DIGITAL CRIMES AND MODERN SOLUTIONS: ADDRESSING CYBERCRIME UNDER THE BHARATIYA NYAYA SANHITA

Lakshya Malhotra, NMIMS Kirit. P. Mehta School of Law, Mumbai

ABSTRACT

The first computer, developed in the 1940s, was a technological marvel but inaccessible to most, making cyberattacks nearly nonexistent. Today, with rapid digitalization, economies worldwide, including India, are embracing digitization. India's Digital India initiative, launched on July 1, 2015[1], has fostered innovations like BHIM, Telemedicine, and DigiLocker, driving progress while exposing vulnerabilities to cybercrimes[2].

The surge in cybercrimes underscores the need for a robust legal framework. To address this, the Bharatiya Nyaya Sanhita (BNS), 2023, replaces the Indian Penal Code (IPC), 1860, marking a significant modernization. The BNS is a step in the right direction because it recognizes electronic records as primary evidence and makes cyber crimes a part of organized crime[3] with harsher penalties. However, gaps remain. The BNS lacks clear definitions, falls short in addressing the full spectrum of cybercrimes, and risks overlapping with specialized laws, creating potential compliance issues.

This paper highlights the BNS's strengths and limitations, advocating for amendments to include provisions for emerging cybercrimes, enhanced digital forensic tools, and streamlined regulations. A forward-looking legal framework is essential to balance technological progress with security and individual freedoms, ensuring justice in an increasingly digital world.

Keywords: Cybercrime, Data Protection, Cybersecurity Infrastructure, Bharatiya Nyaya Sanhita (BNS) 2023, Cyberterrorism, Artificial Intelligence

[1] Centre, C.S. Digital India, CSC E-Governance Services India Limited. Available at: https://csc.gov.in/digitalIndia

[2] Ministry of Electronics & Information Technology (MeitY) Annual report 2017-18. Available at: https://www.meity.gov.in/writereaddata/files/Annual_Report_2017-18.pdf

[3] JSA Advocates & Solicitors. (2024, July 17). *Stringent measures against cybercrimes in India's new criminal justice system - JSA*. JSA. https://www.jsalaw.com/newsletters-and-updates/stringent-measures-against-cybercrimes-in-indias-new-criminal-justice-system/

Introduction:

India's rapid digitization has boosted economic growth, but it has also led to a sharp increase in cybercrimes, highlighting the urgent need for contemporary legal frameworks. On July 1, 2024, the Indian Penal Code of 1860 was replaced by the Bharatiya Nyaya Sanhita (BNS), 2023, marking a significant advancement in India's criminal justice system. It is intended to tackle contemporary issues such as organized crime, terrorism, and cybercrimes while updating legal provisions while preserving significant elements of its predecessor. The inclusion of cybercrimes under organized crime, which imposes harsher penalties for crimes carried out by syndicates or groups, is one of its major innovations. These days, crimes like extortion, forgery, fraud and hate speech are specifically linked to digital platforms like social media and email. Additionally, under the Bharatiya Sakshya Adhiniyam (BSA), 2023[4], electronic records like emails and posts on social media are accepted as primary evidence, which facilitates investigations and trials.

Despite these measures, noticeable gaps persist in the Bill when examined through the lens of modern digital crimes. For instance, Section 152[5] criminalises any act whether done purposely or knowingly through spoken or written words, signs, visible representations, electronic communication, use of financial means, or otherwise that excites or attempts to excite secession, armed rebellion, or subversive activities, or that encourages separatist sentiments or endangers the sovereignty, unity, and integrity of India, with punishment extending to life imprisonment or up to seven years and a fine. In a similar vein, Section 197(d)[6] seeks anyone who, through spoken or written words, signs, visual representations, or electronic communication, makes or publishes imputations that a class of people cannot uphold India's sovereignty and integrity or bear true faith and allegiance to the Constitution because of their religion, race, language, region, caste, or community or suggests, counsels, advises, propagates, or publishes that such a class should be denied their rights as citizens or makes or publishes any assertion, counsel, plea, or appeal likely to sow discord, animosity, or hatred among communities or disses false or misleading information that puts national security at risk. These provisions, though aimed at protecting sovereignty, may inadvertently criminalise certain forms of electronic communication that seek to address national security threats,

[4] "THE BHARATIYA SAKSHYA ADHINIYAM, 2023" (2023) N–O. 47 THE GAZETTE OF INDIA EXTRAORDINARY
[5] *THE BHARATIYA NYAYA SANHITA, 2023*
[6] Ibid., 5.

highlighting the need for clearer safeguards and modern solutions within the Bharatiya Nyaya Sanhita to tackle cyber crime effectively.

When examining organised crime under the Bharatiya Nyaya Sanhita, Section 111(1)[7] defines it comprehensively to include any continuing unlawful activity such as kidnapping, robbery, vehicle theft, extortion, land grabbing, contract killing, economic offences, cyber-crimes, trafficking of persons, drugs, weapons, or illicit goods or services, as well as human trafficking for prostitution or ransom. Such activities, when carried out by any person or a group acting in concert, singly or jointly, either as members of an organised crime syndicate or on its behalf, using violence, threats, intimidation, coercion, or any other unlawful means to gain direct or indirect material benefit including financial gain shall constitute organised crime. The section further clarifies that an "organised crime syndicate" means a group of two or more persons acting jointly or singly to indulge in any continuing unlawful activity, and "continuing unlawful activity" means a prohibited act that is a cognizable offence punishable with imprisonment of three years or more, committed as part of a syndicate, with multiple charge sheets filed and cognizance taken within the last ten years, and includes economic offences such as criminal breach of trust, forgery, counterfeiting currency or stamps, hawala transactions, mass-marketing frauds, or schemes to defraud banks or financial institutions. However, while these sweeping definitions attempt to cover the evolving nature of organised crime in the digital age, their broad and ambiguous scope particularly in relation to cyber-crimes raises concerns about uneven implementation and potential misuse. Without clear safeguards, this could inadvertently criminalise legitimate forms of digital expression, resulting in a chilling effect on the right to free speech and highlighting the urgent need for balanced, precise drafting and modern investigative frameworks within BNS to tackle organised cyber-crime effectively.

