283

Golden Jubilee
1974-2024

SHRI DHARMASTHALA MANJUNATHESHWARA LAW COLLEGE

CENTRE FOR POST GRADUATE STUDIES & RESEARCH IN LAW, MANGALURU- 575003
(NAAC Re-Accredited with B++ Grade, CGPA 2.9)
(Affiliated to Karnataka State Law University, Hubballi & Recognized by BCI, Delhi)
[Managed by: SDME Society ®]
Sponsored by: Shri Dharmasthala Manjunatheshwara Education Society, (R.) Ujire, D. K.

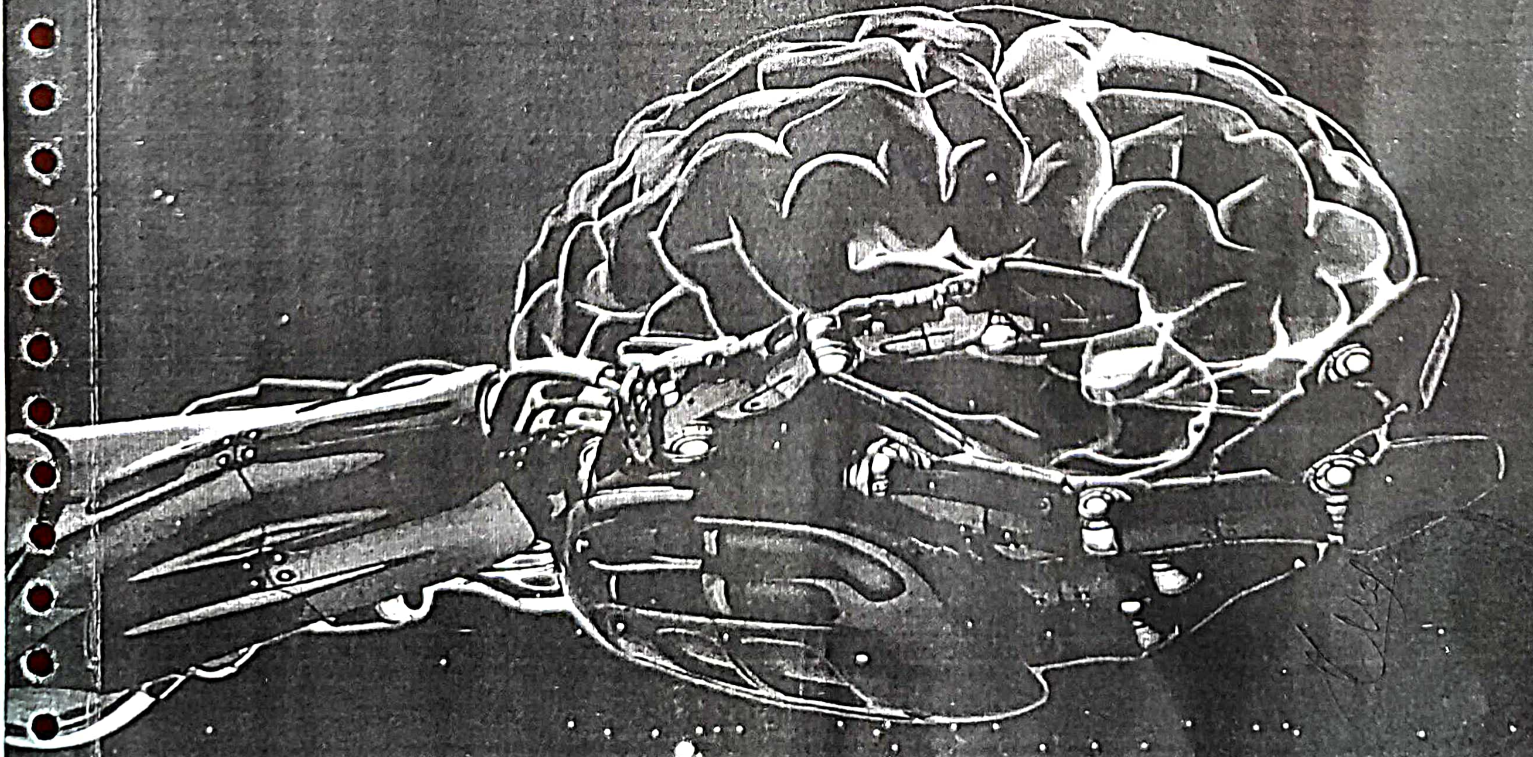
President: Dr. D. Veerendra Heggade

Conference Proceedings of One-Day National Seminar on

ARTIFICIAL INTELLIGENCE AND ITS IMPACTS ON IPR

(Peer Reviewed)

