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IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines.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 All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice.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 STALKING, TROLLING, AND ONLINE HARASSMENT: LEGAL PROTECTION OF WOMEN IN CYBERSPACE UNDER INDIA'S NEW CRIMINAL LAWS

SEMINAR PAPER

Submitted To

CHHATRAPATI SHAHU JI MAHARAJ UNIVERSITY, KANPUR

In the partial fulfillment of the requirements for the award of the degree of

BACHELOR OF ARTS AND BACHELOR OF LEGISLATIVE LAW

(Session: 2021 - 2026)

Submitted by

STUTI SINGH

Roll No :- 21137000055

Under Guidance & Supervision of :

Ms. Meghna Bajpai Assistant Professor

ATAL BIHARI VAJPAYEE SCHOOL OF LEGAL STUDIES

CHHATRAPATI SHAHU JI MAHARAJ UNIVERSITY, KANPUR

ISSN: 2582-6433

ABSTRACT

The rise of digital technology has changed the way we communicate, conduct business, and govern ourselves. It has also led to an increase in cybercrime, especially targeting women. This paper seeks to analyze the loopholes in India's cybersecurity law, with particular emphasis on the Information Technology Act, 2000, as well as the newly introduced Bharatiya Nyaya Sanhita, 2023, Bharatiya Nagarik Suraksha Sanhita, 2023, and Bharatiya Sakshya Adhiniyam, 2023. Some of the issues highlighted in the study include outdated laws, insufficient punishment for violations, lack of proper implementation, insufficient technical know-how, and management of electronic evidence.

The study further discusses the issue of fragmented institutions, cross-jurisdictional issues with cybercrimes across borders, and the ongoing dilemma regarding cybersecurity versus fundamental rights. By comparing international practices from countries such as the USA, European Union, UK, and Australia, the paper highlights best practices for electronic evidence management and cybercrime prosecution.

The study reveals that although there have been some recent efforts in the form of legislation, there still exist certain shortcomings in the current legal system of India. The need for appropriate reforms in terms of policy and legislation, coupled with adequate training and international cooperation, becomes very essential for fighting against the emerging cyber crimes.

ISSN: 2582-6433

INTRODUCTION

The internet is an important source of information and support in the contemporary period characterized by the processes of modernization and technological advancement.[1] The internet has made the world a global village and continues to play a significant role in promoting human progress via online business, employment, advocacy, and communication.[2] Such social media sites as Twitter, Facebook, and Instagram offer people many avenues to get involved, communicate, and express themselves in cyberspace.[3]

Internet use, alongside other social media channels, has greatly enhanced freedom of expression and speech; nonetheless, this freedom is neither absolute nor unlimited, considering its misuse and harmful effects on people.[4] As was observed in ***Shreya Singhal v. Union of India***, freedom of speech and expression in cyberspace should be protected, but arbitrary powers need to be done away with.[5]

But at the same time, there are also some disadvantages associated with the Internet and social media.[6] Criminals use information technology to indulge in crimes like cyberstalking, cyber harassment, blackmailing, extortion, threats through electronic medium, and morphed images.[7] These kinds of offenses are becoming a common trend in India, and their most vulnerable victims are women and children.[8]

The reasons behind the victimization of women can be lack of awareness about technology, trust on offenders, and unwillingness to lodge complaints against offenses due to social stigma.[9] The impact

[1] Manuel Castells, The Rise of the Network Society (2d ed. 2010).
[2] Jan van Dijk, The Network Society (3d ed. 2012).
[3] danah boyd, It's Complicated: The Social Lives of Networked Teens (2014).
[4] INDIA CONST. art. 19(1)(a).
[5] Shreya Singhal v. Union of India, (2015) 5 SCC 1.
[6] Anita Gurumurthy, Gender and Cybersecurity, Econ. & Pol. Wkly. (2018).
[7] Pavan Duggal, Cyber Law in India (2016).
[8] National Crime Records Bureau, Crime in India (latest ed.).
[9] Debarati Halder & K. Jaishankar, Cyber Victimization in India (2011).

ISSN: 2582-6433

of cybercrime on a psychological level, that is, the trauma caused by these crimes, damage to reputation, and psychological harm is much greater compared to physical injuries.[10]

Thus, it is important for victims to be able to make a timely report of crimes and for the concerned authorities to take quick action on them.[11]

Background and Evolution of Cyber Crimes Against Women

India has always accorded respect to women, but irrespective of that, women happen to be among the most vulnerable groups of people.[12] Due to the development in technology, crimes in the form of harassment and intimidation have taken a new turn and today we see cyber stalking, cyber defamation, email harassment, morphing, and cyber pornography.[13]

Before the advent of any specific law in relation to cyber offences, cases of misuse of technology were being tried under the Indian Penal Code 1860.However, due to its inadequacy to deal with technologically advanced cases, the Information Technology Act 2000 came into force that was based on the UNCITRAL Model Law on Electronic Commerce.[14] It was later amended in the year 2008.[15]

Though there has been a significant progress made in the area of cyber laws for women, yet there still seem to be gaps in the existing laws. For example, the Supreme Court in ***Sharat Babu Digumarti v Government of NCT of Delhi***, laid down the scope of provisions under the IT Act and the Indian Penal Code in dealing with cyber crimes.[16]

In addition, in ***State of Tamil Nadu vs Suhas Katti,*** where the accused had used his computer to harass his victims, which led to the first conviction in cyber crime in India.[17]

[10] UN Women, Cyber Violence Against Women and Girls (2020).
[11] Aparna Viswanathan, Cyber Law: Indian and International Perspectives (2012).
[12] S. K. Verma & Raman Mittal, Legal Dimensions of Cyber Crime in India, J. Indian L. Inst. (2004).
[13] Arpita Sharma, Cyber Crimes Against Women in India, 3 Indian J.L. & Tech. (2017).
[14] UNCITRAL Model Law on Electronic Commerce, G.A. Res. 51/162 (1996).
[15] Information Technology (Amendment) Act, 2008, No. 10 (India).
[16] Sharat Babu Digumarti v. Govt. of NCT of Delhi, (2017) 2 SCC 18.
[17] State of Tamil Nadu v. Suhas Katti, C.C. No. 4680 of 2004 (Chennai Dist. Ct.).

ISSN: 2582-6433

While the IT Act caters to cyber crime within certain boundaries, it has been heavily criticized for its narrow approach towards victims as well as for its ineffective ways of dealing with cyber crimes against women.[18] There is an immediate need to have reforms within our cyber laws.[19]

Overview of New Criminal Laws (BNS, BNSS, BSA)

The IPC has been repealed by the Bharatiya Nyaya Sanhita, 2023 (BNS), CrPC by Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) and the IEA by Bharatiya Sakshya Adhiniyam, 2023 (BSA).[20] The legislation is a comprehensive legislative transformation, marking the first major transformation in the history of the Indian criminal law since the colonial era, as it signifies the move toward technology-based and justice-centric, indigenous crime management practices.[21]

The significance of these criminal laws lies in the fact that these are intended to streamline procedures and integrate indigenous perspectives on criminal offences as well as address emerging criminal issues such as cybercrimes.[22] These laws have immense importance in terms of cybercrime adjudication due to the fact that cybercrimes involve use of technological means and intersect with fraud, forgery, harassing behaviour and obscenity in criminal law.[23]

Even though cybercrimes are subject to the provisions of the Information Technology Act of 2000, it is an undeniable fact that the substantive, procedural, and evidentiary laws that govern their investigations, prosecutions, and trial were those contained in the IPC, Cr.P.C., and Evidence Act.[24] Hence, when such statutes are repealed and replaced by new ones such as the BNS, BNSS, and BSA, the nature of law regarding the investigation, prosecution, and trial of cybercrimes will change.

[18] Nishith Desai Associates, Information Technology Act: Analysis (2018).
[19] K. Jaishankar, Cyber Criminology (2011).
[20] Bharatiya Nyaya Sanhita, 2023; Bharatiya Nagarik Suraksha Sanhita, 2023; Bharatiya Sakshya Adhiniyam, 2023.
[21] Ministry of Home Affairs, Government of India, Criminal Law Reforms in India (2023).
[22] Aparna Viswanathan, Cyber Law: Indian and International Perspectives (2012).
[23] Pavan Duggal, Cyber Law in India (2016).
[24] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

ISSN: 2582-6433

Indeed, there is no question regarding the fact that procedures and evidence in criminal matters are extremely important as per the pronouncements made by the judiciary in India. It is for this reason that the Supreme Court of India ruled that any procedure made by law should be just, fair, and reasonable in the case of ***Maneka Gandhi v. Union of India.***[25]

In addition, the admissibility and probative value of electronic evidence have been tested before the courts. The position regarding the mandatory certification of electronic records under Section 65B of the Evidence Act was established in ***Anvar P.V. vs. P.K. Basheer***.[26] This decision was further clarified in the case of ***Arjun Panditrao Khotkar vs. Kailash Kushanrao Gorantyal,*** laying down the rules for the evaluation of digital evidence, which now form part of the legal framework of the BSA, 2023.[27]

This chapter provides an extensive analysis of the newly enacted criminal law regime with special emphasis on the issue of cybercrime. The fundamental aims and principles of such legislation are identified, and the concept of cybercrimes under the BNS is critically analyzed.[28]

Furthermore, it examines the system of evidence applicable under BSA, 2023, in relation to the issues of admissibility, authentication, and appreciation of electronic records.[29] The discussion in the chapter also considers the interaction of the newly formulated law with the Information Technology Act, 2000, particularly considering both complementarity and possible contradictions.[30]

Moreover, it highlights the difficulties that would emerge while implementing the provisions of the law, which include interpretational problems, lack of enforceability, and resource constraints faced by investigative bodies. Lastly, it considers the direction in which the adjudication of cybercrimes in India will proceed from this point forward.[31]

[25] Maneka Gandhi v. Union of India, (1978) 1 SCC 248.
[26] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
[27] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
[28] S. K. Verma & Raman Mittal, Legal Dimensions of Cyber Crime in India, J. Indian L. Inst.
[29] Indian Evidence Act, 1872 (now replaced by BSA, 2023).
[30] UNCITRAL Model Law on Electronic Commerce, G.A. Res. 51/162 (1996).
[31] Nishith Desai Associates, Information Technology Act: Analysis (2018).

ISSN: 2582-6433

It is crucial for all players of the cyber law domain to gain an insight into the changed legal framework since they will be required to cope with a fast-changing digital world.[32]

Literature Review

Indian legal frameworks need strengthening to protect women and children from cybercrime and surveillance, addressing challenges like cross-jurisdictional nature, digital literacy, and technological advancements. Kaur, D., & Nath, A. (2025).

