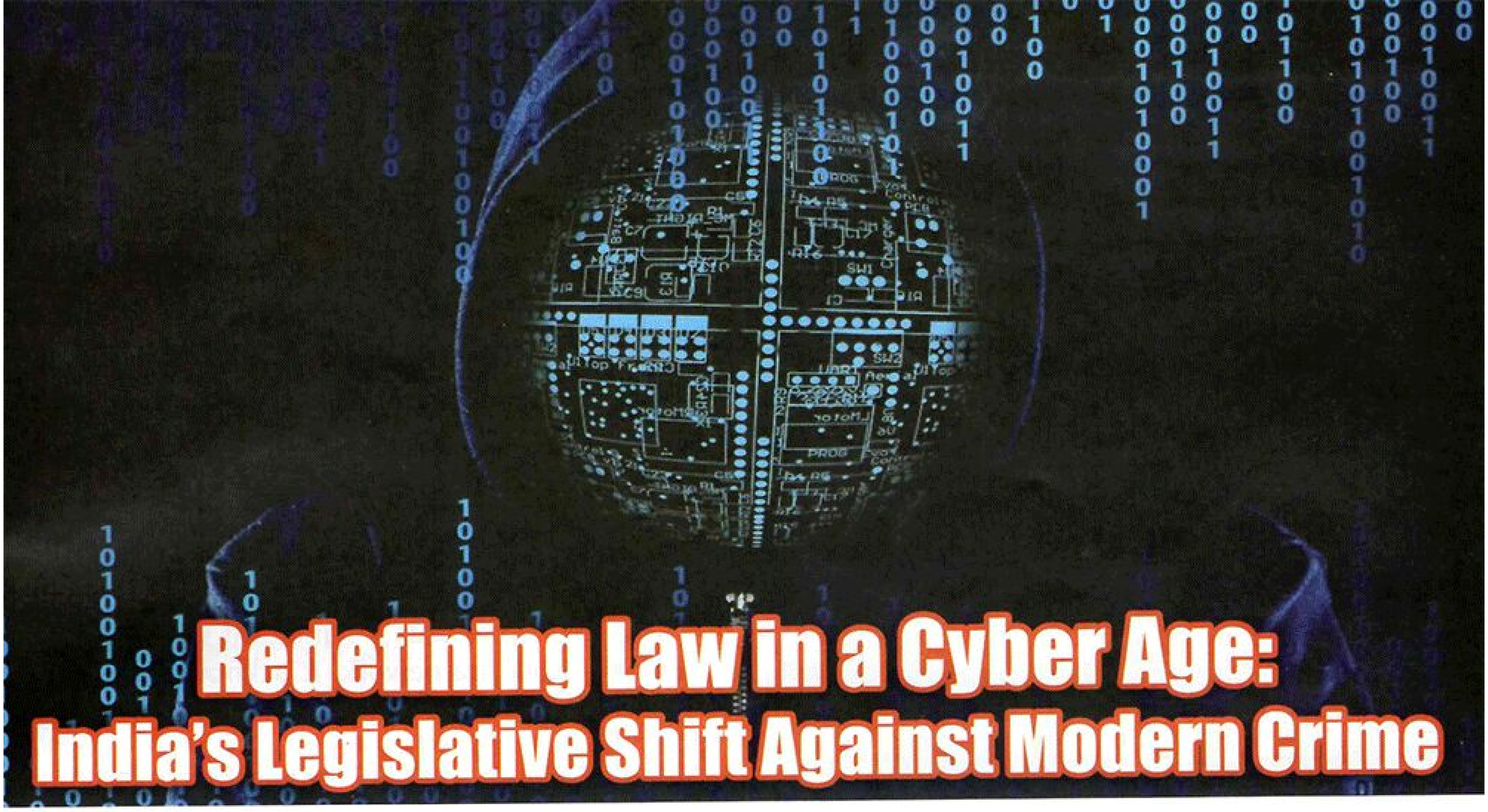


# Redefining Law in a Cyber Age: India's Legislative Shift Against Modern Crime

**PAATHIK MUNI**

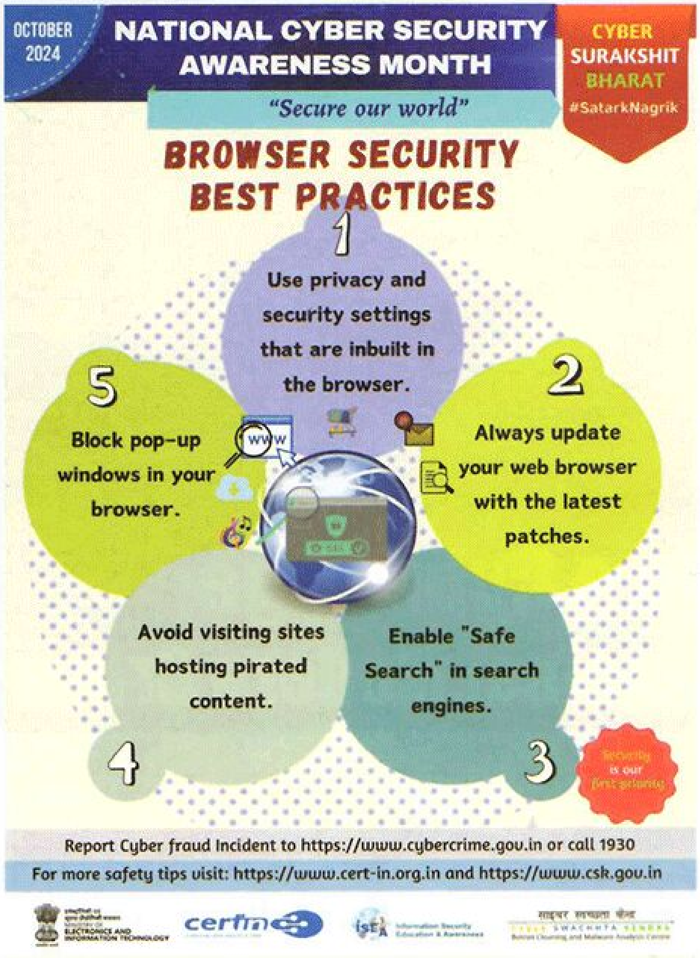
The author is a practicing Cyber Lawyer with over two decades of experience in cybersecurity and data protection.
Email: paathik.muni@gmail.com

**The *Bharatiya Nyaya Sanhita* (BNS) represents a significant shift in India's criminal justice framework. It acknowledges that cybercrime requires a more nuanced approach than traditional crimes. The boundaries of crime have changed. Cybercriminals can operate from any corner of the globe, and law enforcement can no longer rely solely on physical jurisdiction. The BNS is designed to handle such complexity by streamlining investigative processes and ensuring that law enforcement has the authority to pursue criminals across multiple jurisdictions within India. The *Bharatiya Nagrik Suraksha Sanhita* (BNSS) focuses on improving the security of Indian citizens in the digital age by empowering law enforcement agencies to respond more effectively to digital threats.**

As the digital world integrates seamlessly with our daily lives, a new breed of crime has emerged, forcing India's criminal justice system to adapt. In the past, notorious criminals exploited weaknesses in the nation's law enforcement systems, but their operations were constrained by physical borders. Today, crime has evolved—there are no longer territorial boundaries to limit criminals. Instead, we find ourselves grappling with cybercriminals who operate invisibly, manipulating global networks from any corner of the world.

