IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

NAVIGATING THE LEGAL LANDSCAPE OF THE DIGITAL AGE

Divyam Kumar
B.B.A. L.L.B.
University of Mumbai law Academy
(Mumbai University)

Abstract

Cyber Law, also known as Internet Law, refers to the legal principles and regulations that govern the use of the internet and digital technologies. With the rapid advancement of technology, cyber law has become an essential aspect of the legal framework globally. This paper explores the evolution of cyber law, its key components and the challenges faced in its implementation. By analyzing various aspects of cyber law, this research aims to provide a comprehensive understanding of how legal systems are adapting to the complexities of the digital age and what are the areas where it is lacking behind. Several new kinds of cybercrimes came into existence and how our present laws are unable to catch up with the crimes.

Introduction

The internet has revolutionized the way individuals and businesses operate, leading to unprecedented levels of connectivity and data exchange. However, this digital transformation also brings forth a myriad of legal challenges, from data privacy issues to cybercrimes. Cyber law encompasses these legal issues and strives to provide a regulatory framework to address them. However there is a huge lack. This paper will delve into the evolution of cyber law, its critical areas, and the challenges in enforcing these laws. This research paper majorly focuses

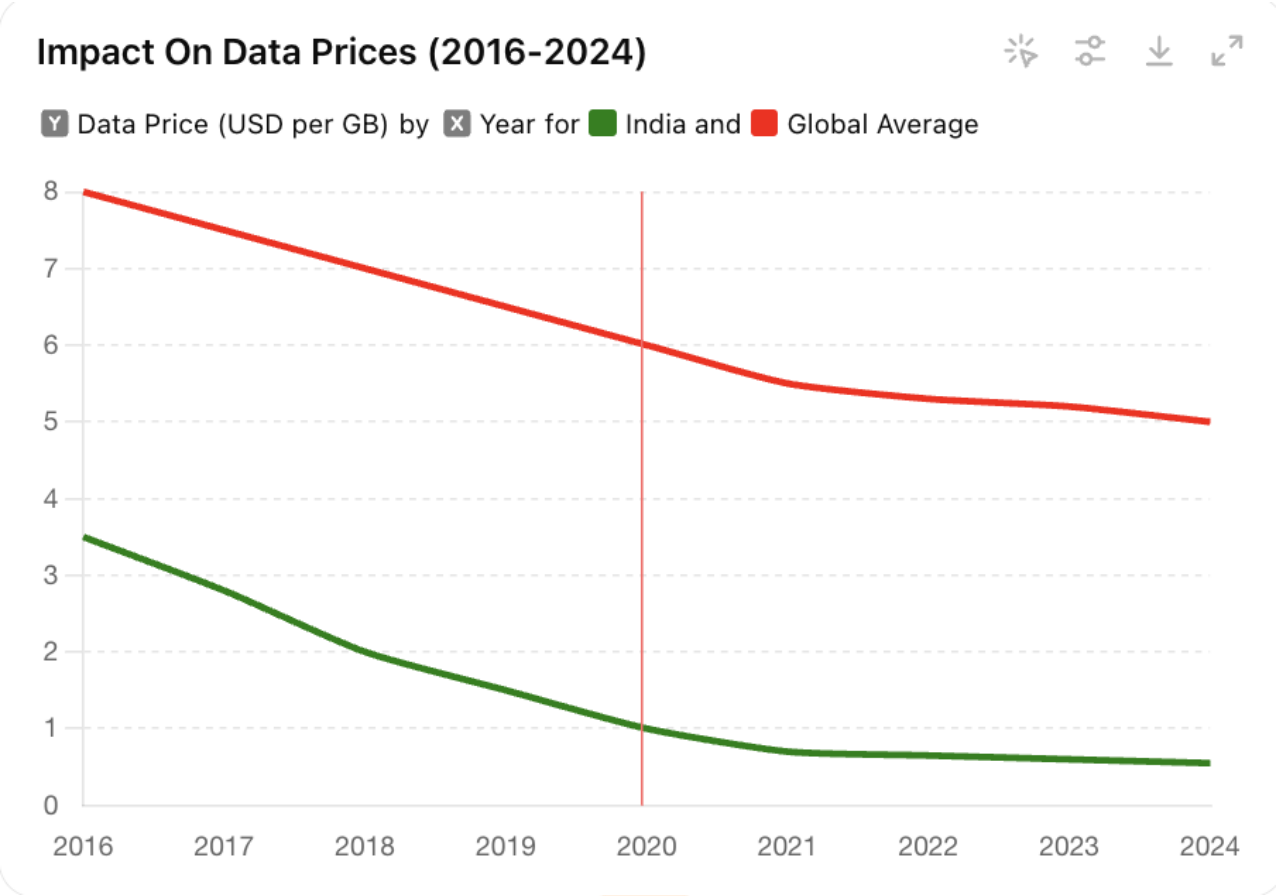
Evolution of Cyber Law

The development of cyber law can be traced back to the late 20th century, coinciding with the rise of the internet. Early legal frameworks focused on addressing computer crimes and the unauthorized access of computer systems. Over time, as the internet became integral to daily life and commerce, the scope of cyber law expanded to include issues like data protection, intellectual property, and e-commerce regulations. The evolution of cyber law in India has been driven by the rapid growth of the internet and digital technologies, transforming the socio-economic landscape. The first major legislative step was the **Information Technology (IT) Act, 2000**, based on the UN Model Law on Electronic Commerce (1996). It aimed to provide a legal framework for electronic governance, recognizing electronic records and digital signatures, and addressing cybercrimes like hacking and identity theft. The latest development in terms of legislation in India which addresses some of these problems is the **Digital Personal Data Protection Act, 2023**. It provides for the processing of digital personal data in a manner that recognizes both the rights of the individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto.

Advancing Technology vs. Evolving Threats

After so much evolution in the cyber law the law is still not sufficient to contain the crime. But as we know law is always behind the crime. Reliance Jio's entry into the Indian telecom market significantly accelerated the internet revolution in India by drastically reducing data prices,

