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

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur.Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time &Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

EVOLVING CYBERCRIME AND INDIA'S LEGAL RESPONSE: A CRITICAL ANALYSIS OF THE IT ACT AND BHARATIYA NYAYA SANHITA, 2023

AUTHORED BY - THARUN R
LL.M. Candidate (Criminal Law), 2024–2025,
CMR University, School of Legal Studies, Bengaluru

Abstract:

In today's increasingly globalized world cybercrime has emerged as one of the most pressing challenges faced by individuals, organizations and governments. The rapid expansion of the digital space has led to a surge in cybercrimes, including data breaches, identity theft, online fraud, and cyber-attacks, all of which have profound social, economic and political implications. As technology advances, the nature of cybercrime evolves, making it more complex and difficult to combat. With the increasing frequency and severity of cybercrimes, there is a growing need for robust legal frameworks to effectively address these threats. This article provides a comprehensive analysis of India's legal provisions related to cybercrime, focusing on the Information Technology Act, 2000 (IT Act) and the Bharatiya Nyaya Sanhita, 2023 (BNS). The article evaluates the effectiveness of the laws in tackling cybercrime, emphasizing various offenses. The article concludes by offering suggestions for strengthening India's legal framework to better confront the ever-evolving landscape of cybercrime.

Keywords: Cybercrime, Information Technology Act, 2000, Bharatiya Nyaya Sanhita, 2023, Legal Framework, Analysis

1. Introduction

In the last several decades, the globe has seen incredible technological progress, with the rise of the internet being only one example. Modern life would not have been possible without the Internet and other forms of modern technology. As we progress farther into the age of networking and digitization, the Internet has enabled the globe to expand in terms of communication, and it continues to do so to this day. While the expansion of cyberspace has undoubtedly brought many advantages, it has also opened up new avenues for criminal activity.

ISSN: 2582-6433

When a computer is either utilized as a weapon or a victim in illegal conduct, it is known as a cybercrime. People who commit cybercrimes have extensive knowledge of technology. Virtual crimes, unlike traditional ones, can be committed without revealing the perpetrators' identities. The issues of identifying the criminals, jurisdiction, and proper application of cyber laws are universal. Additionally, the cyber laws need to constantly keep up with the pace of technical changes to effectively tackle cybercrimes.

There is a worldwide impact and reach of cybercrimes. Businesses and even nations are not safe from these threats; they affect more than just individuals. They involve crimes like unwarranted mass surveillance, cyber terrorism, hacking, cyber pornography, interception of confidential information, copyright infringement/piracy, etc. Issues connected to these crimes are, thus, high-profile in nature.

The Bhartiya Nyaya Sanhita, 2023[1] (BNS), which came into force on 1 July 2024, replaced the Indian Penal Code, 1860 (IPC) and recognizes the growing threat of cybercrime in India. Cybercrimes are now punishable under both the BNS, 2023, and the Information Technology Act, 2000[2], which was revised in 2008[3]. These laws define the nature of cybercrimes and prescribe penalties for them. While the Parliament's efforts to establish a legal framework for cyber regulation are commendable, the effectiveness of these laws remains questionable due to existing grey areas in the legislation.

2. Cyber Crimes in India

Cybercrime is on the rise in India, as reflected in the increasing number of reported cases. However, the country has achieved a significant milestone in cybersecurity by attaining a Tier 1 classification in the Global Cybersecurity Index (GCI) 2024, issued by the International Telecommunication Union (ITU). With an impressive score of 98.49 out of 100, India joins the ranks of 'role-model' nations, demonstrating a strong commitment to global cybersecurity principles.[4] In India, cybercrimes can take many different forms, ranging from hacking and cyberstalking to phishing and fraud. Online financial fraud, credit/debit card fraud, and phishing account for the majority of cybercrimes in India. One of the most prevalent

[1] The Bharatiya Nyaya Sanhita, 2023. No. 45 of 2023 (India).
[2] The Information Technology Act, 2000 No. 21, Acts of Parliament, 2000 (India)
[3] The Information Technology (Amendment) Act, 2008. No. 10, Acts of Parliament, 2009 (India)
[4] Press Information Bureau, India Achieves Tier 1 Status in Global Cybersecurity Index 2024, Ministry of Communications (Sept. 20, 2024), https://pib.gov.in/PressReleasePage.aspx?PRID=2057035.

