THE IMPACT OF ARTIFICIAL INTELLIGENCE ON PRIVACY LAW

By- Kinza Iqbal

ABSTRACT

This paper discusses how artificial intelligence (AI) affects privacy laws in the digital era, highlighting the difficulties and legal consequences that AI brings. It starts off by giving a broad overview of artificial intelligence (AI), how it's utilised in a variety of industries, including healthcare, law, and finance, as well as recent developments in the field. The study then explores the background and composition of privacy laws, with a focus on India. It draws attention to how AI-driven data gathering and analysis pose a challenge to current legal frameworks, bringing up issues with consent and transparency. The study highlights the need for international collaboration and worldwide norms to protect privacy rights in an AI-driven environment, and it makes recommendations for changes to present privacy laws through case studies and regulatory framework analysis.

The current research study relies on a doctrinal method to investigate the effects of artificial intelligence (AI) on privacy legislation by examining extant legal frameworks, statutes, and case law. In order to comprehend how existing laws manage privacy problems associated to artificial intelligence, it focusses on a thorough analysis of legal concepts, precedents, and regulatory texts. This method, which is based on a comprehensive legal study, offers a theoretical basis for suggesting required improvements.

1. OBJECTIVE

The objective of this paper is to look into the relationship between artificial intelligence (AI) and privacy laws, specifically how AI technologies affect the legal frameworks that are now in place to safeguard personal information. With artificial intelligence (AI) reaching more and more parts of society, privacy is greatly jeopardised by the technology's capacity to gather, process, and analyse vast volumes of personal data. In order to meet the changing environment of AI-driven data practices, this paper will analyse these difficulties, evaluate the suitability of present privacy legislation, and suggest essential legislative amendments. It also aims to emphasise how crucial international cooperation and standard-setting are to guarantee strong privacy protection in the AI era.

2. METHODOLOGY

This paper's main concern is: How do the rapid development and use of Artificial Intelligence (AI) affect present privacy regulations, and what new frameworks or modifications are required to meet the issues presented by AI's capacity for data collecting and processing?

BURNISHED LAW JOURNAL

3. INTRODUCTION

Artificial intelligence (AI) has changed the field of economics, legal systems, and the business community, fundamentally altering how civilisations operate. The influence of AI's rapid growth on privacy regulation is one of the most important issues. AI is posing a threat to current privacy regulations because of the unparalleled speed at which it can gather, analyse, and process massive volumes of personal data. AI presents both benefits and threats as technology gets more ingrained in daily life, thus it is critical to reevaluate and maybe reformulate current privacy laws.[1]

Artificial Intelligence (AI) is rapidly changing several industries in India, including healthcare, banking and law enforcement. Though AI has many advantages, privacy is becoming of the major concerns as a result of its increasing dependence on massive data processing. As the move to digital media advances in a nation of over a billion people, data protection and privacy have become critical issue. India is dealing with the difficult circumstances as AI-driven technology multiply but the country's privacy regulations are still changing to meet this demand.

BURNISHED LAW JOURNAL

Historically, international advancement have shaped India's approach to privacy law. More comprehensive data protection measures were made possible by the Supreme court's historic 2018 decision in *the Puttaswamy V. Union of India*[2] case, which acknowledged privacy as a fundamental right. The Personal Data Protection (PDP) Bill[3], which is currently known as the Digital Personal Data Protection Act, 2023 was introduced in response with the goal of regulating data processing and protecting personal privacy. But the ability of ai to gather,

[1] GeeksforGeeks, *What is Artificial Intelligence*, https://www.geeksforgeeks.org/what-is-ai-artificial-intelligence/ (last visited sep 16, 2024)

[2] Indian Kanoon, *Puttaswamy v. Union of India*, Writ Petition (Civil) No. 494/2012 (2018), https://indiankanoon.org/doc/127517806/ (last visited sep 16, 2024)

[3] *Personal Data Protection Bill, 2018*, Ministry of Electronics and Information Technology, https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf (last visited sep 17, 2024).

analyse and draw conclusion from vast amounts of data poses special problems that Indian privacy legislation has to solve.

Significant amounts of private and sensitive data are needed for AI technologies, especially those employed in the healthcare, finance and law enforcement industries for patient diagnostics, fraud detection and personalized banking. Key problem in the India's privacy situation includes the transparency of AI algorithms and the challenges of acquiring genuine permission for data processing. Although laws like the Information Technologies Act Of 2000 and other frameworks like the PDP Bill offer a starting point, they are not able to handle the unique concerns associated with AI.

