INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor
School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC-NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India. India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi. (2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi. Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship. He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi. Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi. He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN- 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

AI FOR ALL, THREATS FOR ALL: MAPPING CYBER SECURITY RISKS IN INDIA'S TECHNOLOGICAL DEMOCRACY

AUTHORED BY - PRABHASH RANJAN
Assistant Professor
(S.K.J. Law College, Muzaffarpur)

Abstract:

In the rapidly digitizing landscape of India, cybersecurity has emerged as a critical concern, particularly with the widespread adoption of Artificial Intelligence (AI) tools by common citizens. From AI-powered chatbots and personal assistants to generative platforms and facial recognition apps, Indian users are increasingly integrating AI into daily life for convenience, productivity, and entertainment. However, this democratization of AI also introduces significant cybersecurity challenges. The lack of digital literacy among a large segment of the population, combined with insufficient regulatory safeguards, exposes users to risks such as data theft, deepfakes, misinformation, AI-driven scams, and privacy violations. This paper argues for a multi-pronged strategy that includes AI regulation, public digital literacy campaigns, robust data protection laws, and ethical AI deployment. Empowering citizens with awareness and enforcing accountability among AI developers are essential steps toward building a secure and resilient cyber ecosystem in India.

Introduction

The integration of Artificial Intelligence (AI) into the daily lives of common citizens in India has increased exponentially in recent years. AI-driven tools such as voice assistants, photo-enhancement applications, AI chatbots, predictive healthcare tools, and real-time language translators are now routinely used by individuals across socio-economic strata. This widespread adoption, facilitated by the proliferation of affordable smartphones and deeper internet penetration, has been further accelerated by policy initiatives such as the Digital India programme.[1] While such technological integration presents opportunities for enhanced service

[1] "Digital India Programme," Ministry of Electronics and Information Technology, Government of India https://www.digitalindia.gov.in (accessed 10 August 2025).

ISSN: 2582-6433

delivery and citizen empowerment, it simultaneously raises profound concerns relating to data security, privacy, and algorithmic abuse.

The common user, often unaware of the underlying mechanics of AI tools, becomes increasingly susceptible to sophisticated cyber threats. Instances of AI-enabled fraud, identity theft, voice cloning, deepfake manipulation, and unauthorized surveillance are on the rise.[2] Such threats not only endanger individual rights but also pose broader challenges to national cybersecurity. Vulnerable sections of society, particularly those with low digital literacy—such as minors, the elderly, and individuals in rural regions—face a disproportionately higher risk.[3]

The existing legal and regulatory framework in India, while progressive in parts, remains inadequate in addressing the specific complexities introduced by AI. The Information Technology Act, 2000 and its ancillary rules, alongside the recently enacted Digital Personal Data Protection Act, 2023, provide a general foundation for data governance.[4] However, these legislations lack direct references to AI and are silent on issues such as algorithmic bias, transparency in automated decision-making, and the liability of AI service providers.[5] The absence of a tailored legal response has resulted in a regulatory lacuna that may hinder both innovation and the protection of fundamental rights.

Notwithstanding these challenges, certain institutional initiatives have sought to engage with the issue. Bodies such as NITI Aayog and the Ministry of Electronics and Information Technology have released policy papers and recommendations advocating for ethical AI deployment and responsible innovation.[6] Yet, these initiatives often remain at a policy level without substantive legislative backing or public outreach mechanisms. A fragmented regulatory approach without binding effect fails to address the realities of AI misuse at the grassroots level.

In light of the above, this paper attempts to explore four core areas: the nature and extent of AI

[2] A. Narayanan, "The Emerging Threat of Deepfakes and AI-enabled Frauds in India," (2023) 12(3) Indian Journal of Cyber Law 45.
[3] R. Sharma, "Digital Literacy and Cyber Vulnerabilities in Rural India," (2022) 14(2) International Journal of Law and Technology 112.
[4] Information Technology Act, 2000; Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).
[5] S. Bhatia, "Algorithmic Accountability and the Indian Legal Framework," (2023) 9(1) NLU Delhi Journal of Technology Law 76.
[6] NITI Aayog, "National Strategy for Artificial Intelligence: #AIforAll" (2015) https://www.niti.gov.in (accessed 15 August 2025).

ISSN: 2582-6433

usage among common people in India; the cybersecurity vulnerabilities associated with such usage; the sufficiency of the current legal framework; and the scope and limitations of governmental and institutional initiatives. It argues that a rights-based, multi-stakeholder regulatory approach is imperative to ensure that AI serves as a tool for inclusion and development, rather than one of exploitation and harm.