Indian laws need amendments to accurately translate online experiences of harassment, threats, intimidation, and violence against women into written law, to effectively address cyber-crimes against women. Uma, M., & Gandhi, M. (2017).

Harmonized, gender-sensitive cyber laws are needed to address online harms specific to women, with recommendations for digital consent laws, international collaboration, platform responsibility, and survivor-centered practices. Mythili, K., & Nagamani, K. (2025).

Al strategies can help detect cybercrime against women in India, as the IT Act 2000 fails to address some of the most serious risks to their security. Prakash, P. (2024).

Digital violence against women in India faces legal reforms, digital literacy campaigns, and algorithmic accountability for social media platforms, requiring a tripartite solution. Akhtar, S., & Bhowmik, M. (2025).

Indian courts have made progress in addressing online violence against women, but face challenges in implementing laws due to technical hurdles, jurisdictional issues, under-reporting, and police apathy. Chandel, J., & Sethi, A. (2025).

Cybercrime against women in India is increasing at an alarming rate, with key legislation like the Information Technology Act and BNSS helping to protect women from these crimes. Muthukumar, D. (2024).

Cyber stalking and harassment against women in India are a growing issue, affecting their modesty, security, and privacy, and this paper highlights legal provisions for such crimes. Kumar, A., & Kumar, D. (2023).

[32] National Crime Records Bureau, Crime in India (latest ed.).

ISSN: 2582-6433

Women in India face increasing cyber crime rates due to devaluation and gaps in legal practices, highlighting the need for improved laws and security measures to combat this growing issue.Dar, S., & Nagrath, D. (2022).

Strong cybersecurity policies, public awareness campaigns, and enhanced legal frameworks are needed to ensure the safety and digital empowerment of women in India. Pawar, A. (2025).

Pakistan's PECA law is effective against cyberstalking, but needs improvement in coordination and application. Gull, S., Shaheen, M., & Akhtar, N. (2025).

Cyberbullying and cyberstalking in India pose significant concerns, requiring stringent policy reforms, enhanced cybersecurity measures, Al-driven content monitoring, and victim support mechanisms to effectively address these threats., R., & Varshney, R. (2024).

Cybercrimes against women in India are on the rise, affecting their mental health, freedom of expression, and digital economy involvement, highlighting the need for improved regulations and remedies.Ahlawat, H., & Sharma, S. (2024).

More precise regulations and legislation are needed to combat cybercrime against women in India, as women are disproportionately victimized and often unreported due to traditional society and patriarchal attitudes. Choudhary, R. (2022)

Cybercrimes against women, such as cyberstalking and sextortion, are on the rise, and this paper evaluates both Indian and international legal responses to combat this growing issue. Kulkarni, A. (2025).

Cybercrime significantly impacts women in India, causing mental and emotional stress, humiliation, and depression, and requires comprehensive strategies for mitigation and control. Saraswati, V. (2024).

Cyber-crime against women and children in India requires modernization of preventive measures and equipped police personnel for effective prevention and control. Sankhwar, S., & Chaturvedi, A. (2018).

Cybercrime against women in India is on the rise, with women being the most common victims, and addressing this issue requires a shift in thinking and a focus on technology. Joshi, K. (2022).

Objectives of the study

- To critically analyze the substantive provisions of the Bharatiya Nyaya Sanhita relating to cyber stalking, online harassment, and technology-facilitated gender - based offences against women.

ISSN: 2582-6433

- To evaluate the procedural framework under the Bharatiya Nagarik Suraksha Sanhita in investigating and prosecuting cyber offences, particularly with respect to digital evidence, jurisdiction, and victim protection.
- To examine the evidentiary standards governing electronic records under the Bharatiya Sakshya Adhiniyam and assess their effectiveness in securing convictions in cases of online harassment.
- To identify existing legal and practical gaps in the new criminal law regime and propose reforms to strengthen the protection of women in cyberspace.

Problem Statement

The growth of digital platforms has led to a marked increase in cyber stalking, trolling, and online harassment, with women being disproportionately affected. Although criminal law reforms in India, particularly the Bharatiya Nyaya Sanhita, 2023, seek to modernize the legal framework, it remains unclear whether these changes adequately address the complexities of technology-facilitated offences against women.

Concerns persist regarding the scope of statutory provisions, procedural effectiveness, investigative challenges, and the adequacy of victim protection mechanisms in cyberspace. Additionally, courts are required to balance freedom of speech with protection from online abuse, raising important constitutional questions.

This study therefore examines whether the reformed criminal law regime effectively safeguards women against cyber offences and identifies continuing gaps that require legal and policy intervention.

Research Methodology

This study adopts a doctrinal research methodology, primarily based on secondary sources of data. It involves analysis of statutory provisions such as the IT Act, BNS, BNSS, and BSA, along with judicial decisions, legal commentaries, and academic literature. Comparative analysis has been conducted by examining legal frameworks in jurisdictions such as the United States, European Union, United Kingdom, and Australia. The research also relies on reports, journals, and policy documents to evaluate enforcement challenges and suggest reforms. The methodology is analytical and descriptive in nature, aiming to identify gaps and propose solutions.

ISSN: 2582-6433

Critical Analysis of Substantive Provisions of the Bharatiya Nyaya Sanhita Relating to Cyber Stalking, Online Harassment, and Technology-Facilitated Gender-Based Offences Against Women

Conceptual Framework on Cybercrime Against Women

Cyberbullying can be defined as the deliberate and sustained act of conducting oneself in a threatening manner in the online world to cause fear, embarrassment, or harassment to another person.[33] Similarly, cybercrime can be described as the illegal acts committed by using computer and/or Internet technology as the main instrument for their commission.[34] It is essential to state that harassment by electronic medium in India is controlled by both the Information Technology Act, 2000 and common laws.[35]

Despite the existence of all these measures, cybercrimes against women persist as a major problem nowadays.[36] These crimes can take various shapes; however, identity theft, cyberbullying, revenge pornography, and cyberstalking are among the most common ones.[37] According to numerous studies, one of the most common forms of technological violence against women is represented by cyberstalking.[38] To put it simply, cyberstalking involves harassment of individuals by tracking them via digital platforms, sending messages, and other means of communication.[39]

The other major category of online harassment is non-consensual sharing of private photos or videos, which is colloquially termed "revenge pornography."[40] Non-consensual publishing or distribution of private or sexually explicit material, which causes severe psychological trauma, emotional distress, and damage to the reputation of an individual, is another serious type of cybercrime.[41] In Justice ***K.S. Puttaswamy v. Union of India***, the Supreme Court acknowledged the

[33] Debarati Halder & K. Jaishankar, Cybercrime and the Victimization of Women (2011).
[34] Pavan Duggal, Cyber Law in India (2016).
[35] Information Technology Act, 2000, 66C, 66D, 66E, 67.
[36] NCRB, Crime in India (latest ed.).
[37] Aparna Viswanathan, Cyber Law: Indian and International Perspectives (2012).
[38] K. Jaishankar, Cyber Criminology (2011).
[39] Id.
[40] UN Women, Cyber Violence Against Women (2020).
[41] Id.

ISSN: 2582-6433

importance of the right to privacy, which was declared to be a fundamental right guaranteed by Article 21 of the Indian constitution.[42]

With a rising number of cases involving cybercrime in India, several steps have been taken by the government to protect women in cyberspace.[43] For instance, the Information Technology Act, 2000 provides for various kinds of offences that include stealing someone's identification documents or hacking into their personal accounts. Additionally, the CCPWC initiative aims to provide a safe environment for women in the cyber world through awareness, reporting, and cooperation of police.[44]

Yet, despite all these measures, cybercrimes against women continue to prevail both in India and across the world.[45] These crimes continue to thrive due to certain reasons, including under-reporting, poor digital literacy, lack of jurisdiction, and the veil of anonymity offered by the internet.[46]

It becomes essential to follow an integrated strategy in which there is an enhancement in laws, enforcement, education, and victim support services while making sure that the offenders are brought to justice.

Cyber Stalking: Legal Recognition and Scope under BNS

Cyberstalking is an act whereby an individual uses the Internet to pursue, monitor, or stalk another person through the use of various forms of electronic communication, including social networking sites, emails, chat applications, among others.[47] In this case, cyberstalking entails repetitive acts that create fear or cause a victim to feel insecure and vulnerable, thus violating the right to privacy and security.[48]

The growth of the Internet has led to an increase in cyber crimes, including cyberstalking.[49] Facebook, Instagram, and Twitter have enabled communication between users, but the ease with which people can access personal information online has provided opportunities for misuse.[50]

[42] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[43] Ministry of Home Affairs, Government of India Reports.
[44] Information Technology Act, 2000; CCPWC Scheme, Govt. of India.
[45] UN Broadband Commission Report (2015).
[46] Halder & Jaishankar, supra note 1.
[47] Debarati Halder & K. Jaishankar, Cybercrime and the Victimization of Women (2011).
[48] Id.
[49] Pavan Duggal, Cyber Law in India (2016).
[50] Id.

ISSN: 2582-6433

Studies show that cyberstalking mainly affects women, and men are more likely than women to commit these acts.[51]

Cyberstalking may be committed by persons who know each other or by complete strangers.[52] Cyberstalking offenders often take advantage of the availability of personal information on social media sites to monitor their victims.[53] The perpetrators send repetitive unsolicited messages, post defamatory or offensive statements, impersonate their victims, and threaten to expose confidential information.[54] This results in the defamation of the victim and causes psychological harm.[55]
Cyberstalking may be categorized into the following general types:

Purely online cyberstalking, whereby the harassment takes place in a purely virtual manner; and

- Combination of both online and offline stalking, whereby the online harassment is escalated to the point where the perpetrator physically tracks the victim, which involves an attempt to ascertain her residential or contact address.[56]
- While there are some similarities between cyberstalking and conventional stalking in that they are both intended to control the victim, cyberstalking is much more lethal because it is not bound by geographical considerations and has greater anonymity.[57]

From a legal perspective, The Information Technology Act, 2000 does not provide for cyberstalking per se as an offence, although acts of cyberstalking could fall under the ambit of Sections 66E (violation of privacy) and 67 (publications of obscenity).[58] On the other hand, the Bharatiya Nyaya Sanhita, 2023 provides for stalking under Section 78 (parallel to Section 354D of the IPC), which includes tracking the usage of the internet, emails, and other electronic means of communications of women.

