of the EU AI Act "intermediaries" referred to as online platforms or entities within the AI value chain have been categorised depending on whether they act as "providers" or "deployers" of the AI systems. The Article 50 defines AI Providers as entities who develop AI systems or place AI systems on the market under their name, including developers of General-Purpose AI (GPAI). Providers must ensure that AI-generated audio, image, video or text outputs in a machine-readable format which is detectable as synthetic.[50]

Providers are expected to offer free-of-charge interfaces (APIs) or public tools that allow third parties to verify the content if it is AI-generated or not. AI-deployers are entities or professionals who use AI systems as part of their business activities excluding private individuals. The responsibilities of deployers are to clearly disclose the image, audio or video content that has been artificially generated or manipulated ("deepfakes"). An AI-generated text published on matters of public interest must be disclosed unless it has gone through human editorial review. Deployers are expected to use a common AI icon standard at the point of first interaction with the user.[51]

The Draft Code of Practice adopts a multilayered technical approach combining visible disclosures with machine-readable watermarking, rejecting any single-tool solution.[52]

The Draft Code of Practice also establishes key exemptions. There are no obligations for the law enforcement if their AI is authorised by law for detection, preventing or investigating criminal offences. Exemptions have been provided for artistic, satirical or creative works which are non-intrusive in nature and do not hamper the enjoyment of work.[53] Labelling is

[49] Council Regulation 2024/1689, art. 50, 2024 O.J. (L) 1689/1 (EU AI Act).
[50] *Id.* art. 50(1).
[51] *Id.* art. 50(2).
[52] EUROPEAN COMMISION, DRAFT CODE OF PRACTICE ON GENERAL-PURPOSE AI MODELS (2024).
[53] Council Regulation 2024/1689, art. 50(4), 2024 O.J. (L) 1689/1 (EU AI Act).

not required for the content if the AI is used as "assistive functions" for standard editing which does not alter the semantics of the input.[54]

The EU model is notable for three features which are absent from India's framework, a value-chain split of responsibility between providers and deployers, exemptions for artistic and satirical expressions, and independent regulatory oversight through EU AI Office. These features offer critical lessons for Indian regulatory design which are examined in sub-section C.

B. The United States: The TAKE IT DOWN Act and Harm-Specific Targeting

Prior to 2025, the United States lacked a proper uniform framework to address the issue of rising non-consensual intimate imagery, including AI-generated deepfakes. The existing laws did not explicitly address digitally fabricated content. In response, the United States Congress enacted the Take It Down Act, signed into law on 19 May 2025,[55] establishing a new comprehensive framework criminalising the publication of NCII including AI-generated digital forgeries.[56] Unlike India's generalised SGI framework the act targets only the most harmful category of synthetic media while leaving political satire, artistic expression, and general AI-generated content unregulated.

The Act categorises offences based on the specific harm caused and demographics of the victims. For adult victims, the government must prove that the publication actually caused harm in psychological, financial or reputational terms. For minors, if the content intends to "abuse, humiliate, harass or degrade," the offender should be penalised. The Act specifically targets "digital forgeries" of deepfakes as a unique category of harm, criminalising them even when no original authentic content exists. Publishing these AI-generated deepfakes is also a federal crime.[57]

[54] *Id.* art. 50(4)(b).
[55] TAKE IT DOWN Act, Pub. L. No. 119-10, 139 Stat.___(2025).
[56] *Id.* § 2.
[57] *Id.* § 3.

The platform must remove reported NCII within 48 hours of receiving a complaint request. It is also required to make "reasonable efforts" to identify and remove identical copies. Failure to comply with these removal requirements will be treated as deceptive or unfair under federal consumer protection law, allowing the FTC to impose sanctions.[58] Platforms are additionally granted immunity from liability for good faith removal of content that constitute NCII, even if later inclined to be lawful content, contrasting sharply with the protection of India's safe harbour under Rule 7.[59]

The Act deliberately exempts political satire, artistic expression and general AI-generated content, reflecting a conscious First Amendment restraint. However, critics including the EFF and CDT have argued the Act's vague language risks capturing lawful content, raising First Amendment concerns despite its narrow scope.[60] Sub-section C draws comparative lessons from both models for Indian regulatory design.

C. Comparative Matrix and Lessons of India

The three regulatory frameworks differ in four specific key areas: scope, expression, duties of the intermediaries, and their oversight methods.[61]

Parameter	India	EU	US
Feature	**IT Amendment Rules 2026**	**EU (AI Act & Draft Code)**	**United States (TAKE IT DOWN Act)**
Scope	**Synthetically Generated Information (SGI)**: Realistic audio, visual, or audio-visual	**Synthetically Content and Deepfakes**: Broadly covers AI-generated audio, image, video, and text.	**Digital Forgeries**: Deepfake intimate visual depictions of an identifiable individual

[58] *Id.* § 4.
[59] *Id.* § 4(b).
[60] ELECTRONIC FRONTIER FOUNDATION, COMMENTS ON THE TAKE IT DOWN ACT (2025).
[61] 2026 Rules, *supra* note 9; Council Regulation 2024/1689, art.50, 2024 O.J.(L) 1689/1 (EU AI Act); TAKE IT DOWN Act, Pub. L. No.119-10,139 Stat.___(2025).

	content likely to be perceived as indistinguishable from real persons or events.		created or altered using AI or software. Also covers authentic NCII.
Expression Protection	Excludes 'good-faith' removal, accessibility tools, and routine document creation. Protection for discussion and advocacy via *Shreya Singhal* precedent.	Explicit exemptions for evidentiary artistic, creative, satirical, or fictional works, requiring only minimal disclosure that doesn't "hamper enjoyment".	Exceptions for good-faith disclosures, lawful purposes (medical/scientific/education), and matters of "**public concern**".
Intermediary Obligations	SSMIs must verify user SHI declarations ex-ante. All intermediaries must label SGI and deploy measures to prevent "prohibited categories".	Providers must ensure machine-readable making (watermarking/metadata). Deployers must disclose AI use at the point of first interaction.	**Covered Platforms** must provide a clear complaint process and make "reasonable efforts" to remove identical copies of reported content.
Safe Harbour	Removal via **automated tools** in compliance with Rules does not violate the Section 79 legal immunity conditions.	Primarily addressed via alignment with the Digital Services Act (DSA) and existing data protection laws.	Platforms are not liable for good-faith removal of content that appears to be unlawful NCII, even if it turns out to be lawful.
Enforcement	**Executive-led**: Level III	AI Office, a Scientific Panel	**Federal Trade Commission**

	oversight by the Central Government via an Inter-Departmental Committee. Orders issued by "**Authorised Officers**".	of Independent Experts, and National Competent Authorities.	**(FTC)** enforces notice and removal as a consumer protection violation. DOJ handles criminal prosecutions.
Takedown Timeline	**Aggressive**: **2 hours** for nudity/ impersonation; **3 hours** for government orders; **36 hours** for deceptive content; **7 days** for general grievances.	Focused on transparency at first exposure. Illegal content (NCII, etc) must be removed "**promptly**" under the DSA framework.	48 hours from receipt of a valid request.

From the EU model, India should learn three lessons. First, there should be a value chain split between AI-developers and platforms instead of burdening all intermediaries equally. Second, to explicitly exempt and protect satire, parody, journalism and artistic expression in the SGI definition. Third, to establish a separate regulatory authority from the Ministry of Electronics and Information Technology ("MeitY") to have an independent oversight in SGI frameworks.

From the US model, India should learn to regulate only the most demonstrably harmful synthetic content rather than all SGI broadly. Second, replace proactive monitoring with a victim-complaint mechanism modelled on the 48-hour TAKE IT DOWN Act process.[62] Third, to establish an independent enforcement equivalent to the FTC separate from MeitY.

[62] TAKE IT DOWN Act, Pub. L. No. 119-10, § 4 (2025).

India's 2026 Rules are simultaneously too broad in scope and too concentrated in enforcement. Both the EU and US model demonstrate effective deepfake regulation without sacrificing free speech and expression. This is a balance India's 2026 Rules have conspicuously failed to achieve.[63]

VI. CONSTITUTIONAL INTERROGATION: FREE SPEECH, DUE PROCESS, AND THE VAGUENESS DOCTRINE

A. Article 19(1)(a) and the Proportionality Test

Article 19(1)(a) of the Indian Constitution guarantees every citizen the fundamental right to speech and expression,[64] a right that the Supreme Court has consistently held to be the cornerstone of the democratic governance.

Any restriction on the freedom of speech and expression must satisfy the four-part proportionality test[65]: legitimate aim, rational connection, least restrictive means, and proportionality impact. While the 2026 Rules pursue a legitimate aim through a rational connection, they fail the 'least restrictive means' and 'proportionality' prongs of the test. While the 2026 Rules pursue a legitimate aim through a rational connection, they fail the 'least restrictive means' and 'proportionality' prongs of the test.

In the IT Amendment Rule 2026, the Rules mandate the labelling of AI- generated content to prevent citizens from deepfake harm which is indeed a necessary step. However, by failing to categorise specific harms, the government mandates a broad labelling requirement for all SGI content that is generated from an AI must be labelled and user verified before publication on intermediaries platforms.[66] On the other hand the EU AI Act has a carved-out model and the US has a harm specific model take it down Act and have clearly defined definition of what a deepfake SGI content is and what actions to be taken against them preventing them from deepfake harm. India nevertheless chose the broadest possible regulatory approach.[67]

[63] 2026 Rules, *supra* note 9, rule 2(1)(wa).
[64] India Const. art. 19, cl. (1)(a).
[65] *Modern Dental College v. State of Madhya Pradesh*, (2016) 7 SCC 353.
[66] 2026 Rules, *supra* note 9, rule 4(1A).
[67] 2026 Rules, *supra* note 9, rule 2(1)(wa).

