INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 1 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

PROTECTING HUMAN RIGHTS IN A WORLD POWERED BY AI

AUTHOR - TANYA CHOUDHARY, STUDENT AT BANASTHALI VIDYAPITH

BEST CITATION - TANYA CHOUDHARY, PROTECTING HUMAN RIGHTS IN A WORLD POWERED BY AI, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 5 (1) OF 2025, PG. 344-352, APIS – 3920 – 0001 & ISSN - 2583-2344.

ABSTRACT

AI has revolutionized various sectors, including communication, governance, healthcare, and education. But the excessive reliance on personal data has become a serious concern in terms of privacy, surveillance, and human rights violations. The AI-driven technologies of facial recognition and predictive analytics have been risky in intrusive surveillance, discrimination, and lack of accountability because of opaque decision-making processes. This paper explores how AI affects the data privacy responsibility of stakeholders-whether governments, businesses, or individuals-and related legal frameworks designed to address these issues. To do this, it looks into international regulations and policies, from the General Data Protection Regulation of the European Union to the California Consumer Privacy Act of the United States, up to India through the Digital Personal Data Protection Act and landmark cases. This paper suggests the need for a balanced approach between innovation and safeguarding basic human rights through advocating for ethical AI practices, transparency, and stronger regulatory measures

Keywords - Artificial Intelligence, Data Privacy, Human Rights, AI Ethics, Surveillance, Algorithmic Bias, GDPR, CCPA, Digital Personal Data Protection Act, AI Governance, Transparency, Accountability, Cybersecurity, Ethical AI, Privacy Laws

Introduction

Artificial Intelligence (AI) has emerged as one of the most transformative technologies of the 21st century, bringing significant changes in almost every dimension of human life, from communication and healthcare to education and governance. On the other hand, along with these numerous benefits, it challenges some basic human rights such as the right to privacy; AI systems mainly depend on very large datasets which include personal data. This dependence on data makes the issue of data misuse, surveillance, and bias in the decision-making processes a concern. Additionally, opaque AI algorithms mean that privacy violation and other violations of human rights are committed with no accountability whatsoever.

One of the most fundamental challenges that arise from AI relates to the trade-off between unleashing its potentiality and protecting human rights. For example, facial recognition technologies and predictive analytics are useful in security and business applications but entail intrusive surveillance and discriminatory profiling. Such issues call for the development of strong ethical frameworks and legal safeguards to ensure the use of AI technologies responsibly. There is a collective responsibility on the part of the government, businesses, and individuals to avoid such risks while furthering innovation. In this paper, we investigate the implications of AI on data privacy and human rights. The discussion comprises AI's effect on data privacy, the role and responsibility of various stakeholders, regulations and laws, and ethical challenges associated with data collection and sharing. Apart from this, we analyze the stance of India on data protection, and review some relevant case laws that emphasize stringent privacy safeguards. This study will look into

these areas and bring forth the importance of protecting human rights in an AI-driven world.

AI's Impact on Data Privacy

AI systems have handled vast data quantities, usually consisting of sensitive personal information. With predictive algorithms and facial recognition, AI tends to rely extensively on data for functioning, giving rise to these issues:

- **Data Surveillance**

AI has enabled unprecedented levels of data surveillance. Governments and corporations can now track, monitor, and analyze individuals' activities in real time using sophisticated AI tools. For instance, facial recognition technologies deployed in public spaces can identify and track individuals without their consent, raising questions about intrusive surveillance and its implications on personal freedoms. Similarly, AI-driven social media algorithms can monitor user behavior, preferences, and interactions, contributing to an erosion of privacy.

- **Profiling and Discrimination**

Profiling by AI systems on large datasets can create user profiles based on their behavior, preferences, and demographic data. Profiling could enhance services like targeted advertising or personalized recommendations but would expose the potential for unfair treatment. For example, hiring algorithms that favor certain demographic groups because the training data is biased could only entrench social inequalities. Another way that AI-based profiling can lead to discriminatory practices is in loan approvals, insurance premiums, and even law enforcement areas, where a lot of marginalization happens towards certain communities.