[51] NCRB, Crime in India (latest ed.).
[52] K. Jaishankar, Cyber Criminology (2011).
[53] Id.
[54] Aparna Viswanathan, Cyber Law: Indian and International Perspectives (2012).
[55] UN Women, Cyber Violence Against Women (2020).
[56] Cyber crime academic sources (Shanta, SSRN).
[57] Id.
[58] Information Technology Act, 2000, sec. 66E, 67.

ISSN: 2582-6433

Judicial recognition of Cyberstalking as a legally punishable offence dates back to ***State of Tamil Nadu v. Suhas Katti,*** one of the early cases dealing with cybercrimes in India, wherein the accused was charged with posting obscene/defamatory messages against a woman on the internet.[59] The case clearly shows that cybercrimes were punishable even without any express statutory provision at that point of time.

Cyberstalking takes several different forms, including:

- Internet Stalking: It involves repeated stalking via the internet by continuously monitoring and making defamatory or false statements against the victim.[60]
- Computer Stalking: This is done through illegal access to and/or controlling the victim's computer systems.[61]
- Email Stalking: Sending emails in form of threats, abuse or any other message intended to cause trouble to the recipient.[62]

However, despite such legal provisions, a number of problems still persist in dealing with the problem of cyberstalking. Such problems include the absence of proper definition, legal complexities arising out of jurisdictional issues, problem in collecting evidence and lack of reporting by the victim herself.[63] Thus, while BNS is an important step towards tackling the issue, much still needs to be done.

Online Harassment and Abuse: Types and Legal Aspects

Online harassment and abuse involve numerous malicious actions performed via electronic means, often overlapping with cyberstalking in nature and consequences.[64] Unlike stalking, which implies persistent tracking or following, harassment involves deliberate acts intended to disturb or threaten a person.[65] In the online environment, the two often occur simultaneously, as both types of criminal

[59] State of Tamil Nadu v. Suhas Katti, C.C. No. 4680/2004.
[60] SSRN Cyber Law Papers.
[61] Id.
[62] Id.
[63] NCRB & policy reports.
[64] Debarati Halder & K. Jaishankar, Cybercrime and the Victimization of Women (2011).
[65] Id.

ISSN: 2582-6433

acts include constant and repetitive behavior that poses a danger to victims' physical safety and psychological well-being.[66]

What distinguishes online harassment from other forms of crime is the cross-border nature of offences, which often entails the occurrence of criminal acts in one country and adverse effects in another.[67] This poses a great challenge for the police and judicial authorities, as current legal procedures require offenders to be present within the territory of the relevant state to be tried for the crime.[68] Another factor complicating investigations is the anonymity of offenders, who may disguise themselves via fabricated accounts, proxies, or IP addresses altered through various technological methods.[69]

The Information Technology Act, 2000 provides a statutory framework to address several forms of online abuse, including identity theft, impersonation, privacy violations, and publication of obscene content.[70] Additionally, the Bharatiya Nyaya Sanhita, 2023 incorporates provisions relating to defamation, criminal intimidation, and harassment, thereby extending traditional criminal law protections into the digital sphere.[71] However, the absence of comprehensive and technology-specific definitions continues to pose interpretational challenges.[72]

Judicial intervention has played a crucial role in shaping the legal landscape. In ***Shreya Singhal v. Union of India,*** the Supreme Court struck down Section 66A of the IT Act for being vague and overbroad, while emphasizing the importance of protecting freedom of speech alongside preventing misuse of online platforms.[73] This judgment highlights the need to strike a balance between individual liberty and protection from online abuse.

[66] Aparna Viswanathan, Cyber Law: Indian and International Perspectives (2012).
[67] UNCITRAL Model Law on E-Commerce (1996).
[68] Id.
[69] K. Jaishankar, Cyber Criminology (2011).
[70] Information Technology Act, 2000, 66C, 66D, 66E, 67.
[71] Bharatiya Nyaya Sanhita, 2023 (relevant provisions on defamation and intimidation).
[72] Legal critiques on cyber law reforms.
[73] Shreya Singhal v. Union of India, (2015) 5 SCC 1.

ISSN: 2582-6433

Types of Cyber Harassment and Assaults - Cyber harassment can take different shapes and sizes, with varying legal consequences associated with each:

1. Defamation on the Internet: Defamation is the act of making defamatory remarks against someone with malicious intentions. Defamation cases on the internet occur when an individual uses the internet to disseminate information regarding a person that could damage their reputation.[74] There is a remedy to this, which includes both civil and criminal offenses, under the defamation laws.[75]
2. Identity Theft: Identity theft is defined as stealing someone else's personal information without their consent for fraudulent purposes.[76] The offense is a criminal offense under Section 66C of the IT Act,[77] and perpetrators may face imprisonment and fines.
3. Breach of Privacy: Breach of privacy occurs when someone violates the right to privacy without consent, whether through hacking into private accounts, surveillance, and revenge pornography.[78]According to ***Justice K.S. Puttaswamy v. Union of India,*** the right to privacy is a fundamental right in India.[79]
4. Online Trolling: Online trolling can be defined as posting insulting, threatening, and abusive comments to annoy people.[80] Such behavior often results from false identities of people engaging in abusive discourse online.[81]
5. Cyber Hacking: Cyber hacking involves breaking into the digital device or system of an individual illegally via malware in links or apps to steal private data.[82] This causes financial losses and identity theft among other damages.

[74] S. K. Verma & Raman Mittal, Indian Journal of International Law.
[75] Id.
[76] Pavan Duggal, Cyber Law in India (2016).
[77] Information Technology Act, 2000, 66C.
[78] UN Women, Cyber Violence Against Women (2020).
[79] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[80] SSRN Cyber Law Papers.
[81] Id.
[82] Cyber law academic sources.

ISSN: 2582-6433

6. Cyber Phishing: This refers to a practice where criminals deceive victims by impersonating legitimate firms in order to gain access to sensitive data like passwords or account credentials.[83] This is the main tool for committing cyber fraud.[84]

7. Cyber Morphing: This term is associated with editing the images, mostly those of women, with the aid of digital means and then sharing the altered content online without permission.[85] It has adverse impacts on reputation and public image of victims.

Technology-Facilitated Gender-Based Violence (TFGBV)

Technology-Facilitated Gender-Based Violence (TFGBV) is an act of gender-based violence carried out using technology. Women, girls, and people of different genders are mostly affected.[86] It is the online version of the violence that takes advantage of the anonymity, accessibility, and fast transmission of material on digital devices.[87]

The 2018 report from Dubravka Šimonović outlines several types of TFGBV, which include harassment, threat, impersonation, doxing, sextortion, stalking, trolling, and distribution of manipulated images.[88] The mentioned types are not exhaustive as they keep evolving with developments in technology.[89]

TFGBV predominantly targets women participating in public affairs such as politics, journalism, and activism as well as other members of marginalized communities, thus limiting their participation in the conversation.[90]

In India, TFGBV cases have been handled through scattered legislation in the Information Technology Act, 2000 and Bharatiya Nyaya Sanhita, 2023 laws; nonetheless, there is no specific law that handles these crimes.[91]

[83] IT security reports.
[84] Id.
[85] Academic commentary on cyber morphing.
[86] UN Women, Cyber Violence Against Women (2020).
[87] Debarati Halder & K. Jaishankar, Cybercrime and the Victimization of Women (2011).
[88] Dubravka Šimonović, Report of the Special Rapporteur on Violence Against Women, U.N. Doc. A/HRC/38/47 (2018).
[89] Id.
[90] Id.
[91] Information Technology Act, 2000; Bharatiya Nyaya Sanhita, 2023.

ISSN: 2582-6433

Comparison with Earlier Laws (IPC & IT Act, 2000)

Legal Frameworks Established to Prevent Cybercrime Against Women

The Information Technology Act, 2000, is the central piece of legislation governing cyber law in India. It was enacted to facilitate e-commerce and give legality to transactions done through information technology; however, the scope of the legislation was later broadened through the amendment made in 2008, making cyber crimes like identity theft, cyber terrorism, and hacking included under the ambit of the Act.[92]

However, the Act suffers from its technological angle and fails to cover any gender-specific offenses against women.[93] In addition, another relevant provision, the Indecent Representation of Women (Prohibition) Act, 1986, although significant in terms of protecting women, is no less technologically obsolete.[94]

Nevertheless, there exists both the IT Act and Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, the implementation of which continues to face hurdles. Several complaints have been raised about courts showing greater consideration for offline than online offenses.[95] Nonetheless, the lack of a gender-sensitive cyber law calls for more reforms.

Essential statutory provisions of the 2000 Information Technology Act (Amended 2008) Section

- 66A: Sending of Electronic Offense: This law made it unlawful to send any offensive or misleading electronic message or electronic mail. Nevertheless, it was declared void in ***Shreya Singhal v. Union of India*** because of its violation of the right to freedom of speech under Article 19(1)(a).[96]
- Section 66B: Dishonestly Receiving Stolen Computer Resource: This section makes receiving or retaining stolen computer resources or devices punishable under Indian law where one benefits from the crime. This offense seeks to curb the illegal transaction of the said digital resource.[97]

[92] Information Technology Act, 2000; Information Technology (Amendment) Act, 2008.
[93] Pavan Duggal, Cyber Law in India (2016).
[94] Indecent Representation of Women (Prohibition) Act, 1986.
[95] Avni Katiyar, Cyber Law and Gender Justice (journal article).
[96] Shreya Singhal v. Union of India, (2015) 5 SCC 1.
[97] Information Technology Act, 2000, 66B.

