IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Artificial Intelligence and Data Privacy: Challenges under Indian Cyber Laws

Swati Pal
Assistant Professor, IPEM Law Academy, Ghaziabad

Dr. Purnima Chaudhary
Head of Department, IPEM Law Academy, Ghaziabad

Abstract

In the era of the digital economy, personal data has emerged as the most valuable asset, with the exponential growth of Artificial Intelligence (AI) technologies in various fields, such as healthcare, finance, governance, and law enforcement, also creating significant threats to individual privacy and civil liberties. India has seen cybersecurity incidents rise from 10.29 lakh in 2022 to 22.68 lakh in 2024, marking a turning point in the country. This paper critically analyses the interplay of AI and data privacy in the context of the existing cyber laws in India, namely, Information Technology Act, 2000, Digital Personal Data Protection Act, 2023, IT (Intermediary Guidelines) Rules, 2021 and CERT-In Directives, 2022. It highlights the lack of automated decision-making rights, algorithmic transparency requirements, and governance of non-personal aggregated data and compares the Indian regime with the EU General Data Protection Regulation (GDPR) and EU AI Act, 2024. Based on this empirical incident data, this paper offers a roadmap for reform of the regulatory environment that includes a regulatory framework specifically for AI, mandatory algorithm auditing, rationalisation of data localisation and the creation of a dedicated AI regulatory body. The study highlights the importance of embedding privacy considerations into the design of their AI systems and the need for responsible AI governance to ensure that India can fulfill its goals as a global powerhouse of AI.

Keywords: Artificial Intelligence, Data Privacy, Indian Cyber Laws, IT Act 2000, DPDP Act 2023, Algorithmic Governance, GDPR, Cybersecurity, Deepfakes, Right to Privacy.

1. Introduction

Artificial Intelligence is no longer a distant dream but a working component of today's digital landscape. AI systems are consuming, matching, and monetizing personal data on a scale never seen before—for predictive healthcare diagnostics and automated credit scoring, among other applications. India, with more than 900 million internet users, and a growing USD 7.8 billion AI industry, faces a unique regulatory dilemma—its legal landscape is rooted in the Information Technology Act, 2000 (IT Act),[1] was written before the advent of AI and is not up to the task of ruling on the new, emerging harms created by machine learning, generative AI and autonomous decision-making systems. The Supreme Court's landmark ruling in

[1]Information Technology Act, 2000, No. 21 of 2000, as amended by the Information Technology (Amendment) Act, 2008, No. 10 of 2009.

Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)[2] Raised privacy to a fundamental right and paved the way for the enactment of the Digital Personal Data Protection (DPDP) Act, 2023.[3] Raised privacy to a fundamental right and paved the way for the enactment of the Digital Personal Data Protection (DPDP) Act, 2023.[4]

This paper consists of six sections: Part II offers a survey of the changing interface between AI and privacy of data. Part III explains the existing legal framework in India and its shortcomings. Part IV makes a comparative analysis with the global benchmarks. Empirical data is provided on India's cybersecurity landscape and threats related to Artificial Intelligence in Part V. Part VI outlines some of the main challenges, while Part VII presents the recommendations for reform.

2. The AI–Data Privacy Interface: A Conceptual Overview

At the heart of AI systems are data-hungry mechanisms. Machine learning models thrive on massive datasets for training, recommender systems learn from behaviour in real-time, natural language processing (NLP) models learn from conversations in real-time, and computer vision systems learn from biometric data, even if without explicit consent. These operations all have particular privacy issues which do not clearly align with traditional data processing.

2.1 The 'Black Box' Problem

One of the hallmarks of sophisticated artificial intelligence systems is their opacity, also known as the 'black box' effect, in which even the AI developers cannot provide a clear explanation of how a model arrives at a decision.[5] It is a central violation of informational consent that a data principal can't give informed consent to an operation if he or she has no idea what is going on. The DPDP Act of India requires the consent of the data subject for processing but does not offer a way to implement the principle if the AI service is a third party whose decision logic is a trade secret and hidden.[6]

2.2 Algorithmic Bias and Discriminatory Profiling

Incorporating historically biased data into AI systems ensures that these systems will reflect and reinforce structural inequities. AI use in India, such as in the allocation of welfare benefits, credit scoring, and bail decisions, may result in discriminatory algorithms that breach the constitutional rights to equality guaranteed by Article 14 and 21 of the Indian Constitution. The DPDP Act centres on the protection of personal data and provides no remedy for discrimination based on non-personal data sets, such as those used in algorithms.

