HACKING LAWS: ALL YOU SHOULD KNOW ABOUT CYBER SECURITY LAWS

Srivathsan N, Sastra Deemed to be University

Bala Nivetha S, Sastra Deemed to be University

ABSTRACT:

"The internet is a double-edged sword, requiring careful regulation to balance privacy, security, and freedom, " which is quoted by Justice Mishra about cyber laws. The greatest threat to every company is cyber crime. The evolution of technology around the world also creates a room for crimes to be committed in that new area. The faster the technology grows, the larger the loophole to commit a crime using that also grows fast. The society as a whole adapted to the fast-changing technology, which also means that there should be a secure technology to use by the society, so the lawmakers have decided to frame laws according the changing technology. Since society depends on technology, a law should be made regarding its direction and control. Currently in INDIA, there are several instances where cyber crime occurs and many people have also ended their lives due to that. In a layman's language, the definition of cyber crimes is the criminal activities that involve the use of computers, digital services, or the internet to commit offences such as hacking, identity theft, fraud, cyber stalking, etc. In 2024, India witnessed a surge in cybercrime, with over 740, 000 cases reported to the Indian Cyber Crime Coordination Centre (I4C) in the first four months alone, and roughly 85% of these reports related to online financial fraud[1]. The important statutory measure taken by the government of India was the IT Act, 2000, and a few more acts after that. This paper revolves around the cyber laws in INDIA, mainly the IT Act, 2000, its objectives and its amendments, how it had evolved, and the relationship between the BNS law and cyber laws was explained briefly. and this paper also throws light on the current issue in cyber laws and the daily challenges faced by the society regarding cyber laws.

[1]https://www.statista.com/statistics/1499739/india-cyber-crime-cases-reported-to-i4c/#:~:text=Over%20740%2C000%20cases%20of%20cyber, on%20the%20rise%20ever%20since

I. INTRODUCTION

Cyber laws in India were framed to control the cyber crimes that are committed using a computer, mobile phone, the internet, etc. However, the IT Act of 2000 did not define cyber crimes properly, but the offences under cyber crimes like hacking and identity theft have a provision under the statute. Referring to the Oxford Dictionary, "*cyber crimes refer to the criminal activities carried out by means of computers or the internet ".* The first case about cyber crime is Yahoo v. Akash Arora (1999)[2], the first case after IT Act 2000 has been passed, was about cyberstalking, which is reported in 2001. In today's digital age, where technology is deeply integrated into our daily lives, the need for legal frameworks to regulate cyberspace has become more critical than ever. Cyber laws refer to the rules and regulations that govern digital interactions, ensuring the security, privacy, and rights of individuals and organizations online. These laws help combat cybercrimes such as hacking, identity theft, financial fraud, cyberbullying, and data breaches.

II. HISTORY OF CYBER LAWS

1. Introduction of the IT Act 2000

The Act was drafted based on the UNCITRAL Model Law on E-Commerce (1996).

The Ministry of Information Technology prepared the IT Bill, 1999, to provide legal recognition to electronic transactions and regulate cyber activities. The IT Bill, 1999, was introduced in the Lok Sabha (Lower House of Parliament) on December 16, 1999. The Bill was discussed, debated, and approved by the Lok Sabha on May 9, 2000. It was then passed by the Rajya Sabha (Upper House) on May 17, 2000. After being passed by both Houses of Parliament, it was sent to the President of India for approval. President K.R. Narayanan gave his assent on June 9, 2000.The Act was notified and came into effect on October 17, 2000It was referred to a Standing Committee for review and suggestions. India adopted the principles of UNCITRAL's Model Law on E-Commerce to provide legal recognition to electronic transactions. The Indian government, under the Ministry of Information Technology, drafted the **IT Bill** to regulate cyber activities. The bill was finalised by a group of officials headed by the then Minister of Information Technology, Pramod Mahajan. It finally came into effect on

[2] 1999IIAD (DELHI)229, 78 (1999)DLT285

October 17, imposing restrictions on all individuals regardless of their nationality and geographic location.