The Digital Personal Data Protection Act of 2023[8] has an impact on privacy as well because it permits the state to access personal information without authorization. However, there are some areas where the current laws need to be improved, and the BNS's introduction of progressive reforms like community service as a sentencing option and updated definitions of crimes like "snatching" or identity-based group murders, as well as its very specific provisions for emerging cybercrimes like cyberstalking or online scams, show that there is always room for improvement. BNS must therefore continue to develop in a way that strengthens its digital

[7] THE BHARATIYA NYAYA SANHITA, 2023
[8] THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

forensic infrastructure, aligns with international standards, and takes into account all the difficulties posed by emerging technologies like artificial intelligence (AI), blockchain, and even the Internet of Things.

Cybercrime under the Bharatiya Nyaya Sanhita (BNS) has become a growing concern as India faces rising digital threats like online fraud, hacking, identity theft, and cyberbullying. While the BNS, along with the Bharatiya Sakshya Adhiniyam (BSA)[9] and Bharatiya Nagarik Suraksha Sanhita (BNSS)[10], introduces updated provisions such as treating electronic records as primary evidence and categorizing organized digital offenses under sections like 111, 316, and 318, significant challenges remain. Fast-evolving technology, the use of AI for deepfakes and advanced hacking, jurisdictional issues with cross-border crimes, lack of technical expertise among legal professionals, and low reporting rates make enforcement difficult.

Landmark judgments like ***Shreya Singhal*** **and** ***K.S. Puttaswamy***[11] emphasize balancing cyber laws with free speech and privacy. To tackle these issues effectively, India must regularly update laws, train legal professionals, improve forensic infrastructure, raise public cyber awareness, and strengthen international cooperation to ensure that the BNS framework keeps pace with modern digital crimes.

Research Objectives:

1. To scrutinize the implications of the BNS 2023 on India's efforts to combat cybercrime.
2. To assess the effectiveness of BNS provisions specifically dealing with cybercrime.
3. To examine the inclusion of cybercrime within the scope of organised crime under BNS.
4. To evaluate the recognition and admissibility of electronic records as primary evidence.
5. To analyse how BNS addresses challenges posed by emerging technologies such as Artificial Intelligence (AI) and the Internet of Things (IoT).

[9] "THE BHARATIYA SAKSHYA ADHINIYAM, 2023" (2023) N–O. 47 THE GAZETTE OF INDIA EXTRAORDINARY
[10] "Bharatiya Nagarik Suraksha Sanhita, 2023"
[11] *Shreya Singhal* and *K.S. Puttaswamy 2015 SC 1523 MANU/SC/0329/2015*

6. To identify the gaps in the current legal framework for dealing with digital crimes.

7. To propose a future-ready legal framework that balances technological advancement with national security, privacy, and individual freedoms.

Research Methodology:-

To get a complete grasp of the subject, the researcher adopted a mixed-methods strategy that blended quantitative and qualitative techniques. In order to acquire information for the study's quantitative component, surveys were administered to Indian enterprises and people concerning their understanding of and compliance with data privacy legislation. Key stakeholders, including government officials, legal professionals, corporate representatives, and members of industry associations, have been interviewed in order to acquire qualitative data. The study's findings have been supported by an examination of key literature, policy papers, and legislative frameworks pertaining to cyber legislation and data protection in India.

1. History of Digital Crimes in India

1.1 Major Cyberattacks in India -

UIDAI Aadhaar Data Breach (2018)[12]: A significant data breach in 2018 exposed the personal and financial information including Aadhaar numbers and bank details of approximately 1.1 billion Indian citizens, with the data illegally sold online after being made publicly available by hackers. This breach highlighted severe vulnerabilities in India's digital security infrastructure. In a more recent and alarming development, a 2023 report by U.S.-based cybersecurity firm Resecurity revealed that the personal data of 81.5 crore (815 million) Indians, allegedly sourced from the Indian Council of Medical Research (ICMR), was found for sale on the dark web. The leaked data includes Aadhaar and passport numbers, phone numbers, and addresses, and was being offered by a threat actor for $80,000. These incidents underscore the urgent need for stronger cybersecurity frameworks and data protection mechanisms in India.

[12] Ahmed N, "How the Personal Data of 815 Million Indians Got Breached | Explained" (*The Hindu*, November 7, 2023)

Pune Citibank Mphasis Call Center Fraud[13]: Some ex-employees of BPO arm of MPhasis Ltd source scammed US Customers of Citibank to the tune of Rs 1.5 crores. It was one of those cyber crime situations that aroused worries of numerous kinds including the role of "Data Protection". The offense was evidently done utilizing "Unauthorized Access" to the "Electronic Account Space" of the clients. It is therefore squarely within the domain of Cyber Crimes.

