Bhartiya Nyay Sanhita and Cyber Crime

Monica Madholia Nandi
Associate Professor, Department of Political Science, Indraprastha College for Women, University of Delhi
Akansha*
Associate Professor, Department of Political Science, Indraprastha College for Women, University of Delhi
**Corresponding Author Email: akanshachandra@ip.du.ac.in*

Abstract: *As part of the Criminal Procedure Code revisions in India, the BNS (Bhartiya Nyaya Sanhita) replaces the IPC (Indian Penal Code). It seeks to simplify and modernize criminal justice processes.*

Cybercrime refers to a broad spectrum of illicit actions carried out through computers or the internet. Identity theft, data theft, phishing, online fraud, hacking, cyberstalking, and other crimes are included in this area.

India's Information Technology Act of 2000 and the Indian Penal Code, which is currently being replaced by BNS, provide the legal foundation for combating cybercrime in India. Because cybercrimes are always evolving, the BNS includes updated rules to handle them as part of the criminal justice system's reform. India has taken measures to address cybercrime and enhance law enforcement agency coordination by forming diverse cybercrime divisions and special investigation teams throughout its states.

This paper aims to examine how, although the IPC has certain laws pertaining to cybercrime, the BNS is structured to address the issue more comprehensively and contemporarily, taking into account the growing importance of digital technology in contemporary legal frameworks. It will also go into detail on how BNS, which recognizes the quick advancement of technology and the ensuing need for updated legal measures, gives a more precise definition and punishments for cybercrimes.

Keywords: Bhartiya Nyaya Sanhita, Cybercrime, Indian Penal Code, Indian legal framework

It was a watershed moment on 1 July 2024, as the British-created three criminal laws were deleted from the Indian legal system. The Indian Penal Code (IPC) was replaced by Bhartiya Nyay Sanhita (BNS), the Criminal Procedure Code was replaced by Bharatiya Nagarik Suraksha Sanhita (BNSS), and the Indian Evidence Act (IEA) was replaced by Bharatiya SakshyaAdhiniyam (BSA). Until 30 June 2024, India was administered by the criminal law – IPC of 1860. The Code had come into force in 1862 in all British Presidencies except the Princely States. "Although several amendments were introduced over time, the archaic penal law was initially drafted with colonial and outdated provisions aimed at suppressing Indians who opposed the British Crown, ensuring absolute control over the territory." (K. S., A. K., 2024)

The Need for New Criminal Laws

Several legal experts have opined that the 163-year-old Code had outlived its utility and had become outdated. It no longer reflected the present realities and evolving societal problems, especially in the wake of technological advancements. The new laws have attempted to modernize the legal framework by addressing issues like organized crime and economic offenses with the support of advanced investigation methodologies and technology. According to former Additional Solicitor General (ASG) and Senior Advocate Pinki Anand:

> Previously, our criminal statutes drafted in 1860, 1872, and 1973 were products of their time. And to keep them relevant, it required an extensive exercise of judicial interpretation…The choice of the people to choose the laws that bind us together is a basic feature of a democratic social contract. The Parliament has reviewed the judgements of the past and the jurisprudence that emerged from our Hon'ble Courts and has made democratic calls on what to keep, what to modify and what to remove. This was a democratic exercise that was needed. It's a revision that was needed. The rust that had settled has been cleansed. (ANI, 2024)

No doubt, the hurried manner in which the draft bills of the three proposed laws were criticized but the intention behind the move has also been appreciated. Advocates of the new laws have pointed out the following merits of the new laws:

(a)Novel procedures like zero-FIR i.e. the FIR can be filed in any police station of India irrespective of the location of the crime or the jurisdiction of the police station, have been introduced in the new criminal laws. Such citizen-

DOI: https://doi.org/10.62656/SIJSS.v24i2.2369

friendly procedures will initiate timely actions regardless of the location of the crime.

(b) Utilization of technology: There will be more reliance on technology to solve cases and deliver justice quickly.

(c) Justice-oriented approach: The laws shift the focus from punishment to justice, and aim to create a more equitable and modern legal system.

