2026 Volume: 02 Issue: 09 www.ijrpa.com ISSN 2456-9995 Research Article

International Journal Research Publication Analysis

Page: 01-17

ARTIFICIAL INTELLIGENCE AND CYBER CRIME IN INDIA: EMERGING THREATS, LEGAL CHALLENGES AND REGULATORY RESPONSES

***Sania Tawa**

India.

Article Received: 02 August 2026
Article Revised: 22 August 2026
Published on: 12 September 2026

***Corresponding Author: Sania Tawa**
India.

DOI: https://doi-doi.org/101555/ijrpa.3749

ABSTRACT

Artificial Intelligence (AI) has become one of the most transformative technologies of the digital age. Its influence touches healthcare, finance, education, governance, communication, business and cybersecurity, amongst other areas. Yet, the same technological capabilities that enable progress can also be misused for criminal purposes. Generative AI in particular has created new opportunities for phishing, identity theft, impersonation, social engineering, deepfake fraud, creation of malicious content and more.

India is particularly vulnerable to such developments due to its rapidly growing digital ecosystem, online financial services, social media platforms, digital identity systems and technology-enabled public services. AI-assisted cybercrime presents distinctive challenges because attacks can be automated, personalized, rapidly scaled and increasingly difficult to distinguish from legitimate human communication.

This paper examines the relationship between artificial intelligence and cybercrime in India and evaluates whether the existing legal and institutional framework is capable of responding to AI-enabled criminal activities. The study analyzes the Information Technology Act, 2000, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, the Digital Personal Data Protection Act, 2023, the Bharatiya Nyaya Sanhita, 2023 and the Bharatiya Sakshya Adhiniyam, 2023 for provisions pertaining to identity theft, cheating by personation, deepfakes, synthetic media, privacy violations, electronic evidence and intermediary responsibility.

The paper further analyzes the significant 2026 amendments and governmental measures pertaining to synthetically generated information, including AI-generated audio, visual and

audio-visual content. The research finds that although India's existing framework provides several legal mechanisms to address AI-enabled cybercrime, challenges remain regarding attribution, digital evidence, cross-border enforcement, technological detection, platform accountability and the rapidly changing nature of artificial intelligence.

The paper proposes a coordinated approach involving stronger digital forensics, specialized AI-cybercrime units, technological authentication mechanisms, public awareness, responsible platform governance, international cooperation and continuous development of technology-neutral legal standards.

1. INTRODUCTION

1.1 Background

The rapid development of Artificial Intelligence has fundamentally changed the digital environment. Artificial Intelligence refers broadly to computational systems capable of performing functions associated with human intelligence, including learning, reasoning, prediction, language processing, image recognition and content generation.

The emergence of generative AI presents a particularly important development. Modern AI systems can produce realistic text, images, audio, video and other digital content. These capabilities have significant legitimate applications, but they can also be exploited for criminal activities.

Cybercrime traditionally involves offences such as unauthorized access, hacking, data theft, phishing, identity theft, online fraud and distribution of malicious software. AI is changing the nature of several of these activities by making them more scalable, personalized and difficult to detect.

For example, an ordinary phishing attack may contain obvious grammatical mistakes and generic language, but AI can assist a criminal to create highly convincing and personalized communication. Similarly, voice-cloning technology can be misused to imitate a person's voice and deceive family members, employees or financial institutions.

The problem is therefore not that artificial intelligence is inherently criminal, but rather that AI functions as a force multiplier for both legitimate cybersecurity and malicious cyber activity.

1.2 AI as a Double-Edged Technology

Artificial Intelligence should be understood as a dual-use technology.

On the positive side, AI can assist cybersecurity professionals by:
detecting unusual network behaviour; identifying malicious patterns; analyzing large volumes of security data; detecting suspicious transactions; improving incident response; identifying fraudulent activity; and assisting digital forensic investigations.

On the negative side, criminals may use AI to:
create convincing phishing communications; imitate individuals; generate fake images and videos; conduct social engineering; automate fraud; create misleading websites; manipulate digital evidence; conduct large-scale online scams; and facilitate other cyber-enabled offences.

Thus, regulation should not attempt to eliminate AI merely because it can be misused, but rather to minimize harmful use while preserving legitimate technological innovation.

