Kelvin Open Science Publishers
Connect with Research Community

Research Article Volume 1 | Issue 2

KOS Journal of Science and Engineering
https://kelvinpublishers.com/journals/science-and-engineering.php

Cyber Law and the Regulation of Digital Platform Examine

Dr. Pallavi Gupta*

Professor and Head, Department of Law, JIMS Engineering Management Technical Campus, India

***Corresponding author:** Dr. Pallavi Gupta**,** Professor and Head, Department of Law, JIMS Engineering Management Technical Campus, Greater Noida, India, E-mail: pallavigupta2000@yahoo.co.in

Received: August 08, 2025; **Accepted:** August 19, 2025; **Published:** August 21, 2025

Citation: Pallavi Gupta. (2025) Cyber Law and the Regulation of Digital Platform Examine. *KOS J Sci and Eng.* 1(2): 1-6.

1. Abstract

The growing use of the internet in the last decade of the 20th century gave rise to a new area of law that known as Cyber Law. In the cyber era and with the invent of artificial intelligence number of digital landscape are rapidly evolved. When artificial intelligence and technology plays a significant role in our daily lives, the question arises, whether existing cyber law is sufficient to handle new type of cybercrime, if committed, or to regulate digital platform if irregularity or misuse committed by anyone or to regulate misuse or damage committed by artificial intelligence. It leads for urgent need of laws to regulate the online world. The primary concern of this research paper is to evaluate whether India is in need for a new legal framework for digital content regulation to control the increasing misuse of the constitutional right to freedom of expression to showcase obscene and violent content on digital platforms, increasing cases of online fraud, deep fake video, data theft etc. The primary concern of this research paper is to find out what are the challenges in regulating digital platforms like YouTube and OTT services' In this research paper, researcher will examine existing cyber laws and regulations of digital platform.

2. Keywords

Cyber law, Digital platform, Cyber security

3. Introduction

"Cyber Law is Guardian of Digital platform" Cyber law, or Information Technology law or digital law is the set of rules and regulations followed by Internet users to ensure safety and security of all parties. This law deals a range of legal disputes including data protection, privacy, cybersecurity, e-commerce, and intellectual property rights in the digital space related to the use of electronic devices, computer networks, increased use of social media, and many other digital platforms. Cyber law establishes an environment that is safe secure and reliable, for individuals, organizations and nations. Therefore, the objective of cyber Law is i) Preserving privacy; ii) Shielding identity; iii) Preventing cybercrime; iv) Strengthening cybersecurity, v) Maintaining national security. Cyber law ensures that individual's privacy rights are protected by ensuring the collection, storage and proper processing of personal data. Cyber law acts as a safeguard for Individuals identities by preventing unlawful access, theft or misuse of identity. This protection helps to prevent impersonation and identity fraud. Cyber law defines boundaries and penalties, for cybercrimes. By doing it discourages individuals from participating in malicious and unlawful activities online. Cyber law provides a more secure and resilient cyberspace by establishing rules and regulations. Cyber law protect infrastructure encompassing computer networks, data storage systems, online services, and national security interests from cyber threats. Examples are Computer Emergency Response Team (CERT-In) Directions to protect data theft.

4. Scope of Cyber Laws

Cyber Laws and regulations covers following sectors.

E-commerce: In e-commerce, consumers share their personal information with the websites. It becomes the brand's responsibility to protect their customer's data. Cyber laws ensure the proper protection of consumer data, it provides the legal framework for secure online transactions, electronic contracts, and digital signatures, ensuring fair and secure business practices, fostering trust and growth in the digital economy.

Online contracts: All online contracts must be in compliance with cyber law. Cyber law professionals are responsible for defining legal requirements and having in place dispute resolution mechanisms.

E-Taxes: Tax offices also have a cyber-law department that handles the online tax transactions. This includes collecting and maintaining tax information for online businesses and ensuring that they comply with online tax laws.

Data protection and privacy: Cyber law regulates how personal data is collected, stored, processed, and used online, ensuring individuals' privacy rights are protected.

Cybercrime: Cyber law defines and addresses online offenses like hacking, phishing, malware attacks, identity theft, and online fraud, holding perpetrators accountable.

Intellectual property: Cyber law protects copyrights, trademarks, and patents in the digital realm, preventing online infringement and plagiarism.

Content regulation: Cyber law addresses issues related to online content, including hate speech, defamation, misinformation, and online harassment.