Information Technology Act, 2000[14] is versatile enough to fit the features of crime not covered by Information Technology Act, 2000 but covered by other statutes since any IPC offence committed with the use of Electronic Documents can be viewed as a crime with the use of a Written Documents. Cheating, Conspiracy, Breach of Trust, etc. are consequently applicable in the aforesaid instance in addition to the provision in ITA-2000. Under ITA-2000 the crime is recognized both under Section 66 and Section 43. Accordingly, the persons involved are responsible for imprisonment and fine as well as a duty to pay damages to the victims to the maximum extent of Rs 1 crore per victim for which the "Adjudication Process" can be used.

SMC Pneumatics (India) Pvt. Ltd. vs. Jogesh Kwatra[15]: In India's first case of cyber defamation, the High Court of Delhi seized jurisdiction over a dispute where a corporation's reputation was being defamed through emails and passed an important ex-parte injunction.

Amongst the many cyber cases in India, in this case, the defendant Jogesh Kwatra being an employee of the plaintiff company started sending derogatory, defamatory, obscene, vulgar, filthy and abusive emails to his employers as also to different subsidiaries of the said company all over the world with the aim to defame the company and its Managing Director Mr. R K Malhotra. The plaintiff filed a complaint for permanent injunction barring the defendant from doing his illegal activities of sending disparaging emails to the plaintiff.

On behalf of the plaintiff, it was alleged that the emails sent by the defendant were distinctly obscene, vulgar, abusive, frightening, humiliating and defamatory in nature. Counsel also stated that the goal of sending the said emails was to tarnish the high reputation of the plaintiff all over India and the world. He further stated that the activities of the defendant in sending the emails had resulted in an invasion of the legal rights of the plaintiff.

[13] *Pune Citibank Mphasis Call center fraud*. (n.d.).
[14] *THE INFORMATION TECHNOLOGY ACT, 2000*
[15] *SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra 2001 Delhi District Court* RFA--268/2014

Further, the defendant is under a responsibility not to transmit the aforesaid emails. It is crucial to mention that after the plaintiff corporation learned the stated employee could be engaged in the matter of sending abusive emails, the plaintiff terminated the services of the defendant.

After hearing lengthy arguments of Counsel for Plaintiff, Hon'ble Judge of the Delhi High Court ordered an ex-parte ad interim injunction, stating that a prima facie case had been brought out by the plaintiff. Consequently, in this cyber fraud case in India, the Delhi High Court restrained the defendant from sending derogatory, defamatory, obscene, vulgar, humiliating and abusive emails, either to the plaintiff or to its sister subsidiaries all over the world, including their Managing Directors and their Sales and Marketing departments. Further, Hon'ble Judge also restricted the defendant from publishing, transmitting or causing to be published any information in the physical world, as also in cyberspace, which is disparaging or defamatory or abusive.

This order of Delhi High Court assumes tremendous significance as this is the first time that an Indian Court assumes jurisdiction in a matter concerning cyber defamation and grants an ex-parte injunction restraining the defendant from defaming the plaintiff by sending derogatory, defamatory, abusive and obscene emails either to the plaintiffs or their subsidiaries.

BSNL, Unauthorized Access[16]: In a leading cybercrime case, the Joint Academic Network (JANET) was hacked by the accused, after which he prohibited access to the authorized users by changing passwords along with removing and uploading files. Making it look like he was authorized personnel, he made changes in the BSNL computer database in their internet users' accounts. When the CBI carried out investigations after establishing a cybercrime case against the defendants, they found that the broadband Internet was being used without any authority. The accused used to hack into the server from various cities like Chennai and Bangalore, amongst others. This investigation was done after the Press Information Bureau, Chennai, filed a complaint. In the ruling by the Additional Chief Metropolitan Magistrate, Egmore, Chennai, the accused from Bangalore would be put to prison for a year and will have to pay a fine of Rs 5,000 under Section 420 IPC and Section 66 of the IT Act.

[16] BHARAT SANCHAR NIGAM LIMITED v. SMART DIVISION PRIVATE LIMITED, 2023 SCC ONLINE DEL 3245

2. Other Major Cyber attacks internationally-

The Yahoo Data Breach[17]: Cybersecurity Ventures highlights that Yahoo still holds the record for the largest known data breach ever, with all 3 billion of its user accounts compromised in 2013. This breach, attributed to state-sponsored hackers allegedly linked to Russia, exposed usernames, email addresses, phone numbers, birthdates, and encrypted passwords and shockingly remained undiscovered for nearly three years. In a separate but related incident, Yahoo was also hacked in 2014, when attackers gained access to account-reset tools for over 500 million users, further demonstrating the company's long-standing security vulnerabilities. The article places Yahoo's breaches alongside other major historical cyber-attacks such as Stuxnet, WannaCry, NotPetya, Equifax, and the SolarWinds attack to show how large-scale, sophisticated intrusions continue to shape global cybersecurity threats. The Yahoo case serves as a stark reminder of the catastrophic impact a single breach can have and underscores the ongoing need for stronger data protection measures, advanced threat detection, and proactive cyber resilience strategies in both private companies and governments worldwide.

The Cambridge Analytica Scandal[18]: In 2018, it was revealed that political consulting firm Cambridge Analytica had harvested data from millions of Facebook users without their consent and used it to influence elections in various countries, including India. In response, the Indian government ordered an investigation into the matter, and Facebook was fined Rs. 5 lakh for each day it failed to comply with the investigation. Despite this action, India's legal system has often been criticised for its slow response to cybercrimes, with many cyber criminals managing to evade punishment. However, the introduction of the Personal Data Protection Bill, 2019, has raised hopes for a more robust and effective approach to tackling such crimes. The bill includes provisions for safeguarding personal data, establishing a dedicated data protection authority, and imposing penalties on violators. While its enforcement remains to be seen, the legislation represents a significant and positive step towards strengthening India's cybersecurity and data protection framework.