(d)Victim-centric approach: The laws prioritize the victim, and consider justice through a victim-centric approach. They prescribe fixed timelines within which the trials and investigation of the crimes would be completed.

(e) Punishments: In 33 crimes, imprisonment sentences have been increased, and in 83 crimes fine amounts have been increased. At the same time, community service as a punishment has been introduced in India for petty crimes. "Community service is defined as work that benefits the community and is intended to reduce the burden on jails." (Naik, 2024)

No doubt, the BNS has introduced significant changes in the old criminal laws of India. It has streamlined the criminal justice system by consolidating offenses and reducing the number of sections from 511 to 358.

Offences through Electronic Means

The nature of criminal activities has changed in recent times. Modern technologies and the ensuing interdependence have opened various avenues for criminal activity to be more common and lucrative, easier to commit, and harder to detect. The changing nature of criminal transgressions has been documented by the NCRB Report 2020, wherein it was pointed out that the 'traditional crimes' have declined and newer crimes like cybercrime have been on the rise ("Editorial: Crime Watch," 2021).

According to *Crime in India (2022),* a National Crime Records Bureau (NCRB) publication, registration of crimes under cybercrimes increased to 24.4% in 2022 compared to 2021. "Around 64.8% of registered cases were of fraud, followed by extortion (5.5%), and sexual exploitation (5.2%)." (Tondak, 2024). The rise in cybercrimes in India is due to the increased usage of digital mediums by a substantial portion of the Indian population. Unlike the pre-covid days, Indians have increasingly started interacting, transacting, and operating through various digital mediums. Thus, cyberspace has emerged as a socially constructed global reality. The technological advancements have transformed the nature of the crimes where the victims can be harmed without actually coming in physical contact with the perpetrator.

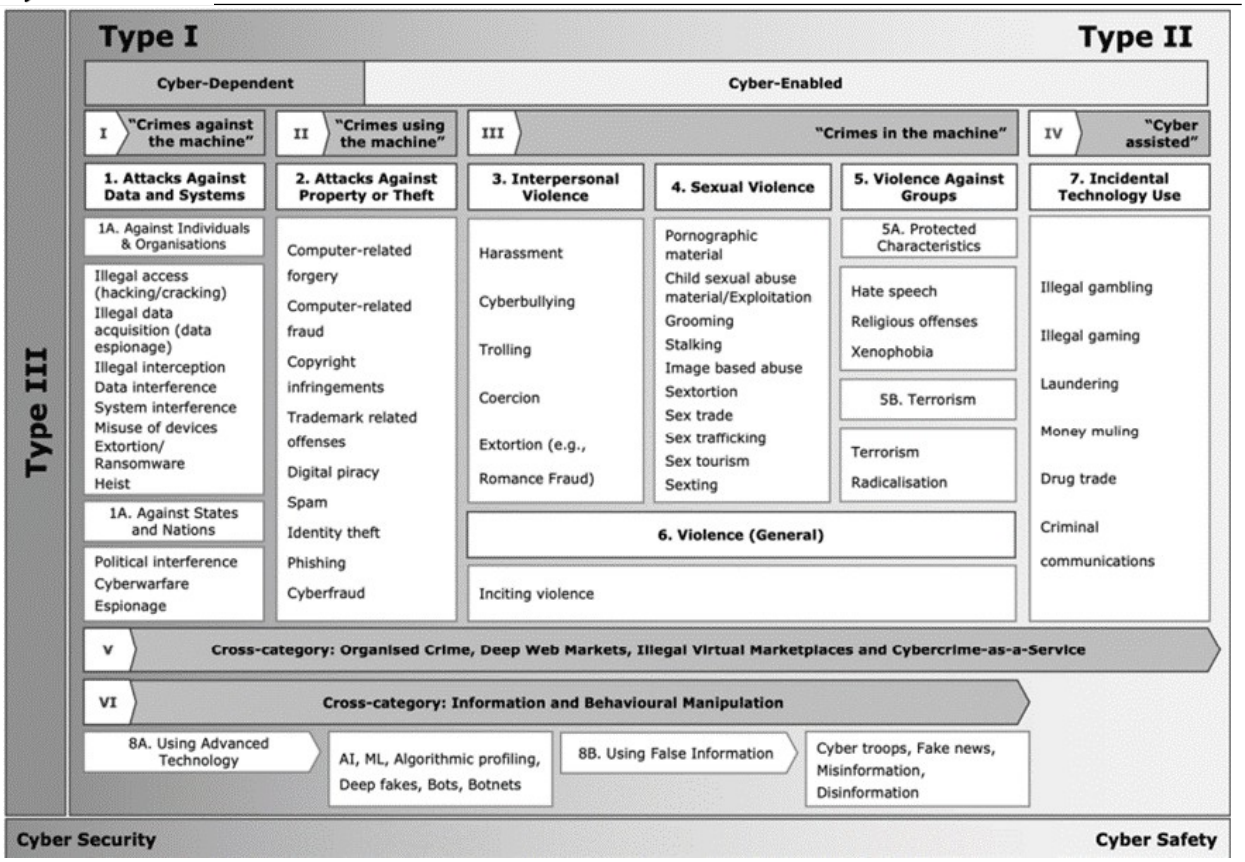
> The United States is experiencing a transformation in how criminals are using technology to invent new types of crime, and are creating new methods for committing traditional crimes. These developments are fundamental in nature. People who never committed crimes before are tempted when they learn how easy it can be to deal drugs or steal thousands of dollars, without ever having to confront a victim face-to-face. Criminal gangs that used to specialize in selling drugs on the street corner, or holding up pedestrians for the cash in their wallets, are switching to crimes they can commit in the privacy of their homes, by clicking keys on a keyboard.(*NEW NATIONAL COMMITMENT REQUIRED: The Changing Nature of Crime and Criminal Investigations*, 2018)