Due to a large volume of data gathered and stored, the AI systems remain an easy point of cyber attacks. In ability to ensure tight data protection and the increase vulnerability to unauthorized access lead to breaks that allow exposing sensitive personal data. Break-ins compromise the individual's privacy; they might suffer other losses in finance, identity theft, and also emotional disturbance. The problem will be even harder to tackle by the absence of accountability mechanisms regarding organizations in managing AI systems.

- **Lack of Transparency**

Opaqueness of many AI systems is the next concern. Even their developers, many of which are described as "black box" algorithms, often do not understand how they operate. This lack of transparency brings the challenge of knowing the pathways through which data is used, stored, or shared, thereby increasing probabilities of privacy violations. Unless accountability structures exist clearly in such contexts, people will have little control over their personal information in an AI-driven world.

The Responsibility of Businesses, Governments, and Individuals

Business

- **Ethical AI Practices**: There is an immediate need for businesses to exhibit transparency, fairness, and accountability in the execution of AI. This is through designing algorithms that aim at minimizing bias and discrimination, explaining AI-driven decisions, and maintaining an inclusive approach while designing and deploying AI. Ethical AI practices include abiding by standards set in place regarding responsible AI usage, which include prioritizing human rights and societal well-being more than profit motives.
- **Adopt Robust Cyber security Measures**: Organizations should develop strong cybersecurity protocols to protect user data. This includes employing advanced encryption techniques, conducting regular security audits, and staying updated on emerging cybersecurity threats. Businesses must also train their employees on data protection best practices to mitigate risks associated with human error.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 1 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

- **Impact Assessments**: Companies need to carry out regular impact assessments of their AI systems on human rights. The impact assessment is carried out to discover the risks in advance and safeguard them so that they can be addressed appropriately. These impact assessments should be inclusive, including data privacy, and other ethical issues, such as algorithmic fairness and inclusiveness. The independence of auditors or ethics boards can also help make these impact assessments more authentic.
- **Ensure Transparency and Accountability:** Transparency is a fundamental aspect of ethical AI practices. Businesses should be transparent about how they collect, process, and use data. Explain AI operations to users in an accessible manner and provide grievance redressed avenues to foster trust and accountability.

Governments

- **Enact Comprehensive Data Protection Laws**: Governments play a significant role in protecting data privacy by setting up robust legal frameworks. The General Data Protection Regulation (GDPR) is a benchmark that ensures accountability in the handling and processing of data.
- **Ensure Regulatory Oversight**: Governments must set up independent regulatory bodies to oversee AI development and deployment. These bodies can enforce compliance with data protection laws and address grievances related to AI misuse.

Individuals

- **Stay Informed About Data Privacy Rights**: Individuals should educate themselves about their rights concerning data privacy. Understanding the implications of AI and data usage empowers individuals to make informed decisions.
- **Use Privacy**-Enhancing Tools and Practices: Tools like virtual private networks (VPNs), secure browsers, and encrypted messaging apps can help individuals safeguard their personal information online.
- **Advocate for Ethical AI Policies**: Citizens can play an active role in advocating for ethical AI practices by participating in public consultations, supporting privacy-focused organizations, and holding businesses and governments accountable.

Regulations and Laws Concerning Privacy

Global Landscape

General Data Protection Regulation (GDPR)

The GDPR is a comprehensive data protection law, implemented since May 2018, which applies to all organizations operating within the European Union or dealing with the personal data of EU citizens. It gives more control to the individual over his personal data and simplifies the regulatory environment for international businesses by unifying data protection regulations in the EU.

Key aspects of GDPR include the following:

- **Consent:** The organizations must ensure that they get explicit, clear consent from individuals before collecting or processing their personal data. Such consent must be informed, unambiguous, and freely given.
- **Right to Access**: Individuals have the right to ask for access to their data and how it's being used.
- **Right to Erasure (Right to be forgotten):** This right enables an individual to request that their personal data be deleted under specific conditions.
- **Data Protection Impact Assessments:** Organizations must undertake these assessments in order to have an understanding of the impact of the data processing activity on privacy.