MeitY centralises regulatory authority, acting as the sole arbiter of content legality while in EU and US they have set up a different regulatory authority to handle deepfake harm, as examined in Part V.

B. Overbreadth, vagueness, and the Suppression of Legitimate Expression

The Information Technology Amendment Rules 2026, has introduced the most proactive and stringent framework across three jurisdictions, marked by overbreadth and vagueness that risk suppressing legitimate expression.

The Indian framework is notably more extensive than the US or EU models due to its ex-ante requirements.[68] The Rule mandates that SSMIs must verify the correctness of user declarations regarding their SGI generated content. Mandating intermediaries for technical verification prior to publication is a broad obligation burdening the platforms to act as active sentinels. Deploying measures to prevent a wide range of content including SGI that results in false electronic records, where there has been no definition on false electronic records in the amendment rules. The rules also prohibit platforms from modification or removing SGI labels of metadata, where this could prevent developers from offering legitimate Al editing tools which may result in stripping metadata during file conversion.[69]

The 2026 Rules attempt to mitigate over-regulation through specific exclusions. Content is only considered as SGI if it is likely to be perceived as indistinguishable from a natural or real-world event. There is a lack of clear standard for "indistinguishability" which may lead to inconsistency by different platforms. Under the *Shreya Singhal's* "void for vagueness" doctrine, a restriction on speech must be defined with sufficient clarity that an ordinary person knows exactly what conduct is prohibited: a standard the SGI definition conspicuously fails to meet.[70] Editing or colour correction may fall within the scope of good-faith activity, but only to the extent that such processes do not misrepresent, alter, or distort the original content. In the absence of clear and granular standards, intermediaries

[68] 2026 Rules, *supra* note 9, rule 4(1A).
[69] 2026 Rules, *supra* note 9, rule 3(3).
[70] *Shreya Singhal,* (2015) 5 SCC 1.

may struggle to distinguish permissible enhancement from material misrepresentation, thereby creating a risk of over-blocking legitimate creative expression.

The enforcement architecture for SGI-related content privileges speed over deliberation, with potentially serious consequences for free expression. Complaints involving nudity or impersonation must be addressed within two hours, while content flagged through court orders or government directions must be taken down within three hours.[71] Since failure to comply may entail the loss of safe harbour protection[72], intermediaries are structurally incentivised to remove content immediately, often without sufficient scrutiny of whether the material constitutes satire, parody, or speech in the public interest. The requirement that SSMIs verify SGI declarations prior to publication may further create a verification bottleneck, suppressing speech until its relevance or immediacy has diminished. Moreover, the obligation to issue quarterly notices to users regarding prohibited content and criminal penalties[73] may reinforce a chilling effect, deterring the creation and dissemination of legitimate AI-generated creative and political expression.

C. Concentration of Executive Power and the Absence of Independent Oversight

The IT Amendment Rules 2026 concentrate regulatory authority exclusively within the executive branch and the absence of independent oversight. The Central Government maintains the authority over the digital media and Al ecosystem through a three-tier structure.[74] The directions to delete or block content are issued by an authorised officer and require a final approval of the Secretary, Ministry of Information and Broadcasting (MIB).[75] The grievances are heard by the Inter Departmental Committee (IDC), chaired by government authorised officers, composed of representatives from Home Affairs, Law Justice, MeitY. A Grievance Appellate Committee (GAC) exists to hear appeals, whose members are also appointed by the Central Government.[76]

[71] 2026 Rules, *supra* note 9, rules 3(1)(d), 3(2)(b).
[72] 2026 Rules, *supra* note 9, rule 7.
[73] 2026 Rules, *supra* note 9, rule 7.
[74] 2026 Rules, *supra* note 9, rules 1B, 7.
[75] *Id.*
[76] *Id.*

In *Shreya Singhal*[77], the Supreme Court upheld Section 69A on the ground that it was accompanied by procedural safeguards, including written reasons, a right to hearing, and oversight by a Review Committee. The 2026 Rules, by contrast, impose substantial obligations without providing any equivalent procedural protections. At the same time, MeitY operates simultaneously as rule-maker, enforcer, and adjudicator, concentrating these functions within a single executive authority without judicial oversight. Such an arrangement raises serious concerns under the principles of natural justice and separation of powers.[78]

The Secretary, MIB has the power to issue interim blocking directions in emergency cases without giving an opportunity of explanation to the publisher or the intermediary. A review committee also exists which is an executive body to meet at least once every two months to record the findings.

In contrast, the EU AI Act distributes regulatory authority through an independent institutional framework with enforcement delegated to the EU AI office and National Competent Authorities,[79] designated by individual member states, ensuring oversight remains separate from the ministry that made the rules. For the US TAKE IT DOWN Act, the primary body to enforce the act is the Federal Trade Commission (FTC), responsible for the notice and removal requirements, treating non-compliance as "deceptive or unfair". Criminal prosecutions are handled by the Department of Justice (DOJ).[80]

Taken together, these features show that the constitutional problem with the 2026 Rules lies not only in the breadth of their obligations, but also in the executive structure through which they are enforced. This concentration of power, without adequate procedural safeguards, creates a risk of suppressing lawful speech and leads to the next question: whether the Rules operate as a form of de facto censorship.

[77] *Shreya Singhal v. Union of India,* (2015) 5 SCC 1, 112.
[78] India Const. art. 50.
[79] Council Regulation 2024/1689, art. 50, 2024 O.J. (L) 1689/1 (EU AI Act),
[80] TAKE IT DOWN Act, Pub. L. No. 119-10, § 3 (2025).

D. The De-Facto Censorship Argument

The Rules do not explicitly censor, but they structurally produce censorship anyway. The introduction of “technical verification" mandate requiring Significant Social Media Intermediaries (SSMIs) to verify the accuracy of user declarations regarding SGIs and removing contents via automated tools bypasses the *Shreya Singhal* judgment under Section 79(3)(b) IT Act and Article 19(2) of the Constitution.[81]

The SGI definition in IT Amendment Rule 2026 is completely vague as it fails to identify how an SGI would be perceived as indistinguishable. In the *Shreya Singhal* case, the Court struck down Section 66A of the IT Act 2000 for the terms which were constitutionally vague.[82]

The pre-publication technical verification mandate may suppress the creative works for political satire or creative works, and leaves no ground for discussion or advocacy to hear the views of the user or intermediaries. No appellate mechanism, no judicial review, no timelines for restoration of wrongly removed content has been described.[83]

The IT Amendment rules requirement for updating users every 3 months for Criminal penalties, including imprisonment could be viewed as a chilling effect on the freedom of speech and expression.[84]

The cumulative effect of these structural pressures completes the transformation this paper identifies, digital intermediaries have been converted from passive harbours into active sentinels, at a constitutional cost that neither the legislature nor MeitY has adequately acknowledged.[85]

[81] *Shreya Singhal v. Union of India,* (2015) 5 SCC 1; Information Technology Act, 2000 § 79(3)(b) (India).
[82] *Shreya Singhal,* (2015) 5 SCC 1, 93.
[83] 2026 Rules, s*upra* note 9, rule 7.
[84] 2026 Rules, *supra* note 9, rule 7.
[85] *Id.*

VII. TOWARDS A BALANCED REGULATORY FRAMEWORK: RECOMMENDATIONS

A. Redefining SGI: narrowing the Scope to Harmful Synthetic Media

The current SGI definition of India is too broad and vague,[86] and it fails to distinguish between malicious deepfake content and creative content for entertainment. The SGI definition must be narrowed to cover only synthetic depictions capable of causing cognisable psychological, electoral, or reputational harm. India should adopt a harm-specific mechanism similar to the dual classification of US Take it down act distinguishing between authentic content and AI-generated digital forgeries.[87] Moreover, as the EU AI Act has protected such content as satire and art,[88] India should do the same. It should exempt creative works like satire, parody, journalism and creative expression from the SGI definition. This narrower definition would fix the problem we identified in Part VI and pass the Article 19(1)(a) proportionality test.[89] This would also satisfy the *Shreya Singhal's* case for void for vagueness and provide sufficient clarity among the intermediaries and the users on what the content falls under the SGI definition.[90]

B. Graduated Intermediary Obligations Based on Risk and Scale

India's current labelling mandates burden all large platforms regardless of their functions of a platform that provides AI tools, and faces the same obligations to the platforms that publish the content.[91] A risk-based, tiered obligation framework should replace the current uniform mandates, scaling requirements according to a platform's reach and technical function. A risk-based, tiered obligation framework should replace the current uniform mandates, scaling requirements according to a platform's reach and technical function. Small platforms should be required to perform basic labelling, medium platforms moderate verification, and large

[86] 2026 Rules, *supra* note 9, rule 2(1)(wa).
[87] TAKE IT DOWN Act, Pub. L. No. 119-10, § 2 (2025).
[88] Council Regulation 2024/1689, art. 50(4) (EU AI Act).
[89] India Const. art. 19, cl. 1(a).
[90] *Shreya Singhal,* (2015) 5 SCC 1.
[91] 2026 Rules, *supra* note 9, rule 4(1A).

SSMIs full verification and proactive monitoring. India can learn from the EU's AI Act where there has been a separate obligation for the platforms who are providers and deployers,[92] and also those who build AI tools from those distributing content.

A tiered approach is more proportionate under Article 19(1)(a),[93] where obligations match capacity and risks rather than imposing uniform burdens that disproportionately harm smaller platforms and stifle innovation. Restoring meaningful safe harbour protections alongside this tiered framework is examined in sub-section C.

