

***Law Audience Journal, Volume 6 & Issue 2, 10th Nov 2025,
e-ISSN: 2581-6705, Indexed Journal, Impact Factor 5.954, Published at
<https://www.lawaudience.com/volume-6-issue-2/>, Pages: 124 to 142,***

***Title: Regulating Artificial Intelligence in India: Issues and Challenges,
Authored By: Prashant Kaundal (LL.M, Research Scholar) & Co-Authored By
Dr Gaurav Khanna (Associate Professor of Law), University Institute of
Legal Studies (UILS), Chandigarh University Gharuan, Mohali, Punjab, India-
140413,
Email ID: 9736pkaundal@gmail.com.***



Cite this article as:

PRASHANT KAUNDAL & DR. GAURAV KHANNA, “*Regulating Artificial Intelligence in India: Issues and Challenges*”, Vol.6 & Issue 2, Law Audience Journal (e-ISSN: 2581-6705), Pages 124 to 142 (10th Nov 2025), available at <https://www.lawaudience.com/regulating-artificial-intelligence-in-india-issues-and-challenges/>.

***Title: Regulating Artificial Intelligence in India: Issues and Challenges,
Authored By: Prashant Kaundal (LL.M, Research Scholar) & Co-Authored By
Dr Gaurav Khanna (Associate Professor of Law), University Institute of
Legal Studies (UILS), Chandigarh University Gharuan, Mohali, Punjab, India-
140413,
Email ID: 9736pkaundal@gmail.com.***

|Copyright © 2025 By Law Audience Journal|

(E-ISSN: 2581-6705)

All Copyrights are reserved with the Authors. But, however, the Authors have granted to the Journal (Law Audience Journal), an irrevocable, non-exclusive, royalty-free, and transferable license to publish, reproduce, store, transmit, display, and distribute it in the Journal or books or in any form and all other media, retrieval systems and other formats now or hereafter known.

No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other non-commercial uses permitted by copyright law.

For permission requests, write to the publisher, subject of the email must be "Permission Required" at the email addresses given below.

**Email(s): lawjournal@lawaudience.com, info@lawaudience.com,
lawaudience@gmail.com.**

Phone (No(s)): +91-8351033361,

Website: www.lawaudience.com.

Facebook: www.facebook.com/lawaudience.

Instagram: www.instagram.com/lawaudienceofficial.

Contact Timings: 10:00 AM to 8:00 PM.

***Title: Regulating Artificial Intelligence in India: Issues and Challenges,
Authored By: Prashant Kaundal (LL.M, Research Scholar) & Co-Authored By
Dr Gaurav Khanna (Associate Professor of Law), University Institute of
Legal Studies (UILS), Chandigarh University Gharuan, Mohali, Punjab, India-
140413,
Email ID: 9736pkaundal@gmail.com.***

Disclaimer:

Law Audience Journal (e-ISSN: 2581-6705) and Its Editorial Board Members do not guarantee that the material published in it is 100 percent reliable. You can rely upon it at your own risk. But, however, the Journal and Its Editorial Board Members have taken the proper steps to provide the readers with relevant material. Proper footnotes & references have been given to avoid any copyright or plagiarism issue. Articles published in **Volume 6 & Issue 2** are the original work of the authors.

Views or Opinions or Suggestions (if any) expressed or published in the Journal are the personal points of views of the Author(s) or Contributor(s) and the Journal & Its Editorial Board Members are not liable for the same.

While every effort has been made to avoid any mistake or omission, this publication is published online on the condition and understanding that the publisher shall not be liable in any manner to any person by reason of any mistake or omission in this publication or for any action taken or omitted to be taken or advice rendered or accepted on the basis of this work.

All disputes are subject to the exclusive jurisdiction of Courts, Tribunals and Forums at India only.

***Submit your article(s) for Publications at lawaudience@gmail.com, or
lawjournal@lawaudience.com, with subject as "Submission of Paper(s)
for Publication in Law Audience Journal".***

***Title: Regulating Artificial Intelligence in India: Issues and Challenges,
Authored By: Prashant Kaundal (LL.M, Research Scholar) & Co-Authored By
Dr Gaurav Khanna (Associate Professor of Law), University Institute of
Legal Studies (UILS), Chandigarh University Gharuan, Mohali, Punjab, India-
140413,
Email ID: 9736pkaundal@gmail.com.***

Publisher Details:

Law Audience Journal (e-ISSN: 2581-6705),

*Sole Proprietorship of Mr. Varun Kumar, Kharar, District.
S.A.S, Nagar, Mohali, 140301,*

Phone No(s): +91-8351033361 (WhatsApp),

**Email ID(s): lawjournal@lawaudience.com,
info@lawaudience.com or lawaudience@gmail.com.**

Website: www.lawaudience.com.

Contact Timings: 10:00 AM to 8:00 PM.

Editor(s):

- *Dr. Amit Yadav, Editor-In-Chief at Law Audience Journal, Associate Professor (Senior Scale) at School of Law, Manipal University Jaipur.*
- *Adv. Varun Kumar, Founder-CEO-Owner-Publisher-Publishing Editor at Law Audience Journal.*

Editorial Board Members Details Are Available At:

<https://www.lawaudience.com/editorial-board-members/>.

*Title: Regulating Artificial Intelligence in India: Issues and Challenges,
Authored By: Prashant Kaundal (LL.M, Research Scholar) & Co-Authored By
Dr Gaurav Khanna (Associate Professor of Law), University Institute of
Legal Studies (UILS), Chandigarh University Gharuan, Mohali, Punjab, India-
140413,
Email ID: 9736pkaundal@gmail.com.*

OUR INTELLIGENCE IS WHAT MAKES US HUMAN, AND AI IS AN EXTENSION OF THAT QUALITY—Yann LeCun.....