- **Penalties**: Non-compliance can attract heavy fines up to €20 million or 4% of annual global turnover, whichever is greater.

California Consumer Privacy Act (CCPA)

The CCPA was enacted in 2018 and went into effect from 2020. It grants data privacy rights to California residents. Its main objective is to protect personal data and provide consumers with more control over how businesses collect and use their data.

Key aspects of CCPA include:

- **Right to Know**: Consumers can ask businesses to reveal the personal information that has been collected about them.
- **Right to Delete**: Consumers can request that their personal data be deleted, although there are exceptions.
- **Right to Non-Discrimination**: Businesses cannot discriminate against consumers for exercising their rights under CCPA.
- **Penalties**: The CCPA carries fines up to $7,500 per violation and has a 30-day cure period to enable the business to rectify issues.

Emerging Trends

AI-Specific Laws on Algorithmic Accountability

Artificial intelligence is now deeply intertwined in almost all spheres of life, with issues about privacy and discrimination becoming major concerns. Governments and regulatory bodies are starting to create specific laws for AI concerning its influence on privacy and data protection.

AI Transparency: There is a push for regulations requiring companies to disclose the logic, reasoning, and data used in AI algorithms. For example, in the EU, the proposed Artificial Intelligence Act includes provisions to ensure that high-risk AI systems are transparent and explainable to users.

Bias and Discrimination: AI systems have to be created to avoid any bias that leads to discriminatory outputs in fields like hiring, lending, and even law enforcement. New AI legislation forces companies to check their algorithms for fairness and accuracy.

Data Use and Privacy: Some new laws, for example, the EU's Digital Services Act, force companies to give explanations about the usage of personal data in the algorithms to avoid the use of AI technologies which breach the set privacy standards.

Penalties for Violating Data Protection Laws

As the number of privacy violations continues to rise and data breaches increase, governments are tightening penalties for non-compliance with data protection laws to ensure greater accountability and safeguard consumers' privacy.

It has set up precedents already by imposing huge penalties on violation cases, but other more countries are adopting similar frameworks. For example, India's Personal Data Protection Bill, which draws from the GDPR, incorporates penalties for mishandling sensitive personal data and a proposed Data Protection Authority to enforce these rules.

Global Consistency: International agreements, such as the EU-US Data Privacy Framework, are aimed at bridging the gap between privacy laws across borders. This framework provides for enforcement mechanisms and ensures that data transfers between the EU and the U.S. are done with the same level of protection.

Consumer Advocacy: There is growing pressure from advocacy groups, regulatory bodies, and governments to hold corporations accountable for failing to protect personal data. Legal scholars and privacy experts are pushing for laws that empower consumers to take action through class-action lawsuits or direct legal action against businesses for breaches.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 1 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Why Privacy Should Be Safeguarded in a Future Impacted by AI

1. Preservation of Autonomy

Surveys have revealed the future realities where AI systems can access the maximum amount of personal data. The preservation of privacy is thus important to prevent loss of individual autonomy. Autonomy is the ability of individuals with respect to making independent and informed decisions. The use or otherwise misusing their personal information erodes the autonomy of an individual to determine his or her own story. Without privacy protections, AI systems could potentially infringe on individuals' personal decisions by using their data to predict behaviors, preferences, and even shape future actions. Ensuring privacy allows individuals to remain the architects of their own choices, unaffected by external manipulation based on their private information.

For instance, AI-driven websites could determine a person's future purchase or his political ideology through behavioral data. Unprotected privacy may mean AI systems dictate individual choices and drive individuals into certain behavior or belief inclination. Protecting privacy also means preventing exploitation through the agency of decision making that's free from the influence of AI-generated predictions.

