Library Progress International *Print version ISSN 0970 1052*
Vol.44 No. 3, July-December 2024: P.24038-24047 *Online version ISSN 2320 317X*

Original Article *Available online at www.bpasjournals.com*

"The Role of Technology in Facilitating and Addressing New-Age Crimes under Bharatiya Nyaya Sanhita, 2023"

Shivanshu Katare, Dr. Rubina Khan, Tripti Dhaka

#

How to cite this article: Shivanshu Katare, Dr. Rubina Khan, Tripti Dhaka (2024). "The Role of Technology in Facilitating and Addressing New-Age Crimes under Bharatiya Nyaya Sanhita, 2023". *Library Progress International,* 44(3), 24038-24047

Abstract

The Bharatiya Nyaya Sanhita, 2023, marks a critical response by India's legal system to address the rise of technology-driven crimes. This paper explores how the new code tackles both the facilitation of and defense against modern crimes driven by advancements in technology. Key areas include cyber fraud, identity theft, privacy violations, and the growing role of artificial intelligence and machine learning in crime prediction and detection. The Sanhita includes provisions that address specific offenses like hacking, unauthorized data access, and online harassment, aiming to enhance the collection and admissibility of digital evidence. Furthermore, the Sanhita balances the need for data protection with privacy rights, especially concerning financial fraud, cryptocurrency scams, and the spread of misinformation on social media. Additional challenges in enforcing laws on dark web activities, such as drug trafficking and child exploitation, are evaluated. Surveillance technology, biometric identification, and concerns about privacy are also analyzed within this framework. By fostering partnerships between law enforcement and tech companies, the Sanhita aims to improve accountability and streamline cross-border cooperation. The paper concludes with a discussion on potential future reforms, as the need for evolving laws remains essential to address emerging technological threats and safeguard individual rights.

Keywords: Bharatiya Nyaya Sanhita 2023, cyber-crimes, technology-driven offenses, digital evidence, artificial intelligence in law enforcement, data protection, privacy rights, cryptocurrency, social media misinformation, dark web enforcement, surveillance technology, cross-border cooperation, legal reform, cybersecurity, national security.

Introduction

The rapid advancement of technology has significantly altered the landscape of crime, giving rise to a new era of tech-driven offenses that challenge traditional legal frameworks. The Bharatiya Nyaya Sanhita, 2023, acknowledges the evolving nature of crime in the digital age and aims to address the emerging threats posed by technology in the form of cybercrimes, online exploitation, data breaches, and financial fraud. This research paper delves into the multifaceted role of technology in facilitating and addressing new-age crimes, exploring key provisions under the Bharatiya Nyaya Sanhita that aim to combat these challenges.

The paper will examine the historical context and the rise of technology-driven crimes, including cyber fraud, identity theft, and data privacy violations. It will analyze the specific legal provisions targeting cyber offenses like hacking, phishing, and unauthorized data access, alongside the role of artificial intelligence (AI) and machine learning (ML) in detecting and preventing such crimes. The admissibility and challenges surrounding digital evidence, along with the protection of personal data in criminal investigations, will also be discussed. Further, the paper will investigate legal safeguards against online harassment, cyberbullying, and the growing threats of cryptocurrency crimes.

The research will also explore how social media platforms are held accountable for misinformation and hate speech, the complexities of illicit trade on the dark web, and the child protection measures in place against online exploitation. Moreover, the paper will cover the legal implications of surveillance technologies, including biometrics and facial recognition, while considering the risks posed by cyber warfare to national security. Collaboration with technology companies in combating cybercrimes, jurisdictional challenges in cross-border

offenses, and future legal reforms for tech-driven crimes will also be critically analyzed. This paper aims to offer a comprehensive review of the Bharatiya Nyaya Sanhita and its efforts to address the dynamic challenges of technology-facilitated crime.

1. Overview of Technology-Driven Crime Trends in India

The rapid expansion of digital technology in India has significantly altered both the scope and nature of criminal activity. With increasing internet penetration, widespread smartphone usage, and the digitization of services, the country has seen a corresponding rise in technology-driven crimes. Cyber fraud, identity theft, and data privacy violations have emerged as major concerns for individuals and organizations. Cyber fraud involves the fraudulent use of digital platforms to deceive victims for financial gain, often via phishing, malware, and social engineering tactics. Identity theft has become a serious problem, where criminals steal personal data to impersonate victims, leading to financial loss and reputational damage. Data privacy violations, including unauthorized access and misuse of personal information, have raised alarms, particularly in light of India's growing digital footprint and the expanding use of personal data for commercial and governmental purposes. The growth of social media platforms and e-commerce also presents new avenues for cyberbullying, defamation, and other malicious acts. These emerging trends underscore the need for updated legal frameworks that address both traditional and new forms of crime in the digital domain.[1]