making high-speed 4G internet widely accessible to the population, which led to a surge in data consumption and propelled India to become one of the world's top mobile data users; essentially democratizing internet access across the country, particularly in rural areas. Jio's entry caused a 35% drop in data prices across India, making it one of the most affordable data markets globally.



It has a lot of good impacts specially in digitalizing India but it too has several negative impacts. It is see that after the advent of JIO's there has been steep surge in cybercrime.

The above table shows the state wise cybercrimes form year 2016 to 2018. This shows a very steep rise in cybercrime in India after the point when internet became cheap.

Bodies, Acts & Rules which deals with Cyber Crime in India –

Cyber law is any law that applies to the internet and internet-related technologies. Areas that are related to cyber law include Cybercrime and cybersecurity. Acts & Rules in relation to cyberspace are increasing in importance every single year with the increase in the use of information and communications technology.

1. **The Information Technology Act, 2000 :** It was the first act which was enacted to give legal sanction to electronic commerce and electronic transactions, to enable e-governance, and also to prevent cybercrime.

2. **Digital Personal Data Protection Act, 2023:** It provides for the processing of digital personal data in a manner that recognizes both the rights of the individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto.

S. No	Category	State/UT	2016	2017	2018	Percentage Share State/UT (2018	Mid-Year Project Population (Lakhs) (2018)+	Rate of Tot Cyber Crim (2018)++
1	State	Andhra Prades	616	931	1207	4.4	520.3	2.3
2	State	Arunachal Pradesh	4	1	7	0	14.9	0.5
3	State	Assam	696	1120	2022	7.4	340.4	5.9
4	State	Bihar	309	433	374	1.4	1183.3	0.3
5	State	Chhattisgarh	90	171	139	0.5	284.7	0.5
6	State	Goa	31	13	29	0.1	15.3	1.9
7	State	Gujarat	362	458	702	2.6	673.2	1
8	State	Haryana	401	504	418	1.5	284	1.5
9	State	Himachal Pradesh	31	56	69	0.3	72.7	0.9
10	State	Jammu Kashmir	28	63	73	0.3	134.3	0.5
11	State	Jharkhand	259	720	930	3.4	370.5	2.5
12	State	Karnataka	1101	3174	5839	21.4	654.5	8.9
13	State	Kerala	283	320	340	1.2	350	1
14	State	Madhya Prade	258	490	740	2.7	814.7	0.9
15	State	Maharashtra	2380	3604	3511	12.9	1213.9	2.9
16	State	Manipur	11	74	29	0.1	30.8	0.9
17	State	Meghalaya	39	39	74	0.3	32	2.3
18	State	Mizoram	1	10	6	0	11.8	0.5
19	State	Nagaland	2	0	2	0	21.3	0.1
20	State	Odisha	317	824	843	3.1	435.5	1.9
21	State	Punjab	102	176	239	0.9	297	0.8
22	State	Rajasthan	941	1304	1104	4.1	765.9	1.4
23	State	Sikkim	1	1	1	0	6.6	0.2
24	State	Tamil Nadu	144	228	295	1.1	754.6	0.4
25	State	Telangana	593	1209	1205	4.4	370.3	3.3
26	State	Tripura	8	7	20	0.1	39.6	0.5
27	State	Uttar Pradesh	2639	4971	6280	23	2230	2.8
28	State	Uttarakhand	62	124	171	0.6	110.6	1.5
29	State	West Bengal	478	568	335	1.2	965	0.3
State	State	Total State(s)	12187	21593	27004	99.1	12997.9	2.1
30	Union Territory	A & N Islands	3	3	7	0	4	1.8