ISBN No.: 978-93-6135-950-7



284

Table of Contents

Title of the Article & Authors — *Page No*

Title of the Article & Authors *Page No*

* * * *

30.
286

UNBOXING RIGHT TO PRIVACY IN THE ERA OF ARTIFICIAL INTELLIGENCE

Mr. Karthik Anand *
Ms. Sreelakshmi S. N. *

Abstract

The widespread acceptance of Artificial Intelligence (AI) technology as a transformative solution to various challenges has significantly alleviated human suffering and workloads, ushering in a revolutionary shift in our operational methods. AI now serves as a guiding force for ethical practices across diverse sectors such as agriculture, health, education, and banking. While the adoption of AI technology is underway, questions about its universal deployment and safety linger, giving rise to ethical and legal concerns. The intersection of AI and cyberspace has particularly intensified issues related to privacy, contributing to a surge in cybercrimes. In India, AI is hailed as a pivotal catalyst for economic growth and regional development. This paper aims to explore the legal oversight of AI in India, emphasizing regulations pertaining to artificial intelligence and cyberspace, with a specific focus on the right to privacy and its implications for the nation's digital economy.

Keywords: ***Artificial Intelligence, Cyber-Space, Digital Economy, Right to Privacy, Ethical Practices, Legal Regulation, Adoption of AI Technology, Human Suffering Reduction, Revolutionary Change, Operational Methods, Sectoral Integration, Privacy Concerns, Cybercrimes, India, Economic Growth, Regional Development***

Introduction

Artificial intelligence (AI) is in its early stages of development in India, arriving relatively late due to the country's status as a developing nation. The advent of this technology can be attributed to the 21st-century technological advancements, spurred by the increased presence of social networking sites and investments from international multinational corporations in India, particularly in the field of research and development in artificial intelligence. This remarkable emerging technology operates based on the cognitive processes of human thinking. Presently, the global

* Assistant Professor in Law., SDM Law College, Mangaluru

** Law Student, Vth B.A.LL.B., SDM Law College, Mangaluru application of artificial intelligence is evident across various sectors of the economy, alleviating burdens and enhancing efficiency through smart technology[1].

Despite the significant strides in AI implementation, India currently lacks a comprehensive legal framework specifically tailored to artificial intelligence. However, it indirectly utilizes the Information Technology Act of 2000 for the control and governance of artificial intelligence applications. Notably, the government has recently passed the Data Protection Bill of 2019 to shape its digital governance framework and address privacy concerns related to data and cyberspace. This legislation will directly encompass the use of artificial intelligence, addressing associated ethical considerations.

1. Definition of Artificial Intelligence:

Artificial Intelligence (AI) is commonly defined as the branch of computer science that aims to create machines or systems capable of performing tasks that typically require human intelligence, such as learning from experience, understanding natural language, recognizing patterns, and solving complex problems.[2] .

Artificial Intelligence (AI) is the simulation of human intelligence in machines that are programmed to think and mimic human actions[3].

Artificial Intelligence (AI) is the field of computer science dedicated to creating systems capable of performing tasks that require human intelligence, such as visual perception, speech recognition, decision-making, and language translation[4].

The relationship between Artificial Intelligence (AI), digital governance, and privacy is intricate and multifaceted, involving both opportunities and challenges. Here's an exploration of how these concepts interconnect:

2. Relationship between Artificial Intelligence, Digital Governance, and Privacy

2.1. Data Collection and Surveillance:

AI systems often rely on vast amounts of data for training and improvement. This raises concerns about mass surveillance and the potential misuse of personal information.[5]

Key issues associated with data collection and surveillance in AI:

2.1.a Invasive Data Collection:

AI systems often require large volumes of data to train and improve their performance. The collection of such data may intrude into individuals' private lives, leading to concerns about the scope and invasiveness of information gathered.

[1] https://niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf

[2] Russell, S. J., &Norvig, P. (2010). Artificial Intelligence: A Modern Approach (p. 1). Pearson.

[3] Nilsson, N. J. (1998). Artificial Intelligence: A New Synthesis (p. 1). Morgan Kaufmann.

[4] Oole, D., Mackworth, A., & Goebel, R. (1998). Computational Intelligence: A Logical Approach (p. 1). Oxford University Press.

[5] Goodfellow, I., Bengio, Y., Courville, A., &Bengio, Y. (2016).Deep Learning.MIT Press.

2.1.b Lack of Informed Consent:

Individuals may not be fully aware of how their data is being used for AI applications. Lack of informed consent raises ethical questions about the right to privacy and autonomy.

2.1.c Surveillance Capitalism:

Some AI applications, especially in the commercial sector, contribute to the growth of surveillance capitalism, where user data is commodified for profit without adequate user control or compensation.