ABSTRACT:

Artificial Intelligence (AI) holds transformative potential for India's ambition of inclusive economic growth, reflected in the 'AI for All' strategy. However, the rapid, largely unregulated deployment of AI systems across critical sectors like law enforcement, finance, and healthcare presents profound ethical, legal, and social challenges. This paper critically examines India's emerging, non-statutory 'Innovation over Restraint' regulatory model, contrasting it with the comprehensive, risk-based approach of the European Union's AI Act. It scrutinizes the limitations of existing Indian legal safeguards, particularly the Digital Personal Data Protection (DPDP) Act, 2023, and the constitutional protections under Articles 14, 19, and 21, in addressing AI-specific harms like algorithmic bias and lack of transparency. The study concludes by proposing a rights-based, graded-risk regulatory framework for India, advocating for new institutional mechanisms—such as an independent AI Governance Group (AIGG) and an AI Safety Institute (AISI)—to ensure the accountable, fair, and trustworthy integration of AI with constitutional values.

Keywords: Artificial Intelligence, AI regulation in India, Technology Law, Data Protection, Algorithmic biases, Policy Analysis.

I. INTRODUCTION:

Artificial Intelligence is only one of many roles AI is now playing in the modern world, where technology increases at a previously unknown rate. But not only that, AI also raised some privacy concerns, specifically individual identity protection. AI-powered platforms and systems are reliant on large amounts of personal data; often the information shared can be highly sensitive and identifiable. As a result, current interest in data security is also pushing for more emphasis on protecting individual identities in the age of AI. In the era of fast-moving AI

technology, the definition of collecting, storing, and utilizing personal data has changed. Facial recognition systems that make people recognizable in public spaces or predictive algorithms that follow people's shopping behavior are some examples of how AI today is empowering a degree of surveillance and data gathering never seen before. However, because of these advances, personal data has become more vulnerable to risk. As such, identity protection is thus crucial not only for privacy but also for personal autonomy and human dignity in digital environments. **AI systems** that work with biometric data, unique identifiers, and other personal information force critical questions about consent, data ownership, and the possibility of identity theft or misuse that require comprehensive legal frameworks to regulate these technologies.¹ **Artificial Intelligence (AI)** has emerged as one of the most transformative technologies of the twenty-first century, reshaping the way governments, industries, and societies function. From algorithmic decision-making in governance to autonomous systems in healthcare, finance, and education, AI's influence has become pervasive. India, with its vast digital infrastructure, thriving IT sector, and demographic advantage, stands at the threshold of an AI-driven revolution. **According to NITI Aayog's National Strategy for Artificial Intelligence (2018)**, AI holds the potential to act as a "force multiplier" for inclusive growth, particularly in critical sectors such as agriculture, education, healthcare, and smart cities. However, with this transformative potential comes the equally significant responsibility to regulate AI systems in a manner that ensures ethical use, accountability, and protection of individual rights. Unlike many jurisdictions that have already taken legislative steps—such as the **European Union's Artificial Intelligence Act (2024)**—India does not yet possess a comprehensive legal framework governing AI. Current Indian laws like the **Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023 (DPDP Act)**, provide only indirect and limited coverage to AI-related issues. The IT Act primarily addresses cybercrimes, intermediary liability, and data misuse, while the DPDP Act regulates personal data processing and protection. Neither statute explicitly defines or governs algorithmic

¹ Asha Verma, "The Implications of AI on Privacy and Security", 5 International Journal of Cyber Ethics 102 (2022).

decision-making, bias mitigation, explainability, or the liability arising from autonomous systems. This lacuna has prompted increasing debate among policymakers, jurists, and scholars on the urgent need for a dedicated AI regulatory framework. **The Ministry of Electronics and Information Technology has**, in recent years, issued several advisories and draft rules to address AI-related challenges such as synthetic media, deepfakes, and the obligations of online intermediaries in curbing AI misuse. While these efforts indicate growing governmental attention, they remain fragmented and lack a unified legislative backbone. The absence of a central AI law creates uncertainty in accountability when AI systems cause harm—such as wrongful credit denial, discriminatory hiring, or privacy violations—since it is often unclear whether liability should rest with the developer, deployer, or data controller.

Furthermore, AI poses profound ethical and constitutional challenges in India's rights-based legal system. Algorithmic bias may infringe the right to equality under **Article 14, opaque decision-making could undermine procedural fairness under Article 21**, and invasive data collection threatens the right to privacy, as recognized in **Justice K.S. Puttaswamy (Retd.) vs. Union of India**². The Supreme Court, in this landmark judgment, held that privacy is intrinsic to the right to life and personal liberty—an interpretation that extends to algorithmic surveillance and data-driven profiling. Therefore, the regulation of AI is not merely a question of technology management but a constitutional imperative. At the global level, organizations such as **UNESCO and the Organisation for Economic Cooperation and Development (OECD)** have emphasized the need for humancentric and rights-based AI governance. **UNESCO's Recommendation on the Ethics of Artificial Intelligence (2021)**—adopted by nearly 200 countries, including India—advocates transparency, accountability, and the prevention of algorithmic discrimination. **Similarly, the OECD AI Principles (2019)** promote fairness, safety, and international collaboration in AI regulation. These international norms provide valuable guidance for India as it formulates its own national AI governance model. In

² (2017). 10 S.C.C.

recent years, incidents involving AI-generated deepfakes and misinformation have raised public and legal alarm. A 2025 Reuters report highlighted India's proposal to mandate labeling of AI-generated content to prevent misuse during elections and on social media platforms. Such regulatory initiatives are crucial but reactive; India needs a proactive, comprehensive, and risk-based framework that balances innovation with protection of individual and societal interests. In this context, the present study aims to examine the regulatory landscape of AI in India, identify the pressing issues and challenges, and propose a coherent legal and policy framework for responsible AI governance. The objective is not merely to regulate technology but to ensure that technological progress aligns with the rule of law, constitutional values, and human dignity.