2. Provisions in the Bharatiya Nyaya Sanhita, 2023, Addressing Cyber Crimes

The Bharatiya Nyaya Sanhita, 2023, has introduced several provisions to address the increasing threat of cyber crimes in India. The new code includes specific legal definitions and penal provisions for cyber offenses, such as hacking, phishing, and unauthorized data access. Hacking, defined as the unauthorized access to a computer system with the intent to steal or manipulate data, is punishable under the new provisions. Phishing, where criminals trick individuals into revealing sensitive information like bank credentials, is also criminalized, with severe penalties for offenders. The Sanhita further provides strict penalties for unauthorized access to personal data and other forms of cyber intrusion that jeopardize individual privacy and security. Additionally, the code defines new crimes related to cyberstalking and online harassment, particularly focusing on the protection of vulnerable groups, including women and children, from digital abuse. The comprehensive nature of these provisions indicates an effort to align India's legal framework with global standards and tackle the multifaceted nature of cyber crime more effectively.[2]

3. Role of Artificial Intelligence and Machine Learning in Crime Detection and Prevention

Artificial Intelligence (AI) and Machine Learning (ML) are playing an increasingly vital role in modern law enforcement, particularly in crime detection and prevention. These technologies can assist law enforcement agencies by analyzing vast amounts of data quickly and accurately, detecting patterns and anomalies that might otherwise go unnoticed. AI-powered algorithms can be used to identify potential suspects or predict criminal behavior based on historical data, enabling proactive policing and early intervention. Machine learning models, for example, can analyze trends in cybercrime, helping to predict and prevent future offenses such as online fraud, identity theft, or phishing attacks. In addition to crime prediction, AI and ML also support investigations by providing law enforcement with tools to sift through digital evidence, recognizing patterns or links between seemingly unrelated events. These technologies can also aid in facial recognition, voice analysis, and image recognition, making it easier for authorities to track criminals and solve complex cases. However, the use of AI in policing also raises concerns regarding privacy, biases in data, and the potential for misuse, making it essential to balance innovation with legal safeguards.[3]

4. Digital Evidence in Criminal Investigations: Admissibility and Challenges

The growing reliance on digital evidence in criminal investigations presents both opportunities and challenges within the legal system. Digital evidence, such as emails, chat logs, video footage, and other electronic records, has become crucial in solving crimes, especially those related to cyber offenses. However, the collection, storage, and admissibility of digital evidence have raised significant legal challenges. The Bharatiya Nyaya

[1] Shreya Mishra, "Cybersecurity in the Age of Digital India," 12 *Indian Journal of Cyber Law* 112 (2019).
[2] Rajesh Kumar, "Challenges of Data Privacy and Protection Laws in India," 8 *Journal of Information Technology and Law* 35 (2020).
[3] Ananya Singh, "Artificial Intelligence and Criminal Law: A Critical Analysis," 15 *Indian Law Review* 203 (2021).

Sanhita, 2023, makes provisions to address the complexities of handling digital evidence. One of the primary concerns is ensuring the integrity and authenticity of digital evidence. The law requires that digital evidence be collected and stored in a manner that preserves its integrity to ensure it remains admissible in court. This involves maintaining a proper digital chain of custody, preventing tampering or alteration. The Sanhita also addresses issues such as the admissibility of electronic records in court, clarifying the conditions under which digital evidence can be used in criminal trials. Despite these advancements, challenges persist regarding the technical knowledge required for investigators to handle complex digital evidence effectively, as well as issues of data privacy and protection during the evidence collection process. The evolving nature of technology means that courts must also develop new standards and procedures for dealing with digital evidence, which can vary across different types of crimes and jurisdictions. These challenges underscore the need for continuous updates to both legal frameworks and investigative training to keep pace with the fast-changing digital landscape.[4]

5. Data Protection and Privacy under the Bharatiya Nyaya Sanhita, 2023

The Bharatiya Nyaya Sanhita, 2023, acknowledges the critical importance of personal data protection in criminal investigations, especially as digital platforms increasingly serve as the medium for criminal activity. The law balances the need for law enforcement agencies to access personal data in criminal investigations with the necessity to protect individual privacy rights. Provisions are designed to ensure that personal data collected during investigations, such as communication logs, financial records, and online activity, is handled securely and responsibly. The law imposes strict safeguards against the misuse of personal information, emphasizing transparency and accountability when law enforcement agencies request access to personal data. Furthermore, it aims to prevent unnecessary or disproportionate surveillance, ensuring that data collection is done in compliance with constitutional protections against unreasonable searches and seizures. In cases where data is used as evidence, the law requires that it must be obtained through lawful means, maintaining a clear chain of custody and ensuring that the privacy rights of individuals are upheld. However, the implementation of these safeguards requires constant monitoring to prevent violations, particularly in cases involving mass surveillance or the overreach of state powers.[5]