2. NATURE OF AI-ENABLED CYBER CRIME

2.1 AI-Assisted Phishing

Phishing involves deceptive communications that cause a person to disclose confidential information or perform an action beneficial to the offender.

AI can make phishing substantially more effective by helping generate:
personalised messages; convincing professional language; multilingual communications; fake customer-support conversations; realistic business emails; and deceptive online content.

CERT-In has recognized that AI language applications can be misused for phishing, scams, misinformation and fake websites.

The legal issue becomes more complicated when AI is merely a tool used by a criminal, with the underlying criminal liability generally attaching to the person who intentionally uses technology to commit the offence rather than to the AI system itself.

2.2 Deepfakes and Synthetic Media

Deepfakes are digitally manipulated or synthetically generated audio, images or videos designed to appear authentic.

They can be used for: impersonation; financial fraud; reputational attacks; misinformation; manipulation; non-consensual intimate imagery; blackmail; and social engineering.

India's regulatory framework was strengthened in February 2026 to address harms associated with synthetically generated information (SGI), including deepfakes and AI-generated content. The Government has stated that the amended framework requires appropriate technical measures, labelling and traceable metadata for permissible synthetic content and addresses unlawful content involving impersonation, children and other harms.

The 2026 MeitY FAQ explains that SGI under the amended IT Rules primarily covers artificially or algorithmically created, generated, modified or altered audio, visual or audio-visual information that appears real or authentic and may be indistinguishable from a real person or event.

2.3 AI-Enabled Identity Theft

Identity theft occurs when an offender fraudulently uses another person's identifying information or credentials.

AI can facilitate identity theft through: synthetic identities; facial imitation; voice cloning; fake social-media profiles; manipulated photographs; and impersonation.

Section 66C of the Information Technology Act, 2000 specifically addresses punishment for identity theft, while Section 66D addresses cheating by personation using a computer resource.

2.4 AI-Enabled Financial Fraud

AI can make financial fraud more convincing by combining:

personal information + synthetic communication + impersonation + automation.

For example, a criminal may impersonate a bank employee, government official, business executive or family member using synthetic voice or visual material.

The legal consequences may involve multiple provisions depending upon the conduct, including cheating, personation, identity theft, fraud and offences under the Information Technology Act.

2.5 AI-Generated Malicious Content

AI may also be misused to assist in producing malicious code or other harmful digital content.

The important question from a legal perspective is not just whether an AI system generated the content, but:

Who intentionally used the system, for what purpose, and what criminal act resulted?

This distinction is important because criminal liability generally involves analysis of the conduct, intention, knowledge and participation of human actors.

3. RESEARCH METHODOLOGY

A doctrinal, analytical and descriptive research methodology is adopted by the present study. The research primarily relies upon secondary legal materials and authoritative sources.

Primary sources include:

The Information Technology Act, 2000; Information Technology Rules, 2021; Digital Personal Data Protection Act, 2023; Digital Personal Data Protection Rules, 2025; Bharatiya Nyaya Sanhita, 2023; Bharatiya Sakshya Adhiniyam, 2023; judicial decisions of the Supreme Court of India; and government notifications and regulatory directions.

Secondary sources include:

Academic literature; Legal commentaries; Government reports; CERT-In publications; Ministry of Electronics and Information Technology publications; and credible research relating to AI and cybersecurity.

Research Objectives -

The research has the following objectives:

To examine the relationship between Artificial Intelligence and cybercrime in India.

To identify major forms of AI-enabled cybercrime.

To analyze India's existing legal framework applicable to AI-enabled cyber offences.

To examine the legal challenges associated with deepfakes and synthetic media.

To analyze issues relating to electronic evidence and digital forensics.

To identify gaps in the existing regulatory framework.

To propose legal and institutional measures for strengthening India's response to AI-enabled cybercrime.

Research Questions -

The research seeks to answer the following questions:

How is Artificial Intelligence changing the nature of cybercrime in India?

Are India's existing cyber laws adequate to address AI-enabled offences?

How should responsibility be determined when AI is used as a tool for committing a cyber offence?

What legal challenges are created by deepfakes and synthetic media?

What reforms are necessary to strengthen India's response to AI-enabled cybercrime?

Hypothesis -

India's existing cyber-law framework provides a substantial foundation for addressing AI-enabled cybercrime, but technological developments in generative AI, deepfakes and automated cyberattacks require continuous legal, institutional and technological adaptation.