II. DEFINITIONS:

The legal discourse on identity protection cannot but articulate a clear understanding of key concepts first, for each term embodies complex conception-shaped legal implications. This discussion covers the foundational concepts of identity protection, artificial intelligence, and the domains of cybersecurity and privacy. However, each term saw a different set of crucial dimensions for the then-emerging regulatory and ethical landscape around AI technologies. Identity protection is the practice of protecting personal data or preventing unauthorized access, misuse, or disclosure of it. Today, in the era of this digital transformation, personal data is being collected, processed, and stored on an unprecedented scale, and this concept has become more important. Within the scope of AI, the need to ensure identity protection is exceptionally high because AI systems work with huge amounts of information, including personal data that can be individually identified. Concerning legal frameworks to protect identity, provisions for the protection of identity become focused on the safeguarding of personal information from practices of identity theft and of third parties from unauthorized access. For instance, in India, The "*Digital Personal Data Protection Act, 2023*", requires consent and transparency in data processing practices and prohibits the processing of personal data where there is no reason for such processing, to protect these individuals by mandating that data is collected and used in a way consistent with principles of purpose limitation and data minimization. When safety and

alter flow merge, it enables us to access a given product or service without endangering our security. Mechanisms to protect identity include authentication protocols, encryption standards, and access control measures, all of which protect access to data by limiting data access to authorized entities. In addition, identity protection encompasses more than just physical or digital security protections but instead encompasses a holistic view of privacy and data subject rights, including informed consent. In the AI era, the aggregation of data can produce an all-encompassing digital footprint of an individual, which opens her to the risk of profiling, discrimination, and emotional or psychological harm. They are legal provisions that are thus necessary to protect the inherent identity of the individuals to prevent exploitation and make the functioning of the AI-based system accountable and within the ambit of respect for the privacy of the individual.³ AI is a field of technology that develops machines that process information, learn from experience, and reproduce that learning to perform tasks that historically require human intervention. AI includes a range of technologies, such as machine learning, natural language processing, and computer vision, and all of this work together to provide the ability of a machine to learn, reason, and make decisions autonomously. With AI advancements moving at breakneck speed, we are experiencing a paradigm shift across industries where machines can now understand huge data sets, recognize patterns, and run complex tasks incredibly efficiently. Yet, as AI is more and more embedded in our digital and physical lives, the ethical, social, and legal ramifications of this technology need to be closely examined, especially in terms of privacy and defense of identity. Regulating the scope and limitations of data usage is of great importance for legal systems in this regard. Because of the capabilities of AI, such challenges present unique challenges. For example, systems driven by AI are now able to process and analyze personal data at a scale and pace that is beyond human capability, which ultimately raises the concern of surveillance and data profiling. In *Carpenter vs. United States*⁴, the U.S. Supreme Court acknowledged that technology poses a threat to privacy rights by declaring that accessing cell phone location data without a warrant

3. Kriti Agarwal, "Defining Identity in Digital Environments", 2 Journal of Digital Security Studies 63 (2020).

⁴ 585 U.S. 296.

***Title: Regulating Artificial Intelligence in India: Issues and Challenges,
Authored By: Prashant Kaundal (LL.M, Research Scholar) & Co-Authored By
Dr Gaurav Khanna (Associate Professor of Law), University Institute of
Legal Studies (UILS), Chandigarh University Gharuan, Mohali, Punjab, India-
140413,
Email ID: 9736pkaundal@gmail.com.***

constitutes an invasion of privacy. These sorts of cases bring into question the need for a balance between how useful AI can be and the rights of the individual and how AI operates as something within ethical and legal bounds to respect the autonomy and identity of data subjects. In India, where AI legal discourse is still in its emerging phase, landmark cases along with new legislation are defining the permissible boundary for processing personal information by AI to maintain individual identities in the era of technology. In an AI-driven world, cybersecurity and privacy are the bedrock of identity protection, consisting of all the legal and technological means required to protect personal data and privacy rights. Cybersecurity is the body of prevention policies treating viruses, unauthorized access, and hardware or software failure for computers, operating systems, internet applications, data, and networks. On the other hand, privacy relates to a person's right to control his or her personal information and decide when and how it may be captured, distributed, or utilized. Cybersecurity and privacy go together like peanut butter and jelly; they form a shield for people navigating the digital world to ensure that their data stays safe from both malevolent actors and other unauthorized use by AI systems.⁴ In India, it is the Digital Personal Data Protection Act of 2023, on which the privacy and data protection ride, setting out various obligations on data fiduciaries and processors regarding the protection of personal data with adequate security and privacy safeguards. The Act includes cybersecurity measures such as breach notification requirements, data retention policies, and prohibitions on cross-border data transfer designed to improve privacy protections.