Understanding Cybercrime

The information technology revolution has been both a boon and a bane for humanity. Cybercrimes are the negative results of this revolution. These crimes have been identified as e-crimes, high-tech crimes, and white-collar crimes. Thomas and Loader (2000) define cybercrime as "computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks." (p. 3) Also, "Cybercrime refers to any type of illegal activity that takes place on cyberspace, involves a network, and results in pecuniary loss." (Jahankhani et al. (2014). Debrati Halder and K. Jaishankar (2016) define cybercrimes as "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/ MMS)." Organizations like the Commission of European Communities (2007, p. 2) define cybercrime as "criminal acts committed using electronic communications networks and information systems or against such networks and systems." In other words, cybercrime is a crime that is committed or carried out using a computer, network, or any other digital device.

It may be pointed out here that there is no agreed-upon and unified definition of 'cybercrime'. However, a clear definition is imperative because "even small variations in the conceptualization of cybercrime could affect the measurement of, and response to, cybercrime behaviors." (Phillips et al., 2022). Barn and Barn (2016) have argued that one of the reasons why the prevention of cybercrimes becomes difficult is because of the unaccounted range of cybercrimes. Consequently, "cybercrime legislation across jurisdictions is neither systematic nor uniform; moreover, the legislation itself is often dispersed across various criminal and civil statutes, which in turn results in fragmented international efforts to tackle cybercrime…" (Phillips et al., 2022). The ever-evolving range of cybercrimes can be understood from the amount of academic research on the classification of cybercrimes. Various approaches like the categorical approach, continuum approach, the Wall (2007) three-category classification system, etc. have been used to comprehend the various categories of cybercrimes. One such comprehensive classification has been done by Phillips et al (2022) in the following table

It may be pointed out here that an exhaustive classification of cybercrimes is essential as "difficulty in classifying cybercrimes hinders the introduction of cybercrime-specific laws and regulations, which leads to significant challenges in policing and prosecuting cybercrime due to the limited understanding and capacity to respond." (Phillips et al, 2022, 391). Such a classification will help develop an effective legal and policy response toward preventing cybercrimes.