2. Introduction of the IT Act 2008 (AMENDMENT to IT Act, 2000)

The Information Technology (Amendment) Act, 2008 was enacted to address emerging issues related to **cyber security, data protection, and electronic governance**. The amendment aimed to strengthen the existing legal framework established by the Information Technology Act, 2000, by introducing new provisions to combat cybercrimes, enhance privacy protections, and regulate intermediaries. The bill was introduced in both houses of Parliament. The Lok Sabha (House of the People) and the Rajya Sabha (Council of States) both need to consider the bill. The bill was read for the first time in each house, and its objectives were discussed. Detailed examination, debate, and discussion took place. Members of Parliament could propose amendments. The bill was referred to a parliamentary committee for further scrutiny. The committee examined the bill clause by clause and submitted its report. The bill was read for the third time, and a final discussion took place. Members voted on the bill in its final form. Both houses of Parliament passed the bill. If there were disagreements between the two houses, a joint sitting could be called to resolve them. After being passed by both houses, the bill was sent to the President of India for assent. Once the President gave assent, the bill became an act. The Information Technology (Amendment) Act, 2008 was passed by the Lok Sabha on December 22, 2008, and by the Rajya Sabha on December 23, 2008. It received the President's assent on February 5, 2009, and was published in the official gazette. The Information Technology (Amendment) Act, 2008 received assent from **President Pratibha Patil** on February 5, 2009.

3. Introduction of DPDPA Act

The Digital Personal Data Protection Act (DPDPA) was formed to address the growing concerns about data privacy and security in India's rapidly expanding digital economy. The Ministry of Electronics and Information Technology (MeitY) released the first draft of the Data Protection Bill in 2018. This draft underwent public consultation and was revised in 2019 and 2021. In 2022, the government introduced the Digital Personal Data Protection (DPDP) Bill, 2022, which was further revised to become the DPDP Bill, 2023. The revised DPDP Bill, 2023, was approved by the cabinet on July 5, 2023. The DPDP Bill was introduced in the Lok Sabha (the lower house of Parliament) on August 3, 2023. The bill was passed by the Lok Sabha on

August 7, 2023, and by the Rajya Sabha (the upper house) on August 9, 2023. The bill received the assent of the President of India on August 11, 2023, and was published in the Official Gazette, becoming the Digital Personal Data Protection Act, 2023. On January 3, 2025, the Ministry of Electronics and Information Technology released the draft Digital Personal Data Protection Rules, 2025, for public consultation to operationalize the provisions of the Act. The Digital Personal Data Protection Act, 2023, received assent from **President Droupadi Murmu** on August 11, 2023.

4. Information Technology Rules

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 were formed by the **Ministry of Electronics and Information Technology (MeitY)** of the Government of India. These rules were issued under the powers conferred by the Information Technology Act, 2000. The rules were introduced to regulate social media platforms, digital news publishers, and other intermediaries to ensure a safer and more accountable digital environment in India. The process began with the drafting of the rules by MeitY, building on the previous Intermediary Guidelines Rules, 2011, and incorporating feedback from various stakeholders. The draft rules were released for public consultation to gather feedback from stakeholders, including industry experts, civil society, and the general public. Based on the feedback received, the draft rules were revised to address concerns and suggestions from various stakeholders. The revised rules were reviewed and approved by the relevant authorities within the Ministry of Electronics and Information Technology. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 were officially notified on February 25, 2021, and published in the Official Gazette of India. The rules came into effect immediately upon their publication in the Official Gazette. Here, they do not require presidential assent.

III. Objective of IT Act 2000

Over the past decade, the rise of technology and electronic commerce has led to a surge in cybercrimes and data-related offences in India. As per the latest news by a renowned paper house, the cybercrime cases increased from 3, 693 in 2012 to 65, 893 in 2022, recording the highest spike rate. The situation became alarming as even data crucial to national security and integrity was at risk. In response, the government opted to regulate activities on electronic mediums and the data stored therein. Thus, the Information Technology Act or IT Act 2000 was

introduced. It was formulated to ensure the lawful conduct of digital transactions and the reduction of cyber crimes, on the basis of the United Nations Model Law on Electronic Commerce 1996 (UNCITRAL Model).

1. Promote efficient delivery of government services electronically or facilitate digital transactions between firms and regular individuals.

2. Impose penalties upon cybercrimes like data theft, identity theft, cyberstalking and so on, in order to create a secure cyber landscape

3. Formulate rules and regulations that monitor the cyber activity and electronic mediums of communication and commerce

4. Promote the expansion and foster innovation and entrepreneurship in the Indian IT/ITES sector.

Features of IT Act 2000

1. The Central Government implements the provisions of this Act to regulate electronic commerce and penalise cybercrime.

2. The Act states the roles and responsibilities of intermediaries as well as conditions under which their liability can be exempted.

3. The Information Technology Act is associated with CERT-In (Indian Computer Emergency Response Team), a nodal agency that is responsible for cybersecurity and cyber incident response.

4. There have been 2 amendments associated with this Act, addressing the technological advancements, implementability concerns and anomalies.

Achievement of IT Act

1. Legal Recognition of Digital Transactions: The IT Act provides legal recognition to electronic records, digital signatures, and online contracts, making e-commerce and electronic governance (e-governance) more streamlined.