C. Restoring the Safe Harbour and Preserving *Shreya Singhal*

Rule 7 of the IT Amendment Rule 2026,[94] makes safe harbour conditional on proactive compliance. If platforms fail to verify SGI declarations, they may lose safe harbour protection under Section 79 of the IT Act 2000.[95] However, the Supreme Court in *Shreya Singhal* held that,[96] intermediaries cannot be required to proactively monitor content as it may restrict freedom of speech and expression.

To restore the Safe Harbour, platforms should only lose Safe Harbour after receiving the actual court order or government notification identifying specific unlawful content and not for failing to proactively detect it.

The Government should introduce a statutory notice and takedown process modelled on the US TAKE IT DOWN Act,[97] where victims report the harmful SGI directly to the platforms, which will trigger a mandatory removal obligation within a defined time frame without active monitoring.

[92] Council Regulation 2024/1689, art. 50(1)-(2), (EU AI Act).
[93] India Const. art. 19, cl. 1(a).
[94] 2026 Rules, *supra* note 9, rule 7.
[95] Information Technology Act, 2000, § 79.
[96] *Shreya Singhal,* (2015) 5 SCC 1.
[97] TAKE IT DOWN Act, Pub. L. No. 119-10, § 4 (2025).

This restoration would bring the framework back into alignment with *Shreya Singhal's* actual knowledge standard and preserve the safe harbour architecture essential to open digital communication.[98]

D. Establishing Independent Oversight and Judicial Review

The 2026 Rules currently centralise all rulemaking and enforcement within MeitY,[99] creating a significant oversight gap that lacks independent judicial review. To address this gap, India should establish an autonomous AI and Digital Media Regulator separate from the ministry, complemented by a multi-stakeholder advisory council of experts to provide a necessary check on executive power. Furthermore, all takedown orders must be subject to mandatory judicial review within a set timeframe to prevent permanent content removal without external scrutiny. By incorporating written reasons and the right to a hearing, this approach restores the vital procedural safeguards mandated by the *Shreya Singhal* ruling,[100] ensuring the rules are both fair and constitutionally sound.

E. Targeted Criminal and Civil Remedies for Victims

The current legal framework, spanning Sections 66C and 66D of the IT Act,[101] and Sections 319 and 353 of the BNS,[102] is fundamentally not suited for the harms caused by deepfakes, as these bailable offences offer no specific remedies for victims. To address this, India should introduce a dedicated non-bailable offence for malicious deepfakes with graduated penalties that distinguish between NCII (Non-Consensual Intimate Imagery), electoral interference, and identity fraud. This should be paired with a civil right of action—inspired by the proposed US DEFIANCE Act.[103] The civil right of action would allow victims to sue for statutory damages without proving exact financial loss. Finally, establishing statutory forensic standards is essential to help courts reliably navigate the "detection gap" where

[98] *Shreya Singhal,* (2015) 5 SCC 1, 93.
[99] *Supra* note 9, rules 1B, 7.
[100] *Shreya Singhal,* (2015) 5 SCC 1, 112.
[101] Information Technology Act, 2000, §§ 66C, 66D.
[102] Bharatiya Nyaya Sanhita, 2023, §§ 319, 353.
[103] *Disrupt Explicit Forged Images and Non-Consensual Edits Act of 2024*, H.R. 7569, 118th Cong. (2024) (not enacted).

automated detection accuracy remains insufficient. By focusing on the actual perpetrators rather than just the platforms, these targeted remedies protect legitimate expression while finally providing meaningful accountability for genuine harm.

VIII. CONCLUSION

The Rashmika Mandanna incident exposed a fundamental governance failure as it did not have a statutory framework to address the synthetic media harm. The IT Amendment Rules 2026 were India's first legislative response to the crisis.[104]

The Rules introduce important innovation. First, the introduction of the SGI definition, labelling mandate, and verification obligations, but the constitutional infirmities are significant. The broad SGI definition labelling every content as harmful irrespective of analysing the content whether it is satirical or creative in nature, fails *Shreya Singhal's* void for vagueness standard.[105] Burdening the intermediaries with labelling mandates and verification obligations is turning them from Safe harbour to Active Sentinels. Furthermore, the concentration of executive power with MeitY replicates none of Section 69A's procedural safeguards,[106] as the court upheld in the *Shreya Singhal* case.

Both the EU AI Act,[107] and the US TAKE IT DOWN Act,[108] demonstrates that effective deepfake regulation is achievable without sacrificing the constitutional rights of freedom of speech and expression. India’s failure to adopt a value-chain responsibility model or a harm-specific approach leaves its SGI framework constitutionally vulnerable and comparatively isolated.

The question India must now answer is not whether deepfake should be regulated, they must be, but rather what should be regulated and what to exempt. The more pressing question is whether regulation can be achieved without converting every intermediary into an instrument

[104] *Supra* note 9, rule 2(1)(wa).
[105] *Shreya Singhal*, (2015) 5 SCC 1.
[106] *Shreya Singhal*, (2015) 5 SCC 1, 112.
[107] Council Regulation 2024/1689, art. 50 (EU AI Act).
[108] TAKE IT DOWN Act, Pub. L. No. 119-10 (2025).

of state surveillance. The answer, as this paper has argued, lies not in abandoning the 2026 Rules entirely but in rebuilding them on the constitutional foundations that *Shreya Singhal* laid in 2015.[109]

[109] *Shreya Singhal,* (2015) 5 SCC 1.

GAZA ON TRIAL: INTERNATIONAL HUMANITARIAN LAW AND COMPARATIVE INSIGHTS FROM ENGLISH AND EU LAW

By Gokul B.

VOLUME I | ISSUE I | ARTICLE V

APRIL 2026

The Legalis IP Quarterly

ABSTRACT

The recent hostage crisis in Gaza, where civilians have been caught in an escalation of military activities, has seen urgent negotiations by international powers spearheaded by Egypt and the United States. These attempts, although aimed at the release of hostages, prominently pose serious questions concerning adherence to International Humanitarian Law (IHL) and the safeguarding of civilians under the Geneva Conventions. The act of hostage-taking is a war crime, and the breach of both state and non-state actors underscores the continuing difficulties in applying legal requirements in asymmetric warfare. This article will take a closer look at the international law approach to the crisis, the culpability of the involved parties, and the culpability of the mediators, as well as the implications of the crisis on civilian protection in general. English and EU law comparative insights highlight how national and supranational structures can support international standards, providing tools of prosecution, sanctions, and policy restructuring. This paper aims to sheds light on the relationship between the humanitarian pillars, the legal responsibility and the interplay between diplomatic bargaining by examining the Gaza hostage crisis. It highlights the necessity of enhanced control measures and considerate policy-based interventions to reduce damage, safeguard civilians, and improve the efficiency of international law norms in future conflicts.

Keywords: Gaza hostage crisis, International Humanitarian Law, Geneva Conventions, hostage-taking, war crimes, asymmetric warfare, civilian protection, state responsibility, non-state actors, command responsibility, English law, European Union law, comparative law, mediation liability, counter-terrorism, armed conflict.

I. INTRODUCTION

The prolonged hostage issue in Gaza, characterised by the capturing of civilians in the midst of heightened military action, has received a lot of international concern.[1] Recent talks between Israel, Hamas, and third-party negotiators like Egypt and the United States have concentrated on ensuring the release of hostages and trying to curb civilian deaths. Nevertheless, this has not stopped the crisis, but has signified the multicultural and humanitarian issues of modern armed conflicts, especially in large, high-population cities. The International Humanitarian Law obligates parties in conflict to ensure the safety of civilians and avoid hostage-taking, which is a serious violation in the Fourth Geneva Convention and customary international law.[2]

The laws of war enforce rigid restrictions on the nature of hostilities and provide mechanisms of accountability on violation, which may include prosecution of war crimes.[3] In addition to the humanitarian issues at hand, these norms are used to maintain the overall principles of human dignity and legality during periods of conflict.[4] This article aims to analyse the Gaza hostage crisis in relation to international law with an emphasis on the legal responsibilities of both the state and non-state actors. In order to contextualise the current issues and investigate the possible lessons of the modern conflict resolution, comparative references will be made to English and EU legal frameworks, specifically, the treatment of hostages, civilian protections, and the responsibility of the parties involved in the violation case.[5]

II. INTERNATIONAL HUMANITARIAN LAW OBLIGATIONS

Protecting civilians in times of armed conflict is a fundamental element of International Humanitarian Law, which is codified mainly in the Geneva Conventions of 1949 and in its Additional Protocols.[6] The Fourth Geneva Convention, specifically, calls on the parties that are involved in a conflict to protect civilians against violence, hostage-taking, and coercion.[7] The hostage taking as witnessed in Gaza is a serious violation in violation of Articles 147 of

[1] *Israel PM Benjamin Netanyahu Hopes to Announce Release of All Hostages from Gaza 'in Coming Days'*, The Hindu (Oct. 5, 2025), https://www.thehindu.com/news/international/israel-pm-benjamin-netanyahu-hopes-to-announce-release-of-all-hostages-from-gaza-in-coming-days/article70127282.ece (last visited Oct. 5, 2025).
[2] Geneva Convention (IV) Relative to the Protection of Civilian Persons in Time of War art. 34, Aug. 12, 1949, 75 U.N.T.S. 287.
[3] Rome Statute of the International Criminal Court (adopted 17 July 1998, entered into force 1 July 2002) 2187 UNTS 90, art 8(2)(c)(iii).
[4] Antonio Cassese, *International Law* 420 (2d ed. 2005).
[5] Geoffrey Corn et al., *The Law of Armed Conflict: An Operational Approach* 352 (3d ed. 2024).
[6] Protocol Additional (I) to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 3.
[7] Geneva Convention (IV) Relative to the Protection of Civilian Persons in Time of War arts. 27, 34, Aug. 12, 1949, 75 U.N.T.S. 287.

the Fourth Geneva Convention and considered a war crime in customary international law.[8] In addition to treaty obligations, customary IHL enshrines the core values including distinction, proportionality, and necessity which have the effect of limiting the nature of hostilities in order to safeguard non-combatants. The International Committee of the Red Cross highlights the fact that armed forces, along with non-state actors like armed groups, are obliged by these norms in order to hold them accountable regardless of their recognition as a state.[9]

In comparison, English law authorises the prosecution of a violation of IHL by incorporating war crimes into domestic criminal law, such as the Geneva Conventions Act 1957.[10] Although it is mainly used in cases involving British citizens or offences that occur within the jurisdiction of the UK, these provisions illustrate how international norms are enforced domestically. Also, the EU law covers human-rights considerations in war situations, specifically in the Charter of Fundamental Rights of the European Union, which declares the right to life (Article 2) and the ban on torture and inhuman treatment (Article 4).[11] These frameworks are complementary to IHL requirements, with an emphasis on civilian protection and accountability at the domestic and supranational levels.