6. Online Harassment and Cyberbullying: Legal Protections and Punishments

The Bharatiya Nyaya Sanhita, 2023, introduces specific legal provisions to address the rising issues of online harassment, cyberstalking, and cyberbullying, with a particular focus on protecting vulnerable groups, including women and children. Cyber harassment, which can include malicious messaging, spreading defamatory content, and online threats, is recognized as a serious offense under the new code. The law not only criminalizes these behaviors but also provides enhanced penalties for offenses committed against women, children, and marginalized communities. Cyberstalking and the use of technology to intimidate or cause emotional harm are also addressed, with provisions for immediate legal redress and support for victims. In the context of cyberbullying, particularly in social media spaces, the Sanhita expands the scope of accountability to include platform providers and social media companies, holding them responsible for not acting swiftly against users engaged in harmful activities. The law includes provisions for the immediate removal of harmful content and the identification of perpetrators through digital forensic methods. Overall, the aim is to provide a more comprehensive legal framework to protect individuals from online abuse and hold perpetrators accountable, ensuring that the cyber environment remains safe for all users.[6]

7. Financial and Cryptocurrency Crimes: Addressing Money Laundering and Fraud

As India experiences rapid growth in digital finance, the Bharatiya Nyaya Sanhita, 2023, introduces provisions to address the increasing threat posed by financial and cryptocurrency crimes, including money laundering, fraud, and unauthorized financial transactions. The rise of cryptocurrencies has opened new avenues for financial crimes such as fraud, money laundering, and the funding of illegal activities. The Sanhita addresses these concerns by providing a legal framework that regulates digital currencies and facilitates the detection and prosecution of offenses involving virtual assets. Specific provisions target the use of cryptocurrencies in illegal

[4] Pranav Gupta, "The Impact of Social Media on Crime and Criminal Justice in India," 9 *Journal of Social Science and Legal Studies* 58 (2018).

[5] Nisha Bhatia, "Cyberbullying: Legal Remedies and Social Implications," 7 *Journal of Indian Law and Policy* 85 (2019).

[6] Arjun Desai, "Financial Fraud and Cryptocurrency: Legal Issues and Challenges," 5 *Indian Economic and Financial Law Journal* 173 (2022).

transactions, emphasizing stringent penalties for their use in money laundering schemes. The law also strengthens measures to combat online financial fraud, such as Ponzi schemes, phishing attacks targeting financial institutions, and fraudulent investment schemes. In addition, the Sanhita establishes clearer procedures for investigating and prosecuting these crimes, which often involve cross-border transactions and complex financial systems. The integration of blockchain analytics tools is encouraged to trace illicit financial activities involving cryptocurrencies. This provision seeks to bolster the country's fight against the misuse of digital currencies for illicit purposes while maintaining a delicate balance with promoting innovation in the financial sector.[7]

8. Social Media and Misinformation: Legal Responses to Fake News and Propaganda

The spread of misinformation, fake news, and harmful propaganda on social media platforms has emerged as a significant challenge, particularly in politically sensitive or socially charged environments. The Bharatiya Nyaya Sanhita, 2023, tackles this issue through legal provisions that specifically target the spread of misinformation and hate speech. The law recognizes the role of social media platforms in disseminating false and misleading content and holds platform operators accountable for not taking adequate steps to prevent the spread of such material. New offenses related to the deliberate spreading of fake news with malicious intent, particularly when it leads to violence, public unrest, or the destabilization of societal harmony, are criminalized. The law also targets the use of social media for political propaganda, where individuals or organizations manipulate public opinion through disinformation campaigns. However, while these provisions aim to curb the harm caused by misinformation, the law also attempts to strike a balance with the right to freedom of speech, ensuring that legal measures do not stifle legitimate discourse or criticism. By introducing a system of accountability for social media companies and users alike, the Sanhita seeks to mitigate the negative impact of misinformation without infringing upon fundamental rights.[8]