[17] Magazine C, "Yahoo Still Ranks as the Largest Data Breach in History" (*Cybercrime Magazine*, November 18, 2024)
[18] Graham-Harrison E and Cadwalladr C, "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach" *The Guardian* (September 29, 2021)

3. Legal and Judicial Responses to Cybercrimes

Nasscom v. Ajay Sood[19]: In this case, the Delhi High Court dealt with one of India's earliest reported cases of cyber fraud involving "phishing[20]." The defendants had fraudulently impersonated NASSCOM India's premier software association—via fake emails and websites to extract personal data for recruitment purposes. The Court noted phishing as a form of internet fraud and a civil wrong under Indian law akin to misrepresentation and passing off. The defendants acknowledged wrongdoing and agreed to a Rs. 16 lakh settlement, with the Court issuing a permanent injunction against further misuse of NASSCOM's name. Though the case was resolved via compromise, it set a crucial precedent in recognizing phishing as a cyber tort in Indian jurisprudence.

Avinash Bajaj v. State (NCT of Delhi)[21]: The CEO of Bazee.com was arrested under Section 67 of the IT Act for broadcasting cyber pornography. The court held that the defendant, as a service provider, was not vicariously liable for content created by users and held intermediary protections paramount in cyber laws.

4. Need for Legal Regulations to Ensure Data Protection

Legal regulations form the backbone of protecting personal data in the digital world. These regulations play a very important role in, Legal frameworks ensure that personal data is collected, processed, and used responsibly, preserving individual's privacy and autonomy. Robust regulations help prevent identity theft, fraud, stalking, discrimination, and other malicious activities that exploit sensitive personal information. Laws provide the framework for permissible data processing and make firms responsible for their adherence to these rules. The encouragement of secure technologies and data protection practices drives innovation while protecting personal data. Global uniform standards make compliance with data protection laws easier among international organizations, thus assuring consistency in privacy protection across jurisdictions. Legal regulations protect privacy, prevent data misuse, and provide accountability. They also promote technological advancement and international

[19] National Association Of Software And Service Companies v. Ajay Sood 2005 SCC ONLINE DEL 402
[20] CSRC Content Editor, "Phishing - Glossary | CSRC" <https://csrc.nist.gov/glossary/term/phishing#:~:text=Definitions%3A,legitimate%20business%20or%20reputable%20person.>
[21] *Avnish Bajaj v. State (Nct) Of Delhi. 2004 SCC ONLINE DEL 1160*

cooperation to maintain security in data.

4.1 Cybercrimes Against Women

Cybercrimes disproportionately target women, often violating their privacy, dignity, and emotional well-being. The following are prevalent forms of cybercrimes against women that are not explicitly addressed in the Bharatiya Nyaya Sanhita, 2023. Abusive messages, derogatory comments, or malicious rumors aimed at intimidating or embarrassing women on social media, forums, or chat platforms. The non-consensual sharing of intimate images or videos to retaliate, humiliate, or control the victim. Threats of exposing private information or images to coerce women into providing explicit content or participating in unwanted activities. Using stolen personal information to impersonate women online, often to commit fraud or damage reputations. Establishing trust with women online to exploit them sexually, financially, or emotionally. Persistent harassment through digital platforms, including spreading rumors, creating fake profiles, or encouraging others to join in the abuse. Scammers deceive women into disclosing financial details through phishing emails, fraudulent websites, or malware.

Gender-based hate speech and the promotion of misogynistic ideologies have a profound impact on women's mental and emotional well-being. Similarly, the non-consensual sharing of private images or videos causes immense emotional distress and reputational damage. Addressing these harmful behaviors requires targeted legal reforms, the implementation of advanced technological safeguards, and widespread public awareness. Digital literacy campaigns are equally essential to empower individuals to recognize, prevent, and respond to such violations effectively, ensuring a safer and more respectful online environment.

4.2 Cybercrimes Against Children

The internet's anonymity and accessibility have made children increasingly vulnerable to various cybercrimes. Offenses include the production, distribution, and possession of explicit images or videos involving children, often facilitated through online platforms. Predators exploit social networks, gaming environments, and chat platforms to manipulate children for sexual or financial exploitation. In some cases, children are coerced into sharing explicit content, which is later used to blackmail them for further exploitation or monetary gain. Online platforms and social media are also used to recruit children for commercial sexual exploitation. These crimes exploit children's innocence and trust, underscoring the urgent need for stringent

legal frameworks, advanced technological safeguards, and global collaboration to combat such abhorrent acts.

4.3 Cybercrimes Against the State

Cybercrimes targeting state security and sovereignty pose significant threats by enabling organized crime, terrorism, and anti-national activities. Online platforms on the dark web facilitate the illegal trade of drugs, weapons, and stolen data, while separatist groups and rebels exploit cyber warfare to hack government systems, disrupt critical infrastructure, and spread disinformation, destabilizing governance and public order. State-sponsored cyber espionage further escalates risks by targeting sensitive government networks, military secrets, and critical infrastructure, compromising classified data and essential services. These acts leverage the borderless nature of the internet to remain anonymous, making it challenging to safeguard national integrity. Addressing these threats demands robust cybersecurity measures, global cooperation, and the strict enforcement of cyber laws to ensure a secure and resilient digital environment.