ISSN: 2582-6433

cybercrimes in India is cyber accident scams, in which criminals use phony advertisements or websites to trick victims into clicking on harmful links and downloading malicious software, after which they use the program to gather personal information.

Hacking, the primary worry of corporations, cannot be neglected while talking about cybercrimes. Hackers utilize a range of harmful software, including Trojan horses, spyware, and ransomware, to steal people's data and demand money. With 560 million internet users, India is the world's second-largest online market. In 2024, cybercrime cases in India saw a significant rise. Over 740,000 cases were reported to the Indian Cyber Crime Coordination Centre (I4C) within the first four months of the year alone.[5] Additionally, by September 2024, the total number of cases surged to 1.2 million, with an average of 7,000 cases reported daily.[6] Cybercrime is a growing problem in India, with thieves utilizing increasingly sophisticated tactics to target victims. The country's lack of public knowledge about cybercrime and lack of competent cybersecurity specialists are factors that contribute to this issue. Cyberattacks have recently targeted well-known companies including Tata Power, CDSL, and AIMS (Delhi), which are all considered national essential assets in various areas.

Cybercriminals come from varied backgrounds and can range from solitary hackers to criminal syndicates. In addition to individual hackers that use malware or phishing to steal information from their victims, there are hacker collectives that utilize advanced software to obtain private information and conduct cyberattacks against governments and businesses.

Cybercrime is also being used by organized criminal gangs to generate revenue, and their ability to operate more covertly has been made possible by the growth of the dark web and cryptocurrencies. Though there are cyber regulations in India, cybercriminals work with impunity and keep flourishing. This might be because the law hasn't been applied strictly enough to stop online crime.

3. Legal Framework Governing Cyber Crimes in India

The Cyber law is particularly significant in countries like India, where the internet is widely used. The purpose of the law was to protect people and organizations from cybercrime. It is

[5] Statista Research Department, India: Cyber Crime Cases Reported to I4C 2024, Statista, https://www.statista.com/statistics/1499739/india-cyber-crime-cases-reported-to-i4c/
[6] Cyber Crimes in India 2024: 7,000 Cases Registered Daily!, Aseem Juneja (Dec. 18, 2024), https://aseemjuneja.in/cyber-crimes-in-india/.

ISSN: 2582-6433

possible for other people or organizations to take legal action against a person who violates and contradicts the law's provisions. In the following situations, cyber law might be necessary:[7]

i. In the case of fraudulent transactions, everyone involved in stock-related transaction is protected by the law because all transactions are now done in Demat form.

ii. The majority of Indian businesses use electronic passwords. A business may use this law to prevent the misuse of sensitive data.

iii. Due to rapid technological advancements, a variety of government agencies, including income tax returns and service tax returns, are being completed electronically. Since anyone can misuse these websites by hacking government websites, cyber law is necessary for legal action.

iv. Nowadays, debit and credit cards are used for shipping. Unfortunately, psychiatrists who use the internet have cloned these crypt and debit cards. The technique that makes it possible for a third party to obtain access to your personal information is known as "cloning" of a credit or debit card.[8] The reason this is possible is because violators of Section 66 of the IT Act may face a three-year probationary period and a fine of up to one lakh rupee if they attempt to use an electronic probation in a dishonest or fraudulent manner.

v. electronic communications and digital signatures are typically utilized in business transactions. Anyone involved in the use of electronic communications and digital signatures might easily misuse them.[9] The law protects against these kinds of scammers.

3.1. important Provisions of Information Technology Act, 2000

The Information Technology Act of 2000 and the Bhartiya Nyaya Sanhita 2023 (IPC 1860) are the two primary laws in India that address cybercrimes and provide for their punishment. The Information Technology Act of 2000, also known as the IT Act, was enacted to grant legal status to electronic trade and transactions in India. This law aimed to regulate online activities, promote e-commerce, and address the growing concern of cybercrimes.