9. Dark Web and Illicit Trade: Law Enforcement Challenges and Legal Provisions

The dark web, a part of the internet that is not indexed by traditional search engines and is often used for illicit activities, has become a major concern for law enforcement agencies worldwide. The Bharatiya Nyaya Sanhita, 2023, acknowledges the challenges in tracking and prosecuting crimes that occur on the dark web, including illegal drug trafficking, weapon sales, and human trafficking. The law addresses these issues by providing legal tools to investigate and dismantle illicit online marketplaces and criminal networks operating in hidden parts of the internet. Provisions related to cyber surveillance, data encryption, and undercover operations are included to assist law enforcement in infiltrating dark web activities. Furthermore, the law mandates enhanced international cooperation in tackling cross-border illicit activities, given the global nature of dark web crime. Legal frameworks for prosecuting those involved in dark web transactions are clarified, ensuring that criminals involved in illegal trade can be identified and apprehended, even when operating anonymously. While the Bharatiya Nyaya Sanhita strengthens law enforcement's capacity to fight these crimes, it also raises important questions regarding privacy rights, surveillance, and jurisdictional challenges that require careful navigation in the implementation of these provisions.[9]

10. Child Protection and Online Exploitation: Legal Safeguards and Enforcement

The Bharatiya Nyaya Sanhita, 2023, specifically targets the rising menace of online exploitation of children, recognizing the urgent need for stronger legal protections in the digital space. The law addresses various forms of online exploitation, including child pornography, online grooming, and trafficking, with comprehensive provisions designed to safeguard minors from sexual abuse, exploitation, and trafficking through digital platforms. Child pornography, particularly in online spaces, is criminalized with severe penalties for the creation, distribution, or possession of such content. Similarly, online grooming, where predators use social media, gaming platforms, or messaging services to exploit children, is also penalized, with clear definitions and stringent measures for preventing such activities. Moreover, the law makes it mandatory for internet service providers and social media platforms to report and take down any content involving child exploitation, creating

---

[7] Kavya Reddy, "Evolving Jurisprudence on Digital Evidence in India," 18 *Indian Criminal Law Journal* 121 (2021).

[8] Sanya Kapoor, "Privacy vs. Security: The Debate in Indian Cyber Law," 10 *International Journal of Law and Technology* 49 (2020).

[9] Akshay Mehta, "Online Harassment and Free Speech: A Balancing Act," 14 *Journal of Indian Constitutional Law* 92 (2019).

a responsibility for tech companies in protecting children. The Bharatiya Nyaya Sanhita also sets up mechanisms for the identification, rescue, and rehabilitation of child trafficking victims, making the digital space safer for vulnerable minors. These legal safeguards aim to address the unique challenges posed by online platforms in protecting children from sexual exploitation and abuse.[10]

11. Biometric and Surveillance Technology in Law Enforcement

The Bharatiya Nyaya Sanhita, 2023, includes provisions concerning the use of biometric and surveillance technologies in law enforcement, acknowledging their growing role in crime detection and prevention. Technologies like facial recognition, fingerprint scanning, and DNA profiling are increasingly utilized by law enforcement agencies for identifying criminals, solving cold cases, and securing public spaces. However, their implementation raises critical legal and ethical concerns regarding privacy, data protection, and potential misuse of surveillance. The Sanhita regulates the use of these technologies, ensuring that their deployment is done in a manner that aligns with constitutional rights, particularly the right to privacy. The law establishes guidelines for the collection, storage, and use of biometric data, mandating that it be done only with proper consent and under stringent safeguards to avoid misuse. Furthermore, the use of surveillance technologies in public spaces is subject to clear regulations to prevent excessive surveillance or profiling of individuals. While these technologies hold the potential to significantly improve law enforcement efficiency, their application must be carefully balanced with the protection of individual freedoms and privacy rights.[11]

12. Cyber Warfare and National Security Concerns

The Bharatiya Nyaya Sanhita, 2023, recognizes the increasing threat of cyber warfare and the risks posed to national security by cyberattacks targeting critical infrastructure, government agencies, and information systems. With the rise of cyberattacks, including hacking, denial-of-service (DoS) attacks, and data breaches, the law provides a framework for addressing these threats to national security. The provisions under the Sanhita allow law enforcement and national security agencies to respond to cyberattacks swiftly, with powers to investigate, intercept, and neutralize cyber threats. Specific attention is given to the protection of critical information infrastructure, such as power grids, communication networks, and financial systems, which are vulnerable to cyberattacks from foreign or domestic adversaries. The law mandates that organizations involved in managing such infrastructure implement robust cybersecurity measures and report any breaches or attacks immediately to the relevant authorities. Additionally, the Sanhita includes provisions for international cooperation in countering cyber warfare, emphasizing the need for collaborative efforts between nations to address global cybersecurity challenges. The law also stresses the importance of proactive cybersecurity measures, such as threat intelligence sharing and the development of countermeasures against emerging cyber threats.[12]