2. Cybersecurity and Cybercrime Regulation: The Act establishes provisions to address and penalize cybercrimes such as hacking, identity theft, data breaches, and other forms of misuse of technology.

3. Facilitation of E-Governance: The Act has boosted e-governance initiatives by legitimizing electronic communication, filings, and digital certifications between citizens and government agencies.

4. Encouraging E-Commerce Growth: By legitimizing electronic transactions, the IT Act has been instrumental in promoting the growth of the e-commerce sector in India.

5. Data Protection Framework: The Act lays the foundation for securely handling sensitive personal data, making businesses and organizations accountable for data breaches.

6. International Recognition: The Act aligns with global standards, encouraging foreign investments in the IT and digital sectors in India.

IV. CHALLENGES FACED IN INDIA

The major challenges in cybercrime are the rapid technology developments, the difficulty in tracking and identifying the cybercriminals and the investigation process. A brief hurdle that the cyber security has faced is as follows,

- **Technology**

Cyber criminal on the internet use their sophisticated tools to attack the victim on the internet as technology develops and fosters the infrastructure, on the other hand, it also acts as a loophole for cyber criminals to take advantage of their criminal acts. Ransomware, where criminals encrypt data and demand payment for its release, still remains a significant threat. Phishing, where criminals use deceptive emails or websites to steal personal information, it is still prevalent in India.

- **Legal and regulatory challenges**

The existing laws presented in India might not adequately address the cybercrime, and it finds difficult to address the rapidly growing criminal acts in the internet and also coming to the

jurisdiction it is difficult to find the jurisdiction because the internet flows beyond boundaries. There is a need to create awareness and training for the law agencies and authorities as well as public on cyber crime prevention and response.

- **Weak data protection and privacy laws**

India lacks a proper data protection law, though Digital personal data protection act, is a step made by the government yet it is not fully developed. Thus, there is absence off clear regulations on cross-border data and lack of alignment with global laws like GDPR and also no legal framework for data localization and protection of critical digital assets.

- **Poor implementation and enforcement**

The cyber crime is generally an more technical act where easy tracking or any simple steps to find the accused is not enough for the executive sector to tackle the problem. The laws in India also lack proper legislation to cover up the growing cybercrime acts. As well as the law enforcement agencies often lack cyber forensic expertise and technical training and cyber cases take years to resolve due to judicial delays and lack of specialized cyber courts and the low conviction rate discourages victims from reporting cybercrimes.

- **Regulation in emerging technologies**

The recent AI platforms like AI& deepfakes serves a new platform to commit criminal acts and in such a way there is no legal provision to tackle AI-driven misinformation and fraud, similarly the cloud computing and IoT security, there was no clear rules on who is liable for security breaches in cloud services and internet of things devices. And coming to the social media regulation the current laws fail to effectively control hate speech, fake news, and cyberbullying.

- **Weak legal framework for cyber terrorism and espionage**

The IT Act, 2000, under section 66f, defines cyber terrorism, but it is not comprehensive in dealing with state-sponsored cyberattacks and cross-border digital warfare. There is lack of legal clarity on how to handle nation-state actors, cyber warfare and cyber espionage by foreign entities and India’s defense and intelligence agencies lack a well-defines legal mandate for offensive cybersecurity operations

- **Other challenges**

The minimum necessary eligibility to join the police doesn't include any knowledge of the computer sector, so cybercrime and the promotion of research and development in ICTs is not up to the mark. Security forces and law enforcement are not equipped to address high-tecb crimes.

v. IMPORTANT PROVISONS IN IT ACT, 2000

India's Information Technology Act, 2000 (IT Act) is the primary law governing cybersecurity, digital transactions, electronic governance and cybercrimes. Here are some key provisions:

A) LEGAL RECOGNITION OF ELECTRONIC RECORDS AND SIGNATURES

Sec 4: recognizes electronic records as equivalent to physical records

Sec 5: grants legal validity to digital signatures for authentication

Sec 6: enables government agencies to accept electronic forms and filings

B) CYBER OFFENSES AND PENALTIES

Sec 43: impose penalties for unauthorized access, damage to computer systems, and data theft (civil liability)

Sec 66: defines hacking and identity theft, prescribing punishment (up to 3 years imprisonment and a fine)

Sec 66a (struck down in 2015): criminalized offensive online content but was misused and declared unconstitutional.

Sec 66 b: punishment for dishonestly receiving stolen computer resources (up to 3 years jail, Rs 1 lakh fine).

