INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

CYBER CRIME UNDER THE INFORMATION-TECHNOLOGY ACT: A NATIONAL PERSPECTIVE

AUTHORED BY - PIYUSH GUPTA

Abstract

The rise of digital technologies and increased dependence on the internet have fundamentally changed the Indian society, commerce, and governance. While digital growth has catalysed progress in all aspects, there has been a corresponding evolution of a complex view of criminal activity generally referred to as cybercrime.

In response to the widespread use of the Internet and the concomitant issues regarding cyber-infractions, **The Information Technology Act, 2000**, has been put in place to offer guidance towards the widespread use of the Internet as well as enunciate the countervailing measures to cyber crimes: protection of information, regulation of electronic transactions, and prosecution of various cyber crimes.

This paper seeks to analyze the programs available to combat cyber crime from a distinctively India perspective: considering various objectives of the IT Act, and its judicial amendments and interpretations. This paper also evaluates the extent to which the actual cyber laws in India and the amendments are relevant and effective in light of the fact that the cyber threat environment continues to change.

Keywords: IT Act, Cyber Crime, Data Protection, Law Enforcement, Digital, Privacy, Internet, Electronic transaction, Cyber Terrorism, Fraud.

1. Introduction

India has been transformed into a digitally advanced nation whereby the use of the Internet as a communication tool, as a means of doing business, and as a means of accessing information has been revolutionized. With the growing use of the Internet, India is faced with unprecedented, rapidly changing, and highly innovative computer- and Internet-based criminal acts. These crimes pose a threat to the continued existence, economic well-being, and personal security of the individual.

The Information Technology Act, 2000, was landmark legislation established to give legal

ISSN: 2582-6433

recognition to transactions conducted through electronic data interchange and for the facilitation of the electronic filing of documents with Government agencies. Most importantly, it sought to address the problem of cybercrime, which was in its relative infancy then. The IT Act was based on UNCITRAL Model Law on Electronic Commerce, 1996.

The paper has looked at the legal architecture built around cybercrime by the IT Act from a national perspective. It has discussed the types of cyber offences made punishable under the Act, their corresponding punishments, and the changes that have taken place in the form of its subsequent amendments. It has discussed the application of the Acts provisions through an analysis of rulings by the judiciary, as well as the growth of the contours of Cyber jurisprudence in India.

2. The Legislative Framework: The Information Technology Act, 2000

The IT Act, 2000 is the India's one of the important legislations that address offence related to cybercrime and e-commerce. It gives a legal framework which govern electronic transactions, protect digital data, and combat a wide array of cyber offences. The IT Act also provides extra-territorial jurisdiction, and so, it can also be applied to any offence committed outside India by any person, if the act involves a computer, computer system, or computer network located in India.

2.1 Key Provisions Related to Cybercrime

The Information Technology Act has defined and imposed punishment for various cybercrimes and has provided a dual remedy, civil as well as criminal. Some of them are as follows:

A. Civil Wrongs

- **Sec. 43:** Damage to a Computer, Computer System, etc. - The section refers to certain unauthorized conduct such as gaining access to a computer or a system or securing access to a computer system, downloading information, copying data, introducing or implanting a computer virus or contaminant, and causing interruption to a computer system. - In such cases civil liability has been prescribed.

B. Criminal Offences under the Act

• **Section 65:** It states about is about Document Fraud relating to computer source documents. Destruction, alteration, or concealment of computer source documents that are required to be kept under law is punishable.

• **Section 66:** This section deals with Computer Related Offences. It is a segment of the law that imposes penalties on any act described in section 43 of the IT Act when such actions are

ISSN: 2582-6433

done with dishonest or fraudulent intent.

• **Section 66B:** This section penalizes the act of dishonestly receiving or retaining any stolen computer resource or communication device.

• **Section 66C:** This section provides a punishment for using electronically, fraudulently, or dishonestly any specific identifying features of another person such as that person's password, electronic signature, or any other form of identification that is uniquely theirs.

• **Section 66D:** Punishment for Cheating by Personation by using Computer Resource: This section penalizes cheating by personation through any communication device or computer resource.