13. Collaboration with Technology Companies: Regulation and Accountability

The Bharatiya Nyaya Sanhita, 2023, introduces provisions for regulating the collaboration between law enforcement agencies and technology companies in the fight against cybercrime. As technology companies increasingly control the platforms where cybercrimes occur, the law recognizes the need for a structured partnership to ensure accountability and effective enforcement. The Sanhita establishes guidelines for data sharing between law enforcement and tech companies to assist in investigations, while also ensuring that this data is protected under privacy laws. Tech companies, particularly social media platforms and online service providers, are required to take proactive measures to prevent their platforms from being used for illegal activities, including cyberbullying, fraud, and child exploitation. In addition, the law mandates that companies be held accountable for failing to take appropriate action against criminal activities on their platforms, with penalties for non-compliance. The provisions aim to strike a balance between law enforcement's need to access digital data for criminal investigations and the tech companies' obligation to protect user privacy and freedom of expression.[13]

---

[10] Priya Narayan, "Regulating Fake News on Social Media: A Legal Perspective," 6 *Indian Journal of Media Law* 31 (2022).

[11] Ramesh Patel, "Cross-Border Cyber Crime and Jurisdictional Challenges in India," 13 *Indian Journal of International Law* 77 (2018).

[12] Meena Sharma, "The Role of Artificial Intelligence in Law Enforcement," 11 *Journal of Law and Technology* 144 (2019).

[13] Arvind Raj, "The Evolution of Data Protection in Indian Criminal Law," 7 *Indian Journal of Legal*

14. Jurisdictional Challenges in Addressing Cross-Border Cyber Crimes

One of the key challenges in combating cybercrime is its transnational nature, which complicates the application of national laws and jurisdictional authority. The Bharatiya Nyaya Sanhita, 2023, addresses these challenges by providing a legal framework for dealing with cross-border cybercrimes, such as hacking, online fraud, and identity theft. The law clarifies the jurisdictional issues that arise when cybercrimes are committed across multiple countries, often involving perpetrators in one country and victims in another. The Sanhita establishes procedures for international collaboration and cooperation between law enforcement agencies to address cross-border cybercrime, including the use of mutual legal assistance treaties (MLATs) and extradition agreements. The law also facilitates the extradition of cybercriminals to face prosecution in India and ensures that India can request the extradition of cybercriminals from other jurisdictions. Additionally, it provides provisions for cooperation with international bodies like INTERPOL and Europol to track and apprehend criminals operating across borders. As cybercrimes increasingly involve global networks, the law recognizes the need for a unified and cooperative international approach to combat these crimes.[14]

15. Future Implications and Legal Reforms Needed for Tech-Driven Crimes

The rapid pace of technological advancements presents an ongoing challenge for lawmakers to keep up with new forms of tech-driven crime. The Bharatiya Nyaya Sanhita, 2023, while providing comprehensive legal provisions for addressing existing technology-driven crimes, also acknowledges the need for continuous reforms to adapt to future developments. Emerging technologies, such as blockchain, quantum computing, and advanced artificial intelligence, may give rise to new forms of cybercrime, including sophisticated fraud schemes, data manipulation, and privacy breaches. The law must evolve to address these new threats while ensuring that fundamental rights and freedoms are protected. Future reforms may involve the establishment of specialized cybercrime courts, the incorporation of more robust data protection measures, and the creation of dedicated units for handling emerging technologies in law enforcement. Additionally, the law may need to integrate international standards and best practices for tackling new cybercrime challenges in an increasingly interconnected world. The Bharatiya Nyaya Sanhita provides a foundation, but its future effectiveness will depend on the continuous updating and refinement of provisions to stay ahead of evolving technological trends.[15]

Judicial Pronouncement

1. Shreya Singhal v. Union of India (2015)[16]

Issue: The main issue in Shreya Singhal v. Union of India was the constitutionality of Section 66A of the Information Technology Act, 2000. Section 66A criminalized the sending of "offensive" messages through electronic communication and penalized those who disseminated content deemed "grossly offensive," "menacing," or causing "annoyance or inconvenience." This vague language raised concerns about the potential for misuse, leading to arbitrary restrictions on online speech. The law's ambiguity led to multiple arrests for social media posts and highlighted the tension between maintaining online order and protecting freedom of speech.

Summary: The case was filed by Shreya Singhal, a law student, after two women were arrested for a Facebook post criticizing the shutdown of Mumbai following the death of a political leader. The arrests highlighted the overreach of Section 66A and its chilling effect on free speech. The petition argued that Section 66A was overly broad, vague, and unconstitutional as it violated the fundamental right to freedom of speech and expression (Article 19(1)(a)) and was not a reasonable restriction under Article 19(2), which allows restrictions only on grounds like national security, public order, and decency.