2.3 Generative AI and Deepfakes

Using historically biased data in AI systems will mean that the systems will perpetuate and repeat structural inequities. The implementation of AI in India, for example, in welfare benefit distribution, credit scoring and bail decisions, could lead to discriminatory algorithms that infringe on the constitutional rights of equality (Article 14) and life (Article 21). The DPDP Act focuses on the protection of personal data and

[2]Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCC 1. The nine-judge bench unanimously held that the right to privacy is a fundamental right protected under Part III of the Constitution of India.

[3]Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India). See also: Malhotra, C. & Malhotra, U. (2024). Putting Interests of Digital Nagriks First. Indian Journal of Public Administration, 70(3). https://doi.org/10.1177/00195561241271575

[4]European Commission (2021). Proposal for a Regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act). COM(2021) 206 final. Enacted as Regulation (EU) 2024/1689 of the European Parliament and of the Council. https://doi.org/10.3000/OJL.2024.1689

[5]Al-Khassawneh, Y.A. (2023). A Review of Artificial Intelligence in Security and Privacy: Research Advances, Applications, Opportunities, and Challenges. Indonesian Journal of Science and Technology, 8(1), 79–96. https://doi.org/10.17509/ijost.v8i1.52709

[6]Tandon, U. (2025). Informational Privacy in the Age of Artificial Intelligence: A Critical Analysis of India's DPDP Act, 2023. Legal Issues in the Digital Age, 6(2), 87–117. https://doi.org/10.17323/2713-2749.2025.2.87.117

does not offer remedies in relation to sets of non-personal data, including algorithms,[7] no dedicated deepfake criminalization statute exists, creating substantive enforcement gaps.

3. India's Legislative Framework: Mapping the Legal Terrain

3.1 The Information Technology Act, 2000

India's key cyber legislation, the IT Act 2000, predates the AI revolution by almost 2 decades. The key provisions affecting AI-related uses of data to infringe on privacy are contained in Sections 43A (civil liability for negligent use of sensitive personal data by a body corporate), 66C (identity theft—covers AI use of credentials), 66E (punishment for violation of privacy), and 72A (disclosure of information in breach of lawful contract). Although these provisions are useful for their operational purpose, they are not created with AI-specific threat models and do not offer the level of precision needed to regulate algorithmic processing, automated profiling or AI-generated synthetic media.[8]

3.2 The DPDP Act, 2023: A Landmark but Incomplete Statute

The DPDP Act, 2023 is the most comprehensive legislation in India in response to the governance of personal data. It has its salient features as: (i) consent is the primary rule, (ii) obligations on purpose limitation and data minimization, (iii) obligations on "Significant Data Fiduciaries" and the enhanced obligations, such as algorithmic auditing, (iv) adjudicatory mechanism of Data Protection Board (DPB) and (v) penalties of up to INR 250 crore per contravention.[9]

The DPDP Act, however, has significant gaps with regard to AI, such as its lack of a right to explanation and challenge in automated decision-making; its coverage of non-personal and aggregated data; and its lack of requirements for impact assessment when implementing high-risk AI applications. The Draft DPDP Rules, 2025 released by MeitY[10] have partially closed certain procedural gaps without providing substantive provisions for AI-governance in policies.

3.3 CERT-In Directives and Operational Cybersecurity

One of the shortest reporting windows in the world was put in place in the recent CERT-In (Information Security Practices and Procedures for Protected System) Rules, 2022, which mandated a 6-hour reporting period for cyber incidents. In May 2023, CERT-In issued a separate advisory on Adversarial Threats using Artificial Intelligence (AI),[11] and A new dedicated deepfake advisory, issued in November 2024. These are non-prescriptive, operational guidelines and thus do not have the force of law to systematically correct actions that infringe on the privacy rights of others.