2.1.d Algorithmic Discrimination:

Biases in training data can result in discriminatory outcomes, especially in surveillance applications. Certain groups may be disproportionately targeted or unfairly treated, leading to social and ethical implications.

2.1.e Mass Surveillance and Government Control:

The use of AI in mass surveillance by governments can infringe on citizens' privacy rights and raise concerns about potential abuse of power and erosion of civil liberties.

2.1.f Privacy Erosion in Public Spaces:

AI-powered surveillance systems, such as facial recognition in public spaces, can erode the concept of anonymity and privacy in everyday activities, affecting individuals' freedom and rights.

2.1.g Data Security Risks:

The vast amounts of data collected for AI applications can become targets for cyberattacks, leading to potential breaches and compromise of sensitive information, further jeopardizing privacy.

2.1.h Unintended Consequences:

The deployment of AI in surveillance may lead to unintended consequences, such as false positives, misidentification, and other errors that can have severe repercussions on individuals falsely implicated.

2.1.j Lack of Transparency:

Many AI-driven surveillance systems operate as "black boxes," lacking transparency about the algorithms and decision-making processes. This opacity can hinder accountability and trust.

3. Indian Constitution and Right to Privacy

The recognition of the Right to Privacy as a Fundamental Right in India stems from the landmark Supreme Court judgment in Justice K. S. Puttaswamy (Retd.) vs. Union of India (2017[6]. In this historic ruling, the Court held that the right to privacy is intrinsic to the right to life and personal liberty guaranteed by Article 21 of the Indian Constitution. The judgment emphasized that privacy is a foundational value, essential for the enjoyment of other rights.

[6] Justice K. S. Puttaswamy (Retd.) vs. Union of India, (2017) 10 SCC 1

This constitutional recognition was a pivotal moment, affirming the individual's autonomy over personal data and protection from unwarranted state intrusion. The Court highlighted the dynamic nature of privacy in the digital age and acknowledged the need for a robust legal framework to safeguard this right. The judgment laid the groundwork for subsequent legislative developments, such as the drafting of the Personal Data Protection Bill, 2019[7]This judicial affirmation not only solidified privacy as an inherent and inviolable right but also set the stage for comprehensive legal measures to address evolving challenges in the digital era.

In India, the regulatory landscape for Artificial Intelligence (AI) is evolving, with a focus on data protection, privacy, and ethical considerations. Here's an overview with relevant laws and sections, along with footnotes for further reference:

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

In August 2023, the Indian Parliament approved the Digital Personal Data Protection (DPDP) Act, marking a significant milestone as the inaugural cross-sectoral legislation addressing personal data protection in India.

4.1 Section 3: Definition of Terms

Personal Data: Any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Sensitive Personal Data: Special categories of personal data that require additional protection due to their sensitive nature. This may include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation[8].

4.2 Applicability of DPDP Act 2023

The DPDP Act is applicable to both Indian residents and businesses involved in the collection of data from Indian residents. Notably, it extends its jurisdiction to non-citizens residing in India, whose data processing is linked to any activity associated with the offering of goods or services, even if such processing occurs outside India. For instance, this has implications for a U.S. citizen living in India who receives digital goods or services from a provider based outside India within the country.[9]

[6] Justice K. S. Puttaswamy (Retd.) vs. Union of India, (2017) 10 SCC 1

[7] Personal Data Protection Bill, 2019

[8] Section 3 of Personal Data Protection Bill, 2019

[9] Section 3 The Digital Personal Data Protection Act, 2023

The 2023 act permits the processing of personal data for any lawful purpose. The entity handling the data can proceed with processing either by obtaining the individual's consent or for "legitimate uses," a term elucidated in the legislation[10].

Consent must be given freely, specifically, informatively, unconditionally, and unambiguously with a clear affirmative action and for a particular purpose. The collected data must be limited to what is necessary for the specified purpose. Consumers must be provided with a clear notice containing these details, including the rights of the individual and the grievance redress mechanism. Individuals have the right to withdraw consent if it is the basis for data processing[11].

Legitimate uses encompass situations where an individual has willingly provided personal data for a specified purpose, the provision of subsidies, benefits, services, licenses, certificates, or permits by any agency or department of the Indian state if the individual has previously consented, sovereignty or security reasons, fulfilling a legal obligation to disclose information to the state, compliance with judgments, decrees, or orders, responding to medical emergencies, threats to life, epidemics, threats to public health, and disaster or breakdown of public order[12].

The DPDP Act also establishes rights and obligations for individuals, including the right to a summary of all collected data, knowledge of the identities of data fiduciaries and processors with whom the data has been shared, and the right to correction, completion, updating, and erasure of their data. Additionally, individuals have the right to redress grievances and the ability to nominate persons to receive their data.