Cybersecurity: It focuses on protecting computer systems and networks from unauthorized access, use, disclosure, disruption, modification, or destruction.

Jurisdiction: Cyber law handle with determining legal jurisdiction in cyberspace, where activities can span across borders.

5. Emergence of Digital Landscape or Platform

Digital platforms are software-based, online infrastructure providing a digital space for interaction through different app. These platforms enable users to connect, communicate, and transact with each other or with the platform itself. It facilitates the exchange of information, goods, services, or value. Digital platforms create value also by connecting different users, enabling the exchange of information, resources, and ideas. Infect these platform acts as a central hub for users, customers, and partners to access and utilize various applications, data, & services as well. These platforms foster environments or network where multiple users, community and businesses can interact & collaborate. India's digital landscape is characterized by a wide range of platforms, from e-commerce and social media to digital payments and government initiatives. Digital India initiatives have also fostered platforms for e-governance, education, and healthcare.

6. Nature of Digital Platform

Nature of Digital platforms varies as per nature of activities take place. In India followings are prominent digital platforms in wide use.

6.1. Social media platforms

These platforms allow users to create and share content, connect with others, and engage in social interactions -e.g., **Facebook, instagram, and youtube-** India has a large user base for these platforms, making them crucial for social networking, content consumption, and marketing.

WhatsApp: A widely used messaging platform for both personal and business communication.

LinkedIn: A professional networking platform used for job searching, recruitment, and business networking.

6.2. E-commerce platforms

These platform facilitate the buying and selling of goods and services (e.g., **Flipkart, Amazon, Myntra, Snapdeal, Reliance Jiomart and others.** These are leading e-commerce platforms in India, offering a wide range of products and services).

6.3. Digital payments platforms

These platform enables the user to make payment from anywhere in very easy manner. E.g.-**Unified Payments Interface (UPI):** A government-backed system that enables instant, real-time bank-to-bank transfers, facilitating digital payments across various apps. (e.g. **Paytm, PhonePe, Google Pay, and BharatPe).** These are popular digital payment apps that leverage UPI and other technologies to provide convenient payment options.

6.4. Cloud computing platforms

These platforms provide computing resources and services over the internet (e.g., Amazon Web Services, Microsoft Azure etc.).

6.5. Marketplaces

These digital platforms connect buyers and sellers, facilitating transactions (e.g., ride-sharing platforms, food delivery apps).

6.6. Content platforms

These digital platforms enable users to create, share, and consume various forms of media (e.g., YouTube, Spotify).

6.7. Collaboration platforms

These digital platforms support teamwork and project management (e.g., Slack, Microsoft Teams).

6.8. Government digital platforms

Aadhaar: The world's largest digital identity platform, providing a unique identification number to Indian citizens.

DigiLocker: A platform for storing and sharing digital documents and certificates, promoting paperless governance.

DIKSHA: A platform for digital learning and knowledge sharing in the education sector.

UMANG: A platform that provides access to various government services through a single mobile application.

CoWIN: The platform used for managing and tracking COVID-19 vaccinations.
AarogyaSetu: A contact tracing and health awareness

mobile app.

e-Sanjeevani: A telemedicine platform for remote doctor consultations.

GeM (Government e-Marketplace): A platform for government procurement of goods and services.

BHIM: A UPI-based mobile payment app developed by the government.

API Setu: A platform for accessing and utilizing various government APIs.

6.9. Other notable platforms

Hotstar: A popular video-on-demand and live streaming platform, especially for sports content.

Account aggregators: A new category of financial data platforms that enable secure sharing of financial information between regulated entities.

These are just some examples of the diverse and rapidly evolving digital landscape in India. The growth of these platforms is driven by increased internet access, government initiatives, and a growing preference for digital solutions across various sectors.

7. Existing Cyber Law in India to Handle Cyber Crime

The following laws and institutions collectively form the legal framework for addressing cybercrimes and regulating digital activities of various platforms in India.

- **The Information technology Act, 2000 (IT Act)** provides legal recognition for electronic documents and transactions, facilitating e-commerce and digital communication. It establishes various cyber offenses such as hacking, data theft, and spreading of viruses. The IT Act has been amended to address evolving cyber threats, including those related to cyber terrorism, child pornography, and identity theft. The IT Act empowers the government to intercept, monitor, or decrypt information for national security purposes.

- **The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) rules, 2011**, aim to safeguard sensitive personal data and promote reasonable security practices. These rules introduced a three-tier grievance redressal mechanism for online platforms and mandated the removal of unlawful content.