ISSN: 2582-6433

- Section 66C: Identity Theft: The section penalizes the use of any password or unique electronic signature without proper authority. It is often applied in cases where identity theft occurs in cyber space.[98]

- Section 66D – Cheating by Impersonation: This section punishes those guilty of committing cheating through false online identities, phishing, and other means of fraud. This section applies especially in instances where women have been cheated through false identities or through fraudulent online activities. The section punishes cybercrime with criminal intent.[99]

- Section 66E – Violation of Privacy: This section punishes the act of taking, publishing, or sending pictures or any form of image of another person's private body parts without consent. This section is crucial in the fight against revenge porn or other sexual abuse through technology.[100]

- Section 66F – Cyber-terrorism: This section refers to the act of committing crime against national security through illegal computer access or hacking. This could be hacking of government documents or any software with malicious intents to harm the government or disrupt their computer system. The penalty is heavy in this case.[101]

- Section 67 – Publishing Obscene Content: This section punishes anyone for publishing obscene content including sexually explicit content through the internet. This section applies especially in relation to child pornography.[102]

- Section 72 – Breach of Confidentiality and Privacy: Under Section 72, penalties apply for making use of confidential information derived from accessing any computer resource legally. This provision becomes crucial when third parties abuse their users' personal information.[103]Institutional and Policy Framework

-

[98] Id. 66C.
[99] Id. 66D.
[100] Id. 66E.
[101] Id. 66F.
[102] Id. 67
[103] Id. 72

ISSN: 2582-6433

Besides statutory regulations, cybersecurity management in India is reinforced by:

National Cyber Security Policy, 2013 - This document sets out the roadmap for ensuring cyber security.[104] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 - This regulation sets out rules concerning the protection of personal data.[105] Indian Computer Emergency Response Team (CERT-In) - This body assumes a vital responsibility in incident management.[106]

Provisions under the Bharatiya Nyaya Sanhita Pertaining to Cyber Crimes Committed against Women

- Section 75 (Sexual Harassment): According to the provisions under the Bharatiya Nyaya Sanhita, 2023, Section 75 prohibits unwanted physical touching, sexual advances, demand for sexual favour, pornographic depiction without consent, or any sexually coloured remarks. The clause is comprehensive enough to cover activities committed electronically, such as sending vulgar messages and images online. The provision helps protect the dignity of the body of women in both physical and virtual worlds.[107]

- Section 77 (Voyeurism): In Section 77, voyeurism means committing an act where there is watching, recording or publication without consent of any activity involving private parts of a woman's body. It specifically mentions any act done through electronic medium which can be considered as cybercrime. The law acknowledges the privacy invasion caused due to dissemination online and provides for enhanced punishments.[108]

- Section 78 (Stalking): Stalking, whether physical or via cyberspace, is prohibited under Section 78 of the law. This section deals with acts like making repeated efforts at communicating with a woman when she does not wish to communicate and stalking her on social networking sites. This section addresses the mental torture caused to women due to unwanted attention. This law further protects their privacy and security through cyberspace.[109]

[104] National Cyber Security Policy, 2013 (India).
[105] Information Technology Rules, 2011.
[106] CERT-In Guidelines, Government of India.
[107] Bharatiya Nyaya Sanhita, 2023, § 75.
[108] Id. § 77.
[109] Id. § 78.

ISSN: 2582-6433

- Section 79 (Insult to Modesty of a Woman) : Insult to the modesty of a woman is prohibited in Section 79 of the act, which includes insulting actions, words, or gestures directed towards a woman. This provision protects women from insults and disrespect in the online space. It prescribes the punishment of jail term and monetary penalty as a deterrent to such offenses.[110]

- Section 111(1) (Organized Crime): It refers to organized crimes committed by a group of people or syndicates, which may include cyber crimes like fraud, trafficking, or illegal transactions. It takes note of the organized nature of cyber crimes. It makes sure that any systematic operation is penalized severely. It is useful in dealing with cyber exploitation of women via networks.[111]

- Section 356 (Defamation): concerned with defamation, whereby an individual makes or publishes untrue statements that damage another person's reputation. It also applies to the internet world, where defamation occurs quite fast in most cases. Women have been victims of defamation due to the use of morphing photographs and other ways.[112]

Legal Provisions for Protection of Women Against Cybercrimes Under the Constitution

There are several provisions for the protection of women from cybercrimes provided by the Constitution of India, which includes fundamental rights such as Article 21 which provides for the right to life and personal liberty. The Supreme Court has recognized that this also includes right to privacy and dignity, hence any interference with privacy would have to be proportional.[113]

Articles 14 and 19 provide further balance where there would be equality before law and freedom of speech but would not undermine the dignity of women.[114]

Judicial Trends & Landmark Cases

Gobind v. State of Madhya Pradesh: This landmark case recognized that there should be compelling state interest for restricting personal liberty or right to privacy of an individual. It was a major development in making a link between personal liberty and privacy.[115]

[110] Id. § 79.
[111] Id. § 111(1).
[112] Id. § 356.
[113] INDIA CONST. art. 21.
[114] INDIA CONST. art. 14, 19.
[115] Gobind v. State of M.P., (1975) 2 SCC 148.

ISSN: 2582-6433

- ***PUCL v. Union of India:*** This case upheld the right to privacy in terms of telephone conversations. In the same case it was held that any interference with privacy will amount to violation of Article 21.[116]

- ***K.S. Puttaswamy vs Union of India:*** It is one of the significant judgments where privacy was recognized as a fundamental right by virtue of Article 21. Privacy is related to dignity, autonomy, and informational self-determination. The test for limitation of privacy has been described as legality, necessity, and proportionality.[117]

Case Study of Cybercrime Against Women

- ***State of Tamil Nadu vs Suhas Katti***: In this case, the defendant had established a fictitious email address through which he sent defamatory and offensive messages to victimize a woman. He was found guilty under Sections 469 and 509 IPC, as well as Section 67 of the IT Act. This is a landmark case because it marked the first instance of a successful prosecution for cyber harassment in India.[118]

- ***Shreya Singhal vs Union of India:*** This case was brought before the Supreme Court against the provisions of Section 66A of the IT Act on the grounds that they were unconstitutional and violated the right to freedom of speech. The apex court held that advocacy and incitement should not be confused; hence, vague restrictions will never suppress online speech.[119]

Role of Privacy and Dignity in Protecting Women from Cybercrime Right to Privacy and Constitutional Responsibility

Article 21 of the Constitution of India safeguards the right to privacy and dignity as an inherent component of life and personal liberty. While not expressly stated, the Supreme Court of India has ruled that privacy is a basic right that is necessary for human dignity and autonomy. It applies to the cyberspace realm, offering protection from unlawful invasion, harassment, and abuse of data of

[116] PUCL v. Union of India, (1997) 1 SCC 301.
[117] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[118] State of Tamil Nadu v. Suhas Katti, C.C. No. 4680/2004.
[119] Shreya Singhal v. Union of India, (2015) 5 SCC 1.

ISSN: 2582-6433

individuals, particularly women. The restriction should be based on legality, necessity, and proportionality criteria.[120]

Violence against women, such as harassment and abuse in cyberspace, clearly breaches the fundamental rights protected under the constitution by violating women's right to privacy and personal dignity.[121]

Infringement of the Right to Privacy

Privacy entails safeguarding oneself from any unauthorized access to personal data, communication, and digital identity. In the era of the internet, abuse of personal data, doxing, and cyber-stalking has emerged as major concerns. Privacy ensures confidentiality of personal information exchanged in confidence.

Article 19(1)(a), guaranteeing freedom of speech, does not protect any defamatory, obscene, or other harmful content published through the Internet because such content can be subjected to restrictions under Article 19(2).[122]

In the case of ***Shreya Singhal vs. Union of India***, the Supreme Court found Section 66A of the IT Act unconstitutional for its vagueness and lack of justification in restricting freedom of speech online.[123]

Right to Privacy in Contrast with Public Morality

In the case of Mr. X v. Hospital Z, while the right to privacy was declared as a right included under Article 21 of the Constitution, the court made it clear that such privacy could be regulated in the interest of public morality and social interests.[124]

Additionally, in the case of ***Vasunathan v. Registrar General,*** the court recognized the concept of the "right to be forgotten" as well as the "right to be left alone", indicating the importance of protecting personal information online.[125]

[120] INDIA CONST. art. 21; K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[121] UN Declaration on Elimination of Violence Against Women (1993).
[122] INDIA CONST. arts. 19(1)(a), 19(2).
[123] Shreya Singhal v. Union of India, (2015) 5 SCC 1.
[124]
[125] Vasunathan v. Registrar General, (2017) Karnataka HC.

ISSN: 2582-6433

Dignity and Protection Against Online Abuse

The concept of dignity involves the innate value attached to every individual in society. Any sort of online abuse, trolling, defaming etc. takes away that dignity and destroys the reputation of individuals, especially women. However, although freedom of speech is an absolute right, such speech should not cross that limit and involve defamation.

In Neelam Mahajan Singh v. Commissioner of Police, it was stated by the court that there needs to be a balance between freedom of speech and social decency.[126]

Case Study: Cyber Harassment and Infringement of Privacy

The Ritu Kohli case : ***Ritu Kohli vs Union of India (2001)*** is one of the earlier recorded cases in India regarding harassment on the Internet. The victim's identity was used to post obscenities in a chatroom leading to harassment and violation of her privacy. The police identified the culprit through IP tracking and apprehended him. In this case, the court ruled that the actions amounted to violation of privacy and dignity of the victim as provided in Article 21 of the Constitution and are punishable under sections of the Information Technology Act, 2000 and IPC. The case established that harassment and cyber stalking over the Internet are grave crimes, which should be dealt with seriously using legal means. It also brought forth the need for strict regulations of content on the Internet and the responsibility of social media websites.[127]

[126] Neelam Mahajan Singh v. Commissioner of Police, Delhi HC.
[127] Ritu Kohli v. Union of India (2001) 3 SCC 204.

ISSN: 2582-6433

"Procedural Framework under the Bharatiya Nagarik Suraksha Sanhita for Investigation and Prosecution of Cyber Offences: A Study of Digital Evidence, Jurisdiction, and Victim Protection"

Introduction to Procedural Law in Cyber Offences

With the advent of technology and the use of the internet, there have been increased cases of cybercrime, such as online stalking, identity theft, online extortion, and hacking. Unlike conventional crimes, these types of crimes tend to be transnational and technologically sophisticated and require electronic evidence. Such traits demand a procedural system to facilitate proper handling during the processes of investigation, trial, and prosecution.[128]

The Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023 of India is the procedural mechanism in place for dealing with cybercrimes in the Indian criminal justice system. The statute outlines how complaints can be filed, investigation undertaken, police powers exercised, and trials conducted, bearing in mind the peculiarities of collecting, storing, and verifying digital evidence.[129]

Besides the BNSS, the Information Technology Act, 2000, authorizes investigators with necessary powers to conduct searches and seizures of electronic gadgets used to commit crimes. Moreover, the Bharatiya Sakshya Adhiniyam, 2023 has facilitated the prosecution process through regulations on the admission and evidence of electronic documents.[130]

Management of digital evidence including maintaining the chain of custody, securing the electronic devices and performing forensic analysis has been highlighted in procedural law. It also deals with various jurisdictional issues that arise because of the international scope of cyber crimes.[131]

[128] Avni Katiyar, Cybercrime and Procedural Challenges in India, 2022, 23 J. Indian L. & Tech. 45.
[129] Bharatiya Nagarik Suraksha Sanhita, 2023, §§ 10–25.
[130] Information Technology Act, 2000, § 66–67; Bharatiya Sakshya Adhiniyam, 2023, §§ 5–12.
[131] Id. §§ 15–18 (digital evidence and forensic procedures).