Entities responsible for digital personal data, known as data fiduciaries, have defined obligations, such as maintaining security safeguards, ensuring the completeness, accuracy, and consistency of personal data, reporting data breaches to the Data Protection Board of India (DPB), erasing data upon consent withdrawal or the expiry of the specified purpose, appointing a data protection officer, and obtaining the mandatory consent of parents or guardians for children/minors[13].

While the 2023 act retains broad categories of obligations, it differs from the 2019 bill by removing the scope for the regulator, the DPA, to make detailed regulations on these obligations. The law introduces a new category of data fiduciaries known as significant data fiduciaries (SDFs) with additional obligations, including appointing a data protection officer and conducting data protection impact assessments.

The 2023 law revises the stance on data localization, allowing the government to restrict data flows to certain countries for national security purposes. Exemptions from consent and notice requirements, as well as other obligations, are provided in specific cases, such as processing necessary for enforcing legal rights, personal data processing by courts or tribunals, and processing the personal data of non-Indian residents within India.

[10] Section 4, The Digital Personal Data Protection Act, 2023,

[11] Ibid., Section 7(b)

[12] ibid., Sections 11-14

[13] Section 17(1) The Digital Personal Data Protection Act, 2023

The law also grants complete exemptions for certain purposes and entities, including data processing in the interests of India's sovereignty and integrity, security of the state, and public order. The government has the authority to exempt specific classes of data fiduciaries, including startups, from certain provisions. However, a concerning provision allows the government wide discretionary power to declare exemptions from the law for specific data fiduciaries or classes of data fiduciaries, without clear guidance on the basis, categories, and duration of such exemptions.

4.3 How Well Does the DPDP Act, 2023, protect Privacy?

The 2023 Act establishes India's inaugural data privacy law, necessitating the acquisition of consent prior to the processing of personal data and outlining specific exceptions. It grants consumers the right to access, correct, update, and erase their data, along with the right to nomination. Additionally, the law introduces enhanced safeguards for the processing of children's data. For businesses, it imposes purpose limitations, obligations to provide notice of data collection and processing, and mandates security safeguards. The legislation also mandates businesses to establish grievance redress mechanisms. Complaints and grievances will be handled by the Data Protection Board (DPB), which is empowered to issue penalties for noncompliance with the law.Hence, India now possesses a legal framework for data protection, marking a significant milestone. The existence of this law is expected to gradually establish basic standards of behavior and compliance among businesses engaged in data collection. In this context, the government's approach to implementing and enforcing the law becomes a critical factor, raising questions about whether the focus will be primarily on data-heavy businesses or extend across the entire economy.

The exceptions outlined for consent in the first place grant the state significant empowerment, placing state imperatives on a distinct level compared to private entities. While this may be genuinely justified in certain circumstances, such as disasters or emergencies, the law broadens the scope of these situations. Specifically, Section 7(b) of the law allows the government to bypass consent requirements when a government service beneficiary has previously agreed to receive any other benefit from the state. While this may streamline access to the personal data of beneficiaries for obtaining government services, it also introduces the potential for the government to aggregate databases. The true utilization of this provision would necessitate exempting government agencies from purpose limitations that mandate the deletion of personal data after the intended purpose has been fulfilled.

Another instance of this is the set of exemptions granted to the state for investigative, prosecutorial, and national security purposes. Section 17(1)(c) of the law exempts notice and consent requirements, among others, for processing related to the "prevention, detection, investigation or prosecution of any offence or contravention of any law." While understandable, Section 17(2)(a) subsequently provides a blanket exemption from the entire law for any government agency notified by the government.

in the interests of sovereignty, security, integrity, public order, and preventing incitement. Given that Section 17(1)(c) already exists, Section 17(2)(a) implies Parliament's desire to ensure a complete non-application of data protection law to certain state agencies[14].

Provisions like these establish a separate category of activity beyond the purview of data privacy requirements. It is problematic that the Indian state is not subject to many of the constraints applicable to private entities, especially when there is no pressing requirement for such an exception.

Secondly, the discretionary rule-making powers the government holds under the law could, in some cases, undermine the protections provided. For instance, under Section 17(5), the government has the authority to declare that certain provisions of this law will not apply to any business or class of businesses within five years of the law's commencement. There is no timeframe for the operation of this exemption or any guidance on its utilization. While an optimistic interpretation suggests it could provide time for compliance by sunrise industries or startups, Section 17(3) already addresses such exemptions. Consequently, Section 17(5) could potentially be used to defeat the law's purpose. It's essential to note that the law only restricts the government's power to grant these exemptions for an initial five-year period, without providing a limit on their potential duration.[15]

Similarly, the government possesses unguided rule-making powers for exempting businesses from specific requirements regarding the processing of children's data. Sections 9(1) to 9(3) outline certain requirements, including parental consent and prohibitions on profiling. Section 9(4) enables the government to exempt any business or class of businesses from Sections 9(1) to 9(3) "subject to such conditions, as may be prescribed." This provision lacks clarity on the grounds for granting exemptions, determining conditions, and more. Due to this lack of sufficient guidance, this provision is susceptible to misuse.