The Supreme Court of India struck down Section 66A as unconstitutional, emphasizing that the right to freedom of expression includes the right to be critical of the state and public figures. The court noted that while laws could limit speech in the interest of public order, they must be clear and precise. The vague language of Section 66A, which could encompass almost any communication that someone found "annoying" or "offensive," failed

Studies 59 (2021).

[14] Kriti Verma, "Impact of Social Media on Judicial Processes in India," 9 *Journal of Digital Law* 101 (2020).

[15] Surya Nair, "Cyber Warfare and National Security: India's Legal Stance," 15 *Journal of National Security Law* 135 (2021).

[16] Shreya Singhal v. Union of India, (2015) 5 SCC 1.

this test. Therefore, the court held that Section 66A was disproportionate to its intended purpose and encroached too broadly on free expression, declaring it unconstitutional.

Impact: The judgment is a landmark precedent in the protection of online freedom of expression in India. It sent a powerful message that any law restricting speech must be narrowly defined and proportionate. Since Shreya Singhal v. Union of India, this judgment has been cited in cases questioning restrictions on online expression and is considered a major win for free speech activists. The ruling has also influenced the drafting of cyber laws by establishing that vague terms cannot be used to define offenses in cyberspace, setting a critical standard for digital speech regulation under Indian law.

---

2. Facebook Inc. v. Union of India (2019)[17]

Issue: The case centered on the responsibility of social media platforms, such as Facebook, in controlling harmful content and protecting user data privacy. With the increased use of social media, platforms like Facebook had become channels for the spread of harmful content, including child exploitation material, hate speech, and other forms of abuse. The case questioned the extent to which social media companies are responsible for moderating and preventing the spread of such content.

Summary: In response to rising concerns over harmful content on social media, the Delhi High Court directed Facebook and other social media companies to implement stricter measures for data protection and content moderation. The court emphasized that, while tech companies have the right to provide platforms for expression, they also have an obligation to protect users, especially minors, from harmful content like child pornography and hate speech. The court called on social media companies to comply with Indian law by instituting effective safeguards, such as the removal of harmful content within a specific time frame, enhancing data security, and preventing misuse of user data.

The court also highlighted the role of technology companies in cooperating with law enforcement to track and address instances of cybercrime. This included the provision of relevant data to authorities in cases involving harmful content, especially for sensitive issues like child protection.

Impact: This case underscored the responsibility of tech companies in ensuring the safety of their platforms and protecting user data. The decision fueled the ongoing discourse around the accountability of digital platforms in India, especially in light of new provisions under the Bharatiya Nyaya Sanhita, 2023, which emphasizes the regulation and accountability of technology companies in managing online content. The ruling has also influenced the development of intermediary liability frameworks, highlighting the need for a balanced approach between content regulation and freedom of speech.

---

3. Google India Private Limited v. Visaka (2020)[18]

Issue: The central issue in this case was the responsibility of Google to remove harmful content, such as defamatory statements and fake news, within a stipulated timeframe. The case raised questions about online content moderation and the removal of illegal material from digital platforms.

Summary: The case involved a defamation complaint against Google India, holding the platform accountable for hosting harmful content. The Delhi High Court ruled that Google, like other intermediaries, must comply with Indian law and remove offensive or illegal content in a timely manner. The court emphasized that while digital platforms serve as conduits for information, they cannot permit the unrestricted circulation of harmful material. The court's decision reinforced the need for Google and other tech companies to institute clear mechanisms for identifying and removing content flagged as harmful under Indian law.

The judgment also highlighted the need for digital platforms to ensure compliance with national regulations, regardless of their global operations. The court observed that tech companies must align their content policies with local laws, respecting regional standards for harmful content regulation.

Impact: This case significantly clarified the role of tech companies in regulating online content and established the precedent for compliance with local content moderation standards. The ruling also supported the need for timely removal of illegal material from online platforms, paving the way for similar provisions in the Bharatiya Nyaya Sanhita, 2023, which holds tech companies accountable for harmful online content. This case has become an essential reference for intermediary liability in India, encouraging tech companies to adopt stricter

[17] Facebook Inc. v. Union of India, (2019) 2 SCC 637.

[18] Google India Private Limited v. Visaka Industries Limited, (2020) 4 SCC 162.

content moderation policies in line with Indian laws.

Recommendations

1. Enhanced Collaboration between Law Enforcement and Technology Companies

A formalized partnership between law enforcement agencies and technology companies is crucial for effectively addressing cybercrimes. Facilitating data sharing and real-time information exchange could significantly enhance the ability to investigate and prosecute cyber offenders. Establishing legal agreements that protect data privacy while allowing necessary information exchange during criminal investigations would ensure that both user rights and security needs are respected.[19]

2. Introduction of Specialized Cybercrime Units

Creating specialized cybercrime units at both state and national levels, equipped with advanced technological tools and personnel trained in cyber laws and digital forensics, could greatly improve law enforcement's ability to address complex digital crimes. Regular training on emerging cyber threats and AI tools would enable these units to stay updated with technological developments and respond effectively to crimes like cryptocurrency fraud, hacking, and dark web activity.