[7]IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended in 2023. Rule 3(1)(b)(v) and Rule 3(2)(b) impose obligations on social media intermediaries to address AI-generated harmful content including deepfakes.

[10]MeitY (2025). Draft Digital Personal Data Protection Rules, 2025. Ministry of Electronics and Information Technology, Government of India. Released for public consultation in January 2025.

[11]CERT-In (2023). Advisory on Safety Measures to Minimize Adversarial Threats Arising from AI-Based Applications (May 2023). Ministry of Electronics and Information Technology, Government of India. CERT-In (2024). Advisory on Deepfake Threats (November 2024).

Table 1: India's Legislative Framework for AI and Data Privacy

Legislation	Year	Key Provisions (AI/Privacy)	Limitation w.r.t. AI
IT Act	2000 (Amended 2008)	Ss. 43A, 66, 66C, 66E — data protection, identity theft, privacy	No AI-specific provisions; pre-dates modern AI systems
SPDI Rules	2011	Sensitive personal data obligations on body corporates	Silent on automated/AI-driven processing
IT (Intermediary Guidelines) Rules	2021 / Amended 2023	Grievance redressal; deepfake takedown obligations	No algorithmic audit mandate; liability gaps for AI content
DPDP Act	2023	Consent-based processing; Significant Data Fiduciary (SDF) obligations; algorithmic audit for SDFs	Lacks automated decision-making rights; non-personal data excluded
CERT-In Rules	2022	Mandatory 6-hour breach reporting; AI advisory (May 2023)	No proactive AI risk framework; reactive approach

Source: Authors' compilation from primary legislative sources (2024–2025)

4. India's Cybersecurity Landscape: Empirical Evidence

The face of cyber threat in India has changed drastically with the advent of AI-powered attack vectors. The number of cybersecurity incidents reported under the CERT-In has increased from 53,117 in 2017 to nearly 1.32 million incidents in just 10 months of 2023, from January to October. According to the IBM Cost of a Data Breach Report, the average cost of a data breach in India has increased by 28% compared to 2020 to INR 179 million in 2023 and to an all-time high of INR 195 million in 2024.[12]

India alone saw 593 cyberattacks, 388 data breaches, 107 data leaks, and 39 ransomware incidents in the first half of 2024 alone.[13] The exfiltration of the records of approximately 815 million Indian citizens – Aadhaar numbers, passport details and COVID-19 test results – in the 2023 ICMR hack is particularly alarming and offers a prime example of the catastrophic potential of AI-assisted data exfiltration at a national scale.[14]

[12]IBM Security (2023). Cost of a Data Breach Report 2023 — India Results. IBM Corporation. Average cost of INR 179 million reported for India. IBM Security (2024). Cost of a Data Breach Report 2024. Average cost rose to INR 195 million (all-time high). Available at: https://in.newsroom.ibm.com

[13]Cyble Research and Intelligence Labs (2024). India Cyber Threat Landscape Report H1 2024: 593 cyberattacks, 388 data breaches, 107 data leaks, and 39 ransomware incidents reported in H1 2024. Available at: https://thecyberexpress.com/cybercrime-in-india-ncrb-report-2023-2025/

[14]ICMR Data Breach (2023): Approximately 815 million Indian citizens' data including Aadhaar numbers and COVID-19 test results was compromised. Reported by multiple cybersecurity firms and covered in Corbado Security Report (2025). Available at: https://www.corbado.com/blog/data-breaches-India

Table 2: Cybersecurity Incidents and Data Breach Costs in India (2020–2024)

Year	Cybersecurity Incidents (CERT-In)	Avg. Data Breach Cost (INR Mn)	Notable AI-Linked Incidents
2020	~11.58 Lakh	INR 140 Mn	AI-enabled phishing surge (COVID era)
2021	~14.02 Lakh	INR 157 Mn	Deepfake-based fraud; social engineering via chatbots
2022	~10.29 Lakh	INR 165 Mn	AIIMS ransomware attack; AI-automated credential theft
2023	~13.20 Lakh (Jan–Oct)	INR 179 Mn	ICMR breach (815 Mn records); AI deepfake frauds
2024	~22.68 Lakh	INR 195 Mn	Star Health breach (31 Mn records); AI-driven ransomware

