



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2025

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution- Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

CYBER LAW: AN OVERVIEW OF INDIAN CONTEXT

-GAUTHAMI VINOD MANKAME

In recent times our life is intertwined with various digital technologies and cyber related aspects hence there is a rampant need of cyber law and that has become a backbone and safe secure space in the digital ecosystem. Furthermore India is home to a large number of population including the largest user of the Internet and various transformations in the regulation of cyberspace. The increase in the use of cyberspace comes with the serious concern that includes data concerns cyber crime and influence of artificial intelligence in the evolving landscape of cyber space to meet modern needs furthermore a need of India's strong regulatory framework. This blog shall help in understanding the foundation of cyber law in India and the trends followed recently shaping the future of the same.

Firstly one needs to understand what is cyber law at the first place cyber law is also known to be the IT law refers to our legal framework that is governing all the activities in digital platforms this encompasses regulations related to e commerce, data protection and privacy digital signature, intellectual property laws cyber crime and so on in the Internet space. Currently in India cyber law is governed under information technology act of 2000 and is supplemented by various other laws. The key legislation in India for cyber law is information technology act this act was India's First legislation specially designed to address cyber related aspects and electronic commerce that included cyber crimes and digital problems associated with the same it also recognises various components like electronic contracts, signatures done digitally and online communication which are legally valid. Some of the provisions that needs to be looked into is section 43, section 66,



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2025

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution- Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

section 66 C and 66D, And section 67¹ this section broadly gives penalty for unauthorised access and damage to the computer systems it also covers hacking and illegal data access done by any individual in the online spaces furthermore it gives punishment for identity theft and any cheating by impersonation lastly penalises publishing or transmitting obscene materials online and so on are few of the provision which is included in this particular legislation furthermore not specifically a cyber law but various criminal law along with the information technology act supplementing each other penalises punishes for the offenses such as cyberstalking fraud online defamation and so on. Now Digital Personal Data Protection Act of 2023 has various principles of consent, accountability, users rights, placing the responsibility on businesses to protect the personal data and also to identify and notify breaches of such data.

The recent trends in cyber law also consists of an increase in cyber crime. This simply means the digital services are doing so much outreach and so do the cyber threats as well. In India we have seen an increase in phishing attacks, frauds, financial fraud, deep fakes, ransomware etc. Cyber criminals are also targeting various individuals and business owners using sophisticated techniques this leading to often creating pressure on law enforcement agencies who are under pressure to respond faster anti use modernised techniques, one of the authority is CERT- In which is also known as Indian computer emergency response team helps in combating with the cyber security issues they have also issued new guidelines for reporting any incident relating to cyber threat and also introduce cyber security practices.

Furthermore, there has always been growing concern about the data protection and user privacy in a cyber space. The new DPDP Act, 2023, is brought in response to growing concern regarding the same as to how the data has been collected, stored and shared. Various companies have to face

¹ The Information Technology Act, No. 21 of 2000, INDIA CODE (2000), <https://www.indiacode.nic.in/handle/123456789/1999>



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2025

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution- Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

strict rules regarding the retention of data ,right of the users, consent related aspects if not followed or non compliance of the same needs to hefty penalties this lines with the global aspect of EU’s GDPR, indicating India's step towards becoming a trusted data hub. Furthermore, IT Act 2000² is considered outdated as the technologies today are highly developed that includes artificial intelligence, blockchain, quantum computing and so on. The Indian government is also working on Digital India act Which is replacing the information technology act and provide some modern flexible framework for regulating the digital economy of the country, this act will likely address AI and automation, digital competition and antitrust issues as well.As far as the stricter regulation was been considered intermediary guidelines revised to hold OTT providers accountable and other social media platforms as well to be more transparent and accountable as they had to quickly resolve the grievances of the users, remove those contents which were unlawful also appointment of the compliance officer, these new regulations also covered online gaming and advertisements by the influencers. India is now emphasizing on the security of data and digital infrastructure such as systems related to banking, energy, telecom, defense.

Additionally there are various challenges and opportunities in the same sector wherein future of the cyber law in India is closely tied and there is a rapid growth and rampant increase in the technology sector for example there is a need of regulation around the usage of AI and the ethical aspect of it that includes surveillance automation and so on. As there are various agreements which have been done across the globe, there is cross border data flow in aspects of digital trade agreements, data localization and hence it is important to protect the privacy aspect of it as privacy is in a critical stage. There is a need for an increase in awareness especially in countries like India as it has more rural and urban sectors to prevent any scams and frauds such cyber education is

² The Information Technology Act, No. 21 of 2000, INDIA CODE (2000), <https://www.indiacode.nic.in/handle/123456789/1999>



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2025

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution- Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

required to promote and support Digital literacy. Lastly, there needs to be legal capacity building to equip the authorities to handle complex cases.

In conclusion, we know that in this digital age cyber law is no longer an option but an essential law required because the dependency on the usage of the Internet is growing significantly so the legal safeguard needs to be in sync with the emerging use. The switch from information technology act to the proposed digital India act shows the efficiency of the government in actively responding to the various challenges in the digital age . A judicial system that understands the complexities relating to the cyber space.