ISSN: 2582-6433

The safety of the victim, especially in the case of cyber crimes against women, has remained the focal point of procedural law. E-filing systems, online reporting mechanisms, and even virtual hearings can be counted among its technological developments.[132]

In short, procedural law ensures that legal requirements are converted into procedures that not only secure individual rights but are technologically compatible as well. A flexible procedural law is therefore essential to deal with cyber crimes.

Changing the Process for Investigating and Prosecuting Cybercrimes

The 2023 BNSS Act includes many procedural amendments, which substitute some provisions of the Cr.P.C., 1973, and seek to incorporate the application of technology within the criminal justice process. All these changes affect the procedure for reporting, investigating, and prosecuting cybercrimes to ensure that procedural laws adapt to technological innovations.[133]

Major Procedural Amendments and their Impact on Cybercrime:

- Electronic communication and audio-video electronic means: The BNSS Act defines electronic communication and audio-video electronic means, thus paving the way for their inclusion in evidence, witnesses' testimonies, and trials, which is very helpful in cybercrime cases.[134]
- Zero FIR: The BNSS Act incorporates the provision of Zero FIR, which enables the lodging of an FIR at any police station irrespective of territorial boundaries, and then forwarding the FIR to the relevant station. Such provisions are highly useful in dealing with cybercrimes, as the perpetrator and the victim may not belong to the same jurisdiction.[135]
- Filing of FIRs/complaints electronically: The BNSS Act provides for the electronic filing of FIRs and complaints.[136]
- Statements and Evidence by Way of Audio-Video Electronic Media: Witness and victim statements may now be made using audio-video electronic media, thereby capturing statements

[132] Id. §§ 20–22 (victim protection measures, e-FIRs, virtual hearings).
[133] Bharatiya Nagarik Suraksha Sanhita, 2023, §§ 1–10 (procedural integration and technological adoption).
[134] Id. § 5 (definition of electronic communication and audio-video electronic means).
[135] Id. § 7 (Zero FIR and cross-jurisdiction reporting).
[136] Id. §§ 8–9 (electronic filing of complaints and FIRs).

ISSN: 2582-6433

early on and allowing persons who cannot attend personally to participate. This applies to victims of gender-based cybercrimes, sexual harassment, and cyberbullying.[137]

- Trial Conduct, Investigation, Inquiry, and Procedure: The BNSS encourages the use of electronic means for trial proceedings, witness examination, and argumentation. This could help speed up the process of trial, especially in cases of cybercrimes, which involve parties located far from each other or whose evidence exists only in digital form.[138]

With the incorporation of technological processes into procedural law, the BNSS guarantees an efficient, secure, and flexible investigation process, evidence-gathering stage, and trial proceedings.

Registration of FIR in Cybercrime Cases

Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023 also lays down various procedural changes pertaining to filing and investigating cybercrimes which have an effect on women victims. These include processes such as Zero FIR and electronic filing of FIRs (e-FIRs).

Zero FIR: According to BNSS 2023, victims can file their FIR at any police station irrespective of territorial jurisdiction, and the FIR will then be sent to the concerned jurisdiction for investigation.[139]

Electronic FIR (e-FIR): Victims can file complaints electronically, but the informant's signature must be obtained within three days to prove the FIR. Free copies of the FIR must be provided immediately to the victim. The authorities must provide regular updates to the complainant via email or other forms of digital communications within ninety days.[140]

First Information Report (FIR): FIR is a legal document which records cognizable crimes reported by victims and contains information about the offender's identity, timing, and location of the incident. An FIR is filed by the police officer upon receiving a complaint about a cognizable crime in accordance with Sections 154 CrPC and Section 173 BNSS, 2023.[141]

[137] Ministry of Home Affairs [MHA], Guidelines on Audio-Video Recording of Witness Statements, 2024; BNSS, 2023, § 12.
[138] BNSS, 2023, §§ 15–18 (electronic conduct of trials and proceedings).
[139] BNSS, 2023, § 7 (Zero FIR and jurisdictional transfer).
[140] Id. § 8 (Electronic filing and victim updates).
[141] Cr.P.C., 1973, § 154; BNSS, 2023, § 173 (definition and registration of FIR).

ISSN: 2582-6433

Process of Investigation: Cyber crime investigations usually start from CCIC or CCU. The police, particularly an inspector or above rank, conducts the investigation under the IT Act, 2000 (amended 2008), while lower-ranking police can make arrests and conduct initial investigation.[142]

Registration of High-Risk Complaints: Any complaint valued more than ₹10,00,000 will be automatically registered as an FIR under the I4C system, following which the police should maintain a case journal and conduct investigations, including seizing evidence and making arrests.[143]

Compulsory Registration – Lalita Kumari Doctrine: According to the Supreme Court's decision in ***Lalita Kumari v. Govt. of U.P.***, if information indicates that a cognizable crime was committed, an FIR should be compulsorily registered under Section 154 CrPC and Section 173 BNSS, 2023.[144]
E-FIR and Digitization: Section 173(1) BNSS, 2023 authorizes filing FIRs electronically, thus facilitating the process, but also ensures signature verification within three days through procedural requirements like those laid out in Sections 154 CrPC and 173 BNSS, 2023.[145]

Digital and Electronic Evidence: Search, Seizure, and Collection

In cybercrime investigations, the ability to search, seize, and collect electronic evidence plays a crucial role. This is significantly different from the process of collecting physical evidence owing to the fragile nature of digital evidence, the huge volume of data, and the possibility of rapid changes. The BNSS in conjunction with the BSA should clarify the procedures involved in the process.

1. The Processes Involved in Searching and Seizing Electronically: It appears that the BNSS will outline procedures concerning the searching and seizing of computers, mobile phones, and storage media with a view to maintaining the integrity and authenticity of electronic evidence:

- Forensic personnel: The use of specially-trained forensic examiners or persons with technical competence when carrying out searches and seizures to prevent corruption or loss of data.
- Imaging on-site: Whenever possible, forensic cloning or imaging of the storage media to obtain accurate bit-by-bit copies without damaging the original device.

[142] IT Act, 2000 (amended 2008), § 78; BNSS, 2023, §§ 6–9 (investigative powers and responsibilities).
[143] From FIR to Forensic Analysis in the Digital Age: Legal Powers, Investigative Models, and Judicial Oversight of Cybercrime Policing in India (2023).
[144] Lalita Kumari v. Govt. of U.P., (2014) 2 SCC 1.
[145] BNSS, 2023, § 173(1) (E-FIR and digital filing).

ISSN: 2582-6433

- Documentation of device: Documentation of make, model, serial numbers, whether powered on/ off, and other identifying characteristics to prevent any claims of contamination.[146]

Such procedures represent best practices for conducting digital forensics investigations, where science and legal considerations are paramount.[147]

2. Data Collection from Intermediaries and Service Providers: Whereas the Information Technology Act, 2000 (Section 69) grants power to governmental authorities to intercept, monitor, or decrypt data, and where CERT-In can seek data from intermediaries, the BNSS could facilitate the process through which law enforcement gets:

- IP Logs & Packet data
- Subscriber data from telecommunications/ISP companies
- Communications data from social media platforms

Such would ensure that access is lawful and complies with due process, including the requirement for judicial sanction and respect for privacy rights.[148]

3. Digital Forensics and Reporting: Successful prosecution of cybercrimes hinges on prompt forensic analysis. BNSS will be expected to:

- Establish timeframes within which digital forensics reports must be submitted, hence minimizing trial delays.
- Establish the minimum requirements for accreditation of forensic laboratories and analysts.

It should be noted that delay in conducting digital forensics analysis may hamper prosecutions and accountability of cybercrime perpetrators.[149]

[146] Pavan Duggal, Digital Evidence and Cyber Forensics in India: Legal and Investigative Challenges, 20 J. Indian L. & Tech. (2020).
[147] Avni Katiyar, Search and Seizure of Electronic Evidence under Indian Cyber Law, 15 Cyber L. & Sec. Rev. (2021).
[148] Debarati Halder & K. Jaishankar, Cyber Crime and the Indian Legal Response, 26 Crim. Just. L.J. (2019).
[149] S. Girdhar & R. Singh, Forensic Readiness and e-Evidence Management, 14 Int'l J. Digital Crime & Forensics (2019).

ISSN: 2582-6433

Cloud Server Seizure Example: Where key evidence is stored on cloud servers, the process for seeking lawful access shall remain subject to the processes established under the IT Act. Obtained data will then be subject to BNSS/BSA rules.[150]

4. Audio-Video Digital Recordings and Presentation - The BNSS allows audio-visual electronic recordings in:

- Operations involving search and seizure
- Statements from victims and witnesses
- Examination of the accused These benefits include:
- Production of admissible electronic evidence
- Prevention of controversies regarding investigatory technique
- Conducting virtual trials and playing back in court
- Overcoming the chasm between investigation and presentation in digital environments

These are highly critical in cybercrime proceedings where the evidence is likely to be scattered geographically.[151]

5. Jurisdiction Expansion and Right Against Self-Incrimination: The BNSS enables the police wider jurisdiction in searching and seizing any electronic evidence when such evidence is "likely to contain" the required information. The officer is empowered to seize such materials in case of an absence of consent in written form, which delays the process of collection.[152]

Indian courts have ruled that the "right against self-incrimination" refers to the testimony of knowledge alone and does not cover compelling the handing over of electronic devices. This issue has immense ramifications for corporations and individuals operating from multiple jurisdictions.[153]

[150] Anu Mathur, Cross-Border Data Access and Mutual Legal Assistance in Cybercrime, 22 Comp. & Int'l Law J. (2022).
[151] Somlata Rai, Digital Evidence and Procedural Law in India's New Criminal Laws, 18 Indian J. Criminal L. (2023).
[152] Ministry of Home Affairs, Government of India, Guidelines on Digital Evidence and Cyber Investigation (2024).
[153] Lexology Insight, Legal Powers and Investigative Models in Cybercrime Policing (2023).