Source: IBM Cost of a Data Breach Reports (2020–2024); CERT-In Annual Reports; Cyble Research Intelligence Labs (2024)

5. Comparative Analysis: India vs. Global Standards

A comparative legal study shows that there are huge differences between the regulatory regime in India and the gold standard regulatory system of European Union. The EU GDPR (Regulation 2016/679) provides for Data Protection Officers (DPOs) of qualifying entities, Data Protection Impact Assessments (DPIA) for high risk processing, and the right to explanation for automated decision making under Article 22. The EU AI Act 2024, the first comprehensive global governance framework for AI, introduces a risk-based classification framework with requirements for conformity assessment and post-market monitoring of high-risk AI systems.[15]

The vision of 'AI-for-All' was introduced in India by National Strategy for Artificial Intelligence (NITI Aayog, 2018) without going so far as to impose governing frameworks. At the GPAI Summit in New Delhi (2023), India has endorsed the OECD AI Principles.[16] Normative alignment with global standards is excellent, but operationalisation of the domestic legislation is still good.

[16]OECD (2019). Recommendation of the Council on Artificial Intelligence. OECD/LEGAL/0449. Organisation for Economic Co-operation and Development. https://doi.org/10.1787/9789264305519-en. India formally endorsed OECD AI Principles at the GPAI Summit, New Delhi, 2023.

Table 3: Comparative Analysis — EU GDPR, EU AI Act vs. India's Legal Framework

Parameter	EU GDPR (2016/679)	India DPDP Act 2023	India IT Act 2000
Right to Explanation (ADM)	Yes (Art. 22)	Absent	Absent
Algorithmic Audit Mandate	Yes (via DPA)	Only for SDFs	No
Data Breach Notification	72 hours (Art. 33)	Prescribed by Rules	6 hours (CERT-In)
Non-Personal / Aggregated Data	Covered under e-privacy	Not covered	Not covered
AI-Specific Regulation	EU AI Act 2024	None (in progress)	None
Max. Penalty	€20 Mn or 4% global turnover	INR 250 Crore per contravention	INR 5 Crore / imprisonment

Source: Authors' comparative analysis based on GDPR (2016/679), EU AI Act (2024/1689), IT Act 2000, and DPDP Act 2023

6. Key Challenges

6.1 Absence of Automated Decision-Making Rights

The IT Act and the DPDP Act do not give data principals the right to challenge, review or request a human override of decisions made by an automated system and which have a significant impact on them, such as those used by credit bureaus in credit denials, insurance providers in insurance refusal, and police bail officers in bail recommendations. This is an essential deficiency when compared to the GDPR's Article 22 and a big shortfall in the human rights aspect of the regulatory framework for AI in India.[17]

6.2 Governance of Non-Personal and Aggregated Data

The predictive abilities of AI models rely on the processing of aggregated data, each of which is anonymized, but can be de-anonymized through combination or inference attacks. The DPDP Act and SPDI Rules only cover personal data, meaning that this key component of AI systems is not covered by the law. The proposed Non-Personal Data (NPD) Governance Framework (2020) by India has not yet been made law, leading to a policy gap that is being filled by both domestic and foreign AI platforms.India's proposed Non-Personal Data (NPD) Governance Framework (2020) is still in the process of becoming law, which leaves a policy gap that is being filled by both domestic and foreign AI platforms.

6.3 Jurisdictional and Cross-Border Data Flow Challenges

The definition of AI systems is inherently global, as training data can come from various jurisdictions, data centres can be situated in third countries, and inference outputs can be delivered all over the world. The DPDP Act allows Central Government to limit cross-border data transfers to certain countries, but the list of countries has not been notified, nor have transfer safeguards been put in place. This leaves the companies

that want to use AI in their businesses with a cloud of uncertainty and foreign companies using AI in India without enforcement.[18]