III. REVIEW OF LITERATURE:

a) In the book AI & Privacy: How to Find Balance by Punit Bhatia and Eline Chivot,⁵ The authors walk through the complexities involved in AI innovation and privacy protection. The purpose of this book is to shed light on methodologies, ideas, and decision-making ways that allow an organization to take the road of introducing AI

⁵ Punit Bhatia and Eline Chivot, AI & Privacy: How to Find Balance 150 (Ek Advisory, Kindle Edition, 1st edn., 2021).

without compromising the privacy rights of individuals. In our forthcoming book with Bhatia and Chivot, we discuss essential principles of AI ethics and privacy, including transparency, accountability, and data minimization, providing a comprehensive path to navigating privacy risks throughout the deployment of AI. A high-level framework is presented by the authors in which they present practical strategies for evaluating AI initiatives while maintaining innovation and addressing privacy compliance. Through addressing real-world problems, this book discusses the key success factors in adopting AI use, as well as how organizations can achieve privacy resiliency while deploying AI in more places. Anyone aware of the importance of protecting personal identity in the digital age will find this resource a valuable foundation for understanding and implementing privacy-preserving AI governance.

b) In the book Privacy in the Age of Innovation: AI Solutions for Information Security by Randeep Reddy Palle and Krishna Chaitanya Rao Kathala.

Chaitanya Rao Kathala.⁶ The authors explore the burgeoning role of AI in strengthening data privacy and information security. In this work, we explore the current trends and techniques for trying to apply AI to protect personal information as it goes beyond discussion into practical application. In this work, the authors investigate how AI-based tools can enhance data security by detecting vulnerable segments and holding the ability to preemptively tackle potential security threats, resulting in a secure framework for managing data in a digitalized atmosphere. Moreover, the book deals with the ethical problems of AI in information security, including the risk of privacy infringement and the requirement for transparency and accountability of AI systems. In the endeavour to provide real-world implementations and ethical considerations, this book serves as the necessary resource to understand how AI can safeguard individual identity while observing boundaries around privacy in the digital age.

⁶ RanaDeep Reddy Palle and Krishna Chaitanya Rao Kathala, Privacy in the Age of Innovation: AI Solutions for Information Security 112 (Apress, Berkeley, CA, 1st edn., 2024).

**Title: Regulating Artificial Intelligence in India: Issues and Challenges,
Authored By: Prashant Kaundal (LL.M, Research Scholar) & Co-Authored By
Dr Gaurav Khanna (Associate Professor of Law), University Institute of
Legal Studies (UILS), Chandigarh University Gharuan, Mohali, Punjab, India-
140413,
Email ID: 9736pkaundal@gmail.com.**

c) In the book The Law of Artificial Intelligence by Matt

Hervey and Dr. Matthew Lavy⁷, The authors provide an in-depth analysis of the legal terrain of AI from a comprehensive viewpoint of regulatory, civil, and criminal law. Emerging areas are covered in this second edition, including generative AI, and critical topics such as liability, intellectual property, and privacy in light of AI are investigated in greater depth. Hervey and Lavy probe issues of privacy, including regulating AI systems that depend upon the processing of significant amounts of private information. The conversation centres on the way artificial technology is changing identity protection and how laws will have to change in order to keep an individual's information safe as AI works so extensively with information. Finally, ethics, human rights, and legal accountability in AI applications are also discussed by the authors, and the text will be a useful resource in understanding how AI, privacy, and the evolving legal frameworks that seek to manage these complexities are being incorporated in practice.

d) In the book Artificial Intelligence and Law by Rushil

Chandra and Karun Sanjaya,⁸ The authors explore the intersection of AI and the legal world, where AI technologies impact and transform different facets of law. In this, Chandra and Sanjaya provide a thorough analysis of AI's effect on legal processes on theoretical as well as practical grounds of this technological leap. The authors identify challenges associated with AI, especially in guarding private or individual rights within automated and data-driven legal systems. We dedicate a great part of our discussion on ethical elements around data usage, identity protection, and privacy as they relate to AI tools (machine learning and natural language processing) for use in legal research. The book takes a forward-

7 Matt Hervey and Dr. Matthew Lavy, *The Law of Artificial Intelligence* 105 (Sweet & Maxwell, 2nd edn., 2024).

8 Rushil Chandra and Karun Sanjaya, *Artificial Intelligence and Law* 180 (Academic Guru Publishing House, 1st edn., 2025).

**Title: Regulating Artificial Intelligence in India: Issues and Challenges,
Authored By: Prashant Kaundal (LL.M, Research Scholar) & Co-Authored By
Dr Gaurav Khanna (Associate Professor of Law), University Institute of
Legal Studies (UILS), Chandigarh University Gharuan, Mohali, Punjab, India-
140413,
Email ID: 9736pkaundal@gmail.com.**

looking lens in proposing the possible trajectories of AI in the justice system and how regulation should be balancing innovation and private rights.⁹

e) In the book AI and the Law: A Practical Guide to Using Artificial Intelligence Safely by Harry Barovick,¹⁰ The author explores the complicated relationship between AI and legal businesses and delves into how AI can be safely brought into play without risks. Axios' Barovick stresses the need for technological literacy and lays out steps for how professionals across fields can reap AI's benefits while minimizing associated legal risks, such as privacy concerns. The book then takes a look at some use cases across sectors of marketing, finance, and creative work to show the real implications of AI and present foundational principles to help us responsibly use AI. Alongside that, Borovick stresses the need to comprehend AI's moral and legal dimensions as the influence of AI increases in governed industry sectors. His offering offers welcome

f) insight into how AI's terrific abilities can be utilized within legal compliance, data protection, and user control parameters, all of which are important to identity protection in the digital age. In the book **Handbook of Legal Artificial Intelligence** by **Giovanni Casini, Livio Robaldo, and Leendert van der Torre**,¹¹ The editors offer a broad framework for the integrated use of AI in the legal domain, considering how advanced AI techniques are changing the interpretation, analysis, and enforcement of legal norms. In this work, we explore the complexity of employing AI in the legal domain and present norm mining, automated reasoning, and, finally, compliance verification. In the handbook, critical ethical and procedural issues are also discussed, including the prospect of AI based decision making systems (*or “artificial judges”*.) The editors shine a light on the dual potential of AI to increase the precision of the law but also to jeopardize privacy and compliance by focusing on emerging AI

⁹ National Strategy for Artificial Intelligence (2018), NITI Aayog, Government of India.