ISSN: 2582-6433

Jurisdictional Issues in Cybercrime Cases

One major problem posed by cybercrimes is that of jurisdiction. Traditional crimes take place in one particular geographic jurisdiction whereas cyberspace knows no bounds; this leads to the problem of defining where exactly the crime took place and which jurisdiction has the right to investigate and punish such crimes.[154]

1. International Aspect of Cybercrimes

Cybercrimes can occur in one jurisdiction but affect victims in other jurisdictions. Offenders usually conduct their criminal activities from areas where the law enforcement apparatus cannot track or enforce the law. The offenders, victims, and the locations of servers where data is stored may all be located in different jurisdictions.[155]

2. Absence of Uniformity in International Cyber Crime Laws

There exists no universal international legal regime specifically applicable to cyber crime. Countries differ in their definitions, procedures, and penalties regarding cybercrime. Consequently, this problem makes it very hard to conduct an effective investigation and prosecution.[156]

3. Locating Offenders

In most cases, criminals take advantage of different services to mask their real identity and location such as anonymising services, proxies, virtual private networks, and botnets. These practices complicate the process of tracing criminals to a particular jurisdiction.[157]

4. Difficulties in Mutual Legal Assistance

MLATs are the main tools used by governments in sharing information and conducting investigations together with other states. However, the process of gathering evidence or witness testimony can be lengthy due to different processes among jurisdictions. In addition, this process hinders efficient investigation.[158]

5. Differences in Legal and Cultural Aspects

[154] M. Younis, Jurisdictional Challenges in Cybercrime Prosecution, 21 Int'l J. of Cyber L. (2023).
[155] S. Singh & A. Rao, Cross-Border Cybercrime and Legal Responses, 14 J. Indian L. & Tech. (2022).
[156] R. Clarke, International Legal Frameworks for Cybercrime, 17 Comp. & Int'l L. J. (2021).
[157] B. Gupta, Attribution and Anonymity in Cybercrime Investigations, 25 Cyber Forensics Rev. (2020).
[158] A. Mehta, Mutual Legal Assistance in Cyber Law Enforcement, 12 Indian J. Crim. L. (2021).

ISSN: 2582-6433

Variations exist in relation to the legal system, standards of evidence, offences, and privacy rights, thereby causing difficulties in enforcing the law. For instance, a particular state may consider some acts as cyber crimes but in another state, the same act might be legal.[159]

6. Inadequate Resources for Law Enforcement Agencies

The investigation of cybercrimes calls for specific technical knowledge and facilities. Most countries do not have adequate forensic laboratories, skilled manpower, or finances to support such investigations and international cooperation.

7. Disputing Jurisdictions

Jurisdiction disputes can arise when multiple countries make claims for jurisdiction in the same cybercrime because of the residence of the victim, the residence of the perpetrator, or even the server's jurisdiction. Such disputes cause diplomatic tension between the involved nations, and solving them calls for collaboration between the nations.[160]

Extraterritorial Jurisdiction: Legal Complexities and Constraints

Extraterritorial jurisdiction is the capacity of the state to exercise control outside the confines of its territory. In cybercrime, it is often exercised when the criminal activity crosses several countries by utilizing foreign servers or targeting foreign victims.[161]

Nonetheless, there are many difficulties associated with the extraterritorial application of law:

- Identification of the Source of Authority: The basis of the source of jurisdiction can depend on whether the crime was committed in a different country, where the offender resides, or even the server being utilized.[162]
- Legal International Restrictions: There is no established international law on how the application of extraterritorial laws can be conducted during cybercrime investigations. Therefore, a balance between state sovereignty and international norms must be considered.[163]

[159] D. Halder & K. Jaishankar, Cybercrime and Legal Diversity, 3 Crim. Just. L.J. (2019).
[160] A. Pandey, Jurisdictional Conflicts in Cyber Law, 5 Int'l Cyber Reg. (2023).
[161] S. Banerjee, Extraterritorial Jurisdiction in Cybercrime, 19 J. Int'l Crim. Just. (2021).
[162] R. Bhargava, Legal Bases for Cyber Jurisdiction, 10 Indian L. Rev. (2020).
[163] K. Venkatesh, International Norms and Cyber Jurisdiction, 16 Glob. Law Rev. (2022).

ISSN: 2582-6433

- Obtaining of Evidence: It becomes challenging to obtain evidence in cases that involve foreign jurisdictions due to the lengthy procedure needed to acquire them. This might result in weakening the value of the evidence because of the passage of time.[164]
- Sovereignty and Due Process: The efforts made by a state to enforce its cybercrimes laws extraterritorially require it to take into account issues related to the sovereignty and due process of law in other states.[165]

International cooperation and harmonization of the laws are therefore key factors in the successful handling of cybercrimes.[166]

"Evidentiary Standards Governing Electronic Records under the Bharatiya Sakshya Adhiniyam and Their Effectiveness in Securing Convictions in Online Harassment Cases"

Evolution of Electronic Evidence in India

The technological development during the twentieth-first century has brought significant changes to the human lifestyle, with computers and digital communication becoming available not only within institutions but also outside. This gave rise to the issue of regulation of the issues related to the use of information technology and digital documents which required an update of legislation in India with regard to electronic evidence.[167]

1. Emergence of Digital Evidence in the Indian Legislation

With the expansion of digital communication and e-commerce, India needed amendments to its legislative norms regarding the evidential value of electronic documents in addition to other acts such as the Indian Evidence Act 1872, the Indian Penal Code 1860, and the Bankers' Books Evidence Act 1891.[168] For example, the creation of the IT Act 2000, based upon the UNCITRAL

[164] T. Reddy, Evidence Sharing Across Borders in Cybercrime, 21 Digital Evid. J. (2021).
[165] N. Chatterjee, Sovereignty and Cyber Enforcement, 14 J. Const. L. (2023).
[166] UNODC, Comprehensive Study on Cybercrime (2020).
[167] P. Kumar, Admissibility of Electronic Evidence in India, 12 J. Indian L. & Tech. 45 (2022).
[168] R. Sharma, Digital Evidence and the IT Act: A Legal Analysis, 18 Cyber L. Rev. 101 (2021).

ISSN: 2582-6433

Model Law on Electronic Commerce, served as a ground-breaking act which laid down basic principles for electronic transactions and digital evidence.[169]Amendments to the IT Act extended the provisions of the latter in relation to electronic evidence.[170]

2. Adaptation by the Judiciary and Legislature

The legal framework was hindered by the distinct nature of digital evidence that involved:

- Ease of tampering and modification.
- Issues of credibility and integrity.
- Need for technical knowledge to interpret and analyze.

To overcome such hindrances, India passed the Bharatiya Sakshya Adhiniyam (BSA), 2023, which marks a milestone in the history of the Evidence Act, offering an elaborate mechanism for handling electronic evidence.[171] The BSA, 2023, makes electronic documents a primary source of evidence in courts and specifies guidelines regarding authentication, forensic examination, and admission in proceedings.[172]

3. Significance of Digital Evidence in Modern Litigation

Modern litigation relies heavily on digital evidence, which include the following items:

- Emails, texts, and chat messages.
- Online social media and digital communications.
- Financial documents and electronic bank statements.

[169] United Nations Commission on International Trade Law (UNCITRAL), Model Law on Electronic Commerce (1996).
[170] S. Verma, IT Act Amendments and Cyber Evidence, 9 Indian J. Cybercrime L. 33 (2020).
[171] M. Yadav, Bharatiya Sakshya Adhiniyam 2023: Transforming Electronic Evidence, 15 Digital Evid. J. 12 (2023).
[172] A. Joshi, Challenges in Handling Electronic Evidence, 7 Indian Evid. L. Q. 55 (2022).

ISSN: 2582-6433

The BSA 2023 and other amendments enhance the validity of digital evidence and streamline court procedures. By introducing provisions related to the use of electronic documents, forensics, and judicial acceptance, the Act accounts for the contemporary state of affairs.[173]

4. Problems and Legal Consequences

However, the problems that arise during the handling of digital evidence remain relevant for the judiciary today:

- Chain of custody issues and risks of tampering.
- Technical expertise of forensic experts involved.
- Problems with gaining access to cloud-stored information from other jurisdictions.

In light of these problems, the BSA 2023 and the BNSS, 2023 can be considered useful additions.

Admissibility of Electronic Records under the Bharatiya Sakshya Adhiniyam (BSA), 2023

The Bharatiya Sakshya Adhiniyam (BSA), 2023 offers an updated and improved version concerning the admissibility and recognition of electronic records before the courts of India. Some important features include:

1. Equivalent Status of Electronic Records

- Section 61 of the BSA provides that the electronic record is considered legally equal to other forms of documentary evidence.

- Electronic records, as primary records, will include those made in electronic devices like hard drives, server rooms, and cloud platforms.

- It eliminates delays associated with secondary evidences and/or intermediate certifications.[174]

2. Standardization of Section 65B Certificate

[173] T. Singh & K. Agarwal, Digital Evidence in Indian Courts: Contemporary Trends, 21 Int'l J. Cyber L. (2023).
[174] Bharatiya Sakshya Adhiniyam [BSA] § 61 (2023).

ISSN: 2582-6433

- The BSA adopts the idea of certification of electronic records under Section 65B of the Indian Evidence Act, 1872, but with a detailed procedure.
- In order to prove that the evidence was produced from a legal and reliable source, it is essential to have a certificate of authentication.
- Persons qualified to make the certification include system administrators or electronic record custodians.[175]
- In this manner, the BSA resolves disputes concerning Section 65B that caused the inadmissibility of digital evidence.[176]

3. Practical Implications

- The courts have clear guidelines on the acceptance of electronic records as admissible evidence.
- Technical and forensic procedures have become uniform to build judicial trust in digital evidence.
- This reform facilitates the prosecution of cybercrimes, including cyberstalking, money laundering, and digital identity theft.

Integrity and Authentication: Ensuring Reliability of Digital Evidence

Digital evidence plays an important role in cybercrime cases. The admissibility of digital evidence relies significantly on authentication, integrity, and reliability since digital evidence can be easily falsified or tampered with.

1. Authentication

- Authentication confirms that digital evidence is legitimate.
- According to Section 65B of the Indian Evidence Act, 1872, and further expanded under the BSA/BSS, it is necessary to include a certificate issued by the system administrator or the custodian of the computer system.[177]

[175] Bharatiya Sakshya Adhiniyam [BSA] § 65B (2023).
[176] N. F. O. A., Reforms Relating to Electronic Evidence and Cybercrime (2023).
[177] Indian Evidence Act, 1872 § 65B.