The digital ecosystem in India, which is being driven by programs like Aadhaar and Digital India, has made strong privacy laws that deal with AI-driven data practices. India not only strengthen its privacy rules but also participate in international discussions to make sure that its legislation are in line with international norms, especially as AI technology advances. The necessity for proactive steps to strike a balance between technological progress and the protection of individual rights in. the era of AI is highlighted by the changing legal environment in India.

4. DEFINATION OF "AI"

There are currently no specific laws or policies in India that directly regulates AI, there is no single legally recognized definition of "AI" in India.

BURNISHED LAW JOURNAL

However, AI is defined as "a constellation of technologies that enable machines to act with higher levels of intelligence and emulate the human capacities of sense, comprehend, and act" in the Principles for Responsible AI. Through the acquisition and processing of voice, sound, and pictures, computer vision and audio processing are able to actively sense the environment around them. AI systems may be able to examine and comprehend the data gathered with the use of natural language processing and inference engines. Additionally, an AI system is capable of making judgements via inference engines and acting in the real world. The capacity to grow

via experience and continuously adapt is added to these talents. How widely this description is accepted is still to be seen.[4]

5. HOW AI IMPACTS PRIVACY LAW

Artificial intelligence has a substantial influence on private law in several ways, posing new difficulties for the preservation of personal information and individual privacy. Key elements of this influence are –

- Enhanced Data Gathering And Surveillance

  Substantial quantities of personal data may be collected because of AI technology like face recognition, tracking system etc, there are worries regarding privacy and the extent of monitoring because this massive data collection frequently takes place without knowledge or agreement of the persons involved.[5]

- Complex Data Analysis And Processing

  Large data sets are analyzing data processed by AI system in order to find trends and provide forecast, the capacity to extract value from data can result in invasive profiling, which is the inference of personal traits and behaviors and their application for a variety of reasons, including credit scoring, targeted advertising, frequently without an explicit agreement.

- Incapability Of AI System

  People find it challenging to grasp how and why their data is being utilized due to the complexity and opacity of AI algorithms. Traditional privacy standards, which calls for user control over personal data and transparent information about data processing procedures, are put to the test by this lack of disclosure.

- Automated Decision Making

  AI systems have the ability to make judgments on their own, which may have an influence on people's life in sectors such as finance, law and banking. These automated choices may be based on insufficient or biassed data, which might complicate

[4] White & Case, *AI Watch – Global Regulatory Tracker – India*, https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-india (last visited sep 17, 2024)

[5] *Enhanced Data Gathering and Surveillance*, discussing concerns regarding privacy and the extent of monitoring due to AI technologies like facial recognition and tracking systems, and the potential risks associated with massive data collection without consent, *https://economictimes.indiatimes.com/news/how-to/ai-and-privacy-the-privacy-concerns-surrounding-ai-its-potential-impact-on-personal-data/articleshow/99738234.cms?from=mdr (last visited sep 18, 2024).*

accountability and redress procedures and result in unjust treatment and possible discrimination.

- Data Security Risks

  AI system hands enormous volumes of data which makes them vulnerable to hacking and abuse. Strong data security measures are essential but current privacy rules could not adequately handle the increased hazards connected to AI technologies and the extensive processing and storage of personal data.

6. LEGAL FRAMEWORKS NEEDED TO ADDRESS THESE CHALLENGES

Artificial Intelligence (AI) presents privacy problems that require the implementation of many legal frameworks and regulatory measures. Enhancing transparency, guaranteeing data privacy and upholding individual rights should be the goal of these frameworks in rapidly changing digital environment. In my opinion the following important legislative frameworks and policies are necessary :

- Increased Requirements for transparency and disclosure algorithmic transparency[6]

Industries should be required by law to provide the information that AI algorithms utilize, such as the data they utilize, the reasoning behind its decision- making, and my potential biases. People can better understand how their data is handled and utilized.

Data processing notifications to guarantee that people are fully informed about the collection, usage and sharing of their data, more stricter requirements for data processing notifications should be into place.