These cybercriminals exploit vulnerabilities in our digital infrastructure, breaching security walls and accessing sensitive data with ease. In response to these modern challenges, the Government of India has introduced three new criminal laws—

- *Bharatiya Nyaya Sanhita* (BNS),
- The *Bharatiya Nagrik Suraksha Sanhita* (BNSS), and
- The *Bharatiya Sakshya Adhiniyam* (BSA).


OCTOBER 2024

NATIONAL CYBER SECURITY AWARENESS MONTH

"Secure our world"

CYBER SURAKSHIT BHARAT #SatarkNagrik

BROWSER SECURITY BEST PRACTICES

1 Use privacy and security settings that are inbuilt in the browser.

2 Always update your web browser with the latest patches.

3 Enable "Safe Search" in search engines.

4 Avoid visiting sites hosting pirated content.

5 Block pop-up windows in your browser.

Security is our first priority

Report Cyber fraud Incident to https://www.cybercrime.gov.in or call 1930

For more safety tips visit: https://www.cert-in.org.in and https://www.csk.gov.in

These laws aim to address the complexities of modern crime and close the gaps that digital criminals exploit, positioning India's criminal justice system firmly in the 21st century.

In the past, crimes like dacoity were common in India's cities and villages. A group of criminals would break into a home or business, steal goods, and flee. In such a case, the local police would arrive on the scene, gather physical evidence, and interrogate witnesses. The physical nature of the crime left clear evidence—fingerprints, footprints, and witnesses who could testify in court. The crime was confined to a specific location, and the police had a straightforward process to follow.