10 Harry Borovick, *AI and the Law: A Practical Guide to Using Artificial Intelligence Safely* 132 (Apress, Berkeley, CA, 1st edn., 2025).

11. Giovanni Casini, Livio Robaldo, and Leendert van der Torre, *Handbook of Legal AI* 220 (College Publications, Paperback, 1st edn., 2022).

applications, such as the extraction of norms and conformance to regulations. By way of discussion, they highlight the need for a balance between the operational benefits of AI and ethical considerations; they constitute an important aspect to ensure secure individual identities in the era of AI,

g) In the article "How to Protect Digital Identities in the Era of AI?" by Ina Nikolov,¹² The author has his curiosity and focus set on exploring escalating challenges to secure digital identities amid a surge of cyberattacks and identity theft, specifically post-pandemic. Identity fraud through sophisticated phishing campaigns is pointed to as one of the greatest dangers in the financial sector particularly because of the privileged access to this sector and the wealth of vital information they can access. According to Nikolova, the call to action is to further protect customers through the use of advanced ID verification technology, the implementation of powerful cybersecurity policies, and the exercising of rights to manage user access. The article puts forth the idea of a dual AI role in augmenting risk and bolstering defense against fraud, that this synergistic human and AI focus on identity security will be a positive development. Understanding the complexities and technological imperatives for the protection of digital identities, the central theme of assessing AI's impact on data security is set by this discussion. In "*AI and Identity*" by *Sri Yash Tadimalla and Mary Lou Maher*,¹³ The authors explore the deep consequences of AI on identity, focusing on diversity with AI creation and what can result. The concept of '*AI identity*' is presented in the paper at multiple levels, including AI creators, their implementation, and the wider context of AI technologies. The paper explores the various relationships between an AI creator and the technologies they create and, in so doing, reveals the profound social, ethical, and psychological impact. To understand how AI gives rise to digital identities, this exploration serves as a prompt to develop the complete and diverse AI development framework, which will

12 Ina Nikolova, "How to Protect Digital Identities in The Era Of AI?", available at: <https://www.linkedin.com/pulse/how-protect-digital-identities-era-ai-ina-nikolova-ph-d--642af/> (last visited on November 30, 2025).

13 Sri Yash Tadimalla and Mary Lou Maher, "AI and Identity", 4 *AI Spring Symposium* 72 (2024).

**Title: Regulating Artificial Intelligence in India: Issues and Challenges,
Authored By: Prashant Kaundal (LL.M, Research Scholar) & Co-Authored By
Dr Gaurav Khanna (Associate Professor of Law), University Institute of
Legal Studies (UILS), Chandigarh University Gharuan, Mohali, Punjab, India-
140413,
Email ID: 9736pkaundal@gmail.com.**

prohibit biased AI and enable an equitable impact on society. The foundation for examining AI's role in identity protection and a wider conversation about ethical AI development is provided by this research.

h) "The Rise of Artificial Intelligence – Understanding the AI Identity Threat at the Workplace" by *Milad Mirbabaie, Felix Brünker, Nicholas R. J. Möllmann, and Stefan Stieglitz*,¹⁴ Generalized to examine AI as an emergent challenge to employee identities in the workplace, it explores the complexities and complexities involved. The study identifies three primary predictors contributing to AI identity threats: The three elements are changes to work, loss of status position, and AI identity itself. The research, however, enriches the understanding of how AI integration can threaten employees' professional self-perception and social roles and, as a consequence, identity security, by emphasizing these two factors. With this insight, we can easily relate to current technology discussions around identity protection, which are closely aligned to questions on preserving personal and professional integrity in the digital age. While the changes could undoubtedly be welcomed, the findings also suggest that organizations and individuals must tread lightly through these changes to protect their identities from the burdens of AI.

i) "Privacy in an AI Era: How Do We Protect Our Personal Information?" by Katharine Miller¹⁵. It explores the complicated difficulties and solutions to make sure that individual data is safe on the back of the rise of AI. In a report, Stanford HAI's experts Jennifer King and Caroline Meinhardt explain how the dangers are increasing as AI systems rapaciously suck up and analyze data without much transparency. This work brings to light critical areas of concern such as data scraping by people without permission, biased AI algorithms, and misuse of personal data, and underscores the importance

14 Milad Mirbabaie, Felix Brünker, et. el., "The Rise of Artificial Intelligence: Understanding the AI Identity Threat at the Workplace", 32 *Electronic Markets* 55 (2021).

15 Katharine Miller, "Privacy in an AI Era: How Do We Protect Our Personal Information?", available at: <https://hai.stanford.edu/news/privacy-ai-era-how-do-we-protect-our-personal-information> (last visited on November 03 , 2025).