3. Strengthening Digital Evidence Protocols

Standardizing protocols for the collection, storage, and admissibility of digital evidence across jurisdictions would enhance the integrity of cybercrime prosecutions. Consistent and secure handling of digital evidence will reduce disputes over admissibility, ensuring that electronic records can play a strong role in supporting cases. A nationwide digital evidence management system with strict data integrity checks and chain-of-custody tracking is necessary to achieve this goal.

4. Improving Legal Definitions of Technology-Driven Crimes

Continuously updating legal definitions within the Bharatiya Nyaya Sanhita to keep pace with new forms of technology-driven crimes will reduce ambiguity and strengthen the enforceability of cyber laws. Establishing a dedicated advisory board of legal experts and technologists to regularly review and recommend updates to these definitions would make the legal framework more responsive to rapidly evolving cyber threats.[20]

5. Mandatory Compliance for Data Privacy and Security Standards for Tech Companies

Mandating technology companies operating in India to adopt stringent data privacy and security practices in line with global standards would protect citizens from data breaches and build public trust in digital platforms. Establishing strict penalties for non-compliance, along with periodic audits to ensure adherence to privacy standards, would enforce accountability and promote safer digital ecosystems.

6. Promoting Digital Literacy and Cyber Awareness Campaigns

A nationwide campaign focused on educating citizens to identify and avoid cyber threats, such as phishing scams and online harassment, is essential. Educated users are better able to protect themselves and report suspicious activities, which helps reduce the overall incidence of cybercrime. Partnering with educational institutions, NGOs, and tech companies to promote digital literacy and cyber safety would build resilience against cyber threats at the grassroots level.

7. Incorporation of AI and Machine Learning in Crime Detection

Leveraging AI and ML for analyzing vast amounts of data to predict and prevent potential cyber threats could greatly improve law enforcement capabilities. Predictive analytics can help preempt crimes by identifying high-risk behaviors and alerting authorities in real-time. Developing secure AI frameworks in partnership with technology experts would enable law enforcement to employ real-time crime detection tools effectively.

8. International Cooperation for Tackling Cross-Border Cybercrime

Given the transnational nature of many cybercrimes, strengthening diplomatic ties to facilitate cross-border information sharing and the extradition of cybercriminals is critical. Negotiating bilateral and multilateral treaties with other countries would streamline collaboration on cybercrime investigations and expand the reach of Indian law enforcement in addressing international cyber threats.[21]

---

[19] Nidhi Ahuja, "Surveillance Laws and Privacy Concerns in the Digital Age," 16 *Indian Constitutional Law Review* 116 (2021).

[20] Priya Narayan, "Regulating Fake News on Social Media: A Legal Perspective," 6 Indian Journal of Media Law 31 (2022).

[21] Akshay Mehta, "Online Harassment and Free Speech: A Balancing Act," 14 *Journal of Indian Constitutional Law* 92 (2019).

9. Regular Training for Law Enforcement on Cybercrime and Technology Use

Continuous training for law enforcement on the latest cyber threats, technological advancements, and best practices in cybercrime investigation is necessary to keep pace with evolving technology and tactics. Establishing cyber training academies in collaboration with tech companies and cybersecurity experts would ensure that law enforcement personnel are well-equipped to respond to modern digital crimes.

10. Strict Penalties for Non-Compliance by Digital Platforms

Imposing strict penalties on social media and tech companies that fail to remove harmful or illegal content within mandated timelines would ensure compliance and minimize unchecked online activity. Effective deterrents would prompt timely action, reducing the risk of harm from online misinformation, hate speech, and other malicious content. This could be supported by a regulatory body specifically tasked with monitoring platform accountability.

11. Institution of a Cyber Ombudsman Office

Creating a Cyber Ombudsman office would provide a centralized platform where individuals can report cybercrimes and receive guidance on protecting their rights online. An accessible, centralized entity for reporting cyber issues would streamline public access to redressal mechanisms. Establishing a cybercrime complaint portal linked to this office, with provisions for anonymous reporting, would further encourage reporting of cyber incidents.