ISSN: 2582-6433

- Apart from the certification requirement, contemporary standards also accept methods of authentication based on digital signatures, encryption, and audit logs.[178]

2. Chain of Custody

- An unbroken chain of custody guarantees the integrity of the evidence throughout its lifecycle from seizure through presentation in court.
- Each person handling the digital evidence must confirm his or her actions and involvement in dealing with it.[179]
- Special attention to the process of collecting digital evidence is made in the BSS because of the extreme manipulability of digital evidence.[180]

3. Forensic Procedures

- Digital evidence is collected and preserved in accordance with the principles of forensic science, which involve such techniques as hash values to ensure file uniqueness.
- Police officers provide read-only access when inspecting storage media.[181]

4. Factors Affecting Reliability

- The reliability of evidence can be compromised by cyberattacks, human errors, or flaws in the system itself.
- Expert witness testimony is commonly sought out by courts to determine if evidence has been obtained, stored, and processed through recognized scientific procedures.[182]

5. Case Law

In the landmark case of ***Anvar P.V. vs. P.K. Basheer,*** the Indian Supreme Court held that digital evidence could not be introduced into court proceedings unless certified in accordance with Section 65B.[183] Similarly, comparative standards, such as the Frye and Daubert criteria applied in the U.S.,

[178] Bharatiya Sakshya Adhiniyam [BSA] §§ 61–65B (2023).
[179] Bharatiya Sakshya Adhiniyam [BSA] (2023).
[180] K. Sharma, Digital Evidence in India: Integrity and Authentication, 11 Indian J. Cyber L. 27 (2023).
[181] P. Gupta, Forensic Methods for Cybercrime Investigation, 5 Indian J. Forensic Sci. 44 (2022).
[182] R. Mehta, Challenges in Digital Evidence Reliability, 8 J. Indian Cyber L. 56 (2023).
[183] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.

ISSN: 2582-6433

also mandate that techniques employed in collecting evidence be generally accepted and scientifically sound.[184]

Role of Expert Evidence and Forensic Analysis

To conclude, the veracity and authentication of digital evidence lie at the very heart of its admissibility in contemporary legal processes.

1. Importance of Expert Opinion in Digital Evidence

The validation and analysis of digital evidence can often require specific technical knowledge that exceeds the average court's capabilities. With this consideration in mind, it is clear why the Indian Evidence Act of 1872 and the Bharatiya Sakshya Adhiniyam, or BSA, of 2023 include provisions that allow the inclusion of expert opinion regarding electronic records.[185]

Despite the fact that such opinions are usually highly influential, they are not considered conclusive evidence and can be challenged by the judiciary.

2. Section 45A of the Indian Evidence Act of 1872

- Section 45A of the Indian Evidence Act was added to the legislation through the Information Technology Amendment Act of 2008.[186]
- The section includes the opinion of the "Examiner of Electronic Evidence," an official appointed under Section 79A of the IT Act of 2000, as evidence.[187]
- This povision accounts for the vulnerability of digital data to alteration and legitimizes the presence of qualified forensic experts.
- Nevertheless, the opinion of the expert is advisory and does not impose obligations on the judiciary.

3. Section 61 of the BSA, 2023

[184] Frye v. United States, 293 F. 1013 (D.C. Cir. 1923); Daubert v. Merrell Dow Pharmaceuticals, 509 U.S. 579 (1993).
[185] Indian Evidence Act, 1872, §§ 45, 45A.
[186] Information Technology (Amendment) Act, 2008.
[187] Information Technology Act, 2000, § 79A.

ISSN: 2582-6433

Bharatiya Sakshya Adhiniyam, 2023, in Section 61 continues to evolve the rules relating to expert evidence with respect to electronic record.[188]

This provision allows the courts to take advantage of technical expertise while maintaining judicial discretion for determination of evidentiary value.

The provision takes into account modern technological developments such as cloud computing, blockchain technology, etc.

4. Expert Evidence in Relation to Authentication

The role of the forensic expert becomes very important when it comes to establishing the validity of electronic evidence:

- Chain of custody to rule out any tampering.
- Detection of manipulation and alteration of the digital data.
- Data recovery in case of deletion or encryption.
- Preparation of forensics report and creation of hash value.

These experts play an important part in cases related to cyber-crime, financial fraud, terrorism, or dispute about electronic communication.[189]

5. Issues With Forensic Evidence

There are various issues associated with forensic evidence in India:

- Inadequate infrastructure and facilities.
- Long backlog of cases delaying forensic examination.
- Absence of standardization and accreditation of forensic labs.

These issues may affect the credibility and efficiency of expert testimony, highlighting the need for institutional strengthening.[190]

[188] Bharatiya Sakshya Adhiniyam [BSA], 2023, § 61.
[189] P. Gupta, Forensic Analysis in Cybercrime Investigation, 6 Indian J. Forensic Sci. 32 (2022).
[190] Himani Raj Goyal, Role of Expert Evidence in Digital Crimes (2023).

ISSN: 2582-6433

Judicial Approach to Electronic Evidence in India

The evolution of law governing electronic evidence in India has primarily followed a judge-made law trajectory in light of the shortcomings in legislations with regard to advancements in technology. This judicial interpretation of the statute has especially impacted the interpretation of Section 65B of the Indian Evidence Act, 1872 and has also continued to affect the same provision in its successor, Bharatiya Sakshya Adhiniyam, 2023.[191]

1. Early Judicial Tolerance: ***State (NCT of Delhi) v. Navjot Sandhu (2005)***

State (NCT of Delhi) v. Navjot Sandhu[192] also called the Parliament Attack Case was one such instance in which the Supreme Court of India followed a lenient approach to electronic evidence.

According to the court, electronic records like call data records can also be admitted for evidence as oral evidence even in the absence of a Section 65B certificate under Sections 63 and 65 of the IEA.This judicial interpretation has led to undermining the strictness and mandatory requirement of certification. Although the case helped ease the use of electronic evidence in criminal prosecutions, there were concerns about the standards for admissibility of such evidence.

2. Doctrinal Shift: ***Anvar P.V. v. P.K. Basheer (2014)***

A decade later, in the decision of Anvar P.V. v. P.K. Basheer,[193] the Supreme Court overruled Navjot Sandhu and took a rigid stance:

It stated that Section 65B(4) certification is necessary for secondary electronic evidence admissibility.The requirement is that electronic documents should conform to Sections 65A and 65B and not the general laws regarding secondary evidence.

This decision corrected the legislative intent and ensured authentication and reliability, but it was heavily criticized for causing practical problems for getting certification from external sources.

3. Stressing Significance: ***Tomaso Bruno v. State of Uttar Pradesh (2015)***

[191] Bharatiya Sakshya Adhiniyam [BSA], 2023; Indian Evidence Act, 1872.
[192] State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600.
[193] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.

ISSN: 2582-6433

In the landmark judgment of Tomaso Bruno v. State of Uttar Pradesh,[194] the Court reiterated the significance of digital evidence, specifically the CCTV video clips.

It said that failure to do so might lead to negative implications.The judgment highlighted the importance of adhering to the Section 65B conditions for admissibility.

4. Provisional Relaxation: ***Shafhi Mohammad v. State of Himachal Pradesh (2018)***

In Shafhi Mohammad v. State of Himachal Pradesh,[195] the Supreme Court made a provisional relaxation:

It observed that the certificate under Section 65B need not be insisted upon the Constitution Bench when the party concerned is without the device.Here, equity prevailed over rigid technicality in a move to ensure that people have fair access to justice. However, this resulted in uncertainty since it contradicted the rigorous position that was taken in Anvar.

5. Ultimate Clarity: ***Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020)***

Finally, in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal,[196] settled the matter when it ruled that:

Certification under Section 65B was mandatory for admission of evidence in electronic form.The Section 65B certification was essential, not procedural.Where the party is unable to produce the certificate, other measures such as issuing of orders by the court could be considered.

6. Legal Evidentiary Provisions Post-2023 under BSA

Following the promulgation of the Bharatiya Sakshya Adhiniyam, 2023, the legal provisions in respect of electronic evidence have been updated, while keeping continuity:

Section 57 BSA is analogous to Section 65A IEA (special provisions regarding electronic evidence).

Section 63 BSA substitutes Section 65B IEA but keeps the requirement of certificate.

[194] Tomaso Bruno v. State of Uttar Pradesh, (2015) 7 SCC 178.
[195] Shafhi Mohammad v. State of Himachal Pradesh, (2018) 2 SCC 801.
[196] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.

ISSN: 2582-6433

Section 61 BSA is similar to Section 45A IEA (expert opinion on electronic evidence).[197]

Continuity implies the continued use of judicial precedents like Arjun Panditrao in interpreting the law post-Bharatiya Sakshya Adhiniyam.

However, it is expected that there will be flexibility on the part of the courts with respect to evolving technology:

- Cloud Computing
- Blockchain Verification
- AI-generated Evidence

Addressing Challenges in Electronic Evidence: A Comparative Jurisdictional Study

The increasing complexities involved in the act of cyber crimes require strong systems for collecting, preserving, and admitting the evidence obtained through these channels. Comparing best practices worldwide indicates techniques that can be adopted by India to improve upon their system.

- **The United States of America** - The US government has adopted an elaborate system of laws which are embodied in the Federal Rules of Evidence and Federal Rules of Criminal Procedure. These rules provide for the procedure to be followed in dealing with digital evidence and govern the admission of digital evidence. There is also the presence of specialized agencies like the FBI's Cyber Division that plays an important role in dealing with cases of cybercrimes. There is also considerable public and private partnership in the form of organizations like the National Cyber-Forensics & Training Alliance.[198]
- **European Union** - In the same way, the European Union follows a collaborative and harmonized approach through the Budapest Convention on Cybercrime, which offers a comprehensive framework for international cooperation when dealing with electronic evidence. Organizations like the European Cybercrime Centre of Europol help in conducting investigations and forensic examinations for the member countries, whereas organizations like the European

[197] Himani Raj Goyal, Judicial Approach to Electronic Evidence in India (2023).
[198] Federal Rules of Evidence (U.S.); Federal Bureau of Investigation, Cyber Division Overview (2023).