This article also highlights the difficulty of applying IHL to asymmetric warfare, where the line between combatants and civilians continues to grow more blurred. The disparity between legal norms and their application is evident in reports by the United Nations and Human Rights Watch of frequent violation of the principle in Gaza, such as indiscriminate attacks and hostage-taking.[12] Comparative approach reflects that, although international law establishes global norms, their enforcement in practice depends on national internalisation and powerful surveillance systems.

III. HOSTAGE-TAKING AND ACCOUNTABILITY

International Humanitarian Law categorically prohibits hostage-taking, and is a war crime under both treaty and customary law.[13] Article 147 of the Fourth Geneva Convention explicitly refers to the act of hostages taking as a severe violation, requiring the protection of criminals by the states through prosecution or extradition.[14] Hostage-taking is enshrined further in the Rome Statute of the International Criminal Court as a war crime in an international or non-international armed conflict, and the principle of individual criminal

[8] Jean-Marie Henckaerts & Louise Doswald-Beck, *Customary International Humanitarian Law* (Vol. I: Rules) Rule 96 (2005).
[9] Int'l Comm. of the Red Cross, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts* 13 (2023).
[10] Geneva Conventions Act 1957, 5 & 6 Eliz. 2, c. 52, § 1 (U.K.).
[11] Charter of Fundamental Rights of the European Union arts. 2, 4, 2012 O.J. (C 326) 391.
[12] U.N. Hum. Rts. Council [UNHRC], Report of the Independent International Commission of Inquiry on the Occupied Palestinian Territory, Including East Jerusalem, and Israel ¶¶ 42–46, U.N. Doc. A/HRC/56/26 (2024).
[13] Int'l Comm. of the Red Cross, Customary IHL Database, Rule 96: Taking of Hostages, https://ihl-databases.icrc.org.
[14] Geneva Convention (IV) Relative to the Protection of Civilian Persons in Time of War art. 147, Aug. 12, 1949, 75 U.N.T.S. 287.

responsibility of both leaders and combatants.[15] The kidnapping of civilians in the course of active hostilities in Gaza constitutes a direct contravention of these norms, which outlines legal and ethical demands of responsibility.

It lies in the hands of state and non-state. The state of Israel, being a recognised state party to the Geneva Conventions, has an obligation to safeguard civilians during occupation, and ensure that military action is taken in accordance with IHL.[16] On the other hand, the non-state armed group Hamas is, however, bound to respect customary IHL and not commit acts that amount to war crimes, such as hostage-taking.[17] The principle of command responsibility assumes that both parties may charge their leaders with the responsibility to order, condone or close their eyes to illegal activities of subordinates. The international community has intensified the prosecution of those who commit such violations through mechanisms like the ICC regardless of the state affiliation.

English law criminalises hostage-taking by the Taking of Hostages Act 1982 instituting the International Convention of the Taking of Hostages of 1979.[18] British nationals or crimes committed on UK territory can be tried in English courts to enhance domestic responsibility. Other laws also targeted at countering terrorism, including the Terrorism Act 2000, make threats, kidnappings, and any action meant to intimidate a government or people a criminal offense.[19] The EU law also covers hostage-taking in counter-terrorism directives, stipulating that member states must impose penalties against offenders and provide protection to victims.[20] This comparative framework indicates how international standards can converge with domestic legal frameworks to combat crimes involving hostages, which highlights the potential of enforcement mechanisms operating at several levels in an attempt to increase compliance and accountability.

IV. ROLE OF MEDIATORS AND STATE RESPONSIBILITY

An important role in conflict resolution is undertaken by third-party states and mediators, but their intervention is limited by the commitments of international law. Other states like the United States and Egypt, which have mediated between Israel and Hamas regarding hostages in Gaza, should respond to neutrality, non-intervention, and the illegality of aiding the breach of the international humanitarian law. Mediators can use political and logistical leverage, but not legitimise or promote actions that are against international law, such as holding hostages or carrying out indiscriminate attacks against civilians. International law acknowledges that

[15] Rome Statute of the International Criminal Court arts. 8(2)(a)(viii), 8(2)(c)(iii), July 17, 1998, 2187 U.N.T.S. 90.
[16] Int'l Comm. of the Red Cross, State Parties to the Geneva Conventions of 1949 and Their Additional Protocols, https://www.icrc.org.
[17] Int'l Comm. of the Red Cross, Customary IHL Database, Rule 149: Responsibility of Commanders and Other Superiors, https://ihl-databases.icrc.org.
[18] Taking of Hostages Act 1982 (U.K.); International Convention Against the Taking of Hostages, G.A. Res. 34/146, U.N. Doc. A/RES/34/146 (Dec. 17, 1979).
[19] Terrorism Act 2000, §§ 1–3 (U.K.).
[20] Council Directive 2017/541, of the European Parliament and of the Council of 15 March 2017 on Combating Terrorism, arts. 5–7, 2017 O.J. (L 88) 6.

there can be secondary responsibility on the part of states where they offer substantial support or assistance or direction to parties that engage in unlawful acts. It is clear that aiding or assisting the commission of an internationally wrongful act can attract the liability of a state as explicated in the Articles on the Responsibility of States to Internationally Wrongful Acts (2001) of the International Law Commission, even in instances where the act is perpetrated by non-state actors.[21] When it comes to Gaza, mediating states have to walk a very fine line within these legal realms so that as they facilitate negotiations, they do not accidentally break their obligations or undermine accountability.[22]

By comparison, English law limits liability of domestic actors involved in foreign diplomatic mediation, in most cases under statutes dealing with terrorism, hostage-taking, or complying with sanctions. Likewise, EU law requires member states to respect international commitments in pursuing diplomatic or mediation efforts such as the observance of the resolutions of the United Nations Security Council and the observance of human rights standards and norms.[23] These principles strengthen the notion that states serving a mediating role must do what is necessary to resolve conflicts, but do not violate legal standards, and that their actions should not involve a legal or moral responsibility of perpetrating the violations committed by parties to the conflict.

V. IMPLICATIONS AND FUTURE CHALLENGES

The Gaza hostage crisis highlights the ongoing enforcement issues associated with International Humanitarian Law (IHL). Although there are strong prohibitions against hostage-taking and protecting civilians, the application of these in asymmetric wars that feature non-state actors in addition to states remains elusive. These restrictions have made the prosecution of violations difficult due to limited access to conflict zones, political limitations, and the inability to ascribe responsibility, which leads to a notable discrepancy between legal standards and the application of the law. These challenges in enforcement give rise to lessons in English and EU law. The English legislation, including the Geneva Conventions Act 1957 and other counter-terrorist laws, shows that it is crucial to incorporate international norms domestically to make prosecution and responsibility possible.[24] In a similar manner, EU structures facilitate compliance with the human rights requirements and the application of penalties, which offer a well-organised approach to reinforce international law.[25] These reveals domestic and supranational mechanisms, how local enforcement can be used to reinforce larger international initiatives, as well as making sure that legal obligations are not just aspirational.

[21] Int'l Law Comm'n, *Responsibility of States for Internationally Wrongful Acts*, art. 16, U.N. Doc. A/56/10 (2001).
[22] U.N. Charter art. 2(7); Int'l Comm. of the Red Cross, *Commentary on the First Geneva Convention* (updated 2016).
[23] Consolidated Version of the Treaty on European Union art. 21, Mar. 13, 2012, 2012 O.J. (C 326) 13.
[24] Geneva Conventions Act 1957 (U.K.); Terrorism Act 2000 (U.K.).
[25] Charter of Fundamental Rights of the European Union arts. 2,4, 2000 O.J. (C 364) 1; Council Directive 2017/541, supra note 20.

Looking forward, the crisis in Gaza implies that there is a necessity to reinforce legal systems, develop new surveillance systems, and take proactive initiatives in formulating policies. Reforms may involve broadening jurisdictional authority to war crimes, increased responsibility of non-state actors and use of related lessons in other legal systems to strengthen civilian protection. Also, there should be long-term international cooperation and mediation practice which strongly focuses on IHL adherence to reduce the upcoming crisis. Through examining these implications, policymakers and legal academics can devise measures that, in addition to strengthening the normative capacity of international law, can enhance its positive impact on the effectiveness thereof in protecting vulnerable populations.

VI. CONCLUSION

The Gaza hostage crisis demonstrates the lasting importance of International Humanitarian Law (IHL) to govern armed conflict and protect people. The existence of hostage-taking, non-selective attacks, and intrusions by both state and non-state actors explains the importance of strong enforcement mechanisms and accountability structures. The English and EU law comparatives emphasise the importance of domestic and supranational integration of international norms and how local legal systems can be used to supplement world norms to ensure adherence and punish its breach. Moving ahead, the crisis highlights the need to enhance monitoring, increase legal redress to victims, and improve mediation guidelines to match IHL principles. Through these lessons, policymakers and law scholars can be better equipped to tackle humanitarian issues and increase the normative and practical efficacy of international law in modern conflicts.