4.5 Cybercrimes Against the Human Body

Modern cybercrimes have evolved significantly, often leaving a profound impact on an individual's mental and physical well-being. These offenses can cause severe psychological harm and, in some cases, physical consequences. Some notable examples include:

4.6 Cyberbullying and Harassment

Cyberbullying involves using digital platforms to harass, intimidate, or threaten individuals, often resulting in emotional distress, depression, and, in extreme cases, suicide. Another prominent case is the Vishakha Meena case (2016) from Rajasthan. Vishakha, a teenager, died by suicide after facing relentless online bullying and harassment. She was humiliated on social media platforms, where personal photos were morphed and circulated without her consent. The bullying escalated to a point where it deeply affected her mental health, leading to her tragic death.

4.6.1 Online Shaming and Doxxing

In India, online shaming and doxxing[22] have become increasingly prevalent, often leaving victims emotionally shattered. For instance, the case of a college student in Kerala who faced public humiliation after a private video was leaked online highlights the devastating impact of such acts. Her personal details were shared widely on social media, leading to intense harassment, social isolation, and emotional distress. This incident demonstrates how public shaming and doxxing can destroy an individual's sense of safety and mental well-being, emphasizing the urgent need for stronger digital privacy protections.

4.6.2 Internet Trolling

India has witnessed numerous cases where internet trolling has caused severe mental health consequences. One notable example is Bollywood actress Anushka Sharma, who faced a barrage of online trolling and blame after India's cricket team faced losses in major matches. The relentless negative comments and personal attacks on social media took a toll on her mental health. Such trolling often escalates from casual banter to targeted harassment, causing anxiety, depression, and emotional exhaustion, showing the darker side of unchecked digital spaces.

4.6.3 Exposure to Graphic Content and Online Radicalization:

The psychological effects of exposure to graphic content and online radicalization are evident in cases like that of young individuals recruited by extremist organizations in India through online platforms. In one instance, a teenager from Kerala was reportedly radicalized through exposure to extremist propaganda on social media, leading to his recruitment by a terrorist group. The trauma of engaging with violent or manipulative content online can profoundly affect mental stability, pushing vulnerable individuals into harmful and life-altering paths.

4.6.4 Deepfake Technology[23]:

In India, deepfake technology has started to emerge as a tool for blackmail and harassment. A

[22] Venugopal S, "What Is Doxxing and What Can You Do If It Happens to You?" (*The Hindu*, April 14, 2024) <https://www.thehindu.com/sci-tech/technology/what-is-doxxing-and-what-can-you-do-if-it-happens-to-you/article68045978.ece>

[23] "Deepfakes, Explained | MIT Sloan" (*MIT Sloan*, July 21, 2020)

recent case involved a woman in Delhi whose morphed videos were circulated online by an acquaintance after a dispute. These fake videos caused significant reputational damage and emotional distress, highlighting the horrifying potential of deepfakes to ruin lives. The victim faced public shaming and professional fallout, underlining the need for stringent regulations to curb the misuse of artificial intelligence technologies.

4.7 Cybercrimes Against Entities:

On July 18, 2024, WazirX[24], one of India's leading cryptocurrency exchanges, suffered a major cyberattack that resulted in a loss of approximately $234.9 million (about ₹2,000 crore) in investor funds, affecting both retail and institutional investors. The stolen assets were siphoned from the exchange and transferred to a new address by the Lazarus Group — a North Korean hacker collective also known as the Guardians of Peace or Whois Team, believed to operate under the North Korean government's direction. Active since 2010, the group has been linked to numerous high-profile cyberattacks worldwide.

In this attack, the hackers exploited WazirX's multisignature wallet system, which required approvals from three out of five WazirX signatories and one from Liminal to process transactions. By creating a fake WazirX account, depositing tokens, and trading Gala (GALA) tokens, the hackers initially drained the hot wallet before targeting the cold wallet. When legitimate signatories accessed the multisig wallet, the attackers altered the smart contract controlling it, giving themselves full control and eliminating the need for WazirX's keys, allowing them to drain all remaining funds.

Prior to the breach, WazirX had reported holding around $500 million in digital assets in its June 2024 proof-of-reserves disclosure. Following the attack, the exchange suspended crypto trading on July 18, 2024. In January 2025, the Singapore High Court permitted Zettai PTE LTD, WazirX's parent company, to convene a meeting with creditors to vote on a recovery plan for the lost assets.

[24] Team WC, "WazirX Cyber Attack: Key Insights and Learnings - WazirX Blog" (*WazirX Blog*, September 6, 2024)

5. Other cybercrimes

5.1 Identity Theft:

Identity theft involves stealing personal data, like Aadhaar numbers or credit card details, to commit fraud or other crimes. For example, when a cybercriminal uses a victim's identity to open credit accounts or make unauthorized purchases, the financial losses can be crippling. Beyond monetary damage, victims often face emotional distress and the time-consuming task of reclaiming their stolen identity and rectifying fraudulent transactions.

5.2 Cyber Fraud:

Cyber fraud includes scams like phishing emails or fake online stores that exploit trust to steal money or property. Imagine a person purchasing a luxury item, like a designer watch, from what seemed to be a genuine website, only to realize later that the product was never delivered. Such scams leave victims not only out of pocket but also questioning their online security and trust in digital marketplaces.

5.3 Ransomware Attacks:

In ransomware attacks, cybercriminals encrypt files or lock systems, demanding payment to restore access. A small business, for instance, could find itself unable to access critical customer records or financial data unless a ransom is paid. This disrupts operations, causes revenue losses, and leaves business owners grappling with fear and uncertainty over whether their data will ever be recovered.