Source: Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. Forensic Sciences, 2(2), 390. https://doi.org/10.3390/forensicsci2020028

India's new criminal laws and cybercrimes

On 21 May 2021, it was reported that Air India was subjected to a cyber-attack. Personal details of around 4.5 million customers around the world were compromised. In another incident, in 2014, India's critical infrastructure was under cyberattack by a group called Operation Crouching Yeti. The group "specifically targeted key sectors vital for the country's functioning, including power, telecommunications, and transportation." (STL Digital, 2023). Like any other country, the Indian economy is increasingly becoming vulnerable to cybercrimes. Therefore, it has developed a cyber security framework to tackle the menace of cybercrimes. "While India does not have an exclusive, unitary cybersecurity law, it uses the IT Act and multiple other sector-specific regulations to promote cybersecurity standards." (Chin, 2023).The Information Technology (IT) Act of 2000 is the primary legislation dealing with cybersecurity, data protection, and cybercrime. Its key features are:

- "Granting statutory recognition and protection to electronic transactions and communications;
- Aiming to safeguard electronic data, information, and records;
- Aiming to prevent unauthorised or unlawful use of computer systems; and
- Identifying activities such as hacking, denial-of-service attacks, phishing, malware attacks, identity fraud, and electronic theft as punishable offenses." *(A Comparison of Cybersecurity Regulations: India, n.d.)*

The Indian cyber security framework can be understood by studying the Information & Technology Act, 2000 (along with its Amendments) and the provisions relating to cybercrimes in Bhartiya Nyaya Sanhita (BNS). In fact, BNS has referenced the Information Technology Act, 2000, and BNSS for definitions of technological terms that are not expressly defined but used in BNS. Like the old criminal laws of India, Bhartiya Nyaya Sanhita does not define the term 'cybercrime'. This broader scope in recognising criminal activity across various electronic platforms will enhance the detection and deterrence of cybercrimes.

Provisions relating to various cybercrimes are as follows:

(1) Cyber Defamation: When defamation occurs in cyberspace, it may be punished under Section 356 of BNS along with Sub section 4 and 66 of the IT Act. Thus, the perpetrator may get a punishment of imprisonment which may extend up to three years, or may be fined for up to five lakh rupees, or both. (IT Act, 2000). Under BNS, 'community service' has been added as an alternate punishment.

(2) Forgery: There are several ways to commit forgery using digital means. Falsification of documents, phishing, digital forgery, or identity theft will be punished under Section 335, 336-338 of the BNS along with the provisions of the IT Act. Earlier, under IPC, the punishments for these crimes

were scattered under various sections like Section 463, Section 464, and Sections 465-469. The IT Act provides up to three years of punishment or Rs one lakh as a fine.

A special section has been provided in the BNS for forging documents or electronic records and using them as genuine ones. Sections 340 (1) & (2) of the BNS will be applied against the person along with Section 66 D of the IT Act.

(3) Cyber stalking: Punishment under cyber stalking will be given under Sections 78 & 79 of the BNS. Section 79 pertains to situations where the modesty of a woman is outraged. The person may be imprisoned for up to three years. He shall also be liable to a fine. No specific mention has been made in the IT Act concerning the cyber stalking.

(4) Cyber pornography: Sections 294-296 of the BNS discuss the punishments for cyber pornography wherein obscenity is displayed through songs, acts, or the sale of obscene books/ objects using digital forums. "Definitions such as the meaning of 'obscene material' under Section 294 of BNS have been expressly extended to include content shared electronically, such as revenge porn or violent videos." (*Stringent Measures against Cybercrimes in India's New Criminal Justice System - JSA*, 2024) The person shall be liable to pay a fine and also will be imprisoned. Along with that, the IT Act specifies imprisonment of up to three/ five years and a fine of five/ ten lakhs for cyber pornography under Sections 67, 67 A & 67 B.

(5) Cheating: The illegal act of cheating has been dealt with in Section 318 of the BNS. The upper limit of imprisonment is increased from one year to three years. The act of cheating by personation is punishable under Section 319. The upper limit of imprisonment is increased from three years to five years. The cybercrime of cheating will also be dealt with under Section 66 D of the IT Act.