Beyond Territorial Sovereignty:

Reconstructing Legal Integrity in the Metaverse

By Tejpratap Singh

VOLUME I | ISSUE I | ARTICLE VI

APRIL 2026

The Legalis IP Quarterly

ABSTRACT

The arrival of the virtual reality-based metaverse has raised complex legal issues across countries worldwide. These legal systems are ever-evolving; however, in the context of the metaverse, which is itself transitional and immaterial, keeping up with legal developments has become a complex challenge.

The current global technological laws have territorial jurisdiction. Only a few jurisdictions, such as the European Union, the United States, China, Singapore, and the United Arab Emirates, have developed relatively advanced legal frameworks for digital assets. Most other countries have not made comparable progress in regulating the metaverse, largely because of its borderless nature, which transcends territorial laws and conventional jurisdictional boundaries. It thus becomes incredibly complicated to impose municipal laws on the use of the metaverse. These raise genuine questions, such as who should be held accountable for arising liabilities, who will have jurisdiction to preside over any violations of intellectual property (IP) in the metaverse, and which laws would specifically apply.

The scope of this research will be on the jurisdictional friction between sovereign states and Decentralised Autonomous Organisations (DAOs). It will also investigate the civil liabilities that have arisen from disputes over virtual property and the regulatory gaps that exist in the protection of the user's "Biometric Sovereignty" within the existing framework of international data privacy laws.

The central argument is that the current "Westphalian" architecture of territorial sovereignty is incapable of transitioning to the decentralised model of the metaverse. This research is to find out and prevent global 'regulatory race to the bottom', So that the international community can adopt a system

of metaverse-specific laws or "Lex Metaversi", a self-implied, code based on legal framework which uses smart laws (laws embedded through coding in the system so that it can be self-imposed) to enforce IPR and commercial agreements automatically, therefore replacing reactive litigation with proactive, algorithmic integrity.

Keywords: *Metaverse; jurisdiction; territorial sovereignty; Westphalian sovereignty; decentralised autonomous organisations (DAOs); virtual property; civil liability; intellectual property rights; digital assets; biometric sovereignty; data privacy; international data protection law; cross-border regulation; regulatory gaps; lex metaversi; smart contracts; code-based governance; algorithmic enforcement.*

I. INTRODUCTION

The rapid transition of the global digital order from the two-dimensional, screen-mediated interfaces of Web 2.0 to the three-dimensional, immersive environments commonly described as the metaverse marks a fundamental shift in social, economic, and legal interactions.[1] As this technological transformation accelerates, the idea of legal integrity, understood as the coherence, ethical alignment, and effectiveness of regulatory frameworks across both physical and virtual domains, becomes central to contemporary legal thought.[2] The metaverse is not merely a collection of gaming platforms; rather, it is a collaborative virtual space shaped by the convergence of enhanced physical reality and persistent digital environments, thereby challenging traditional legal concepts such as territorial sovereignty, personal identity, and property rights.[3] The current legal landscape remains marked by significant regulatory gaps and fragmented ethical standards, as existing digital and technological laws often provide vague or inadequate definitions of foundational concepts. Such shortcomings risk generating legal uncertainty, ethical dilemmas, and a broader erosion of public trust in digital institutions. For the metaverse to

[1] Oleksandr Baranov et al., Digital Transformations of Society: Problems of Law, (2026) https://www.researchgate.net/publication/379237287 [https://doi.org/10.31435/rsglobal/057].
[2] Oleh Semenenko et al., Forecasts of Transformation in Legal Regulation of Artificial Intelligence for Cybersecurity in Ukraine's Defence Sector, (2025) https://www.researchgate.net/publication/398050452 [https://doi.org/10.18226/25253824.v9.n14.02].
[3] Mariia Viktorivna Dubniak, Digital Transformation from Informatization to Artificial Intelligence in Administrative Services in Ukraine, (2024) https://www.researchgate.net/publication/387940489 [https://doi.org/10.69635/978-1-0690482-1-9-ch15].

achieve legal integrity at the global level, a doctrinal transformation is required, one that moves beyond isolated domestic approaches towards a transborder standard model capable of harmonising legal and technical norms across decentralised ecosystems.

In this context, the present study adopts a doctrinal and comparative methodology to analyse the emerging legal challenges posed by the metaverse. It critically examines existing legal regimes, particularly the Information Technology Act, 2000 and the European Union's General Data Protection Regulation, to identify jurisdictional gaps in decentralised digital spaces.[4] It also employs a comparative approach to evaluate how the United States, the European Union, and India regulate virtual property and biometric information within their respective legal systems. By integrating primary legal materials, such as statutes, regulations, and relevant legal principles, with secondary academic and analytical sources, this paper develops an analytical framework for governance in the metaverse. Against this backdrop, the study explores the multifaceted legal issues surrounding metaverse regulation, with particular emphasis on intellectual property, jurisdictional conflict of laws, and the pressing need for a coherent global governance framework.

II. EVOLUTION OF DIGITAL PERSONA AND IDENTITY

Human identity has increasingly extended into the online sphere through the notion of the "digital persona", which functions as a necessary representation of the self in a networked society. Alongside it, a related layer of identity has emerged, sometimes described as the "digital unconscious".[5] At present, however, technological systems largely determine how digital identity is constructed, often relying on data mining and profiling to reduce fluid, complex human individuality into rigid, generalised categories. In the absence of coherent legal and ethical frameworks, society, institutions, and experts remain at a fragile, insufficiently developed stage in understanding the implications of these digital selves.[6]

[4] H. Krasnostup, New Media Formation and Prospects of Legal Regulation, (2012) https://www.researchgate.net/publication/367507277 [https://doi.org/10.37750/2616-6798.2012.2(5).271844].
[5] O. Baranov, Civilization Mission of Digital Transformations, (2023) https://www.researchgate.net/publication/373970035 [https:doi.org/10.37750/2616-6798.2023.3(46).287067].
[6] Oleksii Kostenko, Artificial Intelligence (AI) and the Metaverse: Legal Aspects, (2022) https://www.researchgate.net/publication/363777021 [https://doi.org/10.32782/2524-0374/2022-8/66] (last visited Apr. 11, 2026).

The development and operation of the digital persona are shaped by four principal forms of agency: personal agents, namely individuals who often lack technical knowledge and awareness; technological agents, including software systems that frequently depend on stereotyped profiling; institutional and legal agents, whose regulatory frameworks remain inadequate to prevent misuse; and communal agents, such as peers and commercial actors, who may interact with or exploit digital data in ethically problematic ways.[7] Addressing these vulnerabilities requires a comprehensive and interdisciplinary framework rather than isolated technological solutions. Such a framework should integrate insights from sociology, systems engineering, data representation, and network science to enable individuals to manage their digital personae in a secure, ethical, and informed manner.[8]

III. PROBLEM OF IDENTITY VERIFICATION IN DECENTRALISED SPACES

While digitalisation has made contemporary life more efficient, it has also rendered individual privacy increasingly vulnerable, as digital identities are often stored in centralised systems that give users only limited control over their data.[9] Decentralised identity offers an important alternative by enabling individuals to control their credentials across distributed networks and reducing reliance on centralised points of failure.[10] Its practical adoption, however, faces a serious obstacle. If decentralised identity systems require users to manage complex cryptographic keys or navigate unintuitive interfaces, many are likely to abandon them in favour of familiar but less secure centralised platforms, thereby undermining the very purpose of decentralised identity.

A viable decentralised identity framework must therefore prioritise usability. The management of digital credentials should be as simple and accessible as using an online banking application. Achieving this objective requires international cooperation to develop widely accepted verification protocols, together

[7] Griselda Acosta, Eric Smith & Vladik Kreinovich, Analytical Techniques for Gauging Accuracy of Expert Knowledge: A Simple System-Based Explanation of the Dunning-Kruger Effect, (2020) https://www.researchgate.net/publication/341183632 [https://doi.org/10.1007/978-3-030-46413-4_6].
[8] O. Baranov, Social and Digital Transformation: A Source of Legal Problems, (2021) https://www.researchgate.net/publication/356238670 [https://doi.org/10.37750/2616-6798.2021.3(38).243807].
[9] D. de Kerckhove & C. Miranda, What is a digital persona? (2014) https://addi.ehu.es/bitstream/handle/10810/71850/Texto_De_Kerckhove_Miranda.pdf?sequence=1&isAllowed=y [https://doi.org/10.1386/tear.11.3.277_1].
[10] Saurav Bhattacharya, *The Paradox of Progress: Can Decentralized Identity Fix the Privacy Crisis?*, Forbes Nonprofit Council (Nov. 6, 2024 at 07:30 EST), https://www.forbes.com/councils/forbesnonprofitcouncil/2024/11/06/the-paradox-of-progress-can-decentralized-identity-fix-the-privacy-crisis/ [https://perma.cc/CR8L-DKX9] (last visited Apr. 11, 2026).

with balanced regulatory frameworks that protect users without impeding innovation. For businesses, the transition to user-controlled identity systems may demand significant investment in technology and training, but it also offers substantial long-term benefits. By reducing the need to store sensitive personal data, firms can lower the risk of major data breaches, ease compliance burdens under regimes such as the General Data Protection Regulation, and foster greater transparency and trust in their relationships with users.[11]

IV. INTELLECTUAL PROPERTY LAW CHALLENGES IN METAVERSE

As the digital persona extends into immersive, decentralised environments commonly described as the metaverse, the convergence of virtual and augmented reality with blockchain raises significant intellectual property challenges. One major concern relates to the protection of valuable virtual goods, including digital wearables, virtual real estate, and other digital assets, which are increasingly vulnerable to unauthorised reproductions of well-known brands. Nike's action against StockX over NFTs linked to Nike-branded sneakers illustrates how digital replication can dilute brand value and mislead consumers. In response, major companies have begun registering trademarks for virtual goods and services to secure their presence in digital environments.