5.4 Cyber Extortion:

Cyber extortion involves threats to release sensitive information or disrupt systems unless a ransom is paid. For example, a company might face demands from hackers threatening to leak confidential client data. Such incidents not only lead to financial strain but also cause reputational damage, shaking the trust of clients and employees alike.

5.5 Cyber Vandalism:

Cyber vandals deface websites, disrupt online services, or alter data, causing financial and

reputational harm. A business that finds its website defaced or critical systems disrupted may lose customers and incur steep costs to restore operations. Beyond the financial impact, the business may also face public embarrassment and a loss of trust among its clientele.

6. Role of Artificial Intelligence in Facilitating Digital Crimes: A Modern Challenge for the Bharatiya Nyaya Sanhita

Artificial Intelligence (AI) has emerged as a transformative force in the digital age, but it is equally becoming a potent enabler of cybercrime. Under the Bharatiya Nyaya Sanhita (BNS), India seeks to modernize its criminal law framework, yet addressing AI-driven crimes requires special attention. Criminals are now leveraging AI in several sophisticated ways that traditional laws struggle to tackle.

Artificial Intelligence (AI) has swiftly become a transformative force across industries worldwide, streamlining workflows, boosting productivity, and enabling unprecedented levels of automation. Many companies initially adopted generative AI tools like ChatGPT to assist with tasks such as drafting, translation, or data summarization, and gradually began developing proprietary AI systems to automate even complex operations. However, these advancements are not confined to legitimate business applications alone; organized crime groups are exploiting AI in parallel ways, reimagining how illicit activities are planned and executed.

Initially, cybercriminals deployed AI to enhance existing tactics for example, translating phishing emails into multiple languages to target victims globally, or scanning massive code repositories to locate exploitable vulnerabilities more efficiently. These early applications mirrored legitimate uses of AI but were weaponized to expand the scale and impact of cybercrime.

The next frontier for criminal networks is the creation of autonomous AI systems capable of executing illegal tasks without human oversight. This could include AI agents that independently identify system weaknesses, breach networks, and extract sensitive information, or even sabotage critical infrastructure like water treatment plants. Such self-operating malicious systems would not only multiply the speed and reach of attacks but also make detection and intervention significantly more difficult.

6.1 Deepfakes & Synthetic Media

AI tools can generate hyper-realistic fake videos and audio recordings, enabling fraud, defamation, and large-scale misinformation campaigns that damage reputations or sway public opinion. With the right AI tools, anyone can create fake scenarios or images of individuals even without ever meeting them. Celebrities and influencers are especially vulnerable, as publicly available photos make it easier to generate fake content and exploit their reputation for profit. Deepfakes are also increasingly used to produce non-consensual pornographic material, creating grave cybersecurity and privacy risks for anyone whose image is accessible online.

Deepfake technology represents another alarming misuse of AI, enabling the creation of fabricated audio, video, or images that mimic real individuals. Criminals have used such tools to impersonate executives in so-called "business email compromise" scams, defraud organizations, or extort victims. Regulatory bodies and financial institutions have recently raised alerts regarding the spike in fraudulent schemes involving deepfake media. Moreover, AI has made it easier to create synthetic identities composites of stolen real-world data that criminals use to open fraudulent accounts and conduct illicit transactions anonymously.

6.2 AI-Enabled Phishing & Malware

Generative AI can craft highly convincing phishing emails and fraudulent websites, drastically increasing the success rates of online scams. These tools can easily produce authentic-looking messages that target individuals holding sensitive information, with the goal of stealing data or money. Such sophisticated AI-generated phishing tactics make it more difficult for ordinary users to detect scams.

6.3 Automated Cyberattacks

AI-powered systems can automate hacking attempts, including brute force attacks and advanced vulnerability scanning. This automation makes cyber intrusions faster, more adaptive, and harder to defend against, significantly raising the stakes for cybersecurity experts and law enforcement alike. AI systems are also optimizing ransomware strategies by pinpointing the most critical files or systems to encrypt, maximizing leverage against victims.

Nation-states have been observed integrating AI into cyber-espionage campaigns, where machine learning helps breach secure systems that traditional malware struggles to penetrate.

6.4 Social Engineering Bots

AI-driven chatbots can convincingly impersonate humans, tricking unsuspecting individuals into revealing confidential data or transferring money. These bots can adapt their language and tone to build trust quickly, making social engineering attacks far more effective and harder to detect.

6.5 Attacks on AI Systems

Cybercriminals do not just use AI; they attack it too. Through techniques like data poisoning and adversarial attacks, criminals can manipulate AI systems, undermining the reliability of AI-dependent services such as facial recognition, fraud detection, or automated content moderation. This creates serious risks for sectors that rely heavily on AI technologies.

7. Key Challenges for the BNS

While the BNS includes provisions on cyber fraud and identity theft, AI-specific crimes present unique hurdles. Proving the source and authorship of AI-generated content can be technically challenging. Determining criminal liability when AI systems operate autonomously is still a grey area. The rapid pace of AI advancements often outpaces legislative updates, leaving gaps in the law. Additionally, addressing cross-border AI crimes is complicated by limited international cooperation and jurisdictional constraints.

7.1 Emerging Uses: How Criminals Leverage AI

Criminal groups, fraudsters, and even state-backed actors are increasingly harnessing AI to enhance the sophistication of their operations. The automation of phishing campaigns through AI-generated content allows attackers to produce realistic, personalized messages at scale, bypassing conventional security filters. Similarly, AI tools are now being used to craft adaptable malware capable of evading detection by real-time security systems.

Reports, such as the 2024 US Treasury assessment on AI risks in the financial sector, have noted that even low-skilled threat actors can now deploy sophisticated malware previously

accessible only to advanced cybercriminals. This democratization of complex attack tools heightens the threat landscape for financial institutions and other vulnerable sectors.