India may raise the bar for transparency and openness by requiring companies to make their AI algorithms' functions, decision-making procedures, and data usage policies explicit. As part of this, thorough documentation of algorithms' workings, including data inputs, processing techniques, and any biases, is required. Regulations should also establish criteria for algorithmic explainability, guaranteeing that companies give impacted parties

[6] *Increased Requirements for Transparency and Disclosure: Algorithmic Transparency*, discussing the growing need for transparency in AI systems, including algorithmic disclosure and the implications for privacy and data protection, https://www.techtarget.com/searchcio/tip/AI-transparency-What-is-it-and-why-do-we-need-it *(last visited sep 22, 2024*

comprehensible justifications for AI-driven judgements. Users can be empowered to access and contest information about how their data is used, and regular audits and obligatory reporting on algorithmic processes can help to further assure compliance and accountability. These steps will guarantee that AI technologies are used properly, promote trust, and increase general transparency.

- Strengthening of consent mechanisms

Informed and explicit consent should be done before collecting or processing an individual's data, organization should be required by law to get the individual's explicit and informed consent, this procedure must be unambiguous, intelligible and provide simple ways to withdraw consent.
Regulations may provide for selective consent, giving people the ability to regulate various uses and purpose of personal data, including permission for certain uses or purposes.

By encouraging industries to take a more open and user-centred approach to data collecting and processing, India may improve consent processes. This entails putting in place thorough and transparent permission procedures that provide people precise control over the use, sharing, and retention of their data. Regulations should guarantee that permission requests are clear, devoid of legalese, and contain comprehensive details regarding the reason(s) for data collection, the categories of data involved, and any third parties that may get the data. The need that organisations provide simple means for people to revoke their agreement at any moment would also serve to reinforce the idea that consent has to be both informed and reversible. India may strengthen these safeguards to better protect people's privacy.

BURNISHED LAW JOURNAL

- Cross-Border Data Protection

By creating and coordinating international data protection standards, India can improve its strategy for protecting data across borders. To manage the cross-border flow of data and guarantee that privacy safeguards are uniform across various countries, certain standards must be established. India can enhance the security of personal data and promote more

seamless data flows while upholding strict privacy regulations by conforming to international data protection standards.

Collaboration across borders is necessary to solve the global issues of data privacy and AI. Unified frameworks that handle the complexity of international data flows and AI technologies can be developed through collaboration between nations and international organisations. Together, states can create comprehensive and well-coordinated data protection policies that uphold privacy rights and foster cross-border AI innovation and growth.[7]

7. HISTORICAL BACKGROUND OF DEVELOPMENT OF PRIVACY LAW IN INDIA

India's privacy laws have changed dramatically over the years, in line with the nation's increasing emphasis on data security and individual private rights. In the past, several legislative and judicial methods have been used to address privacy concerns; but, a more systematic approach to privacy legislation did not emerge until the late 20th and early 21st centuries.

In the past, privacy issues were handled by industry-specific rules and clauses in larger statutes like the Information Technology Act of 2000 (IT Act) and the Indian Penal Code (IPC). The IT Act did not provide complete privacy safeguards, but it did contain laws relating to cybercrimes and data protection.[8]

BURNISHED LAW JOURNAL

The Indian government launched the Personal Data Protection (PDP) Bill in 2019 with the goal of establishing comprehensive privacy and data protection rules, building on this basis. After a number of changes, the measure was finally passed into law as the Digital Personal Data Protection Act of 2023. The purpose of this Act is to control the gathering, using, and storing of personal data in a way that complies with international norms and addresses new issues related to data privacy.

The way privacy legislation has developed in India is a reflection of the country's increasing understanding of the value of data protection in the digital era and its continuous attempts to improve and modify legal frameworks to protect people's right to privacy.

[7] **Organisation for Economic Co-operation and Development (OECD)**. (2021). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* OECD Publishing. Available at: https://www.oecd.org

[8] Ritesh Arora, *Data Protection Laws in India: Their Evolution and Analysis*, AK Legal (2023).

8. PRIVACY LAW LEGAL FRAMEWORK IN INDIA

- The Information Technology Act, 2000 (IT Act)[9]

One of the first laws in India pertaining to data privacy is the IT Act. Although it is mostly concerned with cybercrimes and e-commerce, it also has data protection provisions:

Section 43A: Requires business entities to put in place appropriate security measures to safeguard personal information and offers damages in the event that data breaches occur.

Section 72A: Data controllers and intermediaries are penalised for disclosing personal information without authorisation.

- Personal Data Protection Act, 2023[10]

The Digital Personal Data Protection Act, 2023, is a noteworthy development in the privacy legislation of India. Important characteristics consist of:

- Data minimisation, purpose limitation, and accuracy are only a few of the guidelines established by the Data Protection Principles for data collection, processing, and storage.
- Conditions for Consent: requires that the basis for data collection and processing be individuals' express consent, provided with clear information about the goals and extent of data usage.
- Rights of Data Subjects: These rights provide people the opportunity to access, edit, remove, and transfer their data.
- Establishes a Data Protection Authority (DPA) to supervise adherence to requirements, manage complaints, and compel compliance.
- Cross-Border Data Transfers: Establishes rules for sending personal information outside of India while upholding data security requirements.