The metaverse also depends heavily on user-generated content, which complicates ownership and enforcement. Platforms such as Roblox often require users to grant broad licences over their creations, raising concerns about the fair allocation of rights and the potential exploitation of creators.[12] At the same time, users may reproduce protected works, create virtual replicas of famous structures, or design avatars and accessories incorporating trademarked elements. Platform moderation systems, which often rely on automated detection, are poorly equipped to assess legal distinctions such as fair use, parody, or transformative use. As a result, unlawful uses may persist, while lawful expression may also be incorrectly restricted.

These difficulties are compounded by the decentralised structure of virtual environments, which weakens traditional territorially grounded enforcement mechanisms.[13] Infringers may operate across

[11] *Id.*
[12] *Terms of Use,* Roblox Corp., https://en.help.roblox.com/hc/en-us/articles/115004647846-Roblox-Terms-of-Use [https://perma.cc/U6QL-QJRA] (last visited Apr. 11, 2026).
[13] Eur. Union Intell. Prop. Off., Impact of the Metaverse on Infringement and Enforcement of Intellectual Property (2024) https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2024_Impact_of_t

jurisdictions through pseudonymous accounts, making it difficult for rights holders to identify responsible actors or pursue effective remedies.[14] Although NFTs and smart contracts offer certain technological advantages, including verifiable ownership records and automated royalty payments, their practical use remains limited by regulatory uncertainty, uneven adoption, and fragmented legal frameworks.[15] A more coherent and internationally coordinated legal response is therefore necessary if creativity and commerce are to coexist sustainably in the metaverse.

V. ENFORCEMENT OF IP RIGHTS IN A BORDERLESS DIGITAL SPACE

A new frontier of intellectual property (IP) enforcement in this metaverse world is largely characterised by the decentralised and borderless nature of virtual worlds. IP enforcement relies traditionally on jurisdictional boundaries. All the traditional mechanisms of enforcement become difficult to sustain in the metaverse, where fake digital products, unauthorised replicas, and IP violations may circulate across topographies and platforms with little to no constraint.

A key difficulty lies in the very structure of digital spaces. The obscurity of such blockchain-based platforms makes enforcement much harder. Frequently, IP possessors cannot identify the infringers or bring legal action against individuals who work under aliases or across multiple platforms. The absence of legal harmonisation compounds the problem. IP laws vary significantly across jurisdictions, and the lack of harmonisation exacerbates enforcement challenges in the metaverse, as legal systems have not uniformly adapted to virtual goods and related digital assets. While some jurisdictions recognise digital trademarks and other rights for virtual products, others have yet to develop a coherent framework to address these emerging issues.[16]

VI. INTERNATIONAL AND NATIONAL IP LAWS IN THE METAVERSE

he_metaverse_on_IP_infringement_and_enforcement/Impact_of_the_metaverse_on_IP_infringement_and_enforcement_FullR_en.pdf [https://perma.cc/5VS9-QRU4] (last visited Apr. 11, 2026).

[14] Eleonoea Rosati, *From Web 2 to Web 3: Harnessing Blockchain Technology for* IP, EUR. UNION INTELL. PROP. OFF., (Jan. 01, 2024), https://www.euipo.europa.eu/en/news/from-web-2-to-web-3-harnessing-blockchain-technology-for-ip [https://perma.cc/YX3H-KWWB].

[15] Lawrence R. Helfer, *Human Rights and Intellectual Property: Conflict or Coexistence?,* 5 MINN. INTELL. PROP. REV. 47, 47-61 (2003). https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1399&context=mjlst& [https://doi.org/10.24926/15529541.3758].

[16] Helfer, *supra* note 15.

It is essential to understand how both municipal and international IP rights are protected through multilateral instruments such as the Berne Convention for the Protection of Literary and Artistic Works and the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement).[17] These instruments establish the basic framework for copyright, trademark, and patent protection. Their application to the metaverse, however, raises difficult questions about cross-border disputes, legal harmonisation, and the development of norms governing virtual assets and digital transactions.

Domestic IP laws vary considerably in their scope, duration, and enforcement mechanisms. In the metaverse, where users and creators frequently operate across multiple jurisdictions, this diversity creates legal uncertainty; thus, it is imperative that global norms, rather than domestic laws, govern virtual assets and transactions. In the United States, the Digital Millennium Copyright Act provides an important framework for addressing digital copyright issues, including those arising from user-generated content. In the Metaverse, where users and generators frequently gauge multiple authorities, the interplay between public IP laws and the need for harmonisation poses challenges. National laws may need to adapt to accommodate virtual means, user-generated content, and cross-platform deals.[18] In the United States, the Digital Millennium Copyright Act provides an important framework for addressing digital copyright issues, including those arising from user-generated content. Comparable legislation exists in other jurisdictions, but its operation and limitations in immersive virtual environments require closer examination.[19]

VII. DOCTRINAL ASPECT OF THE METAVERSE

The metaverse is examined here through a doctrinal method grounded primarily in library-based legal research. That method involves the close and systematic analysis of primary legal materials, including statutes, regulations, policies, judicial decisions, and international instruments, alongside secondary sources such as academic commentary and scholarly treatises.

[17] Andy Ramos, *The Metaverse, NFTs and IP Rights: To Regulate or Not to Regulate?*, WIPO Mag., June 19, 2022, https://www.wipo.int/en/web/wipo-magazine/articles/the-metaverse-nfts-and-ip-rights-to-regulate-or-not-to-regulate-42603 [https://perma.cc/UAG3-CTSW].
[18] Neha Ahuja, *Commercial Creations: The Role of End User License Agreements in Controlling the Exploitation of User Generated Content*, 16 J. Marshall Rev. Intell. Prop. L. 383 (2017) https://repository.law.uic.edu/cgi/viewcontent.cgi?article=1416&context=ripl [https://perma.cc/9L9G-XUFW].
[19] Sagnik Roy Choudhury, *Trademark Law and E-Commerce: A Review of Legal Challenges and Consumer Protection*, 12 TIJER 4 (2016), https://tijer.org/tijer/papers/TIJER2504160.pdf [https://perma.cc/5T6V-W2YK].

In the context of the metaverse, doctrinal analysis does more than describe existing law. It also tests the capacity of established legal doctrines to respond to immersive and technologically mediated environments.[20] This approach has been applied across several important areas of metaverse law, particularly IP, virtual identity, and platform governance. In copyright law, it is used to assess whether digital assets and user-created avatars may qualify as protectable works, and to examine how platform terms allocate ownership and liability.[21] In trademark law, doctrinal and comparative analysis has exposed the limits of concepts such as "trademark use" and "likelihood of confusion" when applied to platform-based infringement, decentralised advertising practices, and third-party digital sellers.

A similar method has been used in patent law to evaluate whether metaverse-related software and virtual technologies satisfy conventional requirements of novelty and inventive step under existing patent regimes. In criminal law, doctrinal analysis has drawn attention to the inadequacy of traditional offences, particularly where legal definitions continue to depend upon physical contact or bodily harm. Such limitations have prompted some scholars to consider alternative frameworks for addressing harmful conduct committed through digital avatars and virtual environments. The same method has also been used to assess national legal preparedness for the metaverse. For example, textual analysis of Malaysian law has been employed to evaluate the adequacy of existing rules on communications, data protection, contracts, misinformation, virtual harassment, and smart contracts.[22]

VIII. SHOULD THE METAVERSE BE GOVERNED AS A DISTINCT LEGAL JURISDICTION?

The broader internet was eventually brought within the reach of domestic legal systems, but the metaverse presents a stronger case for distinct regulatory treatment because of its immersive, three-dimensional, and quasi-spatial character. These are the primary arguments for treating the metaverse as its own governance, along with the proposed structures and challenges involved.[23]

---

[20] Divya Gopalkrishnan, *Sexual Exploitation of Avatars in the Metaverse: An Intellectual Property Perspective*, 15 Int'l J. Sci. Res. 2 (2026), https://www.ijsr.net/archive/v15i2/SR26210215008.pdf [https://doi.org/10.21275/SR26210215008].
[21] Hafidz Hakimi Haron & Nadiah Arsat, *Zuckerberg's Metaverse and the Unready Malaysian Laws: Quo Vadis?*, Proceedings of the International Conference on Law and Digitalization (ICLD 2022) 123, 123-135 (2022) https://www.atlantis-press.com/proceedings/icld-22/125979423 [https://doi.org/10.2991/978-2-494069-59-6_12].
[22] Ananya Khandare, *The Metaverse: Intellectual Property Challenges in a Virtual World*, (Mar 6, 2025 at 11:43 IST) http://www.globalpatentfiling.com/blog/The-Metaverse-Intellectual-Property-Challenges-in-a-Virtual-World [https://perma.cc/UC9S-R4ES] (last visited Apr. 11, 2026).
[23] Jesse Valente, *Governing the Metaverse*, 9 U.C. Intell. Prop. & Comp. L.J. 2, (2024) [scholarship.law.uc.edu/cgi/viewcontent.cgi?article=1056&context=ipclj] [https://doi.org/10.2139/ssrn.4875434].

Existing legal frameworks remain deeply rooted in physical territory and sovereign jurisdiction. When applied to decentralised and borderless virtual environments, they encounter structural limits, procedural gaps, and interpretive uncertainty. Attempting to fit the metaverse entirely within these inherited frameworks may produce regulatory inconsistency, jurisdictional conflict, and unnecessary constraints on innovation.[24]

A separate governance framework is often defended on grounds of uniformity, efficiency, and institutional suitability. National laws differ significantly in scope and operation, which makes the application of territorially bounded rules to immediate and global virtual interactions increasingly impracticable. A more tailored metaverse framework could provide greater predictability and coherence. It could also support specialised legal mechanisms designed for virtual assets, digital property disputes, avatar-based rights, and other questions that do not fit comfortably within conventional legal categories.