31	Union Territory	Chandigarh	26	32	30	0.1	11.7	2.6
32	Union Territory	D&N Haveli	1	1	0	0	5.3	0
33	Union Territory	Daman & Diu	0	0	0	0	4	0
34	Union Territory	Delhi UT	98	162	189	0.7	195.6	1
35	Union Territory	Lakshadweep	0	0	4	0	0.7	6
36	Union Territory	Puducherry	2	5	14	0.1	14.8	0.9
Union Territory	Union Territory	Total UT(s)	130	203	244	0.9	236	1
Total (A India)	Total (A India)	Total (All Indi	12317	21796	27248	100	13233.8	2.1[1]

3. **The Bharatiya Nayaya Sanhita, 2023:** It is more evolved penal code which is addressing the concerns of this digital era. It is addressing several digital era crimes. It Criminalizes the intentional use of online platforms to promote enmity between groups on the grounds of religion, race, caste, etc. It Penalizes the publication, transmission, or distribution of obscene material, including through electronic means. It criminalizes unauthorized access to computer systems and the theft of digital data. It further deals with cheating and fraudulent activities carried out using online platforms, such as phishing or impersonation.

4. Various regulatory bodies, such as the **"Reserve Bank of India" (RBI**), the "**Insurance Regulatory and Development Authority of India**", the "**Department of Telecommunication" (DOT),** and the "**Securities Exchange Board of India" (SEBI**), have issued circulars mandating their regulated entities to comply with cybersecurity standards. The RBI released the "Guidelines on Regulation of Payment Aggregators and Payment Gateways" in March 2020, which necessitates payment aggregators to store data only in India for unrestricted supervisory access by the RBI.

5. The Ministry of Communication and Information Technology introduced the "**National Cyber Security Policy**" in 2013, promoting a secure online environment, strengthening laws and early warning systems for cyberattacks, and aligning with organizational objectives and international standards.

6. Governance through **CERT-In**. **CERT-In** has been operational since January 2004, and its primary constituency is the Indian Cyber Community. **CERT-In** is a vital agency in India's e-commerce governance, providing cyber security services and coordinating incident response activities. **CERT-In** monitors cyberspace for cyberattacks. It gathers, analyses, and shares e-commerce cyber occurrences. **CERT-In** publishes recommendations, advisories, vulnerability notes, information security practises, procedures, incident prevention, response, and reporting to secure Indian e-commerce.

[1] https://www.kaggle.com/datasets/amritvirsinghx/cyber-crime-statewise?resource=download

Areas where the present cyber laws are lacking behind

Cyber law covers a wide range of issues, each critical to maintaining the integrity and security of the digital environment still there are some areas which needs to be addressed. The primary components include:-

Data Privacy and Protection : Data privacy is a critical concern in the digital age, yet India's cyber laws have struggled to address this issue effectively. Despite the increasing dependence on digital platforms, sensitive personal information of individuals remains vulnerable to breaches, misuse, and exploitation due to inadequacies in the existing legal framework. Although **the Digital Personal Data Protection Act, 2023**, was introduced, it is yet to be fully operational, leaving a significant gap in legal protection. The lack of a clear and enforceable data protection regime has left individuals' sensitive information at the mercy of private entities and cybercriminals.

India saw several data breaches in 2024. In September, millions of personal records, including medical details of Star Health Insurance customers, were leaked online. A UK-based researcher first reported the breach, with claims that a hacker named xenZen had accessed the data.