2. AI Usage Among Common People in India

The advent of Artificial Intelligence (AI) technologies has significantly transformed the digital landscape in India, penetrating the daily lives of individuals across socio-economic strata. With the proliferation of internet connectivity and affordable digital devices, AI tools have become increasingly mainstream, no longer restricted to research laboratories or corporate environments. This section analyses the patterns of AI adoption among the common populace, focusing on popular applications, emerging trends, and the broader context of accessibility and affordability.

2.1 Popular Applications

AI-driven tools have found wide acceptance among Indian users for a variety of day-to-day tasks. Voice assistants such as Google Assistant, Amazon Alexa, and Apple Siri are frequently used for tasks ranging from setting reminders and checking the weather to performing online searches.[7] Language translation tools, powered by Natural Language Processing (NLP), have become indispensable in a linguistically diverse nation, enabling users to interact across different regional languages.[8] Additionally, AI-powered photo enhancement apps, such as FaceApp and Remini, and content generation tools, like Grammarly and ChatGPT, are increasingly popular among students, creators, and professionals.[9]

Service sectors are also witnessing a surge in the use of AI-enabled chatbots for customer support in banking, e-commerce, travel, and telecommunications. These chatbots operate round the clock and provide quick resolution of queries, thereby enhancing user experience and reducing operational burdens on human staff[10]. This diffusion of AI in public-facing services

[7] "Google Assistant, Amazon Alexa, and Apple Siri in India: Adoption and Use Cases," Economic Times Tech (15 March 2023) https://tech.economictimes.indiatimes.com (accessed 15 August 2025).

[8] A. Kumar, "Natural Language Processing and Regional Languages in India," (2021) 7(2) Journal of Artificial Intelligence Research in Asia 54.

[9] "AI Apps Like FaceApp and Remini Gain Popularity Among Indian Users," Hindustan Times (12 July 2022) https://www.hindustantimes.com (accessed 15 August 2025).

[10] S. Mehta, "Chatbots and Service Delivery in India's Banking Sector," (2022) 11(4) Indian Journal of Information Law & Technology 88.

ISSN: 2582-6433

marks a significant shift in the way Indian consumers interact with institutions.

2.2 Emerging Trends

Recent developments indicate a growing reliance on more advanced and nuanced AI applications. The rise of generative AI—capable of creating text, images, and synthetic voices—has enabled new forms of digital expression and engagement.[11] AI-generated art, automated resume builders, voice-over generators, and content summarizers are reshaping how information is produced and consumed. In the fields of finance and healthcare, predictive analytics tools are gaining traction. For example, AI-based investment advisors and credit risk evaluation tools are helping individuals make informed economic decisions, while diagnostic applications are assisting patients with preliminary health assessments based on symptoms and medical history.[12]

Moreover, the integration of AI in smart home devices—such as intelligent lighting systems, surveillance cameras, and home automation hubs—reflects an evolving trend of convenience-driven consumption.[13] These technologies offer not only efficiency but also enhanced security and energy management, especially among middle-class households in urban centers.

2.3 Accessibility and Affordability

A key factor behind the widespread adoption of AI among common people in India is the accessibility afforded by cost-effective technology. The sharp decline in smartphone prices, coupled with competitive internet data tariffs offered by providers like Jio, Airtel, and BSNL, has brought AI-powered tools within reach of millions.[14] According to various reports, India has one of the highest levels of internet penetration among developing economies, with a substantial portion of its rural population coming online for the first time in recent years.[15]

The increasing availability of vernacular content and AI applications that support regional languages further enhances inclusivity. Several domestic startups and government-backed

[11] "The Rise of Generative AI in India," Business Standard (20 February 2023) https://www.business-standard.com
(accessed 15 August 2025).
[12] R. Banerjee, "AI in Indian Healthcare: Challenges and Opportunities," (2023) 15(1) Indian Journal of Health Policy and Technology 22.
[13] "Smart Home AI Devices Enter Indian Market," LiveMint (9 January 2023) https://www.livemint.com (accessed 15 August 2025).
[14] Telecom Regulatory Authority of India (TRAI), "Annual Report on Telecom and Internet Penetration" (2023) https://www.trai.gov.in (accessed 15 August 2025).
[15] Internet and Mobile Association of India (IAMAI), "India Internet 2023 Report" (July 2023) https://www.iamai.in
(accessed 15 August 2025).

ISSN: 2582-6433

initiatives have focused on creating AI solutions that cater to local needs—such as crop advisory tools for farmers, job-finding platforms for informal workers, and education apps for rural students.[16]

While the diffusion of AI across the socio-economic spectrum is a promising development, it also raises questions about digital literacy, informed consent, and data protection. The next sections of this paper shall address the cybersecurity and legal implications of such widespread AI usage.