On October 17, 2000, the Indian Parliament approved the Information Technology Act, 2000

[7] Aishwarya Agrawal, Challenges to Indian Law and Cyber Crime Scenario in India, LawBhoomi (Mar. 14, 2025), https://lawbhoomi.com/challenges-to-indian-law-and-cyber-crime-scenario-in-india/.
[8] Sophia Ellis, What is Cyber Law? A Comprehensive Guide, THE KNOWLEDGE ACADEMY (Feb. 12, 2025), https://www.theknowledgeacademy.com/blog/cyber-law/.
[9] Ibid

ISSN: 2582-6433

(IT Act No. 21 of 2000), which was based on the United Nations Model Law on Electronic Commerce (UNCITRAL), 1996.[10] This landmark legislation was implemented to address the increasing threat of digital crimes and to regulate online transactions. The law focused on crimes such as hacking, identity theft, and cyber fraud, while also providing a framework for electronic governance and the legal recognition of digital signatures.

However, with the continuous advancement of technology and the emergence of new cybercrimes, the original Act required amendments to keep pace with these developments. As a result, in 2008, the Information Technology (Amendment) Act, 2008 was introduced to tackle emerging offenses such as pornography, child pornography, cyberterrorism, and voyeurism. This amendment also introduced significant provisions, such as Section 69, which granted authorities the power to intercept, monitor, or decrypt any information through computer resources. These amendments aimed to address the growing threats of cybercrimes, including phishing, cyberstalking, and cyberterrorism, and to close legal loopholes that hindered effective enforcement.

Furthermore, the Indian Computer Emergency Response Team (CERT-In) was established under the 2008 Amendment to provide technical assistance to law enforcement agencies and respond to cybersecurity incidents. In 2021, additional measures were introduced with the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, which amalgamated the draft Intermediaries Rules of 2018, OTT Regulations, and the Code of Ethics for Digital Media. These rules were designed to regulate social media platforms, digital news media, and online intermediaries, addressing concerns related to misinformation, user safety, and content moderation.

One notable change came in 2015 when the Indian Supreme Court[11] ruled Section 66A of the Information Technology Act, 2000 unconstitutional. This section had criminalized the sending of offensive communications via communication services, but it was criticized for its vague language and potential to restrict free speech. As a result, the provision was struck down, reinforcing the need for clearer and more balanced regulations around digital expression.

[10] Vijaykumar Shrikrushna Chowbe, The Concept of Cyber-Crime: Nature & Scope (Feb. 21, 2011), https://ssrn.com/abstract=1766238.
[11] Shreya Singhal v. Union of India, (2015) 5 SCC 1, Supreme Court of India, March 24, 2015.

ISSN: 2582-6433

In conclusion, while the Information Technology Act of 2000 remains a cornerstone of India's legal framework for tackling cybercrimes, it has undergone multiple amendments to address new challenges posed by rapidly evolving technologies. Some of the main Penalties and offenses listed in IT Act 2000:

- **Section 66**[12]: It focuses on unauthorized actions involving computers or electronic systems. It penalizes anyone who dishonestly or fraudulently engages in activities such as accessing computer systems, altering or destroying data, or causing damage to computer systems or networks without proper authorization. This section is aimed at addressing the misuse of technology, including hacking or other forms of digital vandalism. Violators can face imprisonment of up to three years, a fine of up to five lakh rupees, or both, depending on the nature and extent of the offense.
- **Section 66B**[13]: it addresses the receipt of stolen computer resources or communication devices. It penalizes anyone who dishonestly receives or retains any stolen computer or communication device, knowing or having reason to believe that it is stolen. The section emphasizes the need to discourage the circulation and use of stolen digital assets. Violators can face imprisonment of up to three years, a fine of up to one lakh rupees, or both.
- **Section 66C**[14]: it addresses the offense of identity theft. It penalizes anyone who fraudulently or dishonestly uses another person's identity, such as their electronic signature, password, or other unique identification features, without authorization. This provision aims to protect individuals from the misuse of their digital identity, ensuring accountability for such violations. The punishment for this offense includes imprisonment of up to three years, a fine of up to one lakh rupees, or both.
- **Section 66D**[15]: Section 66D of the Information Technology Act, 2000, deals with the offense of cheating by personation using computer resources. It penalizes anyone who, by impersonating another person, cheats or deceives someone through the use of electronic communication or computer devices. This provision is aimed at addressing cybercrimes like phishing, online scams, and fraudulent impersonation to gain money or sensitive information. The punishment includes imprisonment of up to three years, a fine of up to one lakh rupees, or both.