- The IT Act is **supplemented by other laws like the Bharatiya Sakchya Adhiniyam** 2023. It provides guidelines for collecting and presenting electronic evidence in court. It also recognizes electronic records as evidence in legal proceedings.

- **Bhartiya Nyaya Sanhita (BNS) 2023:** Certain cybercrimes are punishable under the BNS, such as hacking and identity theft.

- **The Digital Personal Data Protection Act of 2023** is a recent addition to India's cyber law landscape, focusing on the protection of digital personal data. It addresses issues related to the collection, storage, and processing of personal data. Introduces principles for handling personal data and establishes a Data Protection Authority.

- **IPR laws- the copyright Act, 1957**: It protects digital content from unauthorized reproduction, distribution, and use.

- **The Protection of children from sexual offences (POCSO) Act**, 2012, play a role in regulating certain types of content on digital platforms.

- **Indecent representation of women Act 1986**, Prohibits indecent representation of women in any manner. It also plays a role in regulating certain types of content on digital platforms.

- **Cable Television networks (Regulation) Act, 1995:** Concerns the certification of cinematograph films for exhibition.

- **Young Persons (Harmful Publication) Act, 1956:** Defines 'harmful publication' as publications that portray the commission of offences, violence, cruelty, or repulsive incidents.

- **The intermediary guidelines and digital media ethics code (IT Rules, 2021):** Mandate self-regulation and content classification.

- The Right to Privacy: under **Article 21 of the indian constitution** the right to privacy is protected.

- **The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016** governs the use and protection of Aadhaar data, India's biometric identity system.

- **The National cyber security policy, 2013** aims to protect information infrastructure in India and strengthen cyber security measures.

- State police departments have dedicated units like **cyber cells and cybercrime investigation units** to investigate cybercrimes.

- **Cyber appellate tribunal (CAT) is e**stablished under the Information Technology Act to hear appeals against decisions made by Adjudicating Officers.

- **International cooperation**: India cooperates with international organizations and other countries to combat cybercrimes that transcend national borders.

8. Existing Regulatory Frameworks to Handle Digital Platform in India

Information Technology Act, 2000 provides a foundation for regulating online content and intermediaries but is seen by some as outdated in the face of rapid technological advancements.

Information Technology rules, 2021, issued under the IT Act, introduced a three-tier grievance redressal mechanism for online platforms and mandated the removal of unlawful content, but this system could not have enforced being challenged in High Courts.

Other laws: The POCSO Act, Indecent Representation of Women Act, and the BNS, 2023, The Intermediary Guidelines and Digital Media Ethics Code (IT Rules, 2021) also play a role in regulating certain types of content on digital platforms but somehow not that much satisfactory.

Initiatives of government: As India moves forward in adopting technologies towards it's realisation of the "Digital India" scheme, there is requirement of robust legal measures and frameworks to safeguard individuals, enterprises and the nation from the diverse risks that come with the digital age.

Cybersecurity measures: India has established the National Cyber Coordination Centre (NCSC) and the Indian Computer Emergency Response Team (CERT- In) to combat cyber threats, data breaches and to improve cybersecurity resilience. The IT Act mandates companies and organisations to report data breaches within a 6-hour window of noticing such data breach to CERT-In, for investigation and response to cyber-attack.

Cybercrime investigation: Specialized cyber cell units have been set up within the police force, specifically for investigating and prosecuting cybercrimes efficiently.

9. Key Features of Digital Platform Regulation

Content Regulation: Governments and organizations are facing with the issue how to regulate content on digital platforms, including issues of hate speech, misinformation, and harmful content like child sexual abuse material.

Competition Concerns: Concern about dominance of some Digital platforms' in various sectors raises questions about fair competition and potential anti-competitive practices.

User safety and privacy: Concern about protection of user data, privacy, and address issues like cyberbullying and online harassment.

Accountability and transparency: There's a growing demand for greater transparency in platform algorithms (operation system) and content moderation practices, and how user data is handled as well as for mechanisms to hold platforms accountable for their actions.

Self-Regulation vs. government regulation: A key debate revolves around whether platforms should be primarily responsible for self-regulation or whether governments should impose stricter regulatory frameworks.

Ex-Ante regulations: Some jurisdictions are moving towards ex-ante regulations, which impose specific obligations on platforms before they engage in certain activities. Examples include the Digital Markets Act in Europe.