7.2 Understanding the Stages of Criminal AI Adoption

Law enforcement agencies, policymakers, and security professionals must develop frameworks to monitor how criminal organizations adopt AI technologies. A helpful model categorizes this progression into three phases:

7.2.1 Horizon Phase: AI's application is mostly theoretical, but its potential for large-scale disruption is clear. For example, countries like North Korea have used sophisticated cyberattacks to fund illicit activities. The integration of autonomous AI could scale such operations drastically, making it even harder to detect and disrupt.

7.2.2 Emerging Phase: In this stage, AI tools are actively used to improve existing criminal operations, though humans still oversee key decisions. Early signs include the use of AI to produce deepfake child sexual abuse material (CSAM)[25], enhance disinformation campaigns, and automate phishing and scam operations.

7.2.3 **Mature Phase:** While largely hypothetical today, this phase would see AI systems surpass human-driven efforts in scale and complexity, autonomously executing tasks such as market manipulation or infrastructure sabotage. Cases like AI agents transacting in cryptocurrency markets demonstrate how AI could evolve to operate financial crimes independently.

8. Prevention and Response: Building AI-Integrated Defenses

Addressing the growing misuse of AI requires a multi-pronged strategy. Technological defenses, such as AI-powered detection systems for deepfakes or anomalous financial transactions, are already showing promise. Enhanced cybersecurity frameworks must integrate machine learning tools that adapt alongside evolving threats.

Equally critical is the development of robust policy and regulatory frameworks. National and international institutions should work together to establish standards for responsible AI use, while ensuring swift action against actors who abuse this technology. Efforts by organizations

[25] "Government of India Taking Measures against Online Pornography" <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2113098>

like INTERPOL and the UN to harmonize AI governance can serve as models for coordinated global responses.

Public education is also key to countering AI-enabled fraud and disinformation. Awareness campaigns must teach individuals to recognize manipulated content and fraudulent schemes, reducing the success rate of AI-driven scams.

Finally, collaborative approaches including public-private partnerships and shared intelligence networks will be crucial. Financial institutions, blockchain forensics firms, and governments must jointly track and disrupt illicit financial flows, leveraging the same AI capabilities that criminals exploit.

9. Recommendations for Enhancing Cybersecurity and Data Protection in India

As cybercrimes evolve in both scale and sophistication, it has become imperative for legal, governmental, and business frameworks to adapt effectively. These efforts are critical to ensuring the safety and security of individuals, organizations, and the nation as a whole. The Bharatiya Nyaya Sanhita (BNS) of 2023[26] represents a significant step forward in addressing cybercrimes through a modernized legal framework. However, additional measures are needed to strengthen its impact, particularly in key areas such as data protection, cybersecurity infrastructure, and public awareness about cyber education. The act marks a crucial step in addressing cybercrimes by integrating provisions related to digital evidence, data protection, and cyber forensic tools. However, to stay ahead of evolving threats and provide better protection for personal data, the following measures are essential:

India's current data protection framework, while progressive, needs reinforcement through comprehensive laws like the proposed Personal Data Protection Bill, 2019. These laws should align with global best practices, establishing clear regulations for the collection, storage, and processing of personal data. Provisions must address data breaches, unauthorized data sharing, and offer robust safeguards for sensitive information.

Laws alone are insufficient without effective enforcement. To ensure compliance, strict penalties and consequences for violations must be implemented. Empowering regulatory bodies to enforce digital security regulations and holding violators accountable will enhance

[26] Ibid. [6]

the effectiveness of these laws.

Educating the public about cybersecurity is essential. The government should initiate widespread campaigns using digital platforms, workshops, and media to raise awareness about safe online practices. Topics like recognizing phishing scams, safeguarding passwords, and understanding cyberbullying should be highlighted to empower individuals to protect themselves online.

A robust Artificial intelligence cybersecurity infrastructure is critical to safeguarding sensitive data and preventing cyberattacks. Both the government and businesses must take proactive steps to strengthen these defenses. The government should prioritize investments in cutting-edge cybersecurity technologies to protect national and financial systems. This includes deploying advanced firewalls, encryption systems, and secure communication protocols to shield both public and private data from threats. Encryption is a cornerstone of data protection. Both government and private entities should adopt robust encryption standards for data storage, transmission, and communication. Mandating encryption for all sensitive data will significantly reduce the risk of unauthorized access. Requiring multi-factor authentication (MFA) for online accounts and systems is a simple yet effective security measure. By mandating MFA, which uses multiple verification steps, organizations can drastically reduce the likelihood of unauthorized access.

With cyber threats evolving rapidly, regular security audits are essential. Identifying vulnerabilities and addressing them through timely updates to software, firewalls, and security systems ensures both public and private sectors stay ahead of emerging risks. Cybersecurity education plays a pivotal role in preventing cybercrimes. Empowering individuals, students, teachers, and employees with knowledge is key to building a secure digital ecosystem. Cybersecurity education should be an integral part of school and university curricula. Young individuals need to learn about online risks, data protection, and how to recognize threats like phishing, scams, and cyberbullying. Special emphasis should be placed on responsible social media usage and the importance of privacy. Employees are often the weakest link in an organization’s cybersecurity chain. Mandatory training programs should focus on recognizing phishing attempts, creating strong passwords, and protecting sensitive company information. Organizations should regularly conduct workshops to ensure employees can mitigate risks effectively. Collaborative campaigns between the government, private organizations, and

educational institutions can amplify cybersecurity awareness. Utilizing engaging formats like short films, documentaries, and public service announcements will effectively communicate key messages about safe online practices. Cyber experts and ethical hackers are essential for identifying and addressing vulnerabilities. Workshops, seminars, and boot camps should be organized to keep these professionals updated on the latest threats and defense strategies. Ethical hackers should be encouraged to collaborate with government agencies to close security gaps. Cybercrimes often transcend borders, requiring coordinated international efforts to address them effectively. India must strengthen mutual legal assistance agreements and extradition treaties with other countries. Such agreements facilitate the tracking and prosecution of cybercriminals operating across borders. Collaboration with global partners to exchange cybersecurity knowledge, best practices, and threat intelligence is vital. This cooperation will help develop common strategies to counteract global cyber threats and enhance collective resilience against emerging cybercrimes.