[14] See, for example, A.N. Parasuraman etc. v. State of Tamil Nadu [SCC (4) 683, 4 Supreme Court Cases 683, Supreme Court of India, 1989]; Agricultural Market Committee v. Shalimar Chemical Works Ltd. [Supp. (1) SCR 164, Supp. (1) Supreme Court Reporter 164, Supreme Court of India, 1997]. In this case, the court observed that "the essential legislative function consists of the determination of the legislative policy and the Legislature cannot abdicate essential legislative function in favor of another..... The Legislature should, before delegating, enunciate either expressly or by implication, the policy and the principles for the guidance of the delegates." See also I.P. Massey, "Chapter 4" in Administrative Law, 10th ed. (Lucknow: Eastern Book Company, 2022), 94-104.

[15] See, for example, Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians, Ministry of Electronics & Information Technology, Government of India, July 27, 2018, 3,https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf: "The EU, at the vanguard of global data protection norms has recently enacted the EU GDPR, which has come into force on 25 May 2018.... It is a comprehensive legal framework.... It is both technology and sector-agnostic and lays down the fundamental norms to protect the privacy of Europeans. . . . We are informed that 67 out of 120 countries outside Europe largely adopt this framework or that of its predecessor."

While other provisions grant the government powers to prescribe conditions and make substantive rules, the examples highlighted above provide minimal guidance. This is problematic when considered against the principles of Indian administrative law, which requires that laws should not confer unguided and excessive discretion on the implementing authority. If misused, such legal provisions have the potential to violate the Indian Constitution.

Thirdly, the design of the DPB is problematic. The board is an independent agency with a limited mandate, and the government will establish mechanisms for selecting and appointing its members. While the law outlines qualifications for members, it does not specify the number of members on the board and only requires one of them to be a legal expert. This is problematic since one of the board's main functions is to issue penalties and directions for noncompliance.

Additionally, the chairperson of the DPB is empowered to authorize any board member to perform "any of the functions of the board and conduct any of its proceedings." There is a possibility that the chairperson may not authorize the legal member of the board to conduct proceedings leading up to the issuance of a penalty. This design lacks an internal separation of functions between members conducting inquiries and the chairperson, potentially compromising impartiality in all cases.

Therefore, while the DPDP Act introduces data privacy protections in law for the first time, certain provisions in the law have the potential to undermine its benefits if the government does not act under them in the most scrupulous manner possible[16].

5. NITI Aayog's AI Policy: NITI Aayog released the "National Strategy for Artificial Intelligence" in 2018, providing policy recommendations. Relevant aspects include ethical AI development and responsible use.[17]

5.1 Ethical AI Development: NITI Aayog likely emphasizes the need for ethical considerations in AI development, including fairness, transparency, and accountability.

5.2 Responsible AI Use: The policy may advocate for responsible AI deployment, ensuring that AI technologies benefit society while minimizing negative impacts.

[16] See, for example, Axel Voss, "Fixing the GDPR: Towards Version 2.0," EPP Group in the European Parliament, May 25, 2021, https://www.axel-voss-europa.de/wp-content/uploads/2021/05/GDPR-2.0-ENG.pdf; Daniel Mikkelsen et al., "GDPR compliance since May 2018: A continuing challenge," McKinsey & Company, July 22, 2019,https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/gdpr-compliance-after-may-2018-a-continuing-challenge; Martin Brinnen and Daniel Westman, What's wrong with the GDPR? Description of the challenges for business and some proposals for improvement, SvensktNaringsliv - Swedish Enterprise, December 2019,https://www.svensktnaringsliv.se/material/skrivelser/xf8sub_whats-wrong-with-the-gdpr-webbpdf_1005076.html/What%27s+wrong+with+the+GDPR+Webb.pdf; Ilse Heine, "3 Years Later: An Analysis of GDPR Enforcement," Strategic Technologies Blog, Center for Strategic & International Studies, September 13, 2021, https://www.csis.org/blogs/strategic-technologies-blog/3-years-later-analysis-gdpr-enforcement; Alec Stapp, "Against Privacy Fundamentalism in the United States," Niskanen Center, November 19, 2018, https://www.niskanencenter.org/against-privacy-fundamentalism-in-the-united-states/.