Sec 66c: punishment for identity theft, including password and electronic signature misuse (3 years jail, Rs. 1 lakh fine)

Sec 66d: punishment for cheating using computer resources, including online frauds (3 years jail, Rs. 1 lakh fine)

Sec 66: punishment for capturing and publishing private images without consent (up to 3 years jail, Rs.2 Lakh fine)

C) CYBER TERRORISM AND NATIONAL SECURITY

Sec 66f: Defines cyber terrorism (e.g. hacking government networks, disrupting critical infrastructure). Punishment: life imprisonment.

Sec 69: empowers the government to intercept, monitor, and decrypt digital communication for security reasons.

Sec 69a: authorizes the government to block public access to any online content (used to ban Chinese apps like Tiktok).

Sec 69b: allows the government agencies to monitor and collect traffic data for cybersecurity purposes.

D) DATA PROTECTION AND PRIVACY

Sec 72: Penalises unauthorized disclosure of personal data by government officials (2 years jail, Rs.1 lakh fine)

Sec 72a: punishment for disclosing personal information in breach of a lawful contract

Sec 43a: imposes liability on companies for failing to protect sensitive personal data.

E) Cyber pornography and online harassment

Sec 67: punishment for publishing obscene content online (up to 3 years jail, Rs 5 lakh fine)

Sec 67a: punishment for publishing sexually explicit content (up to 5 years jail, Rs 10 lakh fine)

Sec 67b: punishment for child pornography (up to 7 years jail, Rs 10 lakh fine)

Sec 67c: mandates data retention by online service providers for investigation purposes.

F) CYBER FRAUD AND FINANCIAL CRIMES

Sec 74: punishment for digital signature fraud

Sec 75: IT act applies to offenses committed outside India, if they impact Indian systems.

Sec 79: grants intermediary liability protection (e.g. social media platforms) but requires compliance with government regulations.

G) ADJUDICATION AND CYBER APPELLATE TRIBUNAL

Sec 46: allows adjudication of cyber crimes and violations under the IT Act.

Sec 47-50: establishes the cyber appellate tribunal (now merged with TDSAT)

These provisions form the backbone of India's cyber laws and are critical for regulating online activities, ensuring cyber security, and punishing cybercrimes. However, the IT act needs amendments to address emerging threats like AI- driven crimes, ransomware and deepfake technology.

VI. LANDMARK CASES

Shreya Singhal V UOI (2015) - AIR 2015 SC 1523

This case challenged the constitutionality of SEC 66A of the IT ACT, 2000 which penalized sending offensive messages through communication services. The supreme court struck down SEC66 A, ruling it unconstitutional for violating the right to freedom of speech and expression under ART 19 (1) a of the constitution.

Yahoo! Inc v Akash Arora and Anr (1999) - 78 (1999) DLT 285

In this case, Yahoo! Inc. sued Akash Arora for operating a website named 'Yahoo India!' which was deceptively similar to Yahoo!'s trademark. The Delhi High Court granted an injunction against Akash Arora, recognizing the principle of passing off in cyberspace and emphasizing the need to protect domain names as trademarks.

CBI v Arif Azim (Sony Sambandh Case) - (2008) 105 DLT 769

Arif Azim was accused of fraudulently ordering Sony products using stolen credit card information through the Sony Sambandh website. The Delhi High Court held him liable under Section 418 of the Indian Penal Code for cheating and Section 66 of the IT Act for hacking.

Tata Sons Limited V Greenpeace International (2011) - 178 (2011) DLT 705

Tata Sons filed a case against Greenpeace for hosting an online game that allegedly infringed on Tata's trademark. The Delhi High Court ruled in favor of Greenpeace, highlighting the balance between trademark rights and freedom of expression in the digital domain.

These cases have significantly contributed to the evolution of cyber law in India, addressing issues ranging from online freedom of speech to intellectual property rights in cyberspace.

VI. CONCLUSION

This paper concludes that there is rapid growth in cyber criminal acts and lesser development in cybersecurity laws. The legislation should be made capable of covering up emerging criminal acts, and proper training must be given to the legal authorities as well as the public. The online platforms promoting to cyber crimes should be revisited and shut down. Public online platforms should be made restricted to the level, and the act of unauthorized access in encrypting data from the online resources should be reduced through various legislations.

Considering the landmark cases like Sheryal Singhal, it is to be observed that India lacks proper legislation in covering cybersecurity laws.

To strengthen this, India should modernize the act to include the emerging threats and implement a robust data protection framework aligning with global standards like GDPR. Improve law enforcement capabilities with cyber forensic expertise, , and enhance international cooperation for tackling cross-border cybercrimes.

Thus a holistic cyber security strategy combining legislation, enforcement, technology, and awareness is essential to protect India’s digital infrastructure and ensure cyber resilience in the face of evolving threats.