IX. HOW A METAVERSE JURISDICTION COULD FUNCTION GOVERNING THIS DISTINCT SPACE REQUIRES INNOVATIVE, DIGITALLY NATIVE MECHANISMS

A proposed model of metaverse governance includes several interrelated elements. Dispute resolution could be conducted through virtual courts and arbitration panels operating entirely within the digital domain. Enforcement, in turn, could rely on smart contracts and blockchain systems to automate compliance and preserve tamper-evident evidentiary records, thereby reducing dependence on traditional physical authorities.

To balance user autonomy with safety, a mongrel governance model is proposed. Under such a model, centralised oversight would ensure coherence, accountability, and institutional coordination, while decentralised, blockchain-enabled rights would protect users in a manner analogous to a digital "bill of rights".[25] Effective digital identity verification would form an equally important part of this framework. Robust verification norms, potentially supported by blockchain-based or comparable identifiers, would be necessary to reduce the anonymity that shields unlawful conduct while still preserving user privacy.

---

[24] Jean-Thomas Arrighi de Casanova, *The Making of the 'Mongrel Nation' – Migration and Territorial Rescaling in Scotland, 1800–1997*, Conference Paper, IMISCOE Annual Conference, Madrid, Spain (Jan. 2016), https://www.researchgate.net/publication/320106960 (last visited Apr. 11, 2026).

[25] David Chalmers, *What Should Be Considered a Crime in the Metaverse?*, WIRED (Jan. 28, 2022, at 09:00 ET), https://www.wired.com/story/crime-metaverse-virtual-reality/ (last visited Apr. 11, 2026).

Metaverse governance, however, cannot exist in complete isolation from the physical world. Conduct within virtual environments, including financial investments, disputes over digital property, and psychological harm arising from virtual misconduct, may have direct and serious real-world consequences.[26]

Traditional governments are therefore unlikely to remain passive where the interests of their citizens are materially affected. Large-scale fraud or substantial economic loss, for example, would almost certainly trigger state intervention. These interconnections point to the need for structured inter-jurisdictional cooperation rather than absolute legal separation. Legal scholars and international organisations have accordingly proposed a framework for relations between virtual and physical legal orders. Such a framework could involve transnational bodies, including the World Intellectual Property Organization, developing model guidelines, bilateral arrangements, and harmonised norms capable of addressing disputes that move across both realms.

[27]

X. THE JURISPRUDENTIAL IMPACT OF HERMES V. ROTHSCHILD

The *Hermès v. Rothschild*, or "MetaBirkins", dispute occupies an important place at the intersection of traditional trademark law and emerging digital markets. The dispute arose when digital artist Mason Rothschild created and sold NFTs associated with images of the Hermès Birkin bag, prompting Hermès to bring claims for trademark infringement, dilution, and cybersquatting. In resolving the matter, the court applied the *Rogers v. Grimaldi* framework in order to balance the avoidance of consumer confusion against the artist's First Amendment interests. The jury ultimately found in favour of Hermès, concluding that Rothschild's use of the Birkin mark was explicitly misleading and awarding damages.

[26] Will Oremus, *Kids Are Flocking to Facebook's 'Metaverse.' Experts Worry Predators Will Follow*, WASH. POST (Feb. 7, 2022), https://www.washingtonpost.com/technology/2022/02/07/facebook-metaverse-horizon-worlds-kids-safety/ (on file with Legalis IP Quarterly); *see also* Anna Maria Collard, *Crime in the Metaverse Is Very Real. But How Do We Police a World with No Borders or Bodies?*, WORLD ECON. FORUM (Aug. 18, 2022), https://www.weforum.org/agenda/2022/08/crime-punishment-metaverse/ (last visited Apr. 11, 2026).

[27] Thayssa Bohadana Martins, *Beyond the Bag: MetaBirkins, Hermès, and the Legal Frontier of NFTs in Trademark Law*, 10 BOLOGNA L. REV. 1 (2023), https://bolognalawreview.unibo.it/article/download/20653/20156/98548 [https://doi.org/10.6092/issn.2531-6133/20653].

The verdict suggested that the NFTs functioned less as protected artistic expression and more as commercial products.[28]

The jurisprudential impact of this verdict is profound, serving as a critical litmus test for how courts will regulate brand identity and creative expression in the metaverse. It provides brand owners with the confidence that their intellectual property rights remain enforceable in virtual environments, establishing that major brands and individual digital creators can be considered direct competitors in the digital space. Likewise, the ruling emphasises that while digital art may retain suggestive rudiments, its commercialisation and branding can still infringe upon established trademarks if it exploits a brand's precisely curated exclusivity and consumer goodwill. Accordingly, this corner case is acting as a catalyst for companies worldwide to proactively acclimatise their legal strategies and register their trademarks specifically for virtual goods.[29]

Artists should take note that it is not the creation of art that is problematic, but rather the manner in which it is branded and packaged to consumers that can infringe on intellectual property rights. It is important to remember, however, that the 'MetaBirkins' case was a US federal jury trial and did not establish any mandatory legal precedent.

In addition, the US Supreme Court is set to hear oral arguments in March in *Jack Daniel's v. VIP Products*, where it will determine whether the humorous use of another's trademark as one's own commercial product is subject to the likelihood-of-confusion analysis used in the 'MetaBirkins' case, or protected under the First Amendment.[30]

XI. WHO WILL BE HELD LIABLE?

Responsibility for intellectual property violations in the metaverse primarily falls on direct infringers and online service providers (OSPs). Direct infringers include individuals or entities that produce, mint, or vend unauthorised digital means, as demonstrated by the case of digital artist Mason Rothschild, who

[28] Hari Priya K., *Adapting to Technological Inventions in Metaverse: Challenges in Indian Patent Law Through Case Law Analysis*, 6 Int'l J. Legal Sci. & Innovation 6 (2024), https://ijlsi.com/wp-content/uploads/Adapting-to-Technological-Inventions-in-Metaverse.pdf [https://doij.org/10.10000/IJLSI.112306].

[29] Danielle Garno & Krithika Rajkumar, *Hermès Win in MetaBirkin Trial: Implications for Fashion Industry*, Global Legal Post (Feb 13, 2023), http://www.globallegalpost.com/news/hermes-win-in-metabirkin-trial-implications-for-fashion-industry-1225165154 [https://perma.cc/S4JG-T2FV]

[30] Bohadana Martins, *supra* note 27.

was held liable for trademark infringement, dilution, and cybersquatting for creating and dealing in unauthorised "MetaBirkins" NFTs. Attribution at the individual level, however, is often complicated by the pseudonymous and decentralised character of blockchain-based environments. Infringers may operate under aliases across multiple platforms, making identification and enforcement considerably more difficult for rights holders. These practical difficulties have prompted increasing attention to the role of platforms that host, facilitate, or distribute infringing content. As a result, rights holders have argued with greater force that online service providers should bear a share of legal responsibility where direct enforcement against individual actors proves ineffective. The scope of such platform liability, however, differs significantly across jurisdictions.[31] The US frequently relies on the Digital Millennium Copyright Act (DMCA) notice-and-takedown framework. The European Union, on the other hand, has moved in a more interventionist direction by imposing affirmative duties on platforms to address violations proactively. Other jurisdictions, including Australia, have adopted more specific statutory approaches to intermediary or secondary liability, although the extent to which such models can be adapted to metaverse disputes remains contested.[32]

XII. WHERE WILL DISPUTES BE RESOLVED?

The borderless, decentralised nature of the metaverse disrupts traditional, terrain-grounded legal authorities. Presently, physical-world public courts retain jurisdiction over metaverse controversies because the fiscal and reputational impacts of virtual violations eventually carry over into the real world. For example, the United States Federal Courts assumed jurisdiction over the trademark controversies in *Hermès v. Rothschild* and *Nike v. StockX*. At the same time, Spanish marketable courts oversaw the *Vegap v. Mango* dispute regarding the unauthorised digitisation of physical oils. The application of domestic law to a global and technologically diffuse environment, however, often produces fragmented enforcement and considerable interpretive uncertainty.[33] To address these inefficiencies, legal scholars advocate treating the metaverse as a distinct legal regime. This approach proposes the creation of digitally native dispute-resolution mechanisms, similar to virtual courts operating entirely in the digital

[31] Maeve Hyer, *Physical Sports Needing Virtual Boundaries? An Analysis of Intellectual Property Issues Arising from Sport NFTs*, Intellectual Property Issues Arising from Sport NFTs, 30 Jeffrey S. Moorad Sports L.J. 91 91-16 (2023) digitalcommons.law.villanova.edu/cgi/viewcontent.cgi?article=1422&context=mslj.
[32] Hari Priya K., *supra* note 28.
[33] Danielle Garno & Krithika Rajkumar, *supra* note 29.

domain, and the application of smart contracts on the blockchain to automatically enforce legal opinions without relying on physical-world authorities.[34]

XIII. XIII. WHAT FRAMEWORKS GOVERN THE METAVERSE?

At present, the metaverse is governed not by a self-contained legal order, but by the extension of existing legal frameworks developed for the physical world. Trademark disputes concerning brand identity, for example, continue to be governed by instruments such as the Lanham Act in the United States and the European Union Trade Mark Regulation in the European Union. Difficulties nonetheless arise when these frameworks are applied to virtual goods. Under the Nice Classification, physical goods such as handbags fall within Class 18, whereas NFTs and downloadable virtual goods are generally placed within Class 9. This has led many brand owners to seek separate trademark registrations specifically covering virtual goods and services. US courts have also relied on the *Rogers v. Grimaldi* test to balance trademark protection against claims of artistic expression under the First Amendment.[35]

Copyright law likewise remains central to disputes involving the unauthorised reproduction of digital artworks, virtual environments, and other protected material, with regimes such as the United States Copyright Act and the European Union's InfoSoc framework continuing to provide the principal legal basis. Consumer protection law has also begun to intersect more directly with intellectual property enforcement in response to digital fraud and deceptive online practices. In India, for instance, the Consumer Protection Act, 2019 and the Consumer Protection (E-Commerce) Rules, 2020 impose obligations relating to transparency, grievance redressal, and platform responsibility. Private ordering also plays an important role. Platform terms of service frequently determine how intellectual property is owned, licensed, and used within virtual spaces, while smart contracts may embed licensing restrictions and transactional conditions directly into digital assets themselves.[36]

XIV. PREFERABLE LEGISLATION: NEW METAVERSE ACT, A DAWN OF A NEW LEGISLATIVE WORLD

[34] Bohadana Martins, *supra* note 26.