[12] S 66; Ibid.
[13] S 66B; Ibid.
[14] S 66C; Ibid.
[15] S 66D; Ibid.

ISSN: 2582-6433

- **Section 66E**[16]: it focuses on protecting individuals' privacy. It penalizes anyone who intentionally captures, publishes, or transmits images of a person's private area without their consent, under circumstances where privacy is reasonably expected. This includes situations where the individual may not be aware that their private space is being recorded or shared. The offense is considered a violation of personal privacy, and the punishment includes imprisonment of up to three years, a fine of up to two lakh rupees, or both.
- **section 66F**[17]: it deals with the offense of cyber terrorism. It criminalizes acts carried out with the intent to threaten the unity, integrity, security, or sovereignty of India or to strike terror among its people. Such acts involve the use of computers, communication devices, or networks to access restricted data, introduce harmful programs, disrupt critical infrastructure, or conduct other activities that endanger national security. The provision ensures severe consequences, with violators facing imprisonment for life.
- **Section 67**[18]: It deals with the publication or transmission of obscene material in electronic form. It penalizes anyone who publishes, transmits, or causes to be published or transmitted any material that is obscene or lascivious, or appeals to prurient interests, through any electronic means. This section is aimed at discouraging the misuse of digital platforms for sharing inappropriate or offensive content. The punishment for violating this provision includes imprisonment of up to three years and a fine of up to five lakh rupees for the first conviction. For subsequent convictions, the punishment increases to imprisonment of up to five years and a fine of up to ten lakh rupees.
- **Section 67A**[19]: it deals with the publication or transmission of sexually explicit content in electronic form. It penalizes individuals who publish, transmit, or cause the electronic publication or transmission of any material that contains sexually explicit acts or conduct. This provision aims to regulate and prevent the misuse of digital platforms for sharing or distributing such inappropriate content. Violators are subject to punishment, which includes imprisonment of up to five years and a fine of up to ten lakh rupees for the first conviction, with stricter penalties of up to seven years imprisonment and a fine for subsequent convictions.

[16] S 66E; Ibid.
[17] S 66F; Ibid.
[18] S 67; Ibid.
[19] S 67A; Ibid.

ISSN: 2582-6433

- **Section 67B**[20]: Section 67B of the Information Technology Act, 2000, focuses on protecting children from exposure to sexually explicit content in electronic form. It criminalizes acts such as publishing, transmitting, or viewing any material depicting children engaged in sexually explicit acts. The section also penalizes activities like enticing or inducing children into such acts through electronic means. Violators face strict penalties, including imprisonment of up to five years and a fine of up to ten lakh rupees for the first conviction, with harsher penalties for subsequent offenses, including imprisonment of up to seven years and a fine of up to ten lakh rupees.

3.2. Key provisions under the BNS[21]

- **Section 75**[22]**:** it addresses sexual harassment committed by exhibiting pornography against a woman's will or making sexually charged statements (physically or electronically). [Section 354A IPC]
- **Section 77**[23]: Voyeurism - Cybercrimes known to as "revenge porn" or "upskirting" that involve the unlawful recording and distribution of private photographs are directly covered under Section 77. It makes it illegal to watch or record a lady doing a private act without getting her permission. [Section 354C IPC]
- **Section 78**[24]: Stalking – this section deals with the crime of stalking, including cyberstalking. This provision focuses on people who consistently follow or keep an eye on a woman's online activity in spite of her obvious lack of interest. Under this clause, someone can be charged with cyber-stalking if they use technology to harass or threaten a woman, for example, by sending her persistent messages, following her around, or making false profiles. [Section 354D IPC]
- **Section 79**[25]: Outraging the modesty of the woman – this provision handles the offence of outraging the modesty of a woman by saying words, producing sounds or gestures, showing things with purpose to insult or invade a lady's private. Although the clause is mostly focused on offline conduct, it can also apply to some cybercrimes, especially those that involve online harassment or threats like deepfakes. The perpetrator's

[20] S 67B; Ibid.
[21] Bhavna Sharma, Cybercrimes Under the Bhartiya Nyaya Sanhita, 2023, Cyber Law: Series 2, Issue 3, MCO Legals (2025), https://www.mcolegals.in/kb/Cyber_Law-_Series_2-Issue_3_Cybercrimes_under_the_Bhartiya_Nyaya_Sanhita,_2023.pdf.
[22] S 75, Bharatiya Nyaya Sanhita, 2023 (India).
[23] S 77; Ibid.
[24] S 78; Ibid.
[25] S 79; Ibid.