[17] NITI Aayog."National Strategy for Artificial Intelligence." 2018.

5.3 Capacity Building: NITI Aayog may stress the importance of building national capabilities in AI through education, research, and skill development.

5.4 Public-Private Collaboration: The policy might encourage collaboration between the public and private sectors to foster innovation and address societal challenges.

5.5 Regulatory Framework: There may be recommendations for establishing a regulatory framework to govern the development and deployment of AI technologies.

5.6 Data Privacy and Security: Ensuring data privacy and security in AI applications may be a crucial aspect of the policy, aligning with broader data protection principles.

5.7 International Collaboration: The document may highlight the importance of engaging with the global AI community, participating in international collaborations, and staying abreast of global AI developments.

6. Telecom Regulatory Authority of India (TRAI):

TRAI has explored regulatory aspects related to AI in the telecommunications sector. It has considered the impact of AI on data privacy and consumer rights.

6. Evolving Legislative and Regulatory Frameworks in India

To ensure the secure utilization and implementation of AI systems, it is imperative to establish regulatory standards and processes at both the international and national levels, particularly in the case of India. The development of many AI systems in advanced nations and their deployment in developing countries raises concerns about whether these systems have undergone thorough assessments for safe integration into significantly different contexts. Emphasizing this need for comprehensive evaluation, India's Working Document Towards Responsible AI for All, formulated by NITI Aayog, envisions India as a potential hub for AI development, producing solutions that can be deployed in other emerging economies, constituting 40% of the world.

The Constitution of India guarantees fundamental rights, encompassing the individual's entitlement to equality, privacy, and freedom of speech and expression, among other rights. These constitutional safeguards are specifically designed to address historical and cultural nuances, preventing various forms of discrimination. However, the incorporation of AI systems has the potential to encroach upon several of these constitutionally enshrined fundamental rights.Therefore, as nations like India formulate regulatory frameworks to oversee the adoption and implementation of AI systems, it becomes crucial to prioritize the following considerations[18].

6.1. Elevating the Standard of Accountability for Government or Public Sector Implementation of AI Systems: Nations should contemplate establishing a more

[18] Jhalak M. Kakkar and Nidhi Singh, "Building an AI governance framework for India", available at https://ccgnludelhi.wordpress.com/2020/09/18/building-an-ai-governance-framework-for-india/ last visited on 5.02.2024

stringent regulatory criterion for the deployment of AI by government entities, acknowledging the profound impact such systems can have on citizens' rights. Instances of government utilization of AI, especially in the distribution of public benefits, surveillance, and law enforcement, warrant heightened scrutiny due to their potential to significantly influence fundamental rights of the populace[19].

6.2. Imperative for a Comprehensive Principles-Based AI Regulatory Framework: Presently, various sectoral regulators are formulating regulations tailored to address specific challenges, including privacy concerns, posed by AI within their domains. While leveraging the expertise of sector-specific regulators and promoting the establishment of regulations tailored to individual sectors is crucial, a fragmented development of AI principles may ensue. To guarantee a cohesive and consistent approach to AI regulation across diverse sectors, it becomes essential to implement a national-level, horizontal overarching framework based on fundamental principles.[20]

6.3 Tailoring Sector-Specific Regulations for Effective AI Oversight: Beyond a comprehensive regulatory framework serving as the foundation for AI regulation, it is equally essential to anticipate the integration of this framework with specific sectoral laws, such as consumer protection, product liability, and personal data protection. Traditional structures of consumer protection and product liability regulations, often based on fault-centric claims, face challenges when applied to AI systems, given issues related to explainability and transparency in decision-making. Establishing the presence of defects in AI products and providing evidence for harm may be intricate for individuals seeking legal recourse. Consequently, consumer protection laws may necessitate adjustments to remain pertinent in the context of AI systems. Additionally, sector-specific legislation, including regulations governing motor vehicles, would require adaptation to facilitate and oversee the deployment of autonomous vehicles and other AI-based transport systems.

6.4. Adapting AI Systems for Safe Development and Deployment: Ensuring the efficient and secure utilization of AI systems necessitates their meticulous design, customization, and training with pertinent datasets tailored to the specific deployment context. The Working Document envisions India as a global hub for AI innovation. Furthermore, India is likely to import AI systems developed in countries such as the US, EU, and China for deployment within its own context[21]. In both scenarios, AI systems operate in environments distinct from their development origins. Failure to appropriately contextualize socio-technical systems like AI to their deployment environments raises heightened concerns regarding safety, privacy, accuracy, and reliability.