2. Anti-exploitation functions

AI technologies, if left unchecked, can exploit personal data for various purposes, often without the individual's awareness. Without robust privacy protections, AI systems can process data in ways that lead to manipulation or even harm. This includes personalized advertisements that exploit vulnerabilities, surveillance that undermines civil liberties and data-driven decisions that might unfairly disadvantage certain groups or individuals.

For instance, AI systems used in recruitment or lending may rely on personal data to make decisions about applicants. If this data is exploited, it could lead to biases, discrimination, or an individual being unfairly excluded based on private characteristics that should not influence the decision-making process.

One advantage of privacy assurance is that exploitation is lessened. For example, the potential manipulative use of personal data will be restricted. Such includes targeting vulnerable individuals by using harmful marketing campaigns or obtaining sensitive information and exploiting it in favor of monetary gains or political favoritism.

3. Technology Trust

For AI technologies to be fully included in society, public trust becomes the essential piece. People must become confident that private information will remain safe and its use responsible and just. As privacy is protected, people shall not be intimidated or reluctant to using new technologies- which limits possible benefits of artificial intelligence. An important privacy would send a statement that companies or governments are for security and wellbeing of all their citizens more likely to engender trust among the public of embracing AI.

A scenario where people are afraid that AI-based medical devices are not safe from others since their health information might end up in unauthorized parties. If privacy safeguards exist, they will be more likely to rely on these systems in giving them their data knowing that it will be guarded. Without such safeguards, fear of misuse may prevent people from using life-changing technologies, hence limiting the rate at which AI can advance.

Gathering and Sharing of Data

Ethical Data Collection:

The process of data collection should be ethical, ensuring that the people involved are well-informed about the use of their data and have the opportunity to give informed consent. Informed consent refers to the fact that users are informed not only about what data is collected but also of the purposes it will be put

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 1 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

to, by whom it will be accessed, and for how long it will be kept. This will then ensure that control over personal information is maintained on the part of the user in order to be able to make informed decisions as to their involvement. In the AI-based world, wherein humongous amounts of data are processed at warp speeds, keeping up ethical collection of data assumes greater importance so that individuals are protected from abuse and exploitation. When users have a feeling of being treated with ethical practices, they can interact more freely and candidly with AI-based technology.

Data Sharing Frameworks:

In a globally connected world with data increasingly distributed across various different organizations, clearly defined frameworks should be in place for the kind of sharing occurring. Such guidelines should include a clear outline for what data could be shared under what conditions to whom. These frameworks should respect privacy, without allowing the means of data sharing to result in unauthorized access and misuse. For instance, patient data shared between hospitals or between researchers and pharmaceutical companies would be very important for advancing the frontiers of medical technology; however, it would be necessary to do so with strict protections that do not expose the sensitive information of individuals.

Minimizing Data Usage:

Encouraging organizations to collect only the data that is necessary for the specific purpose at hand is a key component of privacy preservation. By minimizing the amount of data collected, organizations reduce the risk of misuse and enhance users' sense of security. Secondly, where possible, anonym zing the data reduces even more the likelihood of individuals being identified from personal information. For instance, an organization collecting data for a customer survey should request only information pertinent to the aim of the survey and not gather extraneous information that may offend the user's privacy. By creating an environment where the minimum amount of data is collected, organizations will not only abide by privacy standards but also build public confidence in AI systems and their ability to handle data responsibly.

India Position and Steps Taken by India to Protect Data

Digital Personal Data Protection Act (DPDP Act)

India's Personal Data Protection Bill called the Digital Personal Data Protection Act (DPDP Act) is a landmark legislation designed to regulate the collection, storage, and processing of personal data. It seeks to protect the privacy of the individual by introducing fully-comprehensive guidelines for handling personal data by both the government and the private sector. The bill guarantees control over personal data. Such control allows individuals to determine what should be done with their information: accessed, corrected, and erased. The operations of processing data must be transparent, and therefore, agencies must implement explicit consent before collecting an individual's data. Another feature is the provision of data localization to ensure that sensitive data is stored within India's borders, which is a critical step in securing data from foreign surveillance and exploitation. The bill further provides for an independent regulatory body called the Data Protection Authority of India (DPAI) that would oversee compliance and address grievances. In so far as the processing of personal data is concerned, PDPB envisions a better and safer and more secure place for individuals while ensuring that the privacy of their personal data will not be compromised while AI technologies and data usage proliferate.