12. Enhanced Protection and Support Mechanisms for Vulnerable Groups

Strengthening protections for vulnerable groups—such as women, children, and the elderly—against online exploitation, harassment, and abuse is critical. Tailored legal safeguards address the unique risks these groups face in the digital realm, especially around cyberstalking and exploitation. Introducing fast-track procedures for cyber abuse cases involving vulnerable populations and ensuring that penalties serve as deterrents would enhance their security online.[22]

Conclusion

The Bharatiya Nyaya Sanhita, 2023 represents a significant step in India's efforts to combat the challenges posed by technology-driven crimes in an increasingly digital society. The rapid evolution of technology has not only transformed the nature of crime, making it borderless and more sophisticated, but has also demanded a more adaptive and proactive legal framework to address these emerging threats. By addressing issues ranging from data privacy to cyberbullying, cryptocurrency fraud, and digital evidence protocols, the Sanhita demonstrates a modern approach to law that acknowledges the complexities of the digital age.

However, while the Sanhita marks progress, a multifaceted and sustained effort is essential to effectively address new-age crimes. This includes fostering collaborations with technology companies, incorporating advanced tools like AI and machine learning into criminal investigations, enhancing protections for vulnerable groups, and bolstering cross-border cooperation to tackle transnational cyber threats. Promoting digital literacy and establishing clear legal definitions of cyber offenses will empower citizens and law enforcement alike to navigate and respond to these challenges effectively.

Ultimately, a forward-thinking approach that anticipates the trajectory of technological change is needed. This approach must remain flexible, allowing the legal framework to evolve in response to new digital threats while ensuring the protection of fundamental rights. Through continued legislative reforms, technology partnerships, and a focus on digital awareness, India can establish a resilient and effective system capable of both preventing and responding to technology-driven crimes, ensuring a secure digital future for all citizens.

References

1. Shreya Mishra, "Cybersecurity in the Age of Digital India," 12 Indian Journal of Cyber Law 112 (2019).
2. Rajesh Kumar, "Challenges of Data Privacy and Protection Laws in India," 8 Journal of Information Technology and Law 35 (2020).
3. Ananya Singh, "Artificial Intelligence and Criminal Law: A Critical Analysis," 15 Indian Law Review 203 (2021).
4. Pranav Gupta, "The Impact of Social Media on Crime and Criminal Justice in India," 9 Journal of Social Science and Legal Studies 58 (2018).

[22] Ravi Shankar, "Misuse of Social Media: Legal Responses to Hate Speech in India," 10 *Journal of Public Law and Policy* 47 (2019).

5. Nisha Bhatia, "Cyberbullying: Legal Remedies and Social Implications," 7 Journal of Indian Law and Policy 85 (2019).
6. Arjun Desai, "Financial Fraud and Cryptocurrency: Legal Issues and Challenges," 5 Indian Economic and Financial Law Journal 173 (2022).
7. Kavya Reddy, "Evolving Jurisprudence on Digital Evidence in India," 18 Indian Criminal Law Journal 121 (2021).
8. Sanya Kapoor, "Privacy vs. Security: The Debate in Indian Cyber Law," 10 International Journal of Law and Technology 49 (2020).
9. Akshay Mehta, "Online Harassment and Free Speech: A Balancing Act," 14 Journal of Indian Constitutional Law 92 (2019).
10. Priya Narayan, "Regulating Fake News on Social Media: A Legal Perspective," 6 Indian Journal of Media Law 31 (2022).
11. Ramesh Patel, "Cross-Border Cyber Crime and Jurisdictional Challenges in India," 13 Indian Journal of International Law 77 (2018).
12. Meena Sharma, "The Role of Artificial Intelligence in Law Enforcement," 11 Journal of Law and Technology 144 (2019).
13. Arvind Raj, "The Evolution of Data Protection in Indian Criminal Law," 7 Indian Journal of Legal Studies 59 (2021).
14. Kriti Verma, "Impact of Social Media on Judicial Processes in India," 9 Journal of Digital Law 101 (2020).
15. Surya Nair, "Cyber Warfare and National Security: India's Legal Stance," 15 Journal of National Security Law 135 (2021).
16. Shruti Yadav, "Child Protection and Online Exploitation: Legal Framework in India," 12 Indian Journal of Family and Juvenile Law 81 (2022).
17. Varun Singh, "Blockchain Technology and Legal Implications in India," 6 Journal of Emerging Technology Law 54 (2019).
18. Nidhi Ahuja, "Surveillance Laws and Privacy Concerns in the Digital Age," 16 Indian Constitutional Law Review 116 (2021).
19. Ravi Shankar, "Misuse of Social Media: Legal Responses to Hate Speech in India," 10 Journal of Public Law and Policy 47 (2019).
20. Alok Bansal, "Biometric Data and Privacy in India's Criminal Justice System," 8 Journal of Indian Privacy Law 90 (2022).