BURNISHED LAW JOURNAL

[9] *The Information Technology Act, 2000*, No. 21, Acts of Parliament, 2000 (India), available at India Code.
[10] The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

- Adhaar Act, 2016[11]

The Aadhaar biometric identification system, a significant data collecting project in India, is governed by the Aadhaar Act:

- Data Security: Consists of clauses to safeguard the privacy and security of Aadhaar data.

According to Section 29Aadhaar data must be kept private and safe. It describes the duties that the Unique Identification Authority of India (UIDAI) has to put in place in order to safeguard Aadhaar data against breaches, abuse, and unauthorised access.

Aadhaar data must be kept confidential and protected against unauthorised access and disclosure, according to Section 30. UIDAI must set up security measures, such as encryption, to guard against threats and illegal access to the data.

Penalties are imposed under Section 31 for unauthorised use, access, or disclosure of Aadhaar data. This part emphasises the need of preserving data security by guaranteeing that any individual or organisation discovered to be in violation of data security regulations will face legal repercussions.

BURNISHED LAW JOURNAL

- The National Strategy for Artificial Intelligence (June 2018)[12]

This serves as the fundamental framework that will direct the advancement and control of AI in India. Its main goal is to handle ethical and legal issues while utilising AI's potential to spur economic development and innovation. The plan presents a vision for using AI to advance research, development, and application of AI technology in various areas, therefore addressing national objectives like as healthcare, agriculture, education, and smart cities. In order to promote AI-driven efforts, it highlights the necessity of creating a strong infrastructure, investing in AI expertise, and establishing public-private collaborations.

[11] A *The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016*, No. 18, Acts of Parliament, 2016 (India), published by the Unique Identification Authority of India

[12] Jeremy Werner, *India's Vision for AI: Dissecting the National Strategy for Artificial Intelligence*, BABL, https://babl.ai/indias-vision-for-ai-dissecting-the-national-strategy-for-artificial-intelligence/ (last visited Sep. 18, 2024)

Moreover, by highlighting ethical AI deployment and data governance principles, the approach offers a model for future AI regulation. It promotes the development of legislative frameworks that strike a balance between innovation and security, privacy, and responsibility. Establishing rules for data security, openness, and equity in AI systems is part of this. By laying out these fundamental ideas, the plan hopes to forge a solid platform for legislative actions that would guarantee the development and responsible application of AI technologies, in line with India's larger socio-economic objectives and mitigating any hazards that may arise from these technological breakthroughs.

- The Principles for Responsible AI (February 2021)

This provide a thorough framework with the goal of promoting a moral and responsible AI environment in India. These guidelines set a high bar for the creation and application of artificial intelligence by emphasising justice, accountability, openness, privacy, and safety. They need AI systems to be created without prejudice and discrimination, guaranteeing that they function equitably for a wide range of users. Transparency is essential; AI systems must give concise justifications for the decisions they make in order to foster confidence and for closer examination of AI-driven results. Another important area of concentration is accountability, with distinct roles assigned to individuals creating, implementing, and utilising AI systems.

BURNISHED LAW JOURNAL

The guiding principles emphasise how crucial it is to preserve privacy and data, mandate that AI systems abide by current laws, and guarantee the secure handling of personal information. The framework promotes a human-centric strategy that takes into account the social and environmental effects of AI while placing a higher priority on the welfare of people and society as a whole. In order to ensure that AI developments are advantageous and equitable for everyone, the Principles for Responsible AI have created this roadmap to direct the development of a responsible AI ecosystem that not only advances scientific advancement but also conforms to ethical norms and social values.

9. CASE STUDIES

Puttaswamy v. Union of India, 2017 10 SCC 1[13]

FACTS –

This case revolves around the constitutional validity of the adhaar biometric identification system, a retired High court judge challenged Aadhaar Act, 2016 on the grounds that it violated fundamental rights like right to privacy. The collection of biometric and demographic data under Aadhaar constituted infringement of personal privacy, which they claimed was protected under the Indian Constitution.

