 DOI: *https://doij.org/10.10000/IJLSI.111687*

INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 5 | Issue 5

2023

Cybersecurity in India

ANUBHAV UPADHYAY[1] AND DR. SHIVA UPADHYAY[2]

ABSTRACT

The advent of computer technology has improved human existence in many ways, including its precision, speed, and efficiency. Crime committed via computers presents a significant barrier to the advancement of any nation. Due to the exponential expansion of online criminal activity, it is almost impossible to escape the incorporation of cyber security into our everyday lives. People often focus their attention on the many techniques and technologies that may be utilized to thwart online criminal activity. This article places an emphasis on the legal response to cyber security and centers its attention on the significance of having laws against cybercrime as a means of directly attaining cyber security goals from an Indian perspective.

Keywords: *Cybercrime, cyber law, cyber security, information, communication, internet technology, hacking.*

I. INTRODUCTION

The concept of cybercrime has reached mainstream awareness at this point. Insecurity due to crime severely slows a nation's progress. It slows down the country's economic progress and has negative effects on society as a whole. The advancement of computer technology has improved and facilitated human existence. Accuracy, speed, and efficacy are all improved as a result. The computer is used illegally by criminals, though, and this results in cybercrime. India passed the Information Technology Act,2000 in an effort to prevent cybercrime; the legislation was heavily revised in 2008 to make it more effective. An example of cybercrime is the destruction, modification, interception, concealment, or fabrication of digital information. Because of the global proliferation of information and communication technology, cybercrime has become an international problem (ICTs). Everyone on Earth has felt its effects. If the computer is being used as either a weapon or an object, the conduct is illegal. There has been a persistent push to classify various forms of cybercrime and identify and prevent them in detail. In recent years, cybercrime has emerged as one of the most serious challenges facing all facets of business and society that rely on information technology. Sadly, not all businesses appear to be particularly vigilant in their efforts to identify, handle, and defend against such

[1] Author is a student at Campus Law Centre, University of Delhi, India.
[2] Author is a Professor at Swami Shraddhanand College, University of Delhi, India.

 [ISSN 2581-9453]

dangers.

II. JUDICIAL PRONOUNCEMENTS

- **Tampering with computer source code** - The Andhra Pradesh High Court ruled in *Syed Asifuddin v. the State of Andhra Pradesh*[3] that a mobile phone is a computer both under common use and under the definitions established by the IT Act. Each service provider is responsible for tracking its own unique System Identification Code and assigning a unique identification number to each instrument used to access the service. Accordingly, section 65 of the IT Act applies whenever the Electronic Serial Number (ESN) is changed.
- **Hacking** - The accused in *State of Andhra Pradesh v. Prabhakar Sampath*[4] was found guilty of hacking the complainant company's systems in violation of Section 43(a)[5] read with Section 66[6] of the IT Act. The prosecution had no trouble whatsoever establishing the defendant's guilt. The court ruled that the defendant deserved a harsh sentence since research papers are the result of extensive investigation by trained professionals.
- **Identity theft and cheating by personation** - In *NASSCOM v. Ajay Sood*[7], the defendant posed as the plaintiff in an attempt to phish for sensitive information at a number of different email accounts. Phishing has been ruled to be both a criminal activity and a security risk by the Court. The court also noted that no anti-phishing laws existed in India. According to Indian law, phishing occurs when an online merchant makes a fraudulent representation about the email's origin or sender. This would be a form of passivity as well.
- **Obscenity and Pornography** - After hearing arguments in *Maqbool Fida Hussain v. Raj Kumar Pandey*[8], the Court also made it clear that the criminal justice system is not an instrument that may be abused to violate the rights of individuals, particularly in the creative industries. The judiciary has an inherent responsibility to safeguard fundamental liberties for all citizens.
- In contrast, the accused in *State of Tamil Nadu v. Suhas Katti* utilised the complainant's identity to join pornographic Yahoo groups and upload explicit material there. Because she rejected him as a potential husband, he did this to ruin her name. The offender was found

[3] Syed Asifuddin v. State of Andhra Pradesh, 2005 SCC AP 1100
[4] State of Andhra Pradesh v. Prabhakar Sampath, 1986 AIR 210
[5] Information Technology Act, 2000, § 43(a), No. 21, Acts of Parliament, 2000
[6] Information Technology Act, 2000, § 66, No. 21, Acts of Parliament, 2000
[7] NASSCOM v. Ajay Sood, 119 (2005) DLT 596
[8] MF Hussain v. Raj kumar pandey, 2008 CrLJ 4107

 [ISSN 2581-9453]

guilty of violating Code of Criminal Procedure Articles 469[9] and 509[10] and Information Technology Act Section 67[11] beyond a reasonable doubt.

- **Violation of intellectual property in cyberspace** - The court ruled in the case of *My Space Inc. v. Super Cassettes Industries Ltd* that sections 79[12] and 81[13] of the IT Act, as well as section 51(a)(ii) of the Copyright Act, must be interpreted consistently with one another. A copyright intermediary can still use the safe harbour affirmative defence, provided the addendum to section 81 does not exclude it. In the case of intermediaries, specific expertise is more important than broad familiarity. Furthermore, obligation on an intermediary requires the requirements set out in section 79 of the IT Act to be met.

III. COMPARATIVE STUDY

Our courts—from district courts to the Supreme Court—have seen several cybercrime cases, some of which startled the nation. Cybercrime is spreading due to technology developments. Courts have repeatedly allowed this extension. Various judicial judgements in India involving cybercrimes show that the courts' hands are constrained. Courts must guarantee that people's individual rights aren't harmed. The Court can't replace the legislature, though. It can only rule based on current laws and how they apply to each instance.

NASSCOM v Ajay Sood acknowledged phishing as a cybercrime but found no applicable legislation. When the matter of jurisdiction arose in Maqbool Fida Hussain, the Court could only hope the legislature would fix it. The World Wrestling Entertainment case[xxi] was decided based on the Indian Contract Act.

In the *Air Force Bal Bharti School case*, a 16-year-old kid was arrested for violating IT Act section 67. Since then, courts have clarified that the IT Act and IPC have the same obscenity standard. Theft, fraud, and cheating, among others, have the same elements in the IPC and IT Act when done online. Since 2000's Information Technology Act, cybercrime judicial rulings have improved. In Syed Asifuddin, the Court recognised mobile phones as computer systems under the IT Act, preserving cell phone manufactures' copyright on source code. This judgement was in line with the Act and fast-changing technology. Many saw Shreya Singhal's case as a win. Section 66A of the IT Act was ruled illegal by India's Supreme Court. It stopped internet abuse based on people's opinions/comments.

[9] Information Technology Act, 2000, § 469, No. 21, Acts of Parliament, 2000
[10] Information Technology Act, 2000, § 509, No. 21, Acts of Parliament, 2000
[11] Information Technology Act, 2000, § 67, No. 21, Acts of Parliament, 2000
[12] Information Technology Act, 2000, § 79, No. 21, Acts of Parliament, 2000
[13] Information Technology Act, 2000, § 81, No. 21, Acts of Parliament, 2000

 [ISSN 2581-9453]

The Court has been interpreting and upholding the law. The Court depends on the government and legislature to implement its decisions.

IV. CRITICAL ANALYSIS

- Cybercrime fails traditional investigating methods. Increasing ICT use requires new investigating tools. Cybercrime investigation, prosecution, and trial should involve particular technological skills.
- Choose Jurisdiction is another challenge for the judiciary when dealing with cybercrimes. Cybercrime is global. Determining jurisdiction in such a specific offence is difficult for the criminal justice system. Cybercrime jurisdiction is another UN priority. Even the Indian government acknowledges that deciding cyber jurisdiction is a difficulty for the judiciary. The Supreme Court has ordered the government to build an unified cybercrime reporting system.
- No law protecting online individual rights. IT Act 2000 protects women online. In 2008, Indian lawmakers modified IT Act 2000, however new cybercrime isn't included. Which causes complications for cyber courts.
- Criminal justice drafted national policy and instructed the Indian legislature to reclassify the cyber code.
- Lack of technology equipment, trained staff, and infrastructure hinders judicial processes. In 2017, the Indian parliament reformed cybercrime training and recommended a central organisation.
- There is a mismatch between emerging cybercrime technologies and old criminal justice system expertise. There are no legal procedural rules for new cyber offences and no particular criminal legislation. During cyber trial, judges confronted several trial and judgement challenges.

V. CONCLUSION

Cybercrimes are on the rise, and they are a global problem that may impact everyone. New forms of cybercrime appear to pop up alongside each new technological development. The government and the courts have a shared obligation to keep the criminal justice system current so that it can effectively combat emerging forms of crime and the migration of traditional crimes to the digital realm. The Indian courts must strictly adhere to the letter of the law and may not exceed the authority granted to them by the country's constitution.

 [ISSN 2581-9453]

VI. REFERENCES

- SCC Online
- Jstor
- Manupatra
- LexisNexis
- AIR Online
- EBC Reader
- Sage Journals

*****