Conclusion

The Bharatiya Nyaya Sanhita (BNS) 2023 marks a significant milestone in India's fight against cybercrimes. By categorizing cyber offenses as organized crime, recognizing electronic records as primary evidence, and introducing strict penalties for digital misconduct, the BNS aims to address the growing threats of cybercriminal activity. It emphasizes technological advancements, such as cyber forensics and partnerships with agencies like CERT-In, alongside fostering public-private and international collaborations to build a robust framework against cyber threats.

However, challenges persist. Ambiguities in defining cybercrimes risk inconsistent enforcement, and concerns about free speech overreach and inadequate digital forensic infrastructure must be addressed. To bridge these gaps, legislative refinement, strong implementation, and a balanced approach that safeguards democratic rights are critical. Effective laws must also translate into action at the grassroots level. Public awareness and participation are vital to recognizing cyber threats and advocating for privacy protections. Without societal involvement, laws alone cannot protect against cybercrimes.

Given the global nature of cyber threats, India must continuously evolve its legal frameworks to combat sophisticated attacks like cyberterrorism. Specialized teams, modernized laws, and stringent penalties are essential to tackling these complex crimes. Equally important is

understanding the psychological motivations of cybercriminals, enabling strategies for rehabilitation and ethical awareness. Cybercrimes often cause profound emotional and social damage, operating invisibly yet leaving lasting impacts on trust and relationships. Addressing this "silent violence" requires fostering ethical digital behavior, emphasizing respect, cooperation, and truthfulness in cyberspace.

Ultimately, the success of BNS 2023 hinges on comprehensive enforcement, active public and private participation, and a societal shift toward ethical online practices. By investing in legal reforms, cybersecurity education, and infrastructure, India can build a secure and innovative digital future for all. The dual-use nature of artificial intelligence demands vigilant oversight and innovative defenses. While AI offers transformative opportunities for progress, its potential misuse by sophisticated cybercriminals and nation-state actors presents unprecedented risks. A proactive, collaborative, and adaptable approach grounded in technology, regulation, education, and international cooperation is essential to safeguard digital systems and ensure that AI remains a force for good rather than a weapon for harm.

There is an urgent need to introduce robust AI-specific laws to govern the operation and accountability of AI technologies. Without clear safeguards, AI tools could fall into the wrong hands or behave unpredictably, potentially triggering large-scale cyber warfare and threatening digital security globally. Clearly defining offences involving synthetic and AI-generated data will help close legal loopholes. It is equally important to establish liability for developers and distributors of malicious AI tools. Strengthening digital forensic capabilities will support the authentication of AI-generated evidence in court. Fostering stronger international cooperation will help tackle cross-border AI threats. Lastly, law enforcement agencies must be equipped with AI-based detection and prevention tools to stay ahead of increasingly sophisticated cyber threats.

REFERENCES:

1. Sharmin Kapadia and Priyam Sharma, "'Unorganized' Crime under the Bhartiya Nyaya Sanhita, 2023" (*Bar And Bench - Indian Legal News*, September 4, 2024) <https://www.barandbench.com/columns/unorganized-crime-under-the-bhartiya-nyaya-sanhita-2023>

2. Khetan A and Law L, "Cyber-Bullying: How Should India Legally Equip Itself?" *Live Law* (November 15, 2024) <https://www.livelaw.in/law-firms/law-firm-articles-/cyber-bullying-digital-harassment-indian-child-protection-fund-national-crime-records-bureau-cybercrime-cyber-attacks-social-stigma-abuse-pocso-it-act-275322?utm>

3. JSA Advocates & Solicitors, "Stringent Measures against Cybercrimes in India's New Criminal Justice System - JSA" (*JSA*, July 17, 2024) <https://www.jsalaw.com/newsletters-and-updates/stringent-measures-against-cybercrimes-in-indias-new-criminal-justice-system/>

4. Sharma B and MCO Legals, "Cyber Law: Series 2: Issue 3" (2024) journal-article <https://www.mcolegals.in/kb/Cyber_Law-_Series_2-_Issue_3_-_Cybercrimes_under_the_Bhartiya_Nyaya_Sanhita,_2023.pdf>

5. Centre AD| AFE, "The New Criminal Laws and Their Interface with Technology — Esya Centre" (*Esya Centre*, July 31, 2024) <https://www.esyacentre.org/perspectives/2024/7/31/the-new-criminal-laws-and-their-interface-with-technology>

6. Singh M and Banerjee S, "Cybersecurity Laws and Regulations India 2025" (*International Comparative Legal Guides International Business Reports*, November 6, 2024) <https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/india>

7. "Tackling Cybercrime: Greater Digitisation Leads to Rising Challenges" (*Law.asia*, November 7, 2024) <https://law.asia/india-cybersecurity-legislation-reform/>