• **Section 66E:** This Explains Violation of Privacy and its Consequence Portions of this section covers **cyber voyeurism** encompassing the illegal of capturing and/or displaying or transmitting the private images of any person`s unclothed private body portions without consent.

• **Section 66F:** Punishment of Cyber Terrorism This describes a serious offense under the Act, and such acts are done with the intention of threatening the People of India and/or the the unity, the territorial integrity, and/or security, or sovereignty of the country and/or to intimidate the population. Punishment for such offenses may be life imprisonment.

• **Section 67:** Punishment of Publishing or Transmitting of Obscene Material through Electronic Means. This section concerns the illegal dissemination of obscene and/or disgusting materials and/or disgusting materials and/or horrific content through the Internet and prescribes serious punitive consequences. This section prescribes serious punitive consequences.

• **Section 67A:** Punishment of the Publishing or Transmitting of Material in Electronic Form of Sexually Explicit Conduct,or of Such Conduct.

• **Section 67B:** Punishment for Publishing or Transmitting of Material Depicting Children in Sexually Explicit Acts, etc. in Electronic Form.

This part addresses child pornography. Suggests severe penalties, for offenders as these are serious crimes.

2.2 The Information Technology (Amendment) Act, 2008

In 2008 the IT Act underwent modifications to tackle the changing and advancing characteristics of cyber threats. This revision introduced new crimes including cyber terrorism along with additional data protection measures. It also included the debated Section 66A, which penalized the communication of offensive messages via communication services. However,

ISSN: 2582-6433

the Supreme Court of India in the case of **Shreya Singhal v. Union of India**[1] declared this section void and held it unconstitutional and infringing upon the right, to freedom of speech and expression.

3. The Evolving Landscape of Cybercrime in India: A National Perspective

In India, even with the cyberspace IT Act, cybercrime is on the rise and is expected to continue this surge in coming years. The scope of crime alone, has a wide financial net including fraud, and other forms of gain. The IT Act has no provisions for the scope of crime.

3.1 Trends in Cybercrime

Data provided by National Crime Record Bureau and others like the NCRB show a startling rise in reported cyber incidents over the years. As per the absence of any other data, the main features of the rise in cybercrime are assumed to be:

- **Financial Frauds:** Many reports state over 40% of cyber fraud is in the cyberspace payment banking. Fraud is via psyching users, and misleading fraud alerts, debits, and password fraud in blocked accounts
- **Social Media Crimes**: With the rise of users and the sharing of personal information of users socially and it is social breach of state and abuse of net for unlassed networks.
- **Data Breaches:** Unauthorized access, to government databases resulting in the exposure of sensitive personal and financial data has become a significant concern.
- **Ransomware Attacks:** hese attacks involve software that restricts access, to computer systems until a ransom is paid. Such attacks are becoming more common.
- **Cyber Terrorism:** Terrorist groups exploiting the internet for enlistment spreading propaganda and organizing assaults has become a danger, to national safety.

3.2 Challenges in Investigation and Prosecution

Law enforcement agencies, in India face obstacles when attempting to investigate and prosecute cybercrime cases efficiently. A few of these include:

• **Jurisdictional Issues:** A growing number of cyber fraud work from nations complicating efforts to identify a specific wrongdoer.

• **Lack of Technical Expertise:** Law enforcement need to undergo trainings as they are not well prepared to handle the swiftly advancing technologies and the cybercriminals who take

[1] (2015) 5 SCC 1

ISSN: 2582-6433

advantage of them.

• **Collection and Admissibility of Electronic Evidence:** Electronic evidence requires particular care in its collection and preservation, and this care is neither easily obtained nor easily accomplished.

• **Public Awareness:** Lack of awareness with respect to online safety makes people vulnerable to all sorts of cybercrime and cyberattacks.