3. Cybersecurity Threats Linked to AI Adoption in India

While the adoption of Artificial Intelligence has undoubtedly enhanced convenience and efficiency in daily life, it has simultaneously expanded the spectrum of cybersecurity risks. The use of AI tools by common citizens has created vulnerabilities that are often underestimated due to a lack of digital literacy and awareness. This section examines the key categories of threats, ranging from identity theft and misinformation to AI-driven cyberattacks.

3.1 Identity Theft and Data Exploitation

One of the most significant risks posed by the popularisation of AI is identity theft. Applications such as AI-powered photo and video editors collect vast amounts of biometric and personal data, which, if misused, can facilitate fraudulent activities.[17] For example, deepfake technology—where AI generates highly realistic synthetic videos—has been increasingly deployed for impersonation scams, financial fraud, and reputational harm.[18]

Moreover, AI-enabled apps often demand excessive permissions to access contact lists, microphones, and location data, thereby raising concerns about surveillance and privacy violations. Inadequate regulations and weak enforcement mechanisms in India further exacerbate the possibility of data exploitation by both private corporations and malicious actors.[19]

3.2 Misinformation and Manipulation

AI-generated misinformation represents a critical challenge for Indian democracy. The

[16] "AI for Farmers, Workers, and Students: Indian Startups Lead the Way," The Hindu BusinessLine (21 May 2023) https://www.thehindubusinessline.com (accessed 15 August 2025).
[17] A.Gupta,"AI Apps and Biometric Data Risks,"(2022) 14 (3) Journal of Cyber security and Digital Privacy 47.
[18] Deepfakes Usedin Financial Scams Across India," Times of India (11October2023) [https://timesofindia.indiatimes.com] (https://timesofindia.indiatimes.com) (accessed15August2025).
[19] R.Sharma,"Data Protection Challenges in India,"(2021) 9 (2) Indian Law Review on Technology and Society 102.

ISSN: 2582-6433

proliferation of AI-based content creation tools allows for the mass production of false news, propaganda, and inflammatory messages, which can be disseminated rapidly via social media platforms.[20] Given India's socio-political diversity and sensitivity, such disinformation campaigns have the potential to incite communal violence, manipulate electoral outcomes, and erode trust in democratic institutions.[21]

The emergence of "synthetic media" such as deepfake videos of political leaders has already raised alarms in several state elections.[22] The ability of generative AI to mimic speech and writing styles further blurs the line between authentic and fabricated content, making detection and regulation exceedingly difficult.[23]

3.3 AI-Driven Cyber attacks

The integration of AI into cybercrime has amplified the sophistication of attacks. Hackers are increasingly using AI-powered tools to automate phishing campaigns, bypass security systems, and launch adaptive malware.[24] For instance, machine learning algorithms can analyse user behaviour and craft highly personalised phishing messages, thereby increasing the probability of success.[25]

In India, where a large proportion of the population is newly connected to the internet, such AI-driven attacks exploit digital illiteracy and lack of awareness[26]. Small businesses and individual users are especially vulnerable, as they often lack robust cybersecurity infrastructure. Additionally, ransomware attacks powered by AI-based encryption techniques have been reported to target local enterprises, demanding payments in cryptocurrencies that are difficult to trace.[27]

3.4 Socio-Economic Impact of AI Threats

The consequences of AI-enabled cyber threats extend beyond individual victims. Widespread

[20]"Fake News Powered by AI Tools Ahead of Elections," Indian Express (14 March 2024) [https://indianexpress.com] (https://indianexpress.com) (accessed 16 August 2025).
[21]P.Jha, "Disinformation and Electoral Manipulation in India," (2022) 19 (1) Asian Journal of Political Science 66.
[22]"Synthetic Media Raises Concerns in State Elections," The Hindu (22 November 2023) [https://www.thehindu.com] (https://www.thehindu.com) (accessed 16 August 2025).
[23]M. Thomas,"Generative AI and the Crisis of Trust,"(2023) 12 (2) Technology, Society & Law Review 33.
[24]"Cyber criminals Turn to AI for Sophisticated Attacks," Financial Express (30 January 2024) [https://www.financialexpress.com] (https://www.financialexpress.com) (accessed 16 August 2025).
[25]K.Iyer,"AI-Enabled Phishing and Behavioural Analysis,"(2023) 8 (4) Indian Journal of Cyber crime Studies 21.
[26]National Crime Records Bureau (NCRB), "Cybercrime Report 2023" (December 2023) [https://ncrb.gov.in] (https://ncrb.gov.in) (accessed 16 August 2025).
[27]"AI-Driven Ransomware Hits Indian SMEs," Business Today (7 June 2023) [https://www.businesstoday.in] (https://www.businesstoday.in) (accessed 15 August 2025).