Industry-specific regulations: Some areas, like social media, are seeing the development of specific regulations tailored to the unique challenges and opportunities of those platforms.

Thus regulation of digital platforms is a complex and evolving issue. Worldwide governments are facing this issue with how to balance freedom of expression, user safety, and economic competition. India has the primary Cyber legal framework, but enforcement challenges and the need for a more robust system are driving discussions about potential updates.

10. Concerns over Obscene Digital Content Regulation

The Indian government, Judiciary is examining the need for a new legal framework to regulate digital platforms among concerns over violent and obscene content. After the issue of Ranveer Allahabadia controvercy the government and Judiciary acknowledges increasing public demand for stricter laws against obscene and harmful content on digital platforms, and is currently assessing the need for amendments or a new legal framework. The Union Information and Broadcasting Ministry is examining current laws and the need for a new legal framework to regulate such 'harmful content'. They have asked social media channels and OTT platforms to follow the Code of Ethics prescribed in the IT Rules 2021, and Implement "access control for A-rated content" to prevent children from consuming inappropriate material. The OTT platforms must not transmit any prohibited content and undertake age-based classification of content.

11. Challenges and Issues in Regulation of Digital Platform

There are various challenges are observed in regulation of digital platforms as follows.

Lack a specific regulatory framework

OTT platforms and social media currently lack a clear regulatory framework. Although the IT Rules, 2021, require a three-tier grievance redressal mechanism:

- Level 1: Self-regulation by the platform.
- Level 2: Industry-wide self-regulation.
- Level 3: Government oversight.

This mechanism has been challenged in various HCs, with the Bombay and Madras HCs staying its enforcement. The Kerala HC has restrained coercive action over non-compliance with (Part III of) the IT Rules 2021.Over 15 petitions have been filed against these rules, and the SC has transferred all cases to the Delhi HC for a consolidated hearing.

The role of YouTube and social media intermediaries: YouTube is regulated under the IT Rules but is not liable for user-generated content unless it violates government directives. YouTube functions as a social media intermediary and has limited accountability for content uploaded by individual users. Thus new media services like OTT platforms and YouTube currently operate without a specific regulatory framework, increasing demands for legal amendments.

Enforcement: Enforcing existing regulations and ensuring compliance across diverse platforms remains a challenge.

Self-regulation vs. government regulation: There's ongoing debate about the extent to which platforms should self-regulate versus being subject to direct government oversight.

Balancing freedom of speech and safety: Finding the right balance between protecting free speech and preventing the spread of harmful content is a key challenge.

Impact on innovation: There's a challenge in finding the right balance between regulating platforms to protect users and society, while also fostering innovation and economic growth. Some argue that overly strict regulations could stifle innovation and competition in the digital space.

International cooperation: Digital platforms operate globally, and international cooperation is needed to address cross-border issues.

Harmonizing regulations: Efforts are being made to harmonize regulations across different jurisdictions to avoid fragmentation and ensure a consistent approach.

Adapting to evolving technology: The rapid pace of technological change requires regulations to be flexible and adaptable to new challenges and opportunities.

In essence, the regulation of digital platforms is a complex and evolving area, with ongoing efforts to develop and refine frameworks that address the diverse challenges and opportunities presented by these powerful and pervasive technologies.

12. Conclusion

As technology and electronic communications developed, it became clear that the legal framework, existing at the dawn of the digital age would not be adequate to ensure a secure, fair, and inclusive internet for all users. The laws, regulations and legal precedents that encompass cyber law seek to address:

- **Privacy and Data Protection:** As individuals and organizations began to share vast amounts of personal and sensitive information online, laws were required to protect privacy and regulate the collection, storage, and use of data.
- **Intellectual Property Protection:** The internet has made it easier to reproduce and distribute intellectual property such as music, movies, software, and written content. As a result, laws related to copyright infringement, piracy, and the protection of intellectual property online needed to be updated to reflect the new reality.
- **Cybersecurity and Cybercrime:** With the rise of cyberattacks, hacking, and online fraud, and cyber law helped define and enforce rules related to cybersecurity and to prosecute cybercriminals.
- **E-Commerce and Online Contracts:** As online commerce grew, it became crucial to establish new rules for online contracts, electronic signatures, consumer protection, and dispute resolution for e-commerce transactions.
- **Freedom of Expression and Speech:** The internet expanded the ability of individuals to express their views, but it also raised questions about the limits of free speech and the regulation of hate speech, defamation, and other harmful online content.
- **Internet Governance:** Cyber law has been central to establishing frameworks for governing the internet, including domain name management, internet standards, and regulation of internet service providers.
- **Liability and Responsibility:** Cyber law has been instrumental in defining responsibilities and liabilities for various actors, including online platforms, content creators, and users.
- **Law Enforcement and International Cooperation:** Cyber law has had a role in facilitating cooperation among law enforcement agencies across borders to combat cybercrime and enforce cyber-related laws.