[35] Ananya Khandare, *supra* note 22.

[36] Moulika Sharma & Sanvi Mathur, *From Pixels to Prosecution: Tackling Crime in the Immersive Realms of Metaverse*, VI Sml. L. Rev. 220 220-52 (2023) https://www.hpnlu.ac.in/PDF/a7ef1747-02a4-4384-8104-82ff714e6d54.pdf [https://doi.org/10.70556/hpnlu-slr-v6-I1-2023-09].

A practicable legislative response would be the enactment of a dedicated Metaverse Act, designed to address the distinctive legal, commercial, and regulatory issues arising within immersive digital environments.

Article 1: Definitions and Legal Personhood

The metaverse shall be defined as an interactive, computer-generated three-dimensional ecosystem that integrates virtual and physical realities and enables users to participate through avatars. Avatars shall be recognised not merely as digital objects, but as externalised representations or digital delegates of their human users. Interference with an avatar's personal space may therefore, where appropriate, be treated as interference with the user's personhood. Digital assets, including non-fungible tokens and cryptocurrencies, shall be recognised as electronic records capable of exclusive control.[37]

Article 2: Personal Safety and Metaverse-Specific Offences

The law shall prohibit and criminalise serious forms of non-consensual conduct committed through avatars or immersive technologies. This includes metaverse-specific harms such as virtual sexual assault, persistent unwanted proximity after blocking, non-consensual avatar intrusion, and the creation or dissemination of sexually explicit AI-generated deepfakes of identifiable persons without consent. Such acts shall be treated as serious violations in light of their potential psychological and emotional consequences.

Article 3: Child Protection and Age-Appropriate Design

Digital service providers shall implement commercially reasonable age-verification measures to protect minors from harmful content. Platforms, app stores, and developers shall obtain parental consent where required before minors create accounts, download applications, or make in-app purchases. Age-appropriate design obligations shall include privacy-by-default settings, restrictions on manipulative design practices, and limits on precise geolocation tracking and automated profiling of children.[38]

---

[37] Clare McGlynn & Carlotta Rigotti, *From Virtual Rape to Meta-rape: Sexual Violence, Criminal Law and the Metaverse*, 45 Oxford J. Legal Stud. 554, 554-82 (2025), https://academic.oup.com/ojls/article/45/3/554/8108104 [https://doi.org/10.1093/ojls/gqaf009].

[38] Amber C. Thomson, et. al., *Little Users, Big Rules: Tracking Children's Privacy Legislation*, Mayer Brown (Jan. 28, 2026), https://www.mayerbrown.com/en/insights/publications/2026/01/little-users-big-rules-tracking-childrens-privacy-legislation [https://perma.cc/EU8N-AYFU] (last visited Apr. 11, 2026).

Article 4: Data Sovereignty and Biometric Privacy:

The collection and processing of sensitive biometric and body-based data, including eye-tracking, gait analysis, and brain-computer interface data, shall be subject to strict regulation. Such data may be processed only where strictly necessary and on the basis of clear and informed consent. Data minimisation requirements shall apply, and sensitive information collected for verification or access purposes shall not be retained or sold beyond what is strictly necessary.[39]

Article 5: Digital Commerce, Property, and Taxation

The law shall regulate virtual commerce, digital property, and taxation in order to promote market stability and prevent abuse. Existing financial rules concerning practices such as wash trading and insider trading may be extended to digital markets where appropriate. Smart contracts shall be enforceable only where the requirements of contract law, including offer, acceptance, and genuine consent, are satisfied. Virtual real estate shall be treated as a contractual asset or licensed interest governed principally by platform terms.[40]

Article 6: Commercial Liability and DAO Governance

Liability shall be allocated clearly among metaverse actors. Platform operators shall bear responsibility for system safety and for addressing unlawful content within their control. Individual users shall remain liable for fraud, abuse, or other unlawful conduct committed through their interactions. Entities deploying AI-controlled avatars or non-player characters shall bear responsibility for harmful conduct attributable to those systems. Decentralised autonomous organisations shall be required to adopt a legal structure capable of holding rights, assuming obligations, entering contracts, and bearing liability.[41]

Article 7: Interoperability and Anti-Monopoly Measures

The legislation shall promote interoperability and open standards in order to prevent dominant firms from creating closed and exclusionary digital ecosystems. Users shall, where feasible, be able to transfer their avatars and digital assets across platforms. Dominant metaverse platforms designated as

[39] *Metaverse Legal Frameworks*, Law & More (Jan 4, 2024), https://lawandmore.eu/blog/metaverse-legal-frameworks/ [https://perma.cc/M4F3-PZH5].
[40] Law & More, *supra note 40.*
[41] Jakub Jan Ziety & Rafal Pietraszuk, *A Few Remarks on the Legal Status of DAOs in the European Union and the Republic of Armenia*, 101 State and Law 16, 16-30 (2026) https://www.researchgate.net/publication/400445277 [https://doi.org/10.46991/SL/2025.101.016].

gatekeepers shall be prohibited from engaging in anti-competitive practices, including tying, unfair self-preferencing, and the combining of user data across services without clear consent.[42]

XV. CONCLUSION

The transition to a post-quantum digital civilisation marks a profound ontological shift and calls for a human-centred rethinking of legal, commercial, and educational institutions. The borderless structure of the metaverse and the expanding integration of generative artificial intelligence show the limits of applying analogue legal frameworks to decentralised digital realities. These limits are visible in the difficulty of regulating decentralised autonomous organisations, the growing need to extend trademark protection against digital forms of misappropriation, as illustrated by *Hermès v. Rothschild*, and the urgent need for a harmonised legal framework capable of protecting human identity against unauthorised synthetic replication.

The same structural dislocation is evident within academia. The increasing reliance on scientifically unreliable AI-detection tools, particularly those based on measures such as linguistic "perplexity" and "burstiness", has exposed serious epistemic, ethical, and pedagogical flaws. Such systems have not only produced false accusations against students but have also misclassified established literary works as AI-generated. A punitive model based on detection and discipline is therefore neither normatively defensible nor educationally sound.

A more credible response lies in developing an international, multi-stakeholder governance framework capable of addressing these transformations in a principled manner. Such a framework may draw upon robust human rights standards and other ethical traditions, including the justice-oriented principles associated with *maqasid al-Shariah*. The objective should be to create regulatory and institutional structures that preserve human agency, mental integrity, and fundamental rights, while enabling constructive forms of technological collaboration. The future of the metaverse and AI governance should therefore not be approached solely through reactive policing, but through a coherent legal order designed to ensure that technological progress remains accountable to human dignity and social justice.

[42] Int'l Bar Ass'n, Digital Regulations in the Metaverse Era: Europe, https://www.ibanet.org/document?id=Metaverse-project-Europe [https://perma.cc/6M3P-TTKC] (last visited Apr. 11, 2026).

Closing Remarks

As we conclude this inaugural issue of *The Legalis IP Quarterly*, we reflect on the significant milestone this represents for our organisation. The transition from a conceptualised vision to a tangible collection of scholarship marks the beginning of a dedicated effort to understand the intersection of technology, policy, and law.

The articles contained within this volume have traversed diverse terrains. Our contributors have interrogated the regulatory frontiers of space law and astronaut health protection, and examined the structural inadequacies of e-commerce enforcement in Pakistan. We have explored the systemic threats posed by AI-enabled piracy in India's entertainment sector and the complex transition of digital intermediaries from passive safe harbours to active sentinels under the IT Amendment Rules, 2026.

furthermore, this issue has addressed the fundamental reconstruction of legal integrity in the metaverse and provided critical comparative insights into international humanitarian law regarding the Gaza hostage crisis. Each contribution reinforces our core belief: that the rapid evolution of the digital era demands a corresponding evolution in legal thought.

We are immensely grateful to the authors who entrusted us with their research for this foundational issue. Their work serves as the bedrock upon which our future discourse will be built. furthermore, I must extend my personal gratitude to the Editorial Board, led by Shreya Singh, and the technical review team, led by Dhruv Aditya, for their commitment to maintaining the highest standards of academic integrity throughout this process.

Looking forward, *The Legalis IP Quarterly* remains committed to its role as a research-driven platform. We invite academics, practitioners, and students to engage with our upcoming call for papers for Volume I, Issue II. As we continue to examine the shifting paradigms of Intellectual Property and digital jurisprudence, we welcome diverse perspectives that challenge established norms and propose innovative legal frameworks.

The dialogue does not end with these pages. We encourage our readers to visit our digital platform at www.legalisip.com to participate in our ongoing projects and specialised discourse on the future of law.

OM DWIVEDI

Founder-President

Legalis IP

April 2026