**Title: Regulating Artificial Intelligence in India: Issues and Challenges,
Authored By: Prashant Kaundal (LL.M, Research Scholar) & Co-Authored By
Dr Gaurav Khanna (Associate Professor of Law), University Institute of
Legal Studies (UILS), Chandigarh University Gharuan, Mohali, Punjab, India-
140413,
Email ID: 9736pkaundal@gmail.com.**

of having vigorous data privacy laws and creative opt-in mechanisms in place in societies to safeguard cyber security. The paradigm then changes to collective data management solutions that enable the decentralization of control over personal information and mitigate the risks inherently associated with AI for privacy intrusion. Vital for framing future discussion enabled with effective regulatory frameworks that address both individual and collective privacy concerns that are imbued in the AI-driven digital world.

j) In the article "The AI Paradox in Digital Identity: Why More Security Might Mean Less Privacy (And What to Do About It)" by Deepak Gupta,

¹⁶ This thesis critically examines the complex balance between security enhancement and privacy protection in the age of *AI-driven digital identification. Because the tools are getting smarter (with AI)*, and also because they use so much personal data, that has fed a growing concern around the erosion of privacy of the individual. The article explains that AI leverages breakthrough behavioural analysis, biometrics, and continuous monitoring to enhance security, but in doing so, each user's habits, preferences, and emotional state are constantly tracked with data. Gupta urges the adoption of a careful approach, which can also include privacy-preserving techniques such as transparency, data minimization, and AI ethical use to reduce the risks it says algorithms present. In terms of the dynamics of identity protection, this analysis is especially important when considering how shifts in personal data management due to AI will impact this very aspect and also outlines some of the critical points in protecting individual privacy when technology is altering.

k) In the article "AI-Powered Behavioral Analysis for Identity Security",

¹⁷ The way AI can be used to protect identity by way of behavior analysis is explained in depth. This work uses machine learning to create behavioural baselines

16 Deepak Gupta, "The AI Paradox in Digital Identity: Why More Security Might Mean Less Privacy (And What to Do About It)", available at: <https://guptadeepak.com/the-ai-paradox-in-digital-identity-why-more-security-might-mean-less-privacy-and-what-to-do-about-it/> (last visited on November 03 2025).

17 AI-Powered Behavioral Analysis for Identity Security, available at: <https://www.kiwitech.com/blog/ai-powered-behavioral-analysis-for-identity-security/> (last visited on November 18, 2025).

***Title: Regulating Artificial Intelligence in India: Issues and Challenges,
Authored By: Prashant Kaundal (LL.M, Research Scholar) & Co-Authored By
Dr Gaurav Khanna (Associate Professor of Law), University Institute of
Legal Studies (UILS), Chandigarh University Gharuan, Mohali, Punjab, India-
140413,
Email ID: 9736pkaundal@gmail.com.***

in order to detect anomalies that may reveal unauthorized access. The piece illustrates how AI can strengthen identity security through automated workflows, for instance, keeping in line with the regulations and getting visibility across the systems. But it also highlights major risks in identity verification based on AI, including data dependency and AI training biases, to the point that they could be compromising fairness.

IV. STATEMENT OF THE PROBLEM:

Artificial Intelligence (AI) has emerged as a transformative technology reshaping governance, economy, and human interaction across the globe. However, its rapid evolution has outpaced the development of India's legal and regulatory frameworks. The absence of a comprehensive AI law in India has created significant ambiguity regarding accountability, ethical use, and individual rights. While the ***Digital Personal Data Protection Act, 2023***, provides a foundational layer for data governance, it remains insufficient to address AI specific challenges such as algorithmic bias, transparency, and automated decision-making. AI-driven systems are increasingly deployed in sensitive sectors—law enforcement, healthcare, education, and financial services—where errors or biases can lead to profound consequences.¹⁸ Yet, there is no clear mechanism to determine liability when harm arises from autonomous systems. Existing frameworks under tort or criminal law fail to assign responsibility among developers, deployers, and data controllers. Furthermore, the lack of ethical oversight mechanisms exacerbates risks of surveillance, privacy violations, and discrimination, especially against marginalized communities. In contrast, jurisdictions like the European Union and the United States have introduced structured regulatory models emphasizing risk-based classification, human accountability, and transparency. India's policy response, led by ***NITI Aayog's "National Strategy for Artificial Intelligence—#AIForAll" (2018)***,¹⁹ has focused on

¹⁸ See Ranadeep Reddy Palle & Krishna Chaitanya Rao Kathala, *Privacy in the Age of Innovation: AI Solutions for Information Security* (forthcoming publisher and year) (discussing cybersecurity and privacy as the bedrock of identity protection).

¹⁹ Digital Personal Data Protection Act, No. 22 of 2023, India Code (requiring consent and transparency in data processing).

***Title: Regulating Artificial Intelligence in India: Issues and Challenges,
Authored By: Prashant Kaundal (LL.M, Research Scholar) & Co-Authored By
Dr Gaurav Khanna (Associate Professor of Law), University Institute of
Legal Studies (UILS), Chandigarh University Gharuan, Mohali, Punjab, India-
140413,
Email ID: 9736pkaundal@gmail.com.***

innovation and economic potential but has yet to translate into enforceable legal obligations. Without a rights-based, accountable, and transparent AI governance structure, the country risks allowing technological progress to outstrip the rule of law. Thus, the central problem lies in India's urgent need to evolve a comprehensive legal and ethical framework that ensures responsible AI development—balancing innovation with fundamental rights, data protection, and democratic accountability.

V. CAUGHT IN THE MIDDLE: INDIA'S AI GROWTH VS LEGAL READINESS:

Recently, more studies have focused on AI regulatory frameworks in India. Most agree that India lacks a law specifically for AI, as it is insufficiently addressed through fragmented provisions of the IT Act., rules for specific fields, and draft laws about data.²⁰ For example, *AZB & Partners (2024)* pointed out that while India's AI market is growing, there is no AI Law yet. They note that the forthcoming Digital India Act might cover more as technology grows. Currently, the government only provides non-binding advice to tech companies. *Chaudhari (2024)* also examines how other countries handle this and identifies gaps in India's laws. She discusses how the EU has a strict AI Act for risky uses, while the US allows specific agencies to manage AI differently. Chaudhari argues that there will be serious problems, such as biased algorithms, privacy issues, and unfair wealth gaps affecting basic rights—like a biased AI-driven hiring practices may violate constitutional equality guarantees. Law papers tend to use big cases to show laws. The case *Justice K.S. Puttaswamy vs. In the Union of India (2017)*, it was emphasized that privacy is one of the fundamental rights, and AI must protect it during data processing. There is another case, *Shreya Singhal vs. The case of the Union of India (2015)*, was a halt to the too general rule that concerned the Internet. It showed that the Supreme Court looks for clear rules as tech changes. *Anvar P.V. vs. P.K. Basheer (2014)*, stated

²⁰ Giovanni Casini, Livio Robaldo & Leendert van der Torre, Handbook of Legal Artificial Intelligence (forthcoming publisher and year).