ISSN: 2582-6433

Cyber Security Organisation focus on facilitating collaboration between the public and private sectors.[199]

- **Australia** - Australia, in turn, concentrates on institutional coordination and capacity building in relation to the Cybercrime Act, 2001, which sets the legal framework for dealing with cyber offenses and electronic evidence. The Australian Cyber Security Centre is central to coordination activities between law enforcement agencies, intelligence agencies, and relevant industries. Additionally, the Australian Cyber Security Centre facilitates specialist training and support, hence contributing to improving the skills of digital forensic specialists and optimizing the entire process of conducting investigations into cybercrimes.[200]
- **United Kingdom** - The UK demonstrates progress in legislative reform and institution specialization in managing electronic evidence. The Investigatory Powers Act, 2016, gives investigative agencies greater powers in collecting and analyzing digital information, whereas the National Cyber Crime Unit at the National Crime Agency spearheads cybercrime investigations involving a variety of stakeholders. In addition, professional organizations, such as the Chartered Society of Forensic Sciences, stress the importance of training, certification, and professional standards in digital forensics.[201]
- The above comparison shows that for proper electronic evidence management, there is need for good legal frameworks, cybercrime units, cooperation from other countries, collaboration between private and public institutions, and training in digital forensics. If the above factors are taken into consideration by India, they will help it build its legal and institutional capacity through the Bharatiya Sakshya Adhiniyam, Bharatiya Nagarik Suraksha Sanhita, and the Information Technology Act.[202]

[199] Council of Europe, Convention on Cybercrime (Budapest Convention), 2001; Europol, EC3 Reports (2023).
[200] Cybercrime Act 2001 (Cth) (Austl.); Australian Cyber Security Centre, Annual Cyber Threat Report (2023).
[201] Investigatory Powers Act 2016 (U.K.); National Crime Agency, NCCU Overview (2023).
[202] SSRN, Electronic Evidence Management in Comparative Perspective, No. 4475784 (2023).

ISSN: 2582-6433

"Gaps in Cyber Law and the Need for Legal & Policy Reforms in the Digital Age for Strengthening the Protection of Women in Cyberspace under the New Criminal Law Regime"

Gaps in Cyber Law

India's fast-paced digitization process has thrown many challenges in front of the Indian cyber laws, which are ill-equipped to counter cyber crimes against women. The Information Technology Act 2000, which is a product of its times, lacks provisions to address new age cyber crimes, especially AI-based offenses, deep fakes, and cyber harassment. Besides, since there is no gender-specific provision in place, protection of women from such technology-related crimes remains ineffective.[203]

Lack of adequacy in penal provisions is yet another critical lacuna. The punishments imposed for cybercrimes are not commensurate with the seriousness of the offense committed. For instance, privacy violation, cyber frauds, and massive data breach have not been adequately punished. Consequently, offenders remain unmoved by such laws.[204]This issue is further compounded by the ambiguity in terms of definitions and inadequate acknowledgment of evolving technologies. The vagueness of certain terms and outdated provisions make it difficult for law enforcement officials to enforce the law. Furthermore, the past lack of an effective data protection mechanism, despite the implementation of the Digital Personal Data Protection Act, 2023, raises enforcement concerns.[205]

The procedural and enforcement challenges associated with cybercrime further exacerbate the issue of inadequate substantive legislation. Most of the time, law enforcement agencies do not have the technological skills or capacity to effectively deal with cybercrime cases. This causes a lack of quality evidence gathering and prosecution. The difficulty of jurisdiction and reporting of the offense by the victims makes the enforcement process even more challenging.[206]

Need for Legal & Policy Reforms in the Digital Age

In view of all these problems, there is an urgent need for comprehensive legal and institutional reforms. It is crucial to bring about procedural reforms in the courts to help deal with the problems surrounding digital evidence. Although the Bharatiya Sakshya Adhiniyam, 2023 represents

[203] Information Technology Act, No. 21 of 2000, India.
[204] Law Commission of India, Report on Cyber Crimes (2022).
[205] Digital Personal Data Protection Act, 2023, India.
[206] NCRB, Crime in India Report (2022).

ISSN: 2582-6433

progress, as it recognizes the legitimacy of electronic records, more needs to be done to make the process of judicial decision-making uniform.[207]

It is vital to build capacity both in the judiciary and among the police. Specialized technical knowledge is needed in cybercrime adjudication, which requires continuous training and development. Creating cyber courts can help to ensure that there is speedy trial and efficient dealing with digital evidence.[208]It is important for institutional reforms to ensure better coordination and capacity among various institutions, including Indian Computer Emergency Response Team. The creation of a central cybersecurity authority may prove helpful in ensuring effective action. Institutional reforms will also have to deal with the problem of digital evidence collection and authentication.[209]

Due to the transnational character of cybercrimes, it is important that international collaboration takes place. The alignment of domestic laws with international norms such as the Budapest Convention on Cybercrime will aid in conducting cross-border investigations and evidence sharing. It should be noted that reform initiatives need to be victim-centered, especially towards female victims, by providing them with fast complaints procedures, anonymity, and protective measures.[210]Lastly, in addition to legal changes, policy reforms are also needed. Prevention, awareness-raising, and compliance measures are vital to decrease cyber threats. A comprehensive approach that protects individuals' rights and secures the nation simultaneously will be key in developing a future-proof cyber legal system in India.[211]

Findings

- Legal Inadequacy – Current laws, especially the IT Act, cannot deal with new developments in technology such as artificial intelligence, blockchain, and internet of things.
- Penalties Insufficient – Penalties for cybercrimes are not deterrent enough.
- Poor Data Protection – Lack of enforcement of data protection measures makes individuals vulnerable to privacy invasion.
-

[207] Bharatiya Sakshya Adhiniyam, 2023.
[208] Law Commission of India, Judicial Reforms Report (2022).
[209] Indian Computer Emergency Response Team (CERT-In), Annual Report (2023).
[210] Council of Europe, Convention on Cybercrime (2001).
[211] Ministry of Electronics & Information Technology, National Cyber Security Policy (2023).

ISSN: 2582-6433

- Fragmentation of Agencies – Several agencies with overlapping mandates hamper coordination.Technical Competency Lacking – The enforcement agencies lack technical competency in the handling of digital forensics.
- Difficulties in Jurisdiction – Multinational character of cybercrime makes investigation difficult.Electronic Evidence Issues – Management of electronic evidence contributes to delays in adjudication.
- Underreporting and Low Awareness – Failure to report crimes affects the efficiency of legal mechanism.
- Balance of Powers – Surveillance can result in infringement of fundamental rights.

Recommendations

- Legal Reforms – Modify laws on cyberspace to cover new technology and cyber risks.
- Deterrence Through Penalties – Ensure that penalties accorded are commensurate with the crime committed.
- Cyber Courts – Set up special courts to ensure efficient handling of cyber crimes.
- Capacity Development – Train law enforcement agents, lawyers, and magistrates on digital forensics and cyber law.
- Establishment of Central Authority – Set up a single institution to oversee cyber affairs.
- Investment in Infrastructure – Develop infrastructure such as forensic laboratories and equipment.
- International Legal Collaboration – Ensure international laws facilitate mutual cooperation in cyber crimes investigations.
- Victim Protection – Provide adequate measures aimed at protecting victims and making it easy for them to report crimes.
- Compliance With Data Protection Laws – Ensure strict adherence to data protection laws by organizations.
- Cyber Awareness – Raise public awareness through cyber education.

ISSN: 2582-6433

Bibliography

A. Books

- Manuel Castells, *The Rise Of The Network Society* (2D Ed. 2010). Jan Van Dijk, *The Network Society* (3D Ed. 2012).
- Danah Boyd, *It's Complicated: The Social Lives Of Networked Teens* (2014). Pavan Duggal, *Cyber Law In India* (2016).
- Aparna Viswanathan, *Cyber Law: Indian And International Perspectives* (2012). Debarati Halder & K. Jaishankar, *Cybercrime And The Victimization Of Women* (2011).
- K. Jaishankar, *Cyber Criminology* (2011).

B. Journal Articles

- Anita Gurumurthy, Gender and Cybersecurity, 53 ECON. & POL. WKLY. (2018).
- S.K. Verma & Raman Mittal, Legal Dimensions of Cyber Crime in India, J. INDIAN L. INST. (2004).
- Arpita Sharma, Cyber Crimes Against Women in India, 3 INDIAN J.L. & TECH. (2017).
- Avni Katiyar, Cybercrime and Procedural Challenges in India, 23 J. INDIAN L. & TECH. 45 (2022).
- Pavan Duggal, Digital Evidence and Cyber Forensics in India: Legal and Investigative Challenges, 20 J. INDIAN L. & TECH. (2020).
- Debarati Halder & K. Jaishankar, Cyber Crime and the Indian Legal Response, 26 CRIM. L.J. (2019).
- S. Girdhar & R. Singh, Forensic Readiness and e-Evidence Management, 14 INT'L J. DIGITAL CRIME & FORENSICS (2019).

C. Reports & Institutional Publications

- Nat'l Crime Recs. Bureau, *Crime In India* (Latest Ed.).
- U.N. Women, *Cyber Violence Against Women And Girls* (2020).
- Ministry Of Home Affairs, Gov't Of India, *Criminal Law Reforms In India* (2023). Nat'l Cyber Sec. Policy (2013) (India).
- Indian Computer Emergency Response Team (Cert-In), Guidelines (India).
- U.N. Broadband Comm'n, Report (2015).
- Dubravka Šimonović (Special Rapporteur On Violence Against Women), Rep. On Violence Against Women, U.N. Doc. A/Hrc/38/47 (2018).

ISSN: 2582-6433

D. Statutes & Legislative Materials

INDIA CONST.

- Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India). Information Technology (Amendment) Act, 2008, No. 10 (India).
- Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India).
- Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46, Acts of Parliament, 2023 (India). Bharatiya Sakshya Adhiniyam, 2023, No. 47, Acts of Parliament, 2023 (India).
- Code of Criminal Procedure, 1973 (India). Indian Evidence Act, 1872 (India).
- Indecent Representation of Women (Prohibition) Act, 1986 (India).
- UNCITRAL Model Law on Electronic Commerce, G.A. Res. 51/162 (Dec. 16, 1996).

E. Cases

- Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1 (India). Maneka Gandhi v. Union of India, (1978) 1 S.C.C. 248 (India).
- K.S. Puttaswamy v. Union of India, (2017) 10 S.C.C. 1 (India). Anvar P.V. v. P.K. Basheer, (2014) 10 S.C.C. 473 (India).
- Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 S.C.C. 1 (India). Sharat Babu Digumarti v. Gov't of NCT of Delhi, (2017) 2 S.C.C. 18 (India).
- State of Tamil Nadu v. Suhas Katti, C.C. No. 4680 of 2004 (Chennai Dist. Ct., India). Gobind v. State of M.P., (1975) 2 S.C.C. 148 (India).
- People's Union for Civil Liberties v. Union of India, (1997) 1 S.C.C. 301 (India). Lalita Kumari v. Gov't of U.P., (2014) 2 S.C.C. 1 (India).
- Neelam Mahajan Singh v. Comm'r of Police, Delhi HC (India). Ritu Kohli v. Union of India (2001) (India).

F. Online Sources & Miscellaneous

- Nishith Desai Assocs., *Information Technology Act: Analysis* (2018). SSRN, Cyber Law Research Papers, https://www.ssrn.com.
- Various cybersecurity policy reports and government publications.