4. LEGAL ANALYSIS

4.1 Information Technology Act, 2000

The Information Technology Act, 2000 governs cyber offences in India.

The Act contains provisions dealing with computer-related offences, identity theft, cheating by personation, privacy violations, cyber terrorism, obscene electronic content, preservation of information and intermediary-related obligations.

Section 66C – Identity Theft

Section 66C criminalizes fraudulent or dishonest use of another person's electronic signature, password or other unique identification feature.

This provision can become relevant to AI-enabled identity theft where technology is used to impersonate or unlawfully exploit another person's digital identity.

Section 66D – Cheating by Personation

Section 66D addresses cheating by personation through a communication device or computer resource.

This provision is particularly relevant to AI-generated impersonation.

For example, if a person uses AI-generated voice or video to falsely represent themselves as another person and thereby induce a victim to transfer money, the conduct may attract Section 66D along with other applicable offences.

Section 66E – Violation of Privacy

Section 66E addresses intentional or knowing capture, publication or transmission of images of a person's private area without consent in circumstances violating privacy.

The provision becomes particularly relevant to manipulated or synthetic intimate imagery, although the legal classification of a particular AI-generated image depends on the facts and other applicable provisions.

5. INFORMATION TECHNOLOGY RULES AND AI-GENERATED CONTENT

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 set out due-diligence obligations for intermediaries.

The 2026 amendments significantly strengthen the framework relating to synthetically generated information.

According to the Government, the February 2026 amendments address deepfakes and AI-generated content and require platforms to deploy reasonable technical measures against unlawful synthetic content. The framework also provides for clear labelling and traceable metadata for permissible synthetic content.

impersonation; misleading information; obscene content; harmful content involving children; non-consensual intimate imagery; and other unlawful content.

The 2026 framework is significant because it moves beyond simply punishing individual offenders and places greater emphasis on platform-level preventive measures.

The MeitY FAQ further clarifies that the amended definition of SGI focuses on audio, visual and audio-visual content and excludes certain good-faith editing and accessibility-related activities.

This distinction is important because regulation should not unintentionally criminalize legitimate creative, educational, artistic or accessibility-related uses of AI.

Artificial Intelligence frequently depends upon data. Consequently, data protection and AI regulation are closely connected.

The Digital Personal Data Protection Act, 2023 establishes a framework governing the processing of digital personal data and recognizes the interests of individuals in protecting their personal data.

The Act contains provisions concerning

grounds for processing personal data; notice; consent; certain legitimate uses; obligations of Data Fiduciaries; children's personal data; rights of Data Principals; correction and erasure; grievance redressal; and the Data Protection Board of India.

This is important in the AI context because misuse of personal photographs, voices, biometric-like information and other personal information can facilitate identity theft and synthetic impersonation.

Privacy as a Constitutional Concern

The Supreme Court's decision in Justice K.S. Puttaswamy (Retd.) v. Union of India recognized privacy as a constitutionally protected right and explained that restrictions on privacy must satisfy requirements including legality, legitimate state aim and proportionality.

Thus, AI regulation must balance:

privacy + security + innovation + freedom of expression.

7. BHARATIYA NYAYA SANHITA, 2023

The Bharatiya Nyaya Sanhita, 2023 is relevant because AI-enabled cybercrime does not necessarily fall exclusively under the Information Technology Act.

Depending upon the conduct, offences under general criminal law may also become applicable.

The BNS contains provisions concerning cheating, personation, false documents, electronic records and forgery.

Section 336 specifically recognizes false documents and false electronic records within the law of forgery. It also provides enhanced punishment where forgery is intended for cheating or harming reputation.

This is highly relevant to AI-generated documents, manipulated digital records and certain forms of synthetic impersonation.

Thus, AI-enabled cybercrime should be analyzed through a combined legal framework, rather than through the IT Act alone.

8. ELECTRONIC EVIDENCE AND DIGITAL FORENSICS

One of the most important challenges created by AI is determining whether digital evidence is genuine.

A deepfake can potentially make an innocent person appear to say or do something that never occurred.

Consequently, courts and investigating agencies must consider:

authenticity; source; metadata; chain of custody; device information; digital signatures; timestamps; forensic analysis; and expert evidence.

The Bharatiya Sakshya Adhiniyam, 2023 expressly recognizes electronic and digital records. Section 61 provides that an electronic or digital record cannot be denied admissibility merely because it is electronic or digital, subject to the statutory requirements. Section 63 addresses admissibility of electronic records.

The Supreme Court's decision in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal is particularly important in understanding electronic evidence and the evidentiary requirements applicable to computer-generated records.

In the age of generative AI, however, traditional electronic-evidence principles may increasingly have to be supplemented by sophisticated forensic techniques capable of detecting synthetic manipulation.

9. INTERMEDIARY LIABILITY AND PLATFORM RESPONSIBILITY

Social-media platforms and digital intermediaries play an important role in the distribution of AI-generated content.

The 2026 regulatory framework reflects a shift toward greater platform responsibility. Government material states that intermediaries are expected to deploy reasonable and appropriate technical measures to prevent unlawful synthetic information and to take action against unlawful content. This creates a policy question regarding how much responsibility should be placed on platforms for content generated by their users.

provide mechanisms for reporting harmful synthetic content; respond rapidly to unlawful content; implement appropriate detection mechanisms; preserve relevant evidence where legally required; educate users; provide transparency regarding AI-generated content; and protect legitimate expression and innovation.

At the same time, platforms should not be transformed into private courts responsible for making unrestricted determinations concerning every disputed piece of content.

10. CROSS-BORDER JURISDICTION

Cybercrime frequently crosses geographical boundaries.

An AI-enabled offence may involve:

Attacker → foreign jurisdiction

AI service → another jurisdiction

Platform server → another country

Victim → India

This creates significant problems regarding jurisdiction, investigation, preservation of evidence, obtaining data from foreign companies, extradition, mutual legal assistance and attribution.

The Bharatiya Nagarik Suraksha Sanhita, 2023 contains provisions addressing offences committed outside India and offences involving electronic communications.

Nevertheless, effective enforcement requires international cooperation because domestic legislation alone cannot resolve every cross-border technological problem.

11. MAJOR LEGAL AND PRACTICAL CHALLENGES

11.1 Attribution

The first challenge is identifying the human actor responsible for an AI-assisted offence.

AI may be used by:

an individual; an organized criminal group; a fraud network; an insider; a malicious developer; or multiple actors working together.

Determining who had knowledge and intent can therefore be difficult.

11.2 Rapid Technological Development

Technology often develops faster than legislation.

A law may be drafted to address one type of digital harm while new AI techniques create another.

Therefore, highly technology-specific legislation can quickly become outdated.

11.3 Deepfake Detection

Detection tools are not always perfect.

As synthetic media becomes more sophisticated, technical detection becomes an ongoing contest between generation technology and detection technology.

This makes legal reliance on automated detection alone problematic.

11.4 Lack of Public Awareness

Many cybercrime victims are not aware that AI can imitate:

voices; photographs; videos; writing styles; business communications; and identities.

Public awareness is therefore an important component of cybercrime prevention.

11.5 Digital Evidence

AI makes evidence verification difficult.

A video that appears authentic may not be authentic. Consequentially, investigators and courts increasingly require technical expertise.

11.6 Privacy Versus Security

Greater AI surveillance and detection capabilities may themselves create privacy concerns.

For example, using AI to monitor online behaviour can improve cybersecurity but may also involve significant processing of personal information.

Thus, security measures should satisfy constitutional and statutory privacy requirements.

11.7 Freedom of Expression

Not every synthetic image or video is harmful.

AI can be used for satire, education, cinema, art, accessibility, research and entertainment.

The 2026 MeitY framework itself recognizes exclusions for certain routine and good-faith uses.

Thus, regulation must distinguish between harmful deception and legitimate synthetic expression.

12. FINDINGS

Based on the doctrinal and analytical study, the following findings emerge.

Finding 1: AI is a force multiplier for cybercrime

Artificial Intelligence does not necessarily create entirely new crimes; in many cases, it increases the speed, scale, personalization and effectiveness of existing cyber offences.

Finding 2: Deepfakes represent a major emerging threat

Synthetic audio, images and videos can facilitate impersonation, fraud, misinformation and reputational harm.

Finding 3: India's existing laws provide substantial coverage

The Information Technology Act, BNS, DPDP framework and evidence legislation collectively provide multiple legal mechanisms applicable to AI-related offences.

Finding 4: The regulatory framework is evolving

India's 2026 amendments to the IT Rules demonstrate that the regulatory framework is adapting to the emergence of synthetically generated information.

Finding 5: Attribution remains a challenge

Identifying who should bear responsibility is one of the most challenging legal issues in cases involving multiple actors.

Finding 6: Digital forensic infrastructure is weak

Law-enforcement agencies require expertise in synthetic evidence.

Finding 7: Intermediary due diligence is crucial

Given the centrality of digital platforms in spreading synthetic material, intermediary due diligence should be a cornerstone of the regulatory response.

Finding 8: AI can enhance cybersecurity measures too

The response to AI-powered cybercrime should not be exclusive. AI itself may become a cybersecurity tool

13. SUGGESTIONS

13.1 Develop an integrated AI cybersecurity policy

India should formulate an integrated approach covering at least the intersection between:
Artificial Intelligence + Cybersecurity + Criminal Law + Data Protection + Digital Evidence.
An integrated policy should define roles and lines of responsibility more precisely.

13.2 Create specialised AI-cybercrime units

Specialist units should be established consisting of:

- criminal law experts
- cybersecurity experts
- artificial intelligence specialists
- digital forensics researchers
- experts on data protection and
- electronic evidence lawyers.

These teams could be better equipped to investigate AI-facilitated crimes.

13.3 Fund digital forensic capabilities

India should invest in:

• deepfake detection technologies

• audio forensic tools

• machine vision expertise

• metadata analysis capabilities

• synthetic image identification platforms

• device forensics tools

• and chain-of-custody procedures

13.4 Develop stronger content provenance tools

India should encourage the development of technologies that will enable individuals to assess:

• who created content

• whether it has been altered

• whether AI was involved

• when it was produced

• and whether its authenticity can be verified.

The 2026 framework's emphasis on labelling and traceability is a promising innovation.

13.5 Launch cybersecurity awareness campaigns

The awareness-raising campaign could educate the public about:

• the unreliability of voice messages based solely on familiar voices

• the importance of independently verifying urgent financial requests

• the need to examine suspicious links

• the value of multi-factor authentication

• the importance of reporting impersonation attempts promptly and

• the ability to spot AI-generated content.

13.6 Encourage accountability among platforms

Industry-specific standards could be created covering:

• good reporting practices

• regulatory disclosure transparency

• responsiveness protocols

• suitable inspection technologies

• preservation tools for relevant evidence and
• user notification procedures.

13.7 Strengthen international cooperation

India should promote international cooperation focussing on:
• cybercrime investigation
• digital evidence
• digital evidence
• information sharing
• extradition
• mutual legal assistance and
• general cross-border collaboration with platforms.

13.8 Encourage responsible AI development

The AI industry should adopt key principles including:
• safety by design
• privacy by design
• security by design
• transparency
• accountability and
• responsible use of AI technologies.

13.9 Create judicial and police training programs

The judiciary, prosecutors and police should receive targeted training in:
• AI-generated evidence
• deepfake detection
• digital authenticity verification
• synthetic media identification
• electronic records examination and
• AI-related cybercrime investigation techniques.

13.10 Adhere to technology-neutral legislation

Rather than creating specialised offences for every new technology, Indian legislation should, wherever possible, follow:
harm + intention + conduct + accountability

without distinguishing between types of technological facilitation.
This approach will make laws more resilient to technological change.

14. CONCLUSION

Artificial Intelligence is one of the most important technology innovations of recent years. AI has the potential to transform healthcare, education, commerce, governance and cybersecurity. Unfortunately, the same technologies that can improve society can also be hijacked to advance cybercrime.

AI-facilitated phishing, identity theft, social engineering, financial fraud, impersonation and deepfakes illustrate how cybercrime may be entering a new era where the boundaries between real and artificial digital content can be extremely fluid.

India already possesses a rich legal framework dealing with cyber-related offences. The Information Technology Act, 2000 contains important provisions addressing identity theft, cheating by personation and privacy violations. The Digital Personal Data Protection Act, 2023 establishes a comprehensive legal regime governing digital data processing. The Bharatiya Nyaya Sanhita, 2023 covers electronic dishonest dispositions while the Bharatiya Sakshya Adhiniyam, 2023 provides a modern evidentiary regime concerning electronic and digital materials.

The 2026 amendments to the IT Rules represent a particularly important step since they directly address synthetically generated information including deepfakes and AI-generated audio-visual material. Provisions concerning technical safeguards, labels, metadata requirements, general user awareness and intermediary responsibilities indicate that India appears to be taking targeted measures in relation to AI-related concerns.

Nevertheless, legislative initiatives alone will be insufficient. AI-facilitated cybercrime represents a techno-legal-social problem that requires a multi-pronged response involving government authorities, prosecuting authorities, courts of law, technology companies, cybersecurity expertise, researchers and general citizen awareness.

India should therefore embrace a balanced, risk-based and technology-neutral approach. While regulation should discourage unlawful utilisation, it should avoid limiting lawful innovation, creativity, research or freedom of digital expression.

Ultimately, India's aim should not necessarily be to create an environment of fear around artificial intelligence but rather one where AI development takes place responsibly, is utilised securely and appropriately regulated.

15. REFERENCES

A. PRIMARY LEGAL SOURCES

1. The Information Technology Act, 2000
2. Government of India, The Information Technology Act, 2000, India Code. The Act contains provisions dealing with computer-related offences ranging from identity theft to cheating by personation, privacy protection, cyber terrorism and intermediary-related issues.
3. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021Ministry of Electronics and Information Technology, Government of India.
4. The Digital Personal Data Protection Act, 2023Government of India, Digital Personal Data Protection Act, 2023, Act No. 22 of 2023.
5. The Digital Personal Data Protection Rules, 2025 Ministry of Electronics and Information Technology, Government of India. The Rules were notified on 13 November 2025 providing for phased commencement.
6. The Bharatiya Nyaya Sanhita, 2023 Government of India, Bharatiya Nyaya Sanhita, 2023, Act No. 45 of 2023. Relevant provisions deal with cheating, personation, false electronic records and forgery.
7. The Bharatiya Sakshya Adhiniyam (2023) Government of India, Bharatiya Sakshya Adhiniyam, 2023, Act No. 47 of 2023. Sections 61–63 address electronic and digital records and their admissibility.
8. The Bharatiya Nagarik Suraksha Sanhita, 2023 Government of India, Bharatiya Nagarik Suraksha Sanhita, 2023, Act No. 46 of 2023. The legislation includes provisions relating to electronic communications and offences committed outside India.

B. JUDICIAL AUTHORITIES

1. Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC
2. The judgment established the principle of protection of privacy, identifying fundamental constitutional rights under Article 21 and laying down various principles of legality, legitimate state aim, proportionality and justiciability.
3. Shreya Singhal v. Union of India (2015) 5 SCC 1.

4. The Supreme Court decision is significant to online expression and intermediary liability. The Supreme Court cites this decision among its landmark verdicts.
5. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal
6. (2020) 7 SCC 1.
7. The Supreme Court examined electronic records' evidentiary requirements. The Judgment identified some important principles applicable to electronic evidence.

C. GOVERNMENT AND REGULATORY SOURCES

1. Ministry of Electronics and Information Technology
2. Government of India, documentation about 2026 amendments to IT Rules and syntetically generated information. 2026 Government of India statement identifies a strengthened AI content framework, deepfake provisions, technical safeguards, labelling and traceability.
3. Ministry of Electronics and Information Technology
4. Frequently Asked Questions on the 2026 Amendments to the Information Technology Rules 2021, GoI.
5. CERT-In Indian Computer Emergency Response Team, Directions under Section 70B of the Information Technology Act, 2000.
6. CERT-In Security Implications of AI Language Based Applications, Indian Computer Emergency Response Team.
7. CERT-In Blueprint for Reducing Exposure and Defending against AI-Assisted Vulnerabilities Exploitation in Digital Infrastructure, 2026. The Blueprint deals with organisational measures to reduce exposure to AI-assisted cybersecurity risks.

D. RECOMMENDED ONLINE LEGAL SOURCES

• India Code – Information Technology Act, 2000
• India Code – Digital Personal Data Protection Act, 2023
• India Code – Bharatiya Nyaya Sanhita, 2023
• India Code – Bharatiya Sakshya Adhiniyam, 2023
• CERT-In – AI-Assisted Vulnerability Exploitation Blueprint
• Ministry of Electronics and IT – 2026 SGI FAQ