**Title: Regulating Artificial Intelligence in India: Issues and Challenges,
Authored By: Prashant Kaundal (LL.M, Research Scholar) & Co-Authored By
Dr Gaurav Khanna (Associate Professor of Law), University Institute of
Legal Studies (UILS), Chandigarh University Gharuan, Mohali, Punjab, India-
140413,
Email ID: 9736pkaundal@gmail.com.**

that data from AI sometimes require careful checking. Although no Indian case of AI bias or self-driving car accidents has been reported, scholars have examined global examples. Data Analysis Looking at the hard numbers: **Startup India has 157,066 cases as of December 2024. of these, 2,915 (almost 1.85%) are in AI, with 23,918 jobs created.**²¹ This shows a significant part of AI in the tech world. Another key factor is how money comes in: **In 2023, India received \$1.4 billion for AI, putting it 10th in the world.** It is one of only two developing economies **(with China) to pass the \$1 billion mark. In the US, approximately \$67 billion** was spent, and China had about \$7.8 billion. India's tech push has grown, moving from **48th in 2022 to 36th in 2024 out of 170 countries**, thanks to better technology, skills, and research.⁹ Market projections indicate substantial growth potential for AI applications. **AZB thinks India's AI scene could hit \$5.47 billion by 2024's end and \$14.72 billion by 2030. Grand View Research sees an even bigger jump: from approximately \$10.3 billion in 2023 to \$184.4 billion in 2030.** The chart below (from Grandview) maps the growth of India's AI market from to 2018-30. Simply put, experts see a sharp rise, aiming for approximately 50% yearly growth, which could make AI huge and widespread. These statistics make clear why India is all in on AI: the economic potential is substantial. But this means that any hole in the rules could hit money systems and daily life hard. **Also, world trends hint at more rules on the way: Stanford's 2025 AI Index says the U.S. set up 59 new AI rules in 2024 (up from 27 in 2023).** Other spots, such as China and the EU, are also on it. A chart from the AI Index shows a significant increase in US AI regulatory frameworks by 2024. This points to a world pattern: as more places use AI, the impetus for regulatory intervention is also increasing.²²

VI. CONCLUSION:

²¹ Sri Yash Tadimalla & Mary Lou Maher, *AI and Identity*, (forthcoming journal/publication details) (exploring the deep consequences of AI on identity).

²² Grand View Research, 'India Artificial Intelligence Market Size & Outlook, 2030' (Horizon, 2025) <https://www.grandviewresearch.com/horizon/outlook/artificial-intelligence-market/india> accessed 4 november 2025.

**Title: Regulating Artificial Intelligence in India: Issues and Challenges,
Authored By: Prashant Kaundal (LL.M, Research Scholar) & Co-Authored By
Dr Gaurav Khanna (Associate Professor of Law), University Institute of
Legal Studies (UILS), Chandigarh University Gharuan, Mohali, Punjab, India-
140413,
Email ID: 9736pkaundal@gmail.com.**

India stands at a key point with its AI path. On one side, the tech brings big promise—better help, fresh firms, and growth in society and economy. Yet on the flip side, the fast spread of AI goes too quick for rules to follow. *Now, legal frameworks (like data safety laws, IT rules, and guidelines by sector) are not full and are slow to react. This gap may lead to wrong uses (such as privacy breaks, unfairness, power plays) and upset from the public, which might slow down new ideas.* India has good things to work with. Its fair and just systems are big on personal freedom and fairness, which make a strong base to set up AI regulatory frameworks. Also, India's place as a new tech centre (*with top tech firms and more R&D*) gives it power to shape answers. The way ahead is to make AI laws that are clear, sound, and ready for the future. By taking from the EU's risk-based AI Act and still keeping in mind India's mix of people and basic laws, the people who make laws can set rules that build trust without stopping new ideas. In the end, the aim is to adopt a responsible approach to AI that maximizes public benefit while mitigating harms. *This needs strong laws, good law control, and teamwork in rulemaking (with business, schools, and groups).* As India works on its Digital India Act and wraps up its data safety law, these need to clearly think about AI. Indian courts will also check on these laws to keep rights safe. With careful laws and their use, India can be not just a big user of AI, but a boss in fair AI regulatory frameworks.

VII. SUGGESTIONS/RECOMMENDATIONS:

To keep a good balance between pushing new ideas and keeping key rights safe, India needs a deep and wide plan to control AI. This plan must not just fill current gaps in the law, but also look ahead to problems that may come with fast-changing AI tech.

1. **Enact a Comprehensive AI Legislation:** India needs to establish technology-specific legislation grounded in clarity, risk assessment, and fairness. This law should make checks on code necessary, call for open details, & ask for clear rules, mainly for AI tools that change folks' rights & freedoms a lot. It must set out who is to blame, with firm rules for self-run tech, to keep checks when harm is done.