4. The Role of the Judiciary

The Indian judiciary has been, and continues, to interpret the provisions of the IT Act, and, thus, the Indian judiciary is shaping the future of the virtual world. In the case of **Shreya Singhal v. Union of India**[2], the Supreme Court of India safeguarded IT and the right to free speech and expression in the cyberscape by disabling Section 66A of the IT Act. The courts have enunciated other principles of great importance concerning the admissibility of electronic evidence, which is vital for the prosecution of the cybercrime.

5. The Way Forward: Development of India's Cybersecurity Framework

Cybersecurity is a multidimensional challenge, which will require a well-composed strategy in legislation, technology, and cooperation in the private and the public domains

5.1 Legislative and Policy Recommendations

• **Periodic review and amendment of IT Act:** The IT Act necessitates a timeline for routine assessments and updates, to the IT/cyber laws; without this the Act will become outdated.

• **Data Protection Legislation:** The legal structure of a data protection Act must be legislated to protect the citizens from data breaches. Significant progress has been made in drafting the Data Protection Act, marked by the establishment of the Digital Personal Data Protection Act.

• **Strengthening International Cooperation:** To thoroughly examine and address cybercrimes spanning countries increased cooperation, with international partners is essential.

• **Specialized Cybercrime Courts:** The establishment of specialized courts for the adjudication of cybercrime cases will undoubtedly aid in their expeditious trial.

5.2 Technological and Infrastructural Improvements

• **Capacity Building of Law Enforcement Agencies:** There is a need for continual

[2] (2015) 5 SCC 1

ISSN: 2582-6433

improvement in training and equipping law enforcement agencies with cybercrime

- **Indigenous Cybersecurity Solution Development:** The development of indigenous solutions to sustain threats in cyberspace will emerge as a result of research and development focused on cyber security.
- **Critical Information Infrastructure Protection:** There must be a coordinated effort to protect the country's critical information infrastructure from cyber-attacks.

6. Landmark Judgments and Judicial Interpretation

The impact of the Indian judiciary on the interpretation of the provisions of the IT Act and the creation of the legal scope of cybercrime in the country is immense. The scope of the law and its applicability to the different offenses has been shaped by different landmark decisions.

- **Shreya Singhal v. Union of India (2015**): One of the most important decisions is the Supreme Court of India decision that removed Section 66A of the IT Act, which made it a crime to send 'offensive' messages via any channel of communication. The Court viewed the provision as unconstitutionally vague, as it restricted, and violated one's freedom of speech and expression. The Supreme Court's decision in this case has become the basis of the protection of individuals holding civil liberties in the digital space.[3]
- **Anvar P.V. v. [4]P.K. Basheer**: The Supreme Court explained in 2014 the procedure for the admissibility of electronic evidence under Section 65B of the Indian Evidence Act. The Court also clarified that electronic records produced as documents must accompany a certificate for such documents to be accepted as evidence, which would further enhance the proof of cybercrimes in court.
- **Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)[5]:** Although primarily a case on the right to privacy, this has developed to be a very important case concerning cybercrime as well. By virtue of the right to privacy having been declared a fundamental right, the court further supported the requirements for more rigorous legislation on the unauthorized access of data and online monitoring.
- **National Association of Software and Service Companies v. Ajay Sood & Others (2005)[6]:** In this case, the Delhi High Court held that 'phishing' which takes place on the

[3] (2015) 5 SCC 1
[4] (2014) 10 SCC 473
[5] (2017) 10 SCC 1
[6] 119 (2005) DLT 596

ISSN: 2582-6433

internet is legal. It is internet fraud by a person assuming a different identity to gain the personal information of a user, which the court was referring to as phishing.

7. Conclusion

Cybercrime is a threat put differently every day and so is the potential growth of the economy and the welfare of the citizens of India. Some basic guidelines were put in place with the Information Technology Act of 2000. However, even this legislation cyberspace is a level of complexity that demands a responsive and proactive to close the security gaps. In the pursuit of strategies to attain a knowledge of safe and secure cyberspace, the appropriate balance will come from efficient legislation, technological enhancement, and cooperation at the international level, coupled with awareness among the public. There is no doubt that the effort to achieve a cyber secure India is going to be the result of the collective work of the public, private counterparts, the law enforcement arm, and the government.