(6) Financial/ cyber frauds: For economic offenses, the BNS has increased imprisonment from three years to five years under Section 318. Section 111 (1) (iii) of the BNS defines economic offenses broadly to include crimes such as criminal breach of trust, forgery, counterfeiting, 'hawala transactions', mass-marketing fraud, and schemes to defraud individuals or institutions for monetary gain. This comprehensive definition suggests the legislature's intent to cover sophisticated economic crimes. When such an offense is categorized as 'Organized crime', it results in stricter penalties under Section 111 compared to other sections. (Nathani & Bhalla, 2024). The new law aims to deter cyber criminals from acting in groups or on behalf of syndicates. This aspect of crimes being committed in groups was missing under the IPC. Under the IT Act, 2000, economic offenses will be punished under Sections 43, 65, and 66, wherein the criminal will be imprisoned for up to three years, may be fined up to five lakhs, or both.

(7) Cyber terrorism: Section 113 of the BNS is a new provision. It clearly defines what constitutes a 'terrorist' act. Any person indulging in terrorist activities, as defined under Section 113, may be punished with life imprisonment. Section 66 F of the IT Act also specifies the punishment for terrorist activities as life imprisonment.

Ministries and the Agencies involved in ensuring the cyber security of India

Cybersecurity in India involves a complex, inter-ministerial, and inter-departmental framework, with multiple ministries, departments, and agencies playing vital roles in managing key functions due to its cross-cutting nature.There are five ministries involved in preventing internal cybercrimes in India. These are:

(a)Ministry of Information and Broadcasting: The **Electronic Media Monitoring Centre** (EMMC) is the agency that is operating under the directions of the Ministry of Information and Broadcasting. "EMMC is the premier set-up with advanced technologies to monitor, record, and analyze broadcast content." (*Media Units | Ministry of Information and Broadcasting | Government of India*, n.d.). It is thus, involved in media surveillance.

(b)Ministry of Home Affairs: Several agencies are functioning under the ministry that are involved in ensuring the country's cyber security.

· **National Intelligence Grid (NATGRID)** has been conceived to develop cutting-edge technology to enhance India's counter-terror capabilities. "It is responsible for keeping citizen data in a single database which can be accessed and utilized by officers of RWA, CBI, IB, etc." (Pai, 2016)

· **The Indian Cybercrime Coordination Centre (I4C)** "was established by MHA, in New Delhi to provide a framework and eco-system for Law Enforcement Agencies (LEAs) for dealing with Cybercrime in a coordinated and comprehensive manner." (*Indian Cybercrime Coordination Centre*, 2024)

· **The National Crime Records Bureau (NCRB)** collects and analyzes crime data in India. It also acts as a central repository for this information to assist investigators in tracking crimes and criminals.

· Along with the agencies mentioned above, the prime investigative agencies like the IB (Intelligence Bureau), CBI (Central Bureau of Investigation), and NCB (Narcotics Control Bureau) are also involved in preventing cyber-crimes in certain capacities.

(c)Ministry of Communication & Information Technology: The **CERT-In** (Computer Emergency Response Team) has been set up according to Section 70 B of the IT Act (2000). It has been operational since 2004. It "functions as the trusted referral agency for cyber users in India for responding to cyber security incidents and will assist cyber users in the country in implementing measures to reduce the risk of cyber security incidents." (Ministry of Communication & Information Technology, 2014).

(d) The Ministry of Electronics & Information Technology (MEITY) was carved out of the Ministry of Communication & Information Technology in July 2016. It has divisions that are involved in cyber security like the Cyber Law & Data Governance Division and the Cyber Security R& D Division.

(e)Ministry of Finance: The **Central Economic Intelligence Bureau(CEIB)** is a division operating under the Ministry of Finance. It is the central nodal agency "mandated to gather intelligence/ information on economic offenses and maintain a database of the same for sharing with law enforcement agencies concerned." (*NABARD - National Bank for Agriculture and Rural Development*, 2020).

Apart from the ministries mentioned above, the

Prime Minister's Office is also involved in tackling the problem of cybercrime.