In July, personal information of around 7.9 million customers from Mumbai-based stockbroking firm Angel One was leaked, exposing sensitive details such as bank account numbers. Earlier, in January, a massive breach exposed 750 million individuals' personal data, including Aadhaar information, with the data being sold by threat actors online.[2]

Cybercrimes: Cybercrimes encompass a variety of illegal activities conducted via the internet, including hacking, identity theft, and online fraud. Laws like the Computer Fraud and Abuse Act (CFAA) aim to penalize such offenses and deter cybercriminal activities. Various new types of cybercrimes came into existence in the recent past.
In India digital arrest is a new problem which came into existence. A digital arrest scam is an online scheme designed to deceive victims and steal their hard-earned money. Scammers intimidate their targets by falsely accusing them of illegal activities and then pressure them into making payments under the threat of further consequences. In a digital arrest scam, fraudsters impersonate law enforcement officials, such as CBI agents, income tax officers, or customs officials, and contact victims via phone calls. They then persuade the victims to switch to video communication platforms like WhatsApp or Skype. Using intimidation tactics, the scammers issue fake digital arrest warrants, accusing the victims of offenses like financial fraud, tax evasion, or other legal violations. To make the scam appear credible, they may even stage a police station-like setup during the video call. Under the pretense of "clearing their name," "assisting with the investigation," or making a "refundable security deposit" to an escrow account, victims are pressured into transferring large amounts of money to designated bank accounts or UPI IDs. Once the payment is made, the scammers disappear, leaving the victims to deal with financial losses and potential identity theft. Indians lost **Rs 120.3 crore** in digital arrest scams alone in the first quarter of 2024, according to reports based on **Ministry of Home Affairs (MHA)** data.[3] This form of cyber fraud was one of the top categories of scams reported to the **Indian Cybercrime Coordination Centre** (I4C), which handles cybercrime complaints.

As per **India Today**[4] report, in 2023, online scams in India saw a rise and every other day, there were reports of people losing their hard-earned money to scammers. A lot of these scams were phishing attacks, which basically is the way scammers steal sensitive information like usernames, passwords, bank account information, etc by posing as a legitimate source such as the government, an organisation or a bank. According to a recentresearch conducted by Zscaler, a cloud security company with headquarters in California, India recorded 79 million phishing attacks in 2023.

Economically backward states like Jharkhand became epicenter of crimes like phishing attacks and the law as well as law enforcement agencies were simply not adequate enough to deal with the problem. Apart phishing and digital arrest crime there are several other types of cybercrime like cyber fraud, sexual harassment through internet and several others.
Intellectual Property Rights: With the proliferation of digital content, protecting intellectual property (IP) online has become crucial. Cyber law addresses issues related to copyright infringement, digital piracy, and the protection of trademarks and patents in the digital sphere.

[2] https://www.business-standard.com/finance/personal-finance/avg-data-breach-cost-hit-rs-19-cr-in-2024-16-indians-know-privacy-rights-124102300821_1.html
[3] https://indianexpress.com/article/india/indians-lost-rs-120-crore-in-digital-arrest-frauds-in-january-april-2024-9641952/

[4] https://www.indiatoday.in/technology/news/story/india-recorded-over-79-million-phishing-attacks-in-2023-new-study-suggests-2533497-2024-04-30

Under Section 79 of the Information Technology Act, 2000, Internet Service Providers (ISPs) or intermediaries hosting user-generated content are not held liable for any illegal activities conducted by users on their platforms, provided they have exercised due diligence. This protection is contingent upon compliance with Rule 3 of the Information Technology (Intermediaries Guidelines) Rules, 2011.

For instance:

1. If someone reposts your original videos on their YouTube channel without permission or proper attribution, it constitutes copyright infringement under Section 51 of the Copyright Act, 1957. Such reposting without authorization violates the rights of the original creator.
2. Similarly, if an audiobook version of a copyrighted book is illegally uploaded on YouTube without obtaining a proper license from the author, it also amounts to copyright infringement under Section 51 of the Copyright Act, 1957.

In cases where intellectual property rights are violated, the original creator has the right to seek legal remedies, including an injunction, damages, and compensation. They can also hold YouTube liable for streaming the infringing content. However, YouTube can avoid liability if it proves that:

- It was unaware of the infringement at the time it occurred.
- There were no reasonable grounds to suspect the work was copyrighted.
- The infringing content evaded YouTube's infringement-detection software due to editing or alterations.

In such scenarios, the creator may still be entitled to an injunction and claim a share of the profits generated by YouTube from the infringing content.

It is crucial for platforms like YouTube to demonstrate due diligence and take proactive measures to prevent copyright violations. This includes promptly addressing complaints and issuing DMCA Takedown Notices to individuals who upload copyrighted content without authorization. Failure to do so could result in liability and the obligation to compensate the original rights holders. This is just one of the many instances in which the intellectual property of an individual has been stolen.