ISSN: 2582-6433

activities in these situations may be interpreted as "uttering words," "making sounds or gestures," or "exhibiting objects" in electronic form with the intention of demeaning the woman's modesty. [Section509 IPC]

- **Section 111**[26] - Organized Crime – This provision defines organized crime as a continuing criminal activity undertaken by a group of persons acting in concert. It specifically encompasses cybercrimes within the scope of such actions. This category may include cybercrimes like ransomware, phishing, identity theft, cyberextortion, and botnet operations. [New Section]
- **Section 112**[27]: Petty Organized Crime – it is any theft, snatching, cheating, or other such criminal activity carried out by a gang. While the clause largely focuses on classic types of organized crime, it can also be relevant to some cybercrimes. This is especially true when a gang or organization commits coordinated cyberattacks or scams, such clickbait, phishing, or card skimming. [New Section]
- **Section 152**[28]: Endangering the sovereignty, unity, and integrity of India – This provision deals with offenses that jeopardize India's sovereignty, unity, and integrity. Although it focuses mainly on offline acts, it can also apply to some cybercrimes that pose a threat to national security because it specifically uses the term "electronic communication" to incite secession, armed rebellion, subversive activities, or to foster separatist sentiments or jeopardize India's sovereignty, unity, and integrity. Section 152 covers cybercrime, including disinformation campaigns, cyberwarfare, espionage, and propaganda. [New Section]
- **Section 196**[29]: Encouragement of animosity between various groups based on religion, race, place of birth, residence, language, etc., and actions that are detrimental to the preservation of harmony - It addresses the offence of spreading dissension or hatred between different groups based on numerous criteria, including religion, race, place of birth, language, caste, or community. Although the rule is mostly concerned with offline conduct, it may nevertheless apply to some cybercrimes because it specifically refers to "electronic means" in order to carry out such acts. Section 196 applies to cybercrimes that target people based on their identity or that entail the spread of hate speech or fake news. [Section 153A IPC]

[26]S 111; Ibid.
[27] S 112; Ibid.
[28] S 152; Ibid.
[29] S 196; Ibid.

ISSN: 2582-6433

- **Section 292**[30]: Sale, etc., of obscene literature, etc. – this provision deals with the offence that involves the presentation or exhibition of obscene material. It also covers such demonstrations or exhibitions on internet platforms, i.e., obscene material in electronic form. Cybercrimes that fall under this category include sharing offensive, pornographic, or abusive content. [Section 292 IPC]
- **Section 353**[31]: Statements conducing to public mischief – it addresses the charge of making false statements or spreading rumours that can impair public order or security, including through electronic means. Thus, it is illegal under this clause to spread fake news, hoaxes, hate speech, disinformation, or any other kind of activity that could jeopardize public safety or order. [Section 505 IPC]

4. Conclusion:

India's criminal laws, which have been in place since 1860, were clearly in need of an update to meet the demands of modern society. These laws, though foundational, lacked provisions that could address the challenges of the digital age, especially with the rise of cybercrimes. Recent legislative reforms mark a significant turning point in the evolution of India's criminal justice system. By introducing provisions tailored to today's technological landscape, these reforms aim to combat the increasing prevalence of cybercrimes. While the BNS does not provide a detailed definition of 'cybercrime,' it effectively covers a wide spectrum of offenses facilitated by modern technology, including hacking, phishing, and cyberstalking.

In addition to the BNS, India has already enacted the Information Technology Act of 2000 (IT Act), which was a pioneering effort to regulate cyberspace. However, as the digital world rapidly evolved, the limitations of the IT Act became more apparent. The growing numbers of cybercrimes further emphasized the need for a more comprehensive approach to justice in the digital age. The BNS was designed to address these gaps, offering provisions specifically crafted to handle cybercrimes effectively. By integrating these cyber-related offenses into the larger framework of the criminal justice system, the BNS provides a more cohesive and forward-thinking approach. This ensures that law enforcement is better equipped to tackle the complexities of digital threats while maintaining the integrity of the justice system as a whole.

[30] S 292; Ibid.
[31] S 353; Ibid.