(f)PMO:

· The National Security Council Secretariat (NSCS) has a body called the **National Cyber Security Coordinator (NCSC).** "The NCSC is responsible for streamlining intelligence gathering of other agencies, screening communication metadata, and other activities. It coordinates with different central-level agencies on cybersecurity issues of national importance."(Goswami & Ross, 2023).

· **The Cabinet Committee on Security (CCS)** is the high-level body that oversees decisions such as establishing new organizations or responding to attacks. On the other hand, the **Research and Analysis Wing (RAW)** handles international intelligence collection.

Agencies responsible for external cyber security in India

(a) The Defence Intelligence Agency (DIA) operates under the direct supervision of the Ministry of Defence (MOD). The MOD also oversees the **Defence Research and Development Organization (DRDO)** and the **Institute of Defence Studies and Analyses.** These institutions concentrate on enhancing the nation's offensive and defensive capabilities internationally.

(b) "The Global Cyber Issues Cell operates under the direct control of the Ministry of External Affairs (MEA). This cell tracks the international processes that affect national policymaking." (Pai, 2016).

A Critique of India's Cyber Security Framework

(1) Addressing the problem of multiplicity of agencies: The presence of numerous regulators and overlapping regulations in the same area should be minimized. Multiple compliance requirements, audits, forums, and information-sharing channels consume significant time for organizations handling critical information infrastructure (CII). This often diverts attention from protection efforts to meeting compliance and sharing information.

(2) Balancing act between the need for regulations and the right to privacy: Like all democratic governments, the Indian government is also faced with the challenge of ensuring "that there are appropriate regulations in place that allow them to deal with cybercrime without infringing on online freedoms or providing opportunities for security services to spy on their citizens. Maintaining a balance between protecting citizens from cybercrime and maintaining their Internet freedoms is indisputably difficult and is further complicated by the fact that technology tends to be years ahead of policy." (Turiansky, 2020). The Data Personal Data Protection Act, 2023 is an attempt to achieve a fine balance in this direction. However, critics point out that unfettered discretions have been given to national security agencies to access the personal data of citizens.

(3) Keeping abreast of evolving cybercrimes: It is essential to revise the definitions and provisions in the IT Act to address emerging threats and evolving technologies.

CONCLUSION:

BNS intends to strengthen the legal system in order to ensure that cybercriminals who exploit technology are held accountable and do not evade prosecution because of their actions. The newly enacted criminal laws in India constitute a significant step forward in the process of upgrading the legal structure of the country in order to handle contemporary concerns such as cybercrime and the growing complexity of the digital age. The goal of these reforms is to improve the criminal justice system's accessibility, accountability, and transparency by changing laws that have become obsolete. Their effectiveness, on the other hand, will be contingent upon their being properly implemented, being strictly enforced, and being continuously adjusted to fit the ever-changing requirements of society.

REFERENCES:

1. K.S., A. K. (2024). The Bhartiya Nyaya (Second) Sanhita 2023: An integrated Perspective — A Comprehensive Study and Analysis. *Jus Corpus Law Journal*, 350.

2. As new criminal laws come into effect, here's what different legal luminaries think of their impact on legal system. ANI. (2024, July 1). https://aninews.in/news/national/general-news/as-new-criminal-laws-come-into-effect-heres-what-different-legal-luminaries-think-of-their-impact-on-legal-system20240701071616/

3. Tondak, R., NCRB Report Crime in India 2023: Posted by Crime in Delhi (2024). Crime in Delhi. Retrieved September 3, 2024, from https://crimeindelhi.com/ncrb-report-crime-in-india-2023-posted-by-crimeindelhi/.

4. Editorial: Crime Watch. (2021, September 20). *The Telegraph Online*. Retrieved September 5, 2024, from https://www.telegraphindia.com/opinion/changing-nature-of-crime-in-india/cid/1831399

5. NEW NATIONAL COMMITMENT REQUIRED: The Changing Nature of Crime and Criminal Investigations. (2018). Police Executive Research Forum. https://www.policeforum.org/assets/ChangingNatureofCrime.pdf

6. Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. *Forensic Sciences*, *2*(2), 379–398. https://doi.org/10.3390/forensicsci2020028.