ISSN: 2582-6433

incidents of financial fraud, identity theft, and misinformation disrupt social trust and economic stability.[28] The psychological harm caused by misuse of deepfakes—particularly against women through non-consensual explicit content—has emerged as a pressing concern.[29] Furthermore, as India aims to digitise governance and expand e-services under the "Digital India" initiative, vulnerabilities in AI systems may undermine confidence in state-led technological reforms.[30]

4. Legal and Regulatory Framework in India

India's legal framework for cybersecurity and Artificial Intelligence remains fragmented and in transition. While existing statutes provide partial coverage against AI-related risks, the absence of a comprehensive AI law continues to create regulatory gaps. This section evaluates the principal legal instruments and policies relevant to AI use by common citizens.

4.1 The Information Technology Act, 2000

The Information Technology Act, 2000 (IT Act) serves as the cornerstone of India's cyber law.[31] It criminalises unauthorised access, hacking, identity theft, and cheating through computer resources.[32] However, the Act was enacted at a time when AI technologies were not prevalent, and therefore, it lacks specific provisions to address AI-generated harms such as deepfakes, algorithmic bias, or autonomous decision-making.[33]

Amendments introduced in 2008 strengthened provisions on data protection and cyber terrorism,[34] but these remain inadequate in addressing the complex risks of AI-driven threats. For example, Section 66C penalises identity theft, yet the application of this provision to AI-based impersonation remains legally untested.[35]

4.2 Personal Data Protection Bill, 2019 (Now Digital Personal Data Protection Act, 2023)

After years of debate, India enacted the Digital Personal Data Protection Act, 2023 (DPDP Act), which marks a significant step toward data security.[36]The Act regulates the processing of

[28]V.Rao,"Economic Costs of Cyber crime in India,"(2022) 17(3) Indian Journal of Economics and Policy 112.
[29] "Deepfake Harassment of Women in India," Scroll.in (15 July 2023) [https://scroll.in] (https://scroll.in) (accessed 15 August 2025).
[30]Ministry of Electronics and Information Technology (MeitY), "Digital India Annual Report 2023" (Government of India, 2023).
[31]Information Technology Act, 2000, No.21 of 2000, Government of India.
[32]Ibid, Sections43, 65, 66.
[33]R.Raj, "The IT Act and Emerging AI Threats," (2021) 13 (2) Indian Journal of Law and Technology 54.
[34]Information Technology (Amendment) Act,2008.
[35]P.Mehta,"Identity Theft and the IT Act : An Analysis,"(2022) 10 (1) Journal of Indian Cyber Law 29.
[36]Digital Personal Data Protection Act, 2023, Government of India.

ISSN: 2582-6433

digital personal data, emphasising user consent and corporate accountability.[37]

For AI-related threats, the DPDP Act provides safeguards against misuse of personal data by AI-powered applications.[38] However, the Act has been criticised for granting extensive exemptions to the state, thereby diluting protection for citizens against mass surveillance.[39] Additionally, the absence of explicit references to AI systems creates uncertainty about the extent of compliance obligations for AI developers and platforms.[40]

4.3 Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

The IT Rules, 2021 impose obligations on social media intermediaries to remove unlawful content, including fake news and harmful online material.[41] They require platforms to enable traceability of messages and appoint grievance officers for user complaints.[42]

In the context of AI, these rules are particularly relevant for combating misinformation generated by chatbots, deepfakes, and automated content farms.[43] However, enforcement challenges persist due to the sheer scale of online communication and technical difficulties in tracing AI-generated material.[44] Critics argue that the traceability mandate risks undermining end-to-end encryption, thereby affecting citizens' right to privacy.[45]

4.4 National Cybersecurity Strategy (Draft 2020) and Related Policies

India's Draft National Cybersecurity Strategy (2020) seeks to build robust digital infrastructure, enhance cyber-awareness, and establish effective coordination mechanisms. Though not yet formally adopted, the draft acknowledges the growing challenge of AI-driven cyber threats.[46]

Further, initiatives such as the National Artificial Intelligence Strategy (NITI Aayog, 2015) and

[37]Ministry of Electronics and Information Technology (MeitY), "DPDP Act FAQs" (2023) [https://www.meity.gov.in] (https://www.meity.gov.in) (accessed 16 August 2025).
[38]A. Chatterjee, "AI and Data Privacy in India," (2024) 15 (3) Journal of Technology Regulation 102.
[39]"Critics Slam Wide Ranging State Exemptions in DPDP Act," The Hindu (21 August 2023) [https://www.thehindu.com] (https://www.thehindu.com) (accessed 16 August 2025).
[40]S. Rathi, "Uncertain Compliance Obligations for AI Developers," (2023) 19 (4) National Law School Journal 88.
[41]Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
[42]Ibid, Rule 4.
[43]"Social Media Platforms Face Pressure over AI-Generated Fake News," Indian Express (14May2023) [https://indianexpress.com] (https://indianexpress.com) (accessed 16 August 2025).
[44]A. Sinha, "Challenges in Regulating AI Misinformation," (2022) 15 (1) Indian Journal of Communication Law 77.
[45]National Cybersecurity Strategy (Draft2020), National Security Council Secretariat, Government of India.
[46]"India's Cyber security Roadmap Still Awaited," Business Standard (12 February 2024) [https://www.business-standard.com] (https://www.business-standard.com) (accessed 16 August 2025).

ISSN: 2582-6433

the National AI Portal aim to promote AI development, but they prioritise innovation and economic growth over safety and ethical regulation.[47] This duality reflects a policy dilemma: balancing India's ambition to be an AI hub with the urgent need to protect citizens from AI-enabled harms.[48]

4.5 Judicial Responses

Indian courts have begun to confront issues indirectly related to AI misuse. In Shreya Singhal v. Union of India (2015), the Supreme Court struck down Section 66A of the IT Act, recognising the importance of free speech in the digital domain.[49] In more recent cases concerning privacy, such as Justice K.S. Puttaswamy v. Union of India (2017), the Court affirmed the constitutional right to privacy,[50] which has direct implications for data collection by AI applications.

However, the judiciary has yet to deliver landmark rulings specifically addressing AI-driven harms such as deepfakes, algorithmic discrimination, or automated decision-making.[51] This legal vacuum underscores the urgency of specialised legislation to govern AI technologies.

5. Comparative Perspectives – USA and EU Models

The regulation of Artificial Intelligence (AI) and cybersecurity has emerged as a global policy challenge. While India is still shaping its legal framework, the USA and European Union (EU) have taken distinct regulatory approaches. A comparative analysis provides valuable insights for India's future roadmap.

5.1 United States: Sectoral and Self-Regulatory Approach

The USA lacks a single, comprehensive AI law. Instead, it follows a sectoral approach, combining federal and state-level regulations.[52] Key features include:

AI Bill of Rights (2022): A White House initiative that sets out principles such as safe systems, privacy protections, transparency, and accountability in automated decision-making.[53] While

[47]NITIAayog, "National Strategy for Artificial Intelligence" (2015).
[48]V. Kumar, "AI Innovation vs AI Regulation: The Indian Dilemma," (2021) 20 (2) Asian Journal of Law and Policy 41.
[49]Shreya Singhal v. Union of India (2015) 5 SCC 1.
[50]Justice K. S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1.
[51]M. Bhatia, "Judicial Silence on AI Harms in India," (2024) 11 (3) Law and Technology Review 67.
[52]J. Riedl, "The US Approach to AI Regulation: A Patch work System," (2022) 30 (4) Yale Journal of Regulation 77.
[53]White House, "Blueprint for an AI Bill of Rights" (2022).

ISSN: 2582-6433

non-binding, it serves as an ethical guide for AI deployment.[54]

Sectoral Regulations: Existing laws such as the Health Insurance Portability and Accountability Act (HIPAA) regulate AI in healthcare, while the Fair Credit Reporting Act (FCRA) applies to AI-based credit scoring.[55]

Federal Trade Commission (FTC): The FTC has warned companies against unfair or deceptive use of AI tools, signalling a willingness to regulate AI misuse under existing consumer protection law.[56]

State Laws: Some states have enacted AI-specific measures, such as Illinois' Biometric Information Privacy Act (BIPA), which has been invoked in litigation against facial recognition platforms.[57]

The American model reflects a reliance on self-regulation by industry combined with selective enforcement by regulators. This fragmented framework allows innovation but creates uneven levels of protection for citizens.[58]

5.2 European Union: Comprehensive and Rights-Oriented Approach

The EU has adopted a proactive, rights-centric framework for AI regulation. Its approach is anchored in fundamental rights, human dignity, and consumer protection.

General Data Protection Regulation (GDPR, 2015): Establishes strict standards on data collection, consent, and processing, directly impacting AI applications dependent on personal data.[59]

Artificial Intelligence Act (AI Act, 2024): The world's first comprehensive AI law, introducing a risk-based regulatory model.[60] It classifies AI systems into categories (unacceptable risk, high risk, limited risk, and minimal risk), imposing varying obligations.[61] High-risk AI systems, such as those used in recruitment, law enforcement, and biometric surveillance, face strict compliance requirements.[62]

Enforcement Mechanisms: The EU's approach includes independent supervisory authorities

[54]Ibid
[55]Health Insurance Portability and Accountability Act (HIPAA), Pub. L. 104–191 (1996); Fair Credit Reporting Act (FCRA), 15 U.S.C. §1681.
[56]Federal Trade Commission, "Aiming for Truth, Fairness, and Equity in Your Company's Use of AI" (2021).
[57]Biometric Information Privacy Act, 740 ILC S 14/(Illinois,2008).
[58]M. West, "Fragmented AI Regulation in the US," (2021) 14 (3) Journal of Law and Innovation 114.
[59]General Data Protection Regulation (EU) 2016/679.
[60]European Parliament, "Artificial IntelligenceAct" (Regulation (EU) 2024/1689).
[61]Ibid, Articles5–9.
[62]EU's Landmark AI Act Explained," Politico (14 March 2024) [https://www.politico.eu] (https://www.politico.eu) (accessed 16 August 2025).

ISSN: 2582-6433

with power to impose heavy fines on non-compliant AI developers.[63]

Digital Services Act (DSA) and Digital Markets Act (DMA): These laws regulate large online platforms, mandating transparency in algorithmic operations and accountability for harmful content.[64]

The EU's model is notable for its precautionary principle, which prioritises citizen safety and human rights over unregulated technological growth.[65]

5.3 Lessons for India

The US and EU models represent two contrasting regulatory philosophies:

The US model prioritises innovation, market freedom, and self-regulation, but risks leaving citizens vulnerable to AI-enabled harms.

The EU model demonstrates the benefits of a rights-based, comprehensive legal framework, though critics argue that overregulation could stifle AI innovation.[66]

For India, which aspires to become both a global AI hub and a secure digital democracy, a hybrid model may be most effective. This would involve adopting EU-style safeguards for citizen rights while preserving the US-style flexibility needed for innovation and economic growth.

6. Cybersecurity Challenges Posed by AI for Common Citizens

Artificial Intelligence (AI) has penetrated everyday life in India—through smart phones, digital payments, social media, and e-governance platforms. While AI offers efficiency and convenience, it also creates unique cybersecurity vulnerabilities that directly impact ordinary citizens.

6.1 Data Privacy Risks

AI systems thrive on massive datasets, much of which is personal in nature.[67] The unregulated collection and processing of data leads to:

Unauthorized Profiling: Companies deploy AI to infer sensitive details about users (e.g., health,

[63]GDPR, Chapter VI.
[64]Digital Services Act, Regulation (EU) 2022/2065; Digital Markets Act, Regulation (EU) 2022/1925.
[65]L.Floridi, "The Precautionary Principle and AI Regulation in the EU," (2023) 17 (2) European Journal of Risk Regulation 33.
[66]A. Ghosh, "AI Regulation: Balancing Innovation and Safety," (2024) 12(1) Indian Journal of Comparative Law 59.
[67]N. Khan, "Data as the New Oil: AI and Privacy Risks in India," (2022) 44 (3) Indian Journal of Law and Technology 201.

ISSN: 2582-6433

political views, and financial habits) without consent.[68]

Identity Theft: With deep data pools, criminals can easily impersonate individuals to access bank accounts, SIM cards, or digital wallets.[69]

Surveillance Concerns: Facial recognition tools increasingly deployed in public spaces raise fears of a surveillance state, with little legal protection for citizens.[70]

6.2 AI-Enabled Cybercrime

AI enhances the sophistication of cybercriminal operations. Common risks include:

Deepfakes: Hyper-realistic audio and video manipulations used to commit fraud, harassment, or political misinformation.[71]

Phishing and Social Engineering: AI-driven bots generate convincing phishing emails, mimicking official communication from banks or government bodies.[72]

Automated Attacks: AI can exploit vulnerabilities in systems faster than human hackers, enabling large-scale financial frauds.[73]

For citizens with limited digital literacy, distinguishing genuine from fraudulent communication becomes nearly impossible.

6.3 Financial Security Threats

With India's rapid adoption of digital payments (UPI, mobile wallets, online banking), AI-driven fraud has surged.[74] Examples include:

Voice Cloning Scams: Fraudsters replicate voices of family members to demand urgent money transfers.[75]

Fraudulent Loan Approvals: AI-based lending apps misuse personal data to extract money, often linked with coercive recovery practices.[76]

Crypto and Investment Scams: AI-generated trading bots lure citizens into fraudulent investment schemes.[77]

Such scams disproportionately affect rural and semi-urban citizens who lack cybersecurity

[68]Ibid
[69]S. Gupta, "Identity Theft and AI Misuse," (2021) 12 (2) Journal of Indian Law and Society 67.
[70]Internet Freedom Foundation, "India's Growing Surveillance State," Report (2023).
[71]Chesney & D. Citron, "Deep Fakes: A Looming Challenge for Privacy and Democracy," (2019) 107 California Law Review 1753.
[72]CERT- In, "Advisory on AI-Driven Phishing Attacks,"(2022).
[73]M. Rid, Cyber War Will Not Take Place (Oxford University Press 2020) 214.
[74]Reserve Bank of India, "Trends in Digital Payments 2024," RBI Bulletin (2024).
[75]The Hindu, "AI-Enabled Voice Cloning Fraud Cases Surge in India," (15May2024).
[76]The Wire, "Predatory Loan Apps and AI Algorithms," (22 August 2023).
[77]S. Narayanan, "Crypto Frauds and AI Bots in India," (2023) 15 (1) Economic and Political Weekly 77.