Digital India Program:

India's Digital India Program is the national initiative towards transforming India, step by step, into a digitally empowered society. One of the main goals of this program is to establish secure and strong digital infrastructure that can

support the growing need for data security and privacy as the country embraces emerging technologies, including AI. The program promotes the widespread adoption of digital services and tools while simultaneously focusing on creating a safe digital ecosystem. This also includes the development of secure online platforms for e-governance, financial transactions, and healthcare, among others. As part of the initiative, India has been working on enhancing cyber security, frameworks for secure data storage, and ensuring that citizens' data is protected while accessing digital services. As important, the Digital India Program strongly emphasizes privacy and data security when implementing government programs, ensuring AI technologies and other digital systems working with citizens' data are conceived with robust security.

Case Laws

Justice K.S. Puttaswamy v. Union of India (2017):

The Puttaswamy case is one of the landmark judgments pronounced by the Supreme Court of India wherein the right to privacy was recognized as a fundamental right under the Indian Constitution. The decision changed the very face of Indian law, which was altered on the protection of privacy and related issues concerning data protection and surveillance.

Background: This case was based on a challenge to Aadhaar, the biometric identity project initiated by the Indian government. The petitioners, such as a former judge and senior litigant, Justice K.S. Puttaswamy were of the opinion that the collection of biometrics and the non-consensual basis of Aadhaar being an insistence over government services infringed upon the privacy of the individual. The petitioners argued that the Aadhaar system collects and stores sensitive personal data, which can be vulnerable to misuse and surveillance.

Judgment: In a landmark judgment, the Supreme Court ruled that the right to privacy is a part of the right to life and personal liberty under Article 21 of the Indian Constitution. The Court ruled that privacy is a fundamental right and interference into it needs to be subjected to strict tests under doctrines of necessity, proportionality, and legality. The judgment again underlined that sensitive data had to be guarded and personal data, including the biometric part, cannot be processed without strict adherence to consent, transparency, and accountability principles. The government was instructed to ensure the institution of stringent laws for data protection that would shield the privacy of individuals in this digital era.

Impact:

Constitutional Recognition: The judgment brought India at par with the international privacy standards and stated that privacy is a right inherent to every individual.

Legal Reforms: The judgment led to a discussion and, subsequently, drafting of the Personal Data Protection Bill, which will regulate the processing and protection of personal data.

Aadhaar: Although the Court held the constitutional validity of the scheme of Aadhaar it put very important limitations upon its allowance, specifically with regard to privacy and data protection.

2. Google Spain SL v. Agencia Española de Protección de Datos (2014): This case before the European Court of Justice (ECJ) involved the issue of whether individuals have the "right to be forgotten," that is, the right to request the deletion of personal data from search engine results under certain circumstances.

Background: In the year 2010, a Spanish citizen, Mario Costeja González, filed a complaint against Google Spain, arguing that the search results linked to his name included information on his past debts that were no longer relevant. He considered that these harmed his reputation and privacy. González requested Google to remove the link from its search results.

Judgment: The European Court of Justice ruled that individuals have the right to request the

removal of links to out date or irrelevant personal information from search engine results, even if the data itself is publicly available on websites. This right is subject to certain limitations and must be balanced with the public's right to access information.

: The decision provided a template for people to ask search engines to delete information about them. This was, therefore, the first step in control over personal information.

Privacy vs. Freedom of Information: The decision thus created a delicate balance between rights to privacy and the public's interest in freedom of information in the online sphere. It has been a pivotal moment in global debate on digital privacy rights.

This led to the extension of data protection rights within the European Union and also had a subsequent influence on the implementation of the General Data Protection Regulation (GDPR).

Conclusion

As Artificial Intelligence continues to reshape the fabric of our society that brings it unprecedented opportