INTERNATIONAL RESEARCH JOURNAL OF MANAGEMENT SOCIOLOGY & HUMANITIES

ISSN 2277 – 9809 (online)
ISSN 2348 - 9359 (Print)

An Internationally Indexed Peer Reviewed & Refereed Journal

www.IRJMSH.com
www.isarasolutions.com

Published by iSaRa Solutions

CYBER CRIME AND IMPORTANT JUDICIAL DECISIONS: AN EVOLVING LEGAL LANDSCAPE

Prof. Dr. Ratna R. Bharamgoudar

* Professor of Law, Dean, Karnataka State Law University, Hubballi, Karnataka and Director, KSLU's Law School.

Abstract

The increasing rise in cyber crime in the digital age creates significant challenges for law enforcement and the judiciary. The legislative domain is responsible for policy-making, but judicial decisions provide critical insights about how cyber laws, especially the Information Technology Act of 2000 and other relevant laws, work in the real world. The courts have always upheld constitutional protections, especially Article 19(1)(a) of the Indian Constitution, which protects the right to free speech and expression, even in the digital world. This paper analyses the judicial response to cyber crime in India, emphasizing essential legal principles, case law, and the dynamic interpretation of laws within cyberspace. The paper emphasizes the intricacies of cyber crime by examining landmark cases, addressing jurisdictional challenges, evidence collection difficulties, and the liability of Internet Service Providers (ISPs). It also discusses the limitations of the current legal frame work especially when it comes to cyber crimes that happen across borders. The paper concludes that the judiciary has played a crucial role in bringing legal principles up to date for the digital age. However, more changes are needed to make the legal system better able to deal with the ever-changing nature of cyber crime.

Keywords: Cyber crime, Cyberspace, Information Technology Act, Intermediary liability, Digital platforms.

I Introduction

The rapid advancement of information and communication technology has fundamentally transformed the manner in which individuals, businesses, and governments interact. The internet, digital platforms, and electronic communication systems have created unprecedented opportunities for economic growth, innovation, and social connectivity. However, this digital revolution has also given rise to a new category of criminal activity commonly referred to as *cyber crime.* Cyber crime poses a serious challenge to legal systems worldwide, as offenses committed in cyberspace transcend traditional geographical boundaries, complicate investigation, and demand constant adaptation of legal frameworks[1]. In India, the exponential growth in internet, digital payments, e-governance initiatives, and social media usage has made the country both a global digital leader and a vulnerable target for cyber criminal activities. Cyber crime encompasses a wide range of unlawful acts committed using computers, computer

networks, or digital devices as tools, targets, or places of criminal activity. These offenses include hacking, identity theft, online fraud, cyber stalking, data breaches, and dissemination of obscene or defamatory content, ransomware attacks, and financial scams, among others. Unlike conventional crimes, cyber offenses are often anonymous, technologically complex, and capable of causing widespread harm within a short span of time. The consequences of cyber crime extend beyond financial losses, affecting national security, individual privacy, freedom of expression, and public trust in digital systems. Cyber crime is the most dangerous of all crimes because of the magnitude of the loss it is causing today, the ease with which it is committed; its visibility and the disregard of geographical boundaries; the difficulty in investigation, collection of evidence and the successful prosecution of the cyber criminal[2].

Nature of Cyber Crime

Cyber crime refers to unlawful acts committed through the use of computers, computer systems, digital devices, or the internet, where the computer may function as a tool, target, or place of crime. The nature of cyber crime is fundamentally distinct from conventional offenses due to its technological foundation, transnational reach, and intangible form of harm. Unlike traditional crimes involving physical acts or property, cyber crimes are largely intangible[3]. The harm caused such as data theft, identity fraud, or privacy invasion often occurs in virtual space without physical contact. Digital assets like data, passwords, and online identities are the primary targets. Cyber crimes are inherently border less. An offense may be committed in one country, executed through servers in another, and cause harm in multiple jurisdictions simultaneously. This transnational character creates serious challenges relating to jurisdiction, investigation, extradition, and enforcement[4].

Perpetrators of cyber crime often operate anonymously using fake identities, encrypted networks, VPNs, or the dark web. This anonymity makes identification of offenders difficult, attribution of criminal intent complex and prosecution and conviction rates low. Cyber crimes evolve rapidly with advancements in technology. New forms such as Phishing, Ransomware, Crypto fraud, Deepfake misuse, AI-enabled cyber attacks emerge faster than legislative responses, making cyber crime a dynamic and adaptive form of criminal activity[5]. Cyber crimes can be committed instantaneously and on a massive scale. A single malicious act can affect thousands of individuals, multiple organizations and entire financial or communication systems. This scalability distinguishes cyber crime from traditional offences.

Cyber crimes may have individual victims (identity theft, cyber stalking), corporate victims (data breaches, industrial espionage), Government victims (cyber terrorism, attacks on critical infrastructure). Often, a single cyber offense affects all three simultaneously. The nature of cyber crime heavily depends on electronic evidence, such as Emails, Log files, IP addresses, Digital transactions. Such evidence is fragile, easily alterable, and requires technical expertise for collection and preservation. Cyber crimes may attract Civil liability (compensation for data loss or damage) and also Criminal liability (imprisonment and fines).This dual nature is reflected in cyber law frameworks that combine compensatory and punitive mechanisms[6].

Cyber crimes directly affect Right to privacy[7], Freedom of speech and expression[8], Right to reputation[9], Right to property[10] (digital assets).Hence, cyber crime is not merely a technological issue but a constitutional and human rights concern. Beyond individual harm, cyber crimes threaten economic stability, digital trust, national security and democratic processes. Cyber terrorism and attacks on critical infrastructure highlight the strategic dimension of cyber crime. The nature of cyber crime is complex, evolving, borderless, and technology-driven. Its intangible form, anonymity of offenders, reliance on electronic evidence, and wide-ranging impact distinguish it from conventional criminal activity[11]. Addressing cyber crime therefore requires not only legal regulation but also technological preparedness, international cooperation, and continuous judicial interpretation.

Cyber Crime Regulation in India

Although the Constitution of India does not explicitly refer to cyber crime, several provisions form its constitutional basis. The interpretation of Article 21 by the Supreme Court of India has expanded its scope to include the right to privacy, data protection and informational autonomy[12]. The recognition of privacy as a fundamental right has profound implications for cyber surveillance, data breaches, and online profiling. Online speech enjoys constitutional protection, subject to reasonable restrictions under Article 19(2). The regulation of online content, social media platforms, and intermediaries must conform to constitutional limitations[13].

The Information Technology Act, 2000 (IT Act) is the cornerstone of cyber law in India. Enacted to give legal recognition to electronic records and digital signatures, it also introduced penal provisions for cyber offenses. The objectives of the IT Act are to facilitation of e-commerce and e-governance, legal recognition of electronic records and prevention and punishment of cyber offenses[14]. Section 43 imposes civil liability for unauthorized access, data damage, virus introduction, and denial of access. Compensation may extend to damages suffered by the affected party[15]. Criminal offenses under the IT Act key penal provisions include Section 65 - Tampering with computer source code, Section 66 - Computer-related offenses, Section 66C - Identity theft, Section 66D Cheating by personation using computer resources, Section 66E -Violation of privacy, Section 66F - Cyber terrorism. Sections 67, 67A, and 67B criminalize publication or transmission of obscene content, sexually explicit material, and child sexual abuse material in electronic form. The Information Technology (Amendment) Act, 2008 significantly strengthened the IT Act by expanding the definition of cyber offenses, introducing cyber terrorism and identity theft and enhancing government powers for interception and monitoring. This amendment marked a shift from a facilitative law to a security-oriented framework[16].

The Indian Penal Code 1860 (IPC) supplemented the IT Act by addressing cyber crimes through conventional offenses: Sections 419 & 420 – Cheating and impersonation, Sections 463–471 – Forgery of electronic records, Section 354D – Cyber stalking and Sections 499–500 – Online defamation. The concurrent application of IPC and IT Act ensures comprehensive criminal liability. Regarding procedural framework the Code of Criminal Procedure 1973(Cr

PC) governs investigation, prosecution, and trial of cyber offences. Key procedural aspects include registration of FIR, including zero FIR, search and seizure of electronic devices and jurisdiction in transnational cyber crimes. The lack of territorial constraints in cyber offenses poses jurisdictional challenges for law enforcement agencies[17]. The Indian Evidence Act 1872 was amended to accommodate electronic evidence. Electronic records are admissible subject to compliance with Section 65B certification requirements. Section 45A recognizes the opinion of digital forensic experts, enhancing the evidentiary value of electronic data. Under Section 79 of the IT Act intermediaries enjoy safe harbor protection, provided they observe due diligence and do not actively participate in unlawful acts.

IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 impose obligations on intermediaries relating to content moderation, Grievance redressal and traceability of originators. The enactment of the Digital Personal Data Protection Act, 2023 represents a significant advancement in India's cyber legal framework. The Act regulates collection and processing of personal data, imposes penalties for data breaches and strengthens individual data rights. It complements the IT Act by addressing data- centric cyber risks[18]. India has established specialized institutions such as Cyber Crime Police Stations, Indian Cyber Crime Coordination Centre (I4C) and CERT –In for incident response. These institutions play a critical role in prevention, investigation, and awareness.

India's response to cyber crime, primarily anchored in the Information Technology Act, 2000, represents a significant legislative effort to regulate activities in cyberspace. The Act has provided legal recognition to electronic records and digital signatures, criminalized various forms of cyber misconduct, and established mechanisms for adjudication and enforcement. Complementary provisions under general criminal law now consolidated under the Bharatiya Nyaya Sanhita, 2023 (BNS), Bharatiya Nagarik Suraksha Sanhita (BNSS), and Bharatiya Sakshya Adhiniyam (BSA), which displaced the existing Indian Penal Code (IPC), the Criminal Procedure Code (CrPC), and the Indian Evidence Act, respectively have further strengthened the prosecution of cyber enabled offenses such as cheating, forgery, identity theft, and online harassment. Together, these laws form the backbone of India's cyber crime regulatory framework.

Comparative Perspective: India and International Legal Frameworks

Cyber crime is inherently transnational, often involving perpetrators, victims, servers, and data located in multiple jurisdictions. Domestic cyber laws, therefore, cannot function in isolation. A comparative study of international cyber law frameworks helps evaluate the adequacy of India's legal regime, identify global best practices, and address
gaps relating to jurisdiction, data protection, intermediary liability, and enforcement mechanisms.

The United States follows a sectoral and offense-specific approach to cyber crime regulation. The principal statute is the Computer Fraud and Abuse Act (CFAA), 1986, which criminalizes unauthorized access to protected computers, data theft, and cyber fraud. The key

features broad definition of "protected computer", severe criminal penalties and strong federal investigative powers (FBI, Secret Service).With regard to data protection approach unlike India and the EU, the US does not have a comprehensive data protection statute. Instead, it relies on sector-specific laws Gramm-Leach-Bliley Act 1999[19](GLBA), Health Insurance Portability and Accountability Act 1996[20] (HIPAA) , Federal Trade Commission (FTC) enforcement and State-level privacy laws (e.g., California Consumer Privacy Act)[21]. India's recognition of privacy as a fundamental right provides stronger constitutional safeguards than the US framework, though enforcement remains weaker.

The UK's Computer Misuse Act, 1990 (CMA) criminalizes unauthorized access to computer material, unauthorized acts with intent to impair systems and acts causing serious damage to national security or economy. The Act has been periodically up dated to address ransomware and cyber terrorism. With regard to data protection regime UK follows the UK GDPR, mirroring the European Union's data protection standards even after Brexit. UK law demonstrates better legislative clarity and judicial oversight, where as India relies heavily on delegated legislation (Rules)[22].

European Union (EU) adopts a harmonized approach through directive on attacks against information systems and national cyber crime laws aligned with EU directives. General Data Protection Regulation (GDPR)[23] is considered the gold standard of data protection globally. Key principles include lawful, fair, and transparent processing, purpose limitation and data minimization, Strong consent requirements and heavy penalties for data breaches. India's Digital Personal Data Protection Act, 2023 (DPDP) is business-friendly but comparatively weaker on individual rights and regulatory independence[24].

The Budapest Convention on Cybercrime, 2001[25] is the first international treaty addressing Cyber offenses, Electronic evidence and International cooperation. It facilitates cross-border data access, mutual legal assistance and standardization of cyber crime definitions. The treaty had three prime objectives, including the improvement in investigative techniques, increase in the cooperation among nations, and lastly, harmonizing national laws. Apart from these, the participating countries needed to embrace legislation outlawing specified cyber-related crimes along with several definite evidence-gathering rules. The Council of Europe drew it in Strasbourg, France, and 64 countries that endorsed the Budapest Convention on cyber crime. These countries include Canada, Japan, the Philippines, South Africa, the United States, and others. Some of the significant cyber offenses that the Budapest Convention attended include illegal access, data interference, illegal interception, misuse of devices, system interference, cyber fraud, cyber forgery, offenses in child pornography, and offenses concerning neighboring rights and copyright. India is not a signatory to the Convention, citing concerns over sovereignty, data access without domestic control and limited participation of developing nations in drafting. Its impact on India is that non-participation restricts speedy cross-border investigations and access to international cooperation mechanisms.

However, India advocates for a UN-led cyber crime convention, emphasizing inclusivity and sovereign equality.

In comparative evaluation, strengths of India's Framework are Constitutional recognition of digital privacy, Comprehensive legislation covering cyber crime and data protection and Judicial safeguards against over-criminalization[26]. Its weaknesses include absence of binding international cyber crime treaty, enforcement and technical capacity gaps, over-dependence on executive rule-making and limited protection against state surveillance. India can strengthen its cyber law framework by adopting GDPR-inspired individual data rights, enhancing independence of data protection authorities, joining or aligning with international cyber cooperation frameworks and investing in cyber forensics. The comparative analysis reveals that while India has made significant progress in cyber crime regulation, it lags behind developed jurisdictions in enforcement efficiency, international cooperation, and regulatory independence[27]. A balanced approach borrowing global best practices while preserving constitutional values is essential for addressing the evolving challenges of cyber crime in a digitally interconnected world.

Landmark Judicial Decisions

Shreya Singhal v. Union of India

The decision in Shreya Singhal v. Union of India[28] is a landmark judgment in Indian cyber law and constitutional jurisprudence. It is most renowned for striking down Section 66A of the Information Technology Act, 2000 as unconstitutional. The judgment firmly established that fundamental rights apply with full force in cyberspace, particularly the right to freedom of speech and expression under Article 19(1)(a) of the Constitution of India. The case arose from widespread arrests under Section 66A of the IT Act for posting content on social media platforms such as Facebook and Twitter. A notable incident involved the arrest of two young women in Maharashtra for a Facebook post questioning the shutdown of Mumbai following the death of a political leader. Similar arrests across India highlighted systematic misuse of Section 66A. Shreya Singhal, a law student, filed a writ petition under Article 32 challenging the constitutional validity of Section 66A of the IT Act, Section 69A (blocking of websites) and Section 79 and the Intermediary Guidelines Rules, 2011.

The petitioners contended that Section 66A was vague, overbroad, and arbitrary and contained undefined expressions like annoyance and grossly offensive lacked objective standards. The provision created a chilling effect on free speech and enabled selective and arbitrary enforcement by police authorities. Mere discussion or advocacy was criminalized, contrary to constitutional principles. The arguments of the Union of India were that the provision was necessary to maintain public order. The internet had greater potential for misuse than traditional media. Section 66A fell within the scope of reasonable restrictions under Article 19(2).Safeguards existed through police discretion and judicial oversight[29].

The Supreme Court held that Section 66A was unconstitutionally vague. The Court observed none of the expressions used in Section 66A were defined. What may be "offensive" to one person may not be offensive to another. Vague laws fail to provide clear guidance and invite arbitrary enforcement. The Court relied on the doctrine that vagueness in penal law violates Article 14 (equality before law).The Court held that Section 66A criminalized

Innocent speech, Legitimate criticism, Satire, parody, and dissent. This resulted in a chilling effect on free speech, where citizens self-censor due to fear of prosecution. The Court drew a crucial distinction between discussion, advocacy and incitement. Only incitement can be restricted under Article 19(2). Section 66A punished even discussion and advocacy, which are constitutionally protected[30].

The Court held that "Mere annoyance or inconvenience cannot be grounds for restricting speech." The Court rejected the State's argument that Section 66A maintained public order, stating there must be a direct and proximate link between speech and public disorder just remote or hypothetical connections are insufficient. Section 66A of the IT Act was struck down in its entirety as unconstitutional. Section 69A (blocking of websites) was upheld due to adequate procedural safeguards. Section 79 (intermediary liability) was upheld but read down to protect intermediaries unless they fail to act upon lawful court or government orders[31].

The significance of the judgment is that it ended criminalization of vague online speech, prevented misuse of cyber law against political dissent and strengthened digital civil liberties. While the judgment is widely celebrated, critics argue that striking down Section 66A left a regulatory vacuum. Online abuse and misinformation remain serious concerns. However, the Court clarified that existing penal laws (IPC provisions on defamation, hate speech, incitement to violence) are sufficient if properly enforced. Shreya Singhal v. Union of India stands as a constitutional milestone in the digital age. The judgment reaffirmed that the internet is not a lawless space, but neither is it a space where constitutional freedoms can be diluted. By striking down Section 66A, the Supreme Court protected the essence of free speech and ensured that democracy thrives even in cyberspace.

Suhas Katti v. State of Tamil Nadu

Suhas Katti v. State of Tamil Nadu[32] is a landmark case in Indian cyber law as it represents one of the first successful convictions under the Information Technology Act, 2000. The case is particularly significant for recognizing cyber harassment as a punishable offense and for establishing the admissibility of electronic evidence in criminal trials. The judgment demonstrated the Indian judiciary's early commitment to addressing crimes committed in cyberspace. The accused, Suhas Katti, was known to the complainant, a woman who had earlier rejected his marriage proposal. Following this rejection, the accused began harassing her through the internet by posting obscene, defamatory, and vulgar messages about her on a Yahoo message group; creating false email accounts in her name; publishing her personal details, including her phone number, inviting strangers to contact her. As a result, the complainant received numerous obscene calls and messages, causing mental harassment and reputation harm. She lodged a complaint with the cyber crime cell in Chennai.

The accused was charged under the Information Technology Act, 2000, Section 67, Publishing or transmitting obscene material in electronic form, Indian Penal Code, 1890 Sec~~tion 469, Forgery for t~~he purpose of harming reputation and Section 509, word, gesture, or act intended to insult the modesty of a woman. The prosecution argued that the accused deliberately used digital platforms to harass and defame the complainant. Electronic evidence

including emails, chat logs, and website postings clearly established the accused's involvement. Certified electronic records satisfied the legal requirements under the Evidence Act. The conduct of the accused amounted to cyber stalking and harassment, warranting strict punishment. The defense contended that the accused had been falsely implicated. Electronic evidence could be manipulated and was unreliable. The prosecution failed to conclusively prove authorship of the online messages. The Court rejected the defense arguments and held the accused guilty under all charged provisions[33].

The Court accepted electronic records such as emails and message board postings as valid evidence. It recognized that digital records, when properly authenticated, are reliable and legally admissible. The Court found that the accused acted with clear intent to harass and defame the complainant, satisfying the requirement of mens rea. The Court affirmed that offenses committed using electronic means can attract liability under both the IT Act and IPC simultaneously. The accused was sentenced to Rigorous imprisonment for two years and fine under Section 67 of the IT Act and Imprisonment under IPC Sections 469 and 509 (sentences to run concurrently)[34]. This was one of the earliest custodial sentences imposed for a cyber crime in India.

The judgment has been widely praised for its progressive approach. However, certain limitations remain that the case was decided at the trial court level and lacks appellate- level jurisprudence. Subsequent cases required clearer statutory guidance on electronic evidence, later addressed through amendments and judicial interpretation. Despite these limitations, the case laid the foundation for future cyber crime jurisprudence in India. *Suhas Katti v. State of Tamil Nadu* stands as a pioneering judgment in Indian cyber law. It established that cyber space is not beyond the reach of criminal law and that digital harassment is a serious offense deserving strict punishment. The case marked a turning point in recognizing cyber crimes as real, harmful, and legally actionable, thereby strengthening the rule of law in the digital era.

Avnish Bajaj v. State (NCT of Delhi)

The decision in *Avnish Bajaj v. State (NCT of Delhi)*[35] is a landmark judgment on intermediary liability in India. The case arose in the early phase of e-commerce and addressed a crucial legal question: To what extent can an online platform and its executives be held criminally liable for illegal content uploaded by users? This case laid the groundwork for the doctrine of safe harbor for intermediaries, later codified and strengthened under Section 79 of the Information Technology Act, 2000.

Bazee.com was an online auction platform that allowed users to list and sell products. In 2004, a user uploaded a listing advertising an obscene video clip involving minors. Although the video was not hosted on Bazee's servers, the platform facilitated the listing and payment mechanism. The Delhi Police arrested Avnish Bajaj, the Managing Director of Bazee.com, alleging that he was responsible for allowing the circulation of obscene material. The accused was charged under Section 67 of the IT Act, 2000 (publishing or transmitting obscene material

in electronic form), Section 292 of the IPC (sale of obscene material), Section 294 of the IPC (obscene acts and songs)[36].

The prosecution argued that Bazee.com provided a platform that facilitated the sale of obscene material. The payment gateway and listing approval process amounted to "publication". The Managing Director had a duty to ensure that illegal content was not circulated. Failure to prevent such listings constituted negligence and criminal liability[37].The defense contended that Bazee.com was merely an intermediary, not the creator or publisher of content. The obscene material was uploaded by a third party without the knowledge of the company. There was no mens rea on the part of Avnish Bajaj. Holding intermediaries liable would cripple internet-based businesses and free expression. The IT Act envisages limited liability for intermediaries acting in goodfaith[38].

The Delhi High Court adopted a balanced approach and held that Section 292 IPC (sale of obscene material) could not be directly applied because Bazee.com did not physically sell or possess the obscene material. The platform only provided an electronic space for users. However, the Court held that Section 67 of the IT Act could be attracted because the platform facilitated access to obscene material, adequate content monitoring mechanisms were not in place. The Court allowed prosecution under the IT Act to continue but emphasized that mere designation as CEO does not automatically attract criminal liability[39]. The matter later reached the Supreme Court, which granted relief to Avnish Bajaj by emphasizing that criminal liability requires proof of mens rea and observing that an intermediary cannot be punished solely due to his position recognizing the need for safe harbor protection for intermediaries acting without knowledge[40].This judicial reasoning significantly influenced later amendments to the IT Act.

The case highlighted the absence of clear statutory protection for intermediaries at the time. It directly contributed to strengthening Section 79 of the IT Act, which now grants safe harbor to intermediaries who exercise due diligence. Courts acknowledged that traditional criminal law concepts must be adapted to digital realities and distinguished between publisher, intermediary, and user roles. *Avnish Bajaj v. State (NCT of Delhi)* represents a crucial milestone in the evolution of intermediary liability in India. The case underscored that while cyber space must be regulated to prevent misuse, innovation and freedom of expression cannot be stifled by imposing blanket criminal liability on digital intermediaries. The judgment ultimately paved the way for a more balanced and technology-friendly cyber law regime, ensuring accountability without undermining the growth of the internet economy.

Google India Pvt. Ltd. v .Visaka Industries Ltd.

The judgment in *Google India Pvt. Ltd. v. Visaka Industries Ltd.*[41] is a significant Supreme Court ruling on intermediary liability, defamation in cyberspace, and the interpretation of Section 79 of the Information Technology Act, 2000. The case clarified whether internet intermediaries, such as Google, can be held criminally liable for defamatory content posted by third-party users on their platforms. This decision plays a crucial role in shaping India's approach to free speech, platform responsibility, and digital governance. Visaka Industries Ltd., a manufacturing company, alleged that defamatory content had been published against it

on an online platform (Google Groups). The content was allegedly posted by a third party and was accessible through Google's services. Visaka filed a criminal complaint alleging defamation under the Indian Penal Code against the author of the defamatory content, and Google India Pvt. Ltd., claiming it was responsible as the platform hosting the content. Google India challenged the proceedings, arguing that it was merely an intermediary and not the publisher or author of the content.

Arguments by Google India were that it was merely an intermediary, not the creator or publisher of content. It did not exercise editorial control over user-generated content. Section 79 of the IT Act grants safe harbor to intermediaries. Criminal liability cannot be imposed without mens rea .Proceeding against intermediaries would have a chilling effect on free speech and digital innovation. Visaka Industries contended that Google provided the platform and enabled dissemination of defamatory material. Failure to proactively remove defamatory content amounted to negligence. Intermediaries should not escape liability when harm is caused through their platforms. Safe harbor protection should not apply to criminal defamation[42].

The Supreme Court partly allowed Google India's appeal and laid down important principles. The Court held that an intermediary cannot be equated with a publisher merely because content is hosted on its platform. Criminal defamation requires active participation or knowledge. The Court clarified that Section 79 provides conditional immunity to intermediaries. Safe harbor applies unless the intermediary initiates the transmission, selects the receiver, or modifies the information. Intermediary liability arises only if due diligence is not followed after receiving lawful notice[43].The Court emphasized criminal liability requires strict proof of mens rea. Mere hosting of content does not satisfy criminal intent. Criminal defamation proceedings against intermediaries must be examined cautiously. The Supreme Court observed that dragging intermediaries into criminal trials without prima facie evidence is unjust. Courts must prevent misuse of criminal law against digital platforms. Criminal proceedings against Google India Pvt. Ltd. were set aside. The Court reaffirmed that intermediaries enjoy safe harbor protection under Section 79. Liability may arise only upon failure to comply with lawful take down obligations[44]. *Google India Pvt. Ltd. v. Visaka Industries Ltd.* is a cornerstone judgment in intermediary liability jurisprudence. It reaffirmed that intermediaries are facilitators, not publishers, and that criminal liability must be based on clear intent and participation. Together with *Shreya Singhal* and *Avnish Bajaj*, this case forms the judicial backbone of India's cyber law framework.

Conclusion

The exponential growth of digital technology has profoundly reshaped contemporary society, redefining communication, commerce, governance, and personal interaction. While this transformation has generated immense benefits, it has simultaneously exposed individuals, institutions, and the State to sophisticated forms of cyber crime. In India, where digital adoption has accelerated rapidly through initiatives such as digital banking, e-governance, and online platforms, cyber crime has emerged as a serious and persistent threat. The increasing

frequency, complexity, and transnational nature of cyber offenses underscore the urgent need for a robust, adaptive, and rights-oriented legal framework.

The judiciary has played a crucial and proactive role in shaping cyber jurisprudence in India. Through landmark decisions the courts have reaffirmed the primacy of constitutional values in the digital domain, particularly the protection of freedom of speech and expression, personal liberty, and privacy. Judicial interpretation has also clarified issues related to intermediary liability, electronic evidence, and due process, ensuring that technological regulation does not become a tool for arbitrary State control. These judgments reflect the judiciary's commitment to maintaining a delicate balance between effective cyber crime control and the preservation of fundamental rights.

Despite these legislative and judicial advancements, significant challenges remain. The rapid pace of technological innovation continues to outstrip the capacity of existing laws, creating regulatory gaps that cyber criminals readily exploit. Issues such as cross- border jurisdiction, anonymity of offenders, difficulties in collecting and preserving electronic evidence, and limited technical expertise among law enforcement agencies hinder effective investigation and prosecution. Furthermore, low conviction rates in cyber crime cases highlight systemic weaknesses in enforcement, procedural delays, and inadequate digital forensic infrastructure.

In conclusion, India has made commendable progress in developing a comprehensive legal and judicial framework to address cyber crime. However, cyber law must remain dynamic, forward-looking, and responsive to emerging technological realities. Strengthening enforcement mechanisms, enhancing digital literacy, investing in cyber forensic capabilities, and fostering collaboration between domestic and international agencies are essential for ensuring effective cyber crime prevention and justice delivery. A balanced approach that integrates technological advancement with constitutional safeguards will be vital in securing India's digital future and reinforcing public confidence in the rule of law in cyberspace.

****

References

1 R. Sharma, & A. Gupta, 'Cybercrime Trends in India: A Decade Analysis' (2019) 15 (3) Journal of Cyber Security, 245-267.

2 S. Menon, 'Behavioral Profiling of Cyber Criminal sin India' (2020) 8 (2) International Journal of Digital Crime, 112-134.

3 Arati Shah, 'Cybercrime Chronicles: Exploring the Evolving Landscape of Challenges in the Digital Era.'(2024) 7 A Global Journal of Humanities, 20-24

4 Amit Singh & Praveen Singh Chauhan, 'Navigating Digital Legislation: A Comprehensive Analysis Of India's IT Act And Emerging Cyber Security Challenges' (2023) 29 (4) Computer Integrated Manufacturing Systems,297–321.

5 Supra note2

6 Iqbal,J., & Beigh, B.M. 'Cybercrime in India: Trends and Challenges' (2017) 6 (12) International Journal of Innovations & Advancement in Computer Science, 187–196.

7 Constitution of India, Article 21

8 Constitution of India, Article19 (1) (a)

9 Supra note7
10 Ibid.
11 Ishan Atrey, 'Cybercrime and its Legal Implications: Analysing the Challenges and Legal Frameworks Surrounding Cybercrime, Including Issues Related to Jurisdiction, Privacy, and Digital Evidence' (2023) International Journal of Research and Analytical Reviews.
12 Justice K.S .Puttaswamyv. Union of India, (2017)10 SCC 1.
13 Shreya Singhal v. Union of India, (2015) 5 SCC 1.
14 Vikas Asawat, 'Information Technology (Amendment) Act, 2008: A New Vision through a New Change' (2010) available at ssrn. https://doi.org/10.2139/ssrn.1680152.
15 Information Technology Act, 2000, § 43.
16 Amlan Mohanty, 'New Crimes under the Information Technology (Amendment) Act' (2011) 7 Indian Journal of Law and Technology, 103
17 N. Desai, 'Cyber Crime and Legal Control in India' (2020) 47 (1) Indian Bar Review, 63
18 Amal Chandra C, 'Strengthening India's Cyber Security and Data Privacy Landscape: A Comprehensive Overview' (2024) 70 Indian Journal of Public Administration, 466–478.
19 Gramm-Leach-Bliley Act 1999 sometimes called the Financial Modernization Act, is a federal law that regulates financial institutions' use and disclosure of their customers 'NPI (nonpublic personal information). GLBA defines NPI as "any information received by a financial institution that is not public. Usually, this refers to "personally identifiable financial information. This includes, but is not limited to: social security numbers, credit history, income data, credit card numbers, bank account numbers, addresses, phone numbers, and names.
20 Health Insurance Portability and Accountability Act 1996 is a federal law protecting sensitive patient health information from unauthorized disclosure. Enacted to modernize the healthcare industry, it sets national standards for protecting Protected Health Information (PHI) held by "covered entities" (doctors, hospitals, insurers). It includes Privacy and Security Rules for handling health data.
21 C. Campbell, 'A Review of Data Protection Regulations and the Right to Privacy: The Case of the US and India' (2021) Manohar Parrikar Institute for Defence Studies and Analysis.
22 D. M. Ekadshi, 'Comparative Analysis of Cyber Security Laws of India, United States, and United Kingdom' (2023) 9 International Journal of Law 88–91.
23 The General Data Protection Regulation (GDPR) is a comprehensive EU law, effective May 25, 2018, that mandates strict data privacy and security standards for handling personal data of individuals in the EU/EEA. It grants individuals greater control over their data, requires transparent processing, and imposes heavy fines on global organizations for non-compliance.
24 P. Sharma, 'Comparative Study of GDPR and India's Draft Data Protection Bill' (2019) 27 (1) International Journal of Law and Information Technology,
25 Council of Europe, Convention on Cybercrime (2001) (Budapest Convention).Primarily known as the Council of Europe Convention on Cybercrime, the Budapest Convention or the convention on cyber crime is the world's first international treaty designed to focus on increasing cyber crime. It came Into the picture in 2001 and entered into force on July 1, 2004.
26 Priya Nair, 'Comparative Cybercrime Frameworks: BRICS Perspective'(2022) 12(1) Global Cyber Law Journal,156-178.
27 Supra note 16
28 Shreya Singhal v. Union of India, (2015) 5 SCC 1
29Ibid.
30Ibid. 31Ibid.
32Suhas Katti v. State of Tamil Nadu (CCNo.4680of 2004)
33Ibid. 34Ibid.
35Avnish Bajaj v. State (NCT of Delhi) (2005) 3 Comp L J 364 Del
36Ibid.
37Ibid.
38 Ibid.

39 Ibid.
40 Ibid.
41 Google India Pvt. Ltd. v. Visaka Industries Ltd. (2020) 4 SCC 162
42 Ibid.
43Ibid. 44Ibid.

भारतीय भाषा, शिक्षा, साहित्य एवं शोध

ISSN 2321 – 9726

WWW.BHARTIYASHODH.COM

INTERNATIONAL RESEARCH JOURNAL OF MANAGEMENT SCIENCE & TECHNOLOGY

ISSN – 2250 – 1959 (0) 2348 – 9367 (P)

WWW.IRJMST.COM

INTERNATIONAL RESEARCH JOURNAL OF COMMERCE, ARTS AND SCIENCE

ISSN 2319 – 9202

WWW.CASIRJ.COM

INTERNATIONAL RESEARCH JOURNAL OF MANAGEMENT SOCIOLOGY & HUMANITIES

ISSN 2277 – 9809 (0) 2348 - 9359 (P)

WWW.IRJMSH.COM

INTERNATIONAL RESEARCH JOURNAL OF SCIENCE ENGINEERING AND TECHNOLOGY

ISSN 2454-3195 (online)

WWW.RJSET.COM

INTEGRATED RESEARCH JOURNAL OF MANAGEMENT, SCIENCE AND INNOVATION

ISSN 2582-5445

WWW.IRJMSI.COM

JOURNAL OF LEGAL STUDIES,POLITICS AND ECONOMICS RESEARCH

WWW.JLPER.COM