ISSN: 2582-6433

awareness.

6.4 Psychological and Social Risks

AI-driven cyber threats are not limited to financial loss but extend to **psychological harm:

Cyberbullying and Harassment: AI-generated abusive content spreads faster and more virulently than human-driven attacks.[78]

Misinformation Epidemics: AI-enabled misinformation campaigns polarize communities, eroding social trust.[79]

Addictive Algorithms: Recommendation engines on social media manipulate user behavior, fostering addiction, anxiety, and reduced well-being.[80]

The cumulative effect is a deep erosion of citizen trust in technology.

6.5 State Capacity and Legal Gaps

While India has launched initiatives such as the Digital India Mission and National Cybersecurity Policy (2013), regulatory gaps persist:

Absence of a dedicated AI-specific cybersecurity law;

Weak enforcement of data protection obligations;

Over-reliance on self-regulation by tech companies;

Limited capacity of police and judiciary to investigate AI-driven crimes.[81]

Unless addressed, these challenges will widen the gap between technological advancement and citizen protection.

7. Legal and Constitutional Dimensions in India

The cybersecurity threats posed by Artificial Intelligence (AI) must be examined within India's constitutional framework and the existing statutory regime. While India has begun addressing digital risks through legislation and judicial intervention, gaps remain in effectively regulating AI.

7.1 Constitutional Safeguards

(a) Right to Privacy

[78]M. Duggal, "AI and Cyber bullying," (2022) 10 (4) Journal of Law and Technology 115.
[79]S. Vaishnav, "Disinformation and Democracy in India," (2023) Carnegie Endowment Report.
[80]T. Zuboff, The Age of Surveillance Capitalism (Public Affairs 2019).
[81]National Cysber security Policy, Ministry of Electronics and IT, Government of India (2013).

ISSN: 2582-6433

The Supreme Court in Justice K.S. Puttaswamy v. Union of India[82] recognized the right to privacy as a fundamental right under Article 21 of the Constitution. AI-driven surveillance, profiling, and data collection directly challenge this constitutional protection.

(b) Freedom of Speech and Expression

AI impacts Article 19(1)(a), as deepfakes, misinformation, and algorithmic amplification interfere with citizens' ability to access truthful information.[83] At the same time, state-imposed restrictions on online platforms raise concerns about excessive curtailment of free speech.[84]

(c) Equality and Non-Discrimination

AI algorithms often reflect biases embedded in training datasets. Discriminatory outcomes in recruitment, credit scoring, or policing can violate Articles 14 and 15, which guarantee equality and prohibit discrimination.[85]

7.2 Statutory and Policy Framework

India does not yet have an AI-specific law, but several legal instruments govern aspects of cybersecurity and data protection:

1. Information Technology Act, 2000 (IT Act)

Section 43A: Compensation for failure to protect sensitive personal data.[86]

Section 66: Punishment for computer-related offences.[87]

Section 69: Power of government to intercept and monitor data.[88]

2. Digital Personal Data Protection Act, 2023 (DPDP Act)

Introduces obligations on "data fiduciaries" to ensure data minimization and lawful use.[89]

However, it grants wide exemptions to the State for surveillance, raising concerns of executive overreach.[90]

3. National Cyber Security Policy, 2013

Focuses on protecting critical information infrastructure but is outdated in addressing AI-specific risks.[91]

[82]Justice K. S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[83]A. Roberts, "Deepfakes and Free Speech," (2021) 54 Columbia Journal of Law and Arts 113.
[84]Shreya Singhal v. Union of India, (2015) 5 SCC 1.
[85]Vidhi Centre for Legal Policy, "Algorithmic Bias and Equality in India," Policy Report (2022).
[86]Information Technology Act, 2000, Section 43A.
[87]Ibid., Section 66.
[88]Ibid., Section 69.
[89]Digital Personal Data Protection Act, 2023, Section6.
[90]Internet Freedom Foundation, "Exemptions in DPDP Act: A Constitutional Critique," (2023).
[91]National Cyber Security Policy, Ministry of Electronics and IT (2013).

ISSN: 2582-6433

7.3 Judicial Developments

Courts have begun engaging with issues at the intersection of technology and fundamental rights:

Anuradha Bhasin v. Union of India (2020)[92]: The Supreme Court held that access to the internet is integral to freedom of speech and trade.

Shreya Singhal v. Union of India (2015)[93]: Struck down Section 66A of the IT Act for violating free speech.