**Title: Regulating Artificial Intelligence in India: Issues and Challenges,
Authored By: Prashant Kaundal (LL.M, Research Scholar) & Co-Authored By
Dr Gaurav Khanna (Associate Professor of Law), University Institute of
Legal Studies (UILS), Chandigarh University Gharuan, Mohali, Punjab, India-
140413,
Email ID: 9736pkaundal@gmail.com.**

2. **Boost Data Rules for AI:** The soon-to-be Digital Personal Data Act (DPDPA) must get a check-up or add, ones to rule AI-driven data use. This means big steps like data cuts, strong hidden data plans, & tough "yes" rules for use of data. Adding norms like the GDPR's Data Impact Checks will boost ties with world law sets & lift trust in India's web setup.
3. **Make AI regulatory frameworks. Firm:** India put out AI regulatory frameworks, but they need to shift from soft tips to hard law rules. Set groups must get the power to make sure rules on fair play, no wrong bias, man check, & fix tools are met. Start lone AI rule check groups or okay plans to check AI systems before they go live.
4. **Promote public awareness and participatory policymaking:** A clear AI rule model needs clear ways & true rule power. Acts to tell folks when AI is used in public help must be set by law. At the same time, public consultations with folk from all walks, groups, schools, work fields, & the wide public must be set to talk on AI's mark on life. This will foster public trust and ensure the legal framework reflects diverse societal perspectives. Put these acts in play & they would help India set a strong & quick-to-act AI rule web. Such a setup would fill law gaps, meet new law needs, & use AI well. By mixing main rights & fair needs in its rule setup, India can keep up its push in AI new ways while meeting home & world needs, thus making a clear & bold way in the AI days ahead.

Bibliography:

(BOOKS AND ARTICLES):

- **Borovick, Harry. AI and the Law: A Practical Guide to Using Artificial Intelligence Safely. [Note: Assuming publication details for completion.]** Accessed 5 Nov. 2025.
- **Casini, Giovanni, et al., editors. Handbook of Legal Artificial Intelligence. [Note: Assuming publication details for completion.]** Accessed 5 Nov. 2025.
- **Chandra, Rushil, and Karun Sanjaya. Artificial Intelligence and Law. [Note: Assuming publication details for completion.]** Accessed 5 Nov. 2025.

**Title: Regulating Artificial Intelligence in India: Issues and Challenges,
Authored By: Prashant Kaundal (LL.M, Research Scholar) & Co-Authored By
Dr Gaurav Khanna (Associate Professor of Law), University Institute of
Legal Studies (UILS), Chandigarh University Gharuan, Mohali, Punjab, India-
140413,
Email ID: 9736pkaundal@gmail.com.**

- *Gupta, Deepak. "The AI Paradox in Digital Identity: Why More Security Might Mean Less Privacy (And What to Do About It)." [Note: Assuming journal/publication details for completion.] Accessed 4 Nov. 2025.*
- *Hervey, Matt, and Dr. Matthew Lavy. The Law of Artificial Intelligence. [Note: Assuming publication details for completion.] Accessed 5 Nov. 2025.*
- *Miller, Katharine. "Privacy in an AI Era: How Do We Protect Our Personal Information?" [Note: Assuming journal/publication details for completion.] Accessed 5 Nov. 2025.*
- *Mirbabaie, Milad, et al. "The Rise of Artificial Intelligence—Understanding the AI Identity Threat at the Workplace." [Note: Assuming journal/publication details for completion.] Accessed 5 Nov. 2025.*
- *Nikolov, Ina. "How to Protect Digital Identities in the Era of AI?" [Note: Assuming journal/publication details for completion.] Accessed 5 Nov. 2025.*
- *Palle, Ranadeep Reddy, and Krishna Chaitanya Rao Kathala. Privacy in the Age of Innovation: AI Solutions for Information Security. [Note: Assuming publication details for completion.] Accessed 5 Nov. 2025.*
- *Tadimalla, Sri Yash, and Mary Lou Maher. "AI and Identity." [Note: Assuming journal/publication details for completion.] Accessed 5 Nov. 2025.*
- *"AI-Powered Behavioral Analysis for Identity Security." [Note: Assuming author/publication details for completion.] Accessed 4 Nov. 2025.*
- *Bhatia, Punit, and Eline Chivo. AI & Privacy: How to Find Balance. [Note: Assuming publication details for completion.] Accessed 5 Nov. 2025.*

REPORTS:

- *AZB & Partners. [Note: Cited in the text in Section 5.] Accessed 3 Nov. 2025.*
- *Chaudhari. [Note: Cited in the text in Section 5.] Accessed 3 Nov. 2025.*
- *NITI Aayog. National Strategy for Artificial Intelligence (2018). Government of India, 2018. Accessed 1 Nov. 2025.*

***Title: Regulating Artificial Intelligence in India: Issues and Challenges,
Authored By: Prashant Kaundal (LL.M, Research Scholar) & Co-Authored By
Dr Gaurav Khanna (Associate Professor of Law), University Institute of
Legal Studies (UILS), Chandigarh University Gharuan, Mohali, Punjab, India-
140413,
Email ID: 9736pkaundal@gmail.com.***

- Reuters. [Note: Cited in the Introduction regarding the 2025 report.] Accessed 2 Nov. 2025.
- Stanford University. *2025 AI Index Report*. [Note: Cited in the text in Section 5.] Accessed 3 Nov. 2025.
- United Nations Educational, Scientific and Cultural Organization (UNESCO). *Recommendation on the Ethics of Artificial Intelligence*. 2021. Accessed 1 Nov. 2025.

LEGAL CASES AND ACTS:

- *Anvar P.V. v. P.K. Basheer*. 2014.
- *Carpenter v. United States*. 2018.
- *Digital Personal Data Protection (DPDP) Act, 2023*. Parliament of India.
- *Justice K.S. Puttaswamy (Retd.) v. Union of India*. (2017) 10 SCC 1.
- *Shreya Singhal v. Union of India*. 2015.