Now imagine that same dacoity taking place in the digital world. Instead of physically entering a building, cybercriminals breach a company's digital security system. They access confidential financial information or personal data and transfer it to their own accounts in seconds. In this scenario, there is:

- No physical crime scene,
- No witnesses, and
- No clear jurisdiction.

The evidence is digital—scattered across servers and often hidden behind encrypted firewalls. This shift from physical to digital crime illustrates the need for a new legal framework.

The *Bharatiya Nyaya Sanhita* (BNS), *Bharatiya Nagrik Suraksha Sanhita* (BNSS), and *Bharatiya Sakshya Adhiniyam* (BSA) provide:

- The foundation for tackling these new types of crimes

  Addressing the challenges of jurisdiction

- Evidence collection and
- Prosecution in the digital realm.

The BNS represents a significant shift in India's criminal justice framework. It acknowledges that cybercrime requires a more nuanced approach than traditional crimes.

The boundaries of crime have changed. Cybercriminals can operate from any corner of the globe, and law enforcement can no longer rely solely on physical jurisdiction. In physical crimes like bank robberies, jurisdiction is clear—The local police handle the investigation. However, in cybercrimes, the victim might be in one state, the bank's servers in another country, and the criminal operating from another state of India. The BNS is designed to handle such complexity by streamlining investigative processes and ensuring that law enforcement has the authority to pursue criminals across multiple jurisdictions within India.

The *Bharatiya Nagrik Suraksha Sanhita* (BNSS) focuses on improving the security of Indian citizens in the digital age. With cybercrime increasing in scale and sophistication, the BNSS empowers law enforcement agencies to respond more effectively to digital threats.

Section 176(3) of the BNSS mandates that forensic audits be conducted in cases where the punishment exceeds seven years, particularly in cybercrimes that involve significant financial fraud, data theft, or digital sabotage.

In the digital world, gathering evidence is not as straightforward as it is in physical crime. A cybercrime investigation often involves analysing vast amounts of data, tracing encrypted communication, and tracking digital footprints across multiple platforms. The BNSS ensures that law enforcement agencies are equipped to handle such challenges, providing a framework for forensic technology and digital investigation techniques.

For instance, in cases of cyber fraud, the forensic team might need to analyse the transactional data, review server logs, or track IP addresses across several countries to identify the perpetrators. The BNSS allows law enforcement to work seamlessly across regions within India, ensuring that digital criminals do not escape prosecution due to jurisdictional issues.

The BSA revolutionises how evidence is collected, stored, and presented in court, particularly in cases involving cybercrime. Digital evidence is intangible. That means it can be easily deleted, altered, or concealed.

The BSA introduces stringent protocols for preserving digital evidence, ensuring its integrity throughout the legal process. Digital forensics play a crucial role in cybercrime investigations. In cases involving hacking, identity theft, or online scams, the evidence might include email records, digital signatures, transaction histories, or social media activity. The BSA sets out clear guidelines for collecting this evidence in a manner that makes it admissible in court, ensuring that justice is not delayed or denied due to procedural issues.

One example is in the prosecution of online identity theft. In such cases, the evidence could include IP logs, financial transaction histories, or intercepted communications between the criminal and their victim. The BSA ensures that law enforcement follows a rigorous process to authenticate and present this digital evidence, giving the prosecution a stronger case.

QUICK TIP

*"Secure our world"*

15TH OCTOBER 2024

NATIONAL CYBER SECURITY AWARENESS MONTH

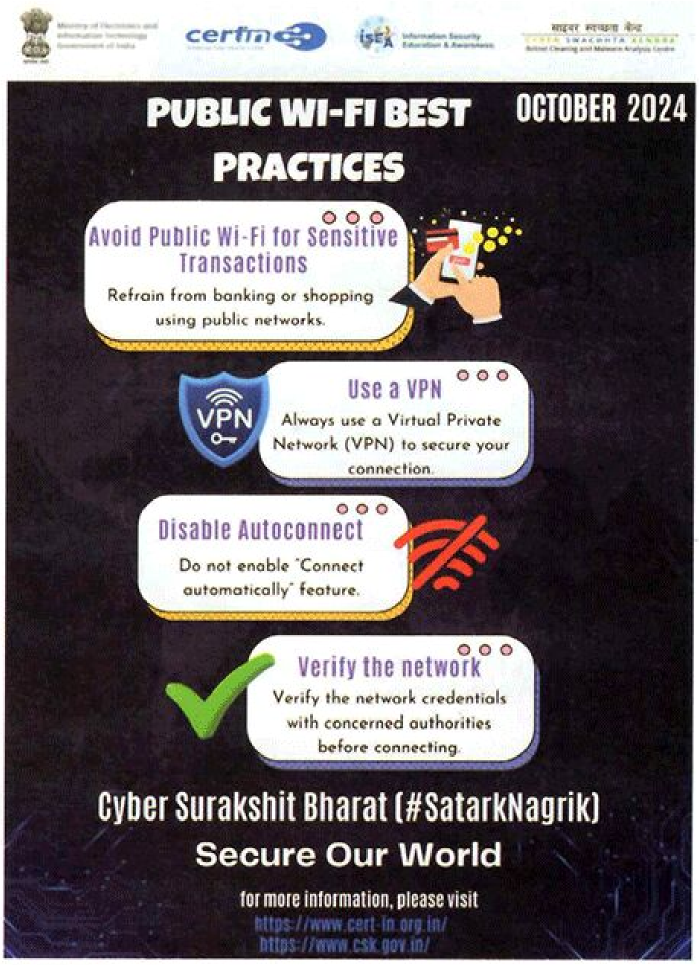
Avoid clicking on shortened URLs without verifying them by expanding the URL.