Ongoing petitions challenge the use of facial recognition by police in public protests, raising concerns about chilling effects on dissent.[94]

7.4 Regulatory Gaps

Despite constitutional and statutory protections, several lacunae remain:

Absence of an AI liability framework to determine responsibility for harms caused by autonomous systems.

Overlapping jurisdiction of regulators (MeitY, RBI, TRAI, CERT-In), creating uncertainty.

Lack of citizen remedies for algorithmic discrimination or deepfake-related harassment.

Weak enforcement of corporate accountability in AI deployment.

These gaps highlight the urgent need for AI-specific legislation balancing innovation with constitutional rights.

8. Policy Recommendations for India

India stands at a crossroads: it must leverage AI for economic growth while ensuring cybersecurity, privacy, and constitutional rights. The following recommendations emerge from comparative and doctrinal analysis:

8.1 AI-Specific Legislation

Enact a dedicated Artificial Intelligence (Regulation and Liability) Act, modeled partly on the EU's AI Act but tailored to Indian realities.[95]

Define liability frameworks for AI-driven harms, including cyber frauds, deepfakes, and algorithmic bias.[96]

[92]Anuradha Bhasinv. Union of India, (2020)3SCC637.
[93]Shreya Singhalv .Union of India, (2015)5SCC1.
[94]IndianExpress,"DelhiPolice'sFacialRecognitionTechFacesLegalChallenge,"(12Jan2024).
[95]European Commission, "Proposal for a Regulation on Artificial Intelligence," COM/2021/206 final.
[96]Usha Ramanathan, "Liability in Automated Decision making," Economic and Political Weekly, Vol. 56, No. 12 (2021).

ISSN: 2582-6433

Mandate impact assessments before deploying high-risk AI systems in policing, welfare distribution, and healthcare.

8.2 Strengthening Cybersecurity

Establish a National AI-Cybersecurity Authority (NACA) to coordinate with CERT-In and NCIIPC.[97]

Expand the scope of the Information Technology Act, 2000, to explicitly cover AI-based cyber threats.

Encourage public-private partnerships to secure digital infrastructure.

8.3 Data Protection and Privacy

Swiftly operationalize the Digital Personal Data Protection Act, 2023 with strict AI-specific safeguards.[98]

Ensure that consent, purpose limitation, and accountability principles apply to AI-powered apps.

Recognize algorithmic transparency and explainability rights for citizens.

8.4 Capacity Building and Literacy

Launch a National AI & Cybersecurity Literacy Mission to educate citizens on:

AI-enabled frauds (deepfakes, phishing).

Safe use of generative AI apps.

Introduce AI ethics and cybersecurity modules in school and university curricula.[99]

8.5 Judicial and Constitutional Role

The Supreme Court should develop jurisprudence on AI and fundamental rights, extending Puttaswamy to AI-driven privacy intrusions.[100]

Establish special cyber benches in High Courts for speedy adjudication of AI-related cybercrimes.

8.6 International Cooperation

India should participate in global AI governance forums (OECD AI Policy Observatory,

[97]CERT- In, "Annual Report on Cybersecurity 2023," Ministry of Electronics & IT, Government of India.
[98]Digital Personal Data Protection Act, 2023 (India).
[99]NITI Aayog, "Responsible AI for All: Strategy Document,"Government of India, 2021.
[100]Justice K. S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

ISSN: 2582-6433

GPAI).[101]

Explore bilateral cooperation with France (rights-based model) and the USA (innovation model).

Advocate for a UN Convention on AI and Cybersecurity to harmonize norms.

Conclusion

Artificial Intelligence (AI) is a double-edged sword for India's digital democracy. On the one hand, it promises efficiency, innovation, and socio-economic transformation. On the other, it creates unprecedented cybersecurity risk, ranging from AI-powered phishing attacks to deepfake-driven misinformation campaigns.

The Indian constitutional framework, particularly Article 21, offers a fertile ground for developing AI rights jurisprudence. However, current laws—such as the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023—remain fragmented and inadequate for the AI age.[102]

The way forward requires:

AI-specific legislation addressing liability, bias, and transparency.

Stronger cybersecurity institutions to counter AI-enabled threats.

Judicial creativity in extending privacy and dignity protections to the algorithmic era.

Citizen empowerment through digital literacy.

International cooperation, positioning India as a norm-shaper in global AI governance.

Ultimately, the legitimacy of India's technological democracy will depend on whether AI tools empower its citizens or entrap them in new forms of digital vulnerability. A responsible, secure, and rights-centric AI regime is not merely a policy choice but a constitutional necessity.

[101]OECD, "AI Policy Observatory," OECD Report, 2022.
[102]Information Technology Act, 2000 (India); Digital Personal Data Protection Act, 2023 (India).