E-commerce Regulations: As online transactions continue to grow, so does the need for legal frameworks governing e-commerce. These regulations ensure fair trading practices, consumer protection, and secure online payment systems. Cyber laws in India, primarily governed by the Information Technology Act, 2000 (IT Act), face significant limitations in effectively regulating the rapidly growing e-commerce sector. These limitations arise due to outdated provisions, the lack of comprehensive frameworks, and enforcement challenges in the dynamic e-commerce environment.

Challenges in Cyber Law Enforcement

Despite the development of comprehensive cyber laws, several challenges hinder their effective implementation:-

Jurisdictional Issues

The global nature of the internet complicates jurisdictional matters, as cybercrimes often cross national borders. Determining the applicable law and the appropriate forum for legal proceedings can be challenging. When any cybercrime arises, the preliminary issue arises is, where would be the jurisdiction of the police station to register the FIR. Then accordingly the case shall be adjudicated in the District Court concerned under which such police station comes.[5] The three new criminal laws has tried to minimise this problem up to some extent but still it is not enough to match with the problem.

[5] https://www.scconline.com/blog/post/2024/03/24/jurisdiction-in-cybercrimes-and-civil-disputes/

Rapid Technological Advancements

The fast pace of technological change often outstrips the ability of legal systems to adapt. Laws may quickly become outdated, necessitating continuous updates and revisions. Rapid technological advancements pose significant challenges to the implementation of cyber laws, as the fast pace of innovation often outstrips the ability of lawmakers and regulators to respond. Existing laws quickly become obsolete as new technologies like blockchain, cryptocurrency, artificial intelligence (AI), and the Internet of Things (IoT) introduce novel legal and ethical dilemmas. Regulatory lag, combined with the difficulty in anticipating the misuse of emerging technologies, creates gaps and loopholes that cybercriminals exploit. Enforcement agencies also face hurdles in tracking and prosecuting sophisticated cybercrimes, often lacking the tools and expertise required to deal with issues such as encrypted communication, ransomware, or AI-driven attacks. Additionally, balancing innovation with regulation is a constant struggle, as over-regulation may stifle progress, while under-regulation risks exploitation. Privacy concerns, the global disparity in technological readiness, and the absence of international consensus on standards further complicate enforcement and policymaking.

Balancing Privacy and Security

Balancing privacy and security is one of the most critical challenges in cyber law, as both are essential but often competing interests in the digital age. Privacy ensures individuals' right to control their personal information and safeguards against surveillance, while security focuses on protecting systems, networks, and data from cyber threats. The conflict arises when measures to enhance security, such as surveillance, data collection, or encryption backdoors, encroach on privacy rights. For instance, governments may seek access to encrypted communications to prevent cybercrimes or terrorism, but such access can weaken encryption standards, leaving users vulnerable to malicious attacks. Similarly, mass surveillance programs aimed at national security may violate citizens' fundamental rights to privacy. Cyber laws must carefully navigate this tension by creating frameworks that prioritize transparency, accountability, and proportionality. Solutions include adopting privacy-by-design principles, limiting data collection to what is necessary, ensuring judicial oversight for surveillance activities, and fostering international cooperation to establish global standards for data protection and cybersecurity. Striking this balance is essential to maintain trust in digital systems while ensuring robust protection against cyber threats.

Lack of International Consensus

Differing national laws and standards can create inconsistencies and conflicts in the enforcement of cyber laws. International cooperation and harmonization of legal frameworks are crucial to addressing these issues effectively. The lack of international consensus in cyber laws is a significant challenge in addressing global cyber threats, enforcing regulations, and protecting individuals and organizations in the interconnected digital landscape. Since cyberspace transcends national borders, harmonized legal frameworks and cooperative mechanisms are essential. However, differing national priorities, legal systems, and geopolitical tensions hinder the creation of a unified approach to cyber laws.

Conclusion

Cyber law is an evolving field that must continuously adapt to the dynamic digital landscape. While significant progress has been made in establishing regulatory frameworks, ongoing challenges require vigilant attention from lawmakers, legal practitioners, and international bodies. As technology continues to advance, cyber law will play a pivotal role in safeguarding the digital environment, protecting individual rights, and promoting secure and fair online interactions. Since the technology is always developing it is impossible for the laws to match with them and address the grievances of the people. My assessment is that the cyberlaws should not be strict and it should be flexible and adaptable with times and situation so that the enforcement agencies can implement it more efficiently.