13. Recommendations

Need for a New Legal Framework: There is gaps in Existing Laws and safeguards as these are fragmented under different laws. New media such as OTT platforms, YouTube and other social media do not fall under a specific regulatory framework. Moreover, YouTube is not made liable for user-generated content. Implementation of the Digital Media Ethics Code (IT Rules, 2021) has been stayed by several high courts. The Supreme Court noted the lack of effective regulations against obscene content and stated that it would act if the government fails to step up. It makes necessary for a holistic and effective legal framework to cover the gaps.

Need a Strong Mechanisms Governing Obscenity in Online Content: Although in Indian Legal system there is number of laws but it lacks effective enforcement mechanism under various laws- like Intermediary Guidelines and Digital Media Ethics Code (IT Rules, 2021), Indecent Representation of Women Act, 1986: Prohibits indecent representation of women in any manner. Bhartiya Nyaya Sanhita (BNS), 2023: Section 294 penalises the sale, distribution, or creation of obscene materials, including books, drawings, and electronic content. Protection of Children from Sexual Offences (POCSO) Act: Penalises the use of children for pornographic purposes or pornographic material. Information Technology (IT) Act, 2000: Section 67 penalises the publication or transmission of obscene material in electronic form. Cable Television Networks (Regulation) Act, 1995: Concerns the certification of cinematograph films for exhibition. Young Persons (Harmful Publication) Act, 1956: Defines 'harmful publication' as publications that portray the commission of offences, violence, cruelty, or repulsive incidents.

Need of Comprehensive Cybersecurity Policy: It is debated that deterrent laws and regulations seek to prevent cybercrime but it will not prevent every hack or ransomware attack. Therefore, it's essential that companies and organizations must establish their own comprehensive cybersecurity policies for safeguarding digital assets and ensuring the confidentiality, integrity, and availability of all data and systems. At a minimum, a cybersecurity policy should cover:

Roles and Responsibilities: Define key roles and responsibilities related to cybersecurity within the organization.

Access Controls: Specify access control principles, strong password requirements, and multi-factor authentication requirements and methods.

Data Classification and Handling: Establish a data classification system and describe how sensitive data should be handled, stored, and transmitted.

Incident Reporting and Response: Outline the process for reporting cybersecurity incidents and the steps to be taken during incident response.

Security Awareness and Training: Describe the organization's security awareness program and encourage employees to stay informed about cybersecurity threats and best practices.

Network Security: Address network security measures, including firewalls, intrusion detection systems, and network segmentation.

Endpoint Security: Define requirements for securing endpoint devices and antivirus/anti-malware software.

Data Backup and Recovery: Outline data backup and recovery procedures, including regular backups and disaster recovery planning.

Vendor and third-party security: Establish guidelines for assessing and monitoring third-party cybersecurity practices and include relevant contract clauses.

Compliance and Legal Requirements: Ensure alignment with relevant industry-specific regulations and legal requirements.

Monitoring and Auditing: Describe the organization's monitoring and auditing procedures for detecting security incidents and policy violations.

Policy Review and Updates: Specify a schedule for policy review and updates to ensure relevance and effectiveness.

Security Incident Communication: Outline communication protocols for notifying employees, customers, and authorities in the event of a data breach or cybersecurity incident.

14. References

1. Alain Strowel, Wouter Vergote. Digital platforms: To regulate or not to regulate? Message to Regulators: Fix the economics first, then focus on the right regulation.
2. https://currentaffairs.khanglobalstudies.com/regulation-of-digital-platforms/
3. https://vajiramandravi.com/current-affairs/regulating-digital-content-in-india/
4. https://www.india.gov.in/website-digitize-india-platform?page=3
5. https://www.axiomlaw.com/guides/cyber-law
6. https://cyberlaws.net/cyber-law-articles/cyber-legal-developments-india-2020/
7. https://iclg.com/briefing/20423-recent-changes-to-the-cybersecurity-regulatory-space-inindia