6.4 Deepfakes and Synthetic Media Governance

The ability of generative AI to create hyper-realistic fake content brings new and profound risks for individuals' reputations, electoral integrity and national security. The IT Rules 2023 include content removal requirements for intermediaries, but the responsibility for AI Deepfakes created by the original producers is also unclear. Lack of any legal obligation for AI content watermarking or provenance authentication restrictions also means Indian law enforcement agencies lack robust forensics tools to trace and hold accountable harms created using deepfakes.[19]

6.5 Data Localization, Security, and AI Training Data Integrity

Ethical AI outputs start with ethical AI training data. Models trained on poisoned or manipulated training data can have wide-ranging discriminatory impacts. The EU AI Act takes action on the issue of training data governance, bias assessment, and integrity audits, which are covered in Article 10 data governance obligations for high-risk AI systems.However, while the EU AI Act addresses the issue of training data governance, bias assessment, and integrity audits, India's legal framework does not.

7. Reform Recommendations

From the doctrinal analysis and comparative benchmarking conducted above, the following recommendations for reform are put forward for the governance architecture for AI and data privacy in India:

7.1 Enact a Dedicated AI Regulation Act

There is a need for a comprehensive and equitable AI Regulation Act in India, based on the EU AI Act's proportionality principles, that extends beyond specific industries and caters to risk levels. Such legislation should: (i) Risk classify AI systems (unacceptable, high, limited, minimal); (ii) Put in place conformity assessment and technical documentation obligations for high-risk AI; (iii) Put in place human oversight obligations for consequential automated decisions; and (iv) Create a National AI Regulatory Authority with adjudicatory and enforcement powers.

7.2 Amend the DPDP Act to Incorporate AI-Specific Rights

The DPDP Act should be amended to include: (i) the right to explanation and human review for AI decisions that have a significant impact on data principals; (ii) require AI impact reports to be published by SDFs with accessible, easy-to-understand language; (iii) mandate that AI impact assessments be carried out prior to any high-risk deployment of AI; and (iv) extend data protection obligations to de-identified datasets used to train AI.

7.3 Legislate Non-Personal Data Governance

The Non-Personal Data Governance Framework should be made legally binding to: (i) govern the commercial use of community data; (ii) create data trusts to provide equitable access to community data; (iii) implement a prohibition on re-identification with criminal liability; and (iv) provide a framework of security requirements for aggregated dataset repositories.

[18]Duggal, P. (2025). Indian Organizations and Cybersecurity: Five Major Trends in 2025. CIO Magazine, April 29, 2025. Dr. Pavan Duggal, Advocate, Supreme Court of India and Expert in Cyber & AI Laws. Available at: https://www.cio.com/article/3973262

7.4 Criminalize Deepfakes and Mandate Content Provenance

A specific provision in the Bharatiya Nyaya Sanhita or a separate Deepfake Prevention Act must: (i) make the production and sharing of non-consensual synthetic media a crime; (ii) establish AI content watermarking using cryptographic provenance standards; and (iii) mandate AI platform operators to establish the detection and removal process by specified deadlines.

7.5 Strengthen CERT-In's AI Cybersecurity Mandate

CERT-In's advisory-driven framework needs to be complemented with mandatory regulations that include: (i) Annual adversarial robustness testing of AI systems in critical sectors; (ii) AI-specific incident response frameworks; and (iii) AI Threat Intelligence Centre within CERT-In for real-time monitoring of AI-driven cybersecurity threats.

8. Conclusion

As India strives to become a global AI superpower, its ability to establish a trusted AI governance framework is closely intertwined with this goal.Building a trusted AI governance framework is an integral part of India's quest to become a global AI superpower while respecting rights. The existing legal framework, which relies on a pre-AI statute and an AI-influenced, but still non-AI data protection law, is not up to the task of handling the multi-dimensional privacy issues created by AI systems. The increasing number of cyber incidents, the widespread use of AI deepfakes, the absence of governance for non-personal data, and the lack of automated decision-making rights all contribute to a structural deficit that threatens individual human dignity and the security of the nation.