7. Barn, R., & Barn, B. (2016, June). An ontological representation of a taxonomy for cybercrime. In *24th European Conference on Information Systems (ECIS 2016)*.

8. Jahankhani, H., Al-Nemrat, A., & Hosseinian-Far, A. (2014). Cybercrime classification and characteristics. In *Elsevier eBooks* (pp. 149–164). https://doi.org/10.1016/b978-0-12-800743-3.00012-8.

9. Halder, D., & Jaishankar, K. (2016). *Cyber Crimes Against Women in India*. Sage Publications Pvt. Limited. http://books.google.ie/books?id=PQdJzQEACAAJ&dq=Cyber+Crimes+against+Women+in+India&hl=&cd=3&source=gbs_api

10. Commission of the European Communities. (2007). Communication from the Commission to the European Parliament, the Council and the Committee of the Regions Towards a general policy on the fight against Cybercrime.

11. Thomas, D., & Loader, B. (Eds.). (2000). *Cybercrime: Law enforcement, security and surveillance in the information age*. Psychology Press.

12. STL Digital. (2023, November 23). 10 Biggest Cybersecurity Attacks in Indian History. *STL Digital*. September 8, 2024, https://www.stldigital.tech/blog/10-biggest-cybersecurity-attacks-in-indian-history/.

13. A comparison of cybersecurity regulations: India. (n.d.). PwC. https://www.pwc.com/id/en/pwc-publications/services-publications/legal-publications/a-comparison-of-cybersecurity-regulations/india.html.

14. See https://www.indiacode.nic.in/show-data?actid=AC_CEN_45_76_00001_200021_1517807324077&orderno=76

15. Nathani, S., & Bhalla, M. (2024, July 11). BNS – Speedy Justice or Colonial Rollover? *Economic Laws Practice*. September 9, 2024, https://elplaw.in/leadership/bns-speedy-justice-or-colonial-rollover/.

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

17. Chin, K. (2023, March 2). Top Cybersecurity Regulations in India [updated 2023] *UpGuard,*https://www.upguard.com/blog/cybersecurity-regulations-india

18. Media Units | Ministry of Information and Broadcasting | Government of India. (n.d.). https://mib.gov.in/media-units

19. Pai, V. (2016, April 15). *An overview of India's cyber security agencies*. MEDIANAMA. https://www.medianama.com/2016/04/223-indias-cyber-security-agencies/.

20. Indian Cybercrime Coordination Centre. (2024, June). Ministry of Home Affairs. Retrieved September 9, 2024, from https://i4c.mha.gov.in/.

21. Ministry of Communication & Information Technology. (2014, January 16). *Ministry of Electronics and Information Technology, Government of India | Home Page*. Www.meity.gov.in. https://www.meity.gov.in/writereaddata/files/G_S_R%2020%20%28E%292_0.pdf.

22. NABARD - National Bank For Agriculture And Rural Development. (2020). Nabard.org. https://www.nabard.org/CircularPage.aspx?cid=504&id=5154#:~:text=Central%20Economic%20Intelligence%20Bureau%20(CEIB)%20is%20the%20central%20nodal%20agency

23. Goswami, S., & Ross, R. (2023, July 3). *Lt. Gen. NairAappointed National Cybersecurity Coordinator*. Bank Information Security. https://www.bankinfosecurity.asia/lt-gen-nair-appointed-national-cybersecurity-coordinator-a-22425.

24. Pai, V. (2016, April 15). *An overview of India's cyber security agencies*. MEDIANAMA. https://www.medianama.com/2016/04/223-indias-cyber-security-agencies/.

25. Naik, Y. (2024b). The Bharatiya Nyaya Sanhita (BNS): A critical examination of India's new penal code. *SSRN Electronic Journal*, 1–5. https://doi.org/10.2139/ssrn. 4884622.

26. Turiansky, Y. (2020, January). *Africa and Europe: Cyber Governance Lessons*. Jstor. https://www.mpi.lu/fileadmin/_migrated/content_uploads/GUIDE_jstor_01.pdf.