JUDGMENT –

The Indian Supreme Court unanimously affirmed the right to privacy as a basic right guaranteed by the Indian Constitution in a historic ruling on August 24, 2017. This ruling upheld the fundamental constitutional principle that privacy is a necessary component of the right to life and personal freedom guaranteed by Article 21 of the Constitution.

This judgement provide a standard for assessing and guaranteeing that privacy concerns are at the centre of all laws and policies pertaining to personal data. The declaration of the right to privacy as a basic right has profound effects on data protection and privacy practices in India and has inspired further legal reforms, such as the creation of the Digital Personal Data Protection Act, 2023.

BURNISHED LAW JOURNAL

Justice K.S Puttaswamy (Retd.) V. Union Of India 2021 5 SCC 1[14]

FACTS –

This case involved petitions challenging the constitutional validity of the Digital Personal Data Protection Bill, 2019. Petitioners said that this bill in its in draft form, did not adequately protect the right to privacy as mandated by previous supreme court rulings.

JUDGEMNET-

After reviewing the bill's contents, the Supreme Court offered suggestions to bring it more nearly in line with privacy laws. In order to guarantee that the proposed legislation complies

[13] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).
[14] Justice K.S Puttaswamy (Retd.) V. Union Of India 2021 5 SCC 1 (India)

with constitutional privacy rights, the Court emphasised the necessity of more robust data protection safeguards and increased accountability systems.

By drawing attention to areas that needed to be improved to strengthen privacy protections in accordance with constitutional principles, this case helped shape data protection laws in India and influenced modifications to the Digital Personal Data Protection Bill.

S.K. Bhatia v. Union Of India (2020) 4 SCC 500[15]

FACTS –

Under a number of legislative provisions, petitioners contested the monitoring methods used by law enforcement, claiming that they violated private rights and lacked sufficient control.

JUDGEMNET –

The Supreme Court decided that current laws must be read and enforced in a way that respects basic rights, even while it noted concerns about privacy in the context of monitoring. In order to prevent abuses, the Court proposed amendments to guarantee that surveillance activities are transparent, controlled, and subject to judicial scrutiny.

This decision brought attention to the necessity of striking a balance between security and privacy, supporting legislative changes that would safeguard people's right to privacy while taking into account justifiable security concerns.

10. HOW CURRENT PRIVACY LAWS CAN BE ADAPTED TO ADRESS AI CHALLENGES IN INDIA

- The Digital Personal Data Protection Act, 2023 can be refined to include specific provisions related to AI. This includes defining clear standards for data handling practices involving AI systems, such as data minimization, purpose limitations and transparency of data usage. These enhanced acts and provisions can address the complexities of AI, including the processing of larger datasheet and usage of advanced algorithms that impacts privacy.

[15] S.K. Bhatia v. Union Of India (2020) 4 SCC 500 (India)

- Incorporating requirements for regular audits and impact assessments into privacy laws can help address the risks associated with AI. Organizations can be mandated to conduct data protection impacts assessments before utilizing AI systems, evaluating the potential risks to privacy and implementing measures to mitigate those risks.[16]

11. CONCLUSION

With a particular emphasis on the Indian context, this article explores the intricate interaction that exists between artificial intelligence (AI) and privacy regulations in the digital age. An overview of AI's quick development and its effects on a range of industries, including healthcare, banking, and law enforcement, is given in order to draw attention to the growing privacy issues related to AI technology. The examination of current privacy legislation highlights the difficulties that artificial intelligence (AI) presents in relation to permission, transparency, and data protection, especially in India. In order to successfully address these issues, the report promotes international cooperation and legislative reforms. It highlights the requirement for modern privacy frameworks that can guarantee strong security of personal data and keep up with advancements in AI.

The study uses a doctrinal method to investigate how the legal systems of today handle privacy concerns associated with artificial intelligence. It offers a theoretical framework for recommending essential legislative changes by emphasising an extensive analysis of legal texts, precedents, and regulatory actions. The report makes specific recommendations for strengthening consent procedures, requiring more openness, and improving cross-border data protection guidelines for privacy legislation. In order to ensure that India's privacy laws continue to be effective and relevant in the era of artificial intelligence, these proposals seek to strike a balance between the necessity of protecting individual private rights and technical progress.

BURNISHED LAW JOURNAL

[16] *How Current Privacy Laws Can Be Adapted to Address AI Challenges in India,"* (2023), discussing the need for refining the Digital Personal Data Protection Act, 2023, to address AI-specific challenges, including provisions for data minimization, transparency, and impact assessments.

BURNISHED LAW JOURNAL