Cyber Surakshit Bharat #SatarkNagrik

Report Cyber security incidents to incident@cert-in.org.in

Report Cyber frauds/crimes to https://www.cybercrime.gov.in or call 1930

For more safety tips visit: https://www.cert-in.org.in and https://www.csk.gov.in



PUBLIC WI-FI BEST PRACTICES

OCTOBER 2024

Avoid Public Wi-Fi for Sensitive Transactions

Refrain from banking or shopping using public networks.

Use a VPN

Always use a Virtual Private Network (VPN) to secure your connection.

Disable Autoconnect

Do not enable "Connect automatically" feature.

Verify the network

Verify the network credentials with concerned authorities before connecting.

Cyber Surakshit Bharat (#SatarkNagrik)

Secure Our World

for more information, please visit

https://www.cert-in.org.in/

https://www.csk.gov.in/

India is no stranger to cybercrime. As one of the fastest-growing digital economies in the world, India has witnessed a dramatic rise in online fraud, data breaches, and cyber espionage.

According to reports, India ranks among the top countries in terms of cyber attacks, with industries such as (1) banking, (2) healthcare, and (3) government being the most vulnerable. The Government of India has recognised this growing threat and has prioritised cybersecurity in its policy agenda. However, the sheer volume of cybercrime cases poses a significant challenge for law enforcement. Many police officers, particularly in smaller towns and rural areas, are not trained to handle complex cybercrime cases. They lack the tools and expertise needed to investigate and prosecute digital crimes effectively.

OCTOBER 2024

NATIONAL CYBER SECURITY AWARENESS MONTH

"Secure our world"

CYBER SURAKSHIT BHARAT #SatarkNagrik

PUBLIC WIFI BEST PRACTICES

1 Always verify the name of the network and login procedures with the concerned staff.

2 Disable Auto-connect to Public WiFi networks.

3 Use an updated antivirus tool in your device.

4 Avoid doing financial and other sensitive transactions using Public Wi-Fi.

5 Switch off Wi-Fi service when not in use.

Report Cyber fraud Incident to https://www.cybercrime.gov.in or call 1930

For more safety tips visit: https://www.cert-in.org.in and https://www.csk.gov.in

This is where the new criminal laws come into play. By modernising the legal framework, the BNS, BNSS, and BSA aim to equip law enforcement with the tools and knowledge they need to tackle cybercrime head-on. Whether it's financial fraud, ransomware attacks, or identity theft, these laws provide a comprehensive approach to addressing the challenges of the digital world.

Digital forensics has emerged as a cornerstone of modern criminal investigations. Just as physical evidence such as fingerprints, footprints, or DNA was crucial in traditional crimes, digital evidence is vital in cybercrimes. However, the collection and analysis of digital evidence is far more complex and requires specialised expertise.

In a physical dacoity, for instance, police officers might collect fingerprints, photograph the crime scene, and interview witnesses.

In contrast, a cybercrime investigation requires analysing encrypted data, tracking digital transactions, and tracking IP addresses.

Digital forensics experts are tasked with uncovering hidden data, retrieving deleted files, and piecing together a digital timeline of the crime.

The BNS and BNSS recognise the importance of digital forensics and include provisions that mandate its use in investigating serious crimes. By incorporating digital forensics into the legal process, these laws ensure that cybercriminals cannot simply delete their tracks and escape prosecution. The BSA also reinforces the role of digital evidence by setting strict guidelines for its preservation and presentation in court.

The BNS, BNSS, and BSA represent a bold step forward in securing India's digital future. By addressing the unique challenges posed by cybercrime, these laws create a framework that positions India to effectively counter the rising threats in the digital space. However, the passage of these laws is just the beginning. For these acts to be truly effective, they need to be supported by a robust law enforcement infrastructure.

This means:

- investing in digital forensic laboratories.
- providing police officers with the tools and training necessary to investigate cybercrimes and
- ensuring that courts are equipped to handle complex digital evidence.
- it also involves updating law enforcement protocols to reflect the realities of the digital world, where crimes happen quickly and evidence can be erased in moments.

India already has specialised cybercrime units in several states, tasked with investigating digital crimes. However, as cybercrime continues to grow in both scale and complexity, there is an urgent need to enhance the capabilities of these units. The introduction of the BNS, the BNSS, and the BSA recognises this need, providing a legislative framework that supports the expansion and modernisation of these units.

The new laws focus on empowering law enforcement to respond more effectively to cybercrime, which means increasing investment in cybercrime units to ensure they have access to the latest tools and methodologies. The collaboration between these units and digital forensic experts will be critical to investigating complex cybercrimes, identifying perpetrators, and building strong cases that lead to successful prosecutions.

The new criminal laws represent a forward-thinking approach to digital security, but they must be seen as part of a larger strategy for adapting to the challenges of the digital age. As technologies like artificial intelligence, blockchain, and quantum computing emerge, new forms of cybercrime will also arise. The Indian legal system must remain agile, updating its frameworks to address these emerging threats.

One key aspect of future-proofing India's legal system is continuing to invest in digital infrastructure and human capital. The law enforcement officers of tomorrow will need a blend of

(1) legal, (2) technological, and (3) forensic skills to keep pace with criminals who are constantly evolving their methods. Moreover, future amendments to the BNS, BNSS, and BSA may be necessary to ensure that India's laws can address crimes related to emerging technologies.

The enactment of the BNS, the BNSS, and the BSA marks a turning point in India's approach to law enforcement.

These laws are a direct response to the growing threat of cybercrime and the need to modernise the country's legal framework to deal with crimes that take place in the digital realm. By focusing on strengthening existing cybercrime units, enhancing digital forensic capabilities, and equipping law enforcement with the tools they need to handle digital threats, India is laying the groundwork for a safer digital future.

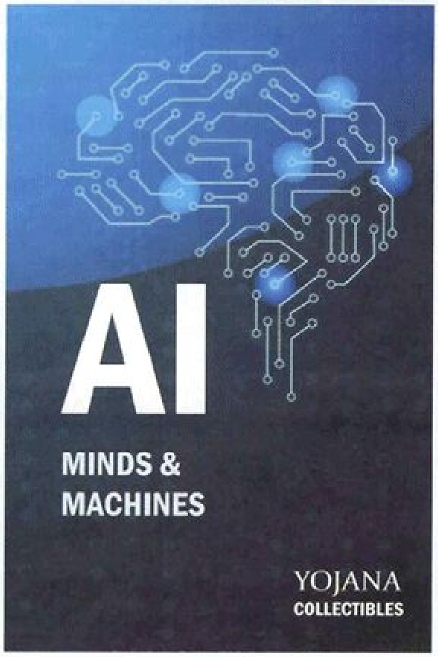
The implementation of these laws will be crucial in protecting India's digital infrastructure and ensuring that businesses, individuals, and institutions are safeguarded from the growing wave of cyber threats.

While the road ahead is challenging, the commitment to securing India's digital infrastructure through these laws represents a crucial step forward. With the right resources, continuous training, and updated legal frameworks, India can confront the challenges of cybercrime and ensure that justice prevails in both the physical and digital realms. ❑

## OUR BOOKS

# AI-Minds & Machines

**Yojana Collectibles**



**Language: English**
**Price: Rs 105**

From revolutionising education and healthcare to optimising finance and agriculture, Artificial Intelligence is rapidly reshaping our world. This book unveils the immense potential of AI, exploring its applications across various sectors. It also delves into the ethical considerations and challenges that come with this powerful technology.

The ongoing pursuit of knowledge and progress in science aligns with this book's exploration of AI's potential to revolutionise various fields. It injects a positive and optimistic outlook on the future of AI development and explores the challenges that lie ahead. Dive into the exciting world of AI and discover how it will transform our lives. ❑

Visit www.publicationsdivision.nic.in to surf through and buy from a wide range of publications highlighting subjects of national importance including India's rich cultural heritage, land and people, art and culture, flora and fauna, Gandhian literature, biographies and speeches, science, and children's literature.