These are all forward-looking, proportionate and coherent steps towards a governance framework for AI, ranging from a dedicated AI Act to amendments to the DPDP that include AI-specific rights, to non-personal data legislation, to the criminalization of deepfakes, to an empowered CERT-In. India has to take a legislative action, as in the age of AI, the absence of regulation is not a non-opinion, it is a policy choice that allows the governance space to be taken by AI systems without proper legal constraints, which hurts millions of data principals who have not yet had their digital rights adequately protected.

References

Statutes and Regulations

1. Information Technology Act, 2000 (No. 21 of 2000), as amended by the Information Technology (Amendment) Act, 2008 (No. 10 of 2009), India.

2. Digital Personal Data Protection Act, 2023 (No. 22 of 2023), Ministry of Electronics and Information Technology, India.

3. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (as amended 2023), India.

4. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, India.

5. CERT-In (Information Security Practices and Procedures for Protected System) Rules, 2022, Ministry of Electronics and Information Technology, India.

6. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). OJ L 119, 4.5.2016.

7. Regulation (EU) 2024/1689 of the European Parliament and of the Council (Artificial Intelligence Act). OJ L 2024/1689. https://doi.org/10.3000/OJL.2024.1689

Cases

8. Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCC 1 (Supreme Court of India).

9. Super Cassettes Industries Ltd. v. Hamar Television Network Pvt. Ltd. & Anr., (2011) 47 PTC 70 (Del.) (Delhi High Court).

Journal Articles and Books

10. Al-Khassawneh, Y.A. (2023). A Review of Artificial Intelligence in Security and Privacy: Research Advances, Applications, Opportunities, and Challenges. *Indonesian Journal of Science and Technology*, 8(1), 79–96. https://doi.org/10.17509/ijost.v8i1.52709

11. Malhotra, C. & Malhotra, U. (2024). Putting Interests of Digital Nagriks First: Digital Personal Data Protection (DPDP) Act 2023 of India. *Indian Journal of Public Administration*, 70(3). https://doi.org/10.1177/00195561241271575

12. Tandon, U. (2025). Informational Privacy in the Age of Artificial Intelligence: A Critical Analysis of India's DPDP Act, 2023. *Legal Issues in the Digital Age*, 6(2), 87–117. https://doi.org/10.17323/2713-2749.2025.2.87.117

13. Zenodo Conference Paper (2025). Reimagining Privacy in the Age of Artificial Intelligence: A Socio-Legal Analysis of India's Digital Personal Data Protection Act, 2023. International Conference, Dr. Ram Manohar Lohiya National Law University, Lucknow. https://doi.org/10.5281/ZENODO.17845100

Reports and Official Documents

14. IBM Security (2023). *Cost of a Data Breach Report 2023 — India Results*. IBM Corporation. Available at: https://in.newsroom.ibm.com

15. IBM Security (2024). *Cost of a Data Breach Report 2024 — India Results*. IBM Corporation. Average breach cost: INR 195 million. Available at: https://in.newsroom.ibm.com

16. CERT-In (2023, May). *Advisory on Safety Measures to Minimize Adversarial Threats Arising from Artificial Intelligence-Based Applications*. Ministry of Electronics and Information Technology, Government of India.

17. CERT-In (2024, November). *Advisory on Deepfake Threats and Protective Measures*. Ministry of Electronics and Information Technology, Government of India.

18. MeitY (2025, January). *Draft Digital Personal Data Protection Rules, 2025*. Ministry of Electronics and Information Technology, Government of India.

19. Government of India, Press Information Bureau (2025). *Curbing Cyber Frauds in Digital India*. PIB Note ID 155384. Available at: https://www.pib.gov.in

20. OECD (2019). *Recommendation of the Council on Artificial Intelligence*. OECD/LEGAL/0449. https://doi.org/10.1787/9789264305519-en

21. Cyble Research and Intelligence Labs (2024). *India Cyber Threat Landscape Report H1 2024*. Available at: https://thecyberexpress.com

22. Duggal, P. (2025). Indian Organizations and Cybersecurity: Five Major Trends in 2025. *CIO Magazine*, April 29, 2025. Available at: https://www.cio.com/article/3973262

23. CMS Law (2026). *AI Laws and Regulations in India: CMS Expert Guide*. Available at: https://cms.law/en/int/expert-guides/ai-regulation-scanner/india