[19] https://vidhilegalpolicy.in/blog/indias-tryst-with-predictive-policing last visited on 05.02.2024

[20] See Reserve Bank of India, 'Report of the Working Group on FinTech and Digital Banking' (November 2017) available at https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/WGFR68AA1890D7334D8F8F72CC2399A27 01.01.2024

[21] NitiAayog, Working Document: Towards Responsible AI for All (2020), available at https://niti.gov.in/sites/default/files/2020-07/Responsible-AI.pdf last visite on 02.02.2024

Given this scenario, there is a critical necessity to focus on the formulation of international norms and domestic regulations. These measures are essential to facilitate the safe utilization and deployment of AI systems that originate in diverse contexts, ensuring they align seamlessly with the unique circumstances of their deployment locations.

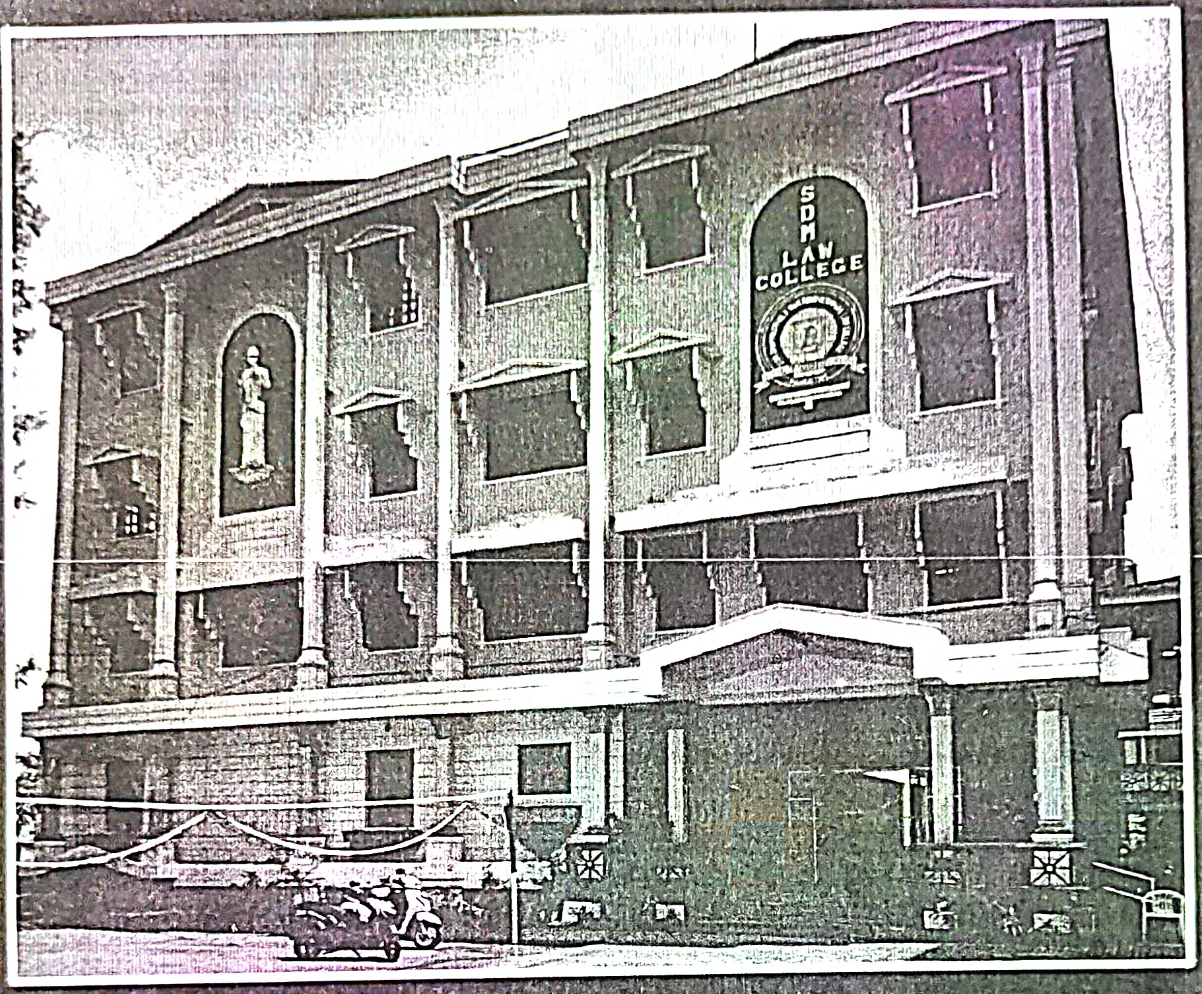
Conclusion

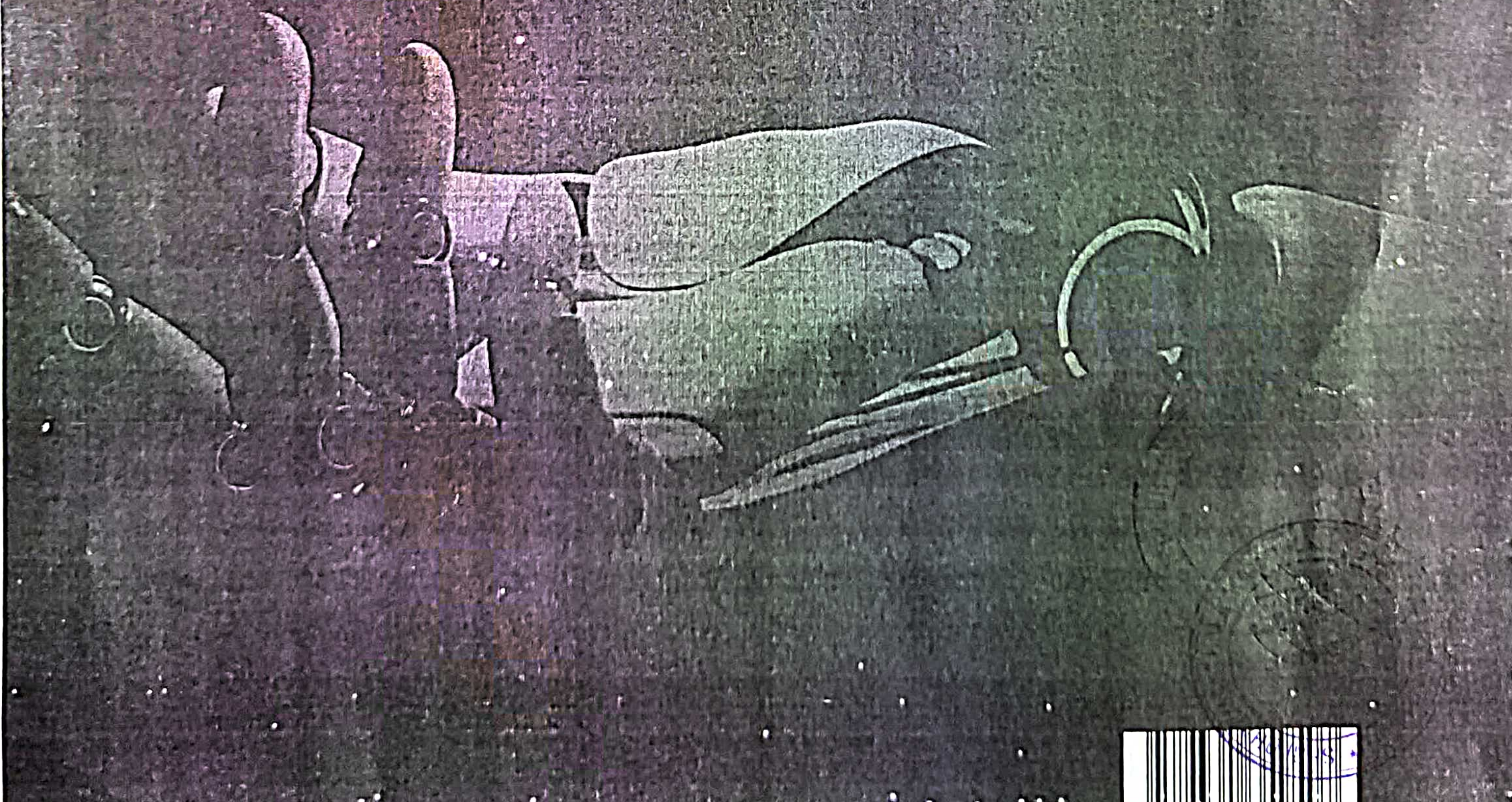
In navigating the future landscape shaped by artificial intelligence, safeguarding the right to privacy becomes non-negotiable. While AI holds transformative potential across various domains, its advancement raises pressing ethical and privacy considerations. It is imperative for governments, businesses, and individuals to comprehend the paramount importance of upholding privacy rights amidst the opportunities presented by AI.

Ensuring that AI progress aligns with individuals' right to privacy mandates the implementation of robust checks and balances, integrating privacy safeguards into AI development practices, and fostering increased transparency and accountability. Elevating the significance of privacy becomes pivotal in striking a harmonious equilibrium between technological advancement and the preservation of fundamental human rights. This concerted effort paves the way for a future where AI is harnessed ethically and responsibly, ultimately benefiting society at large.

* * * *

297





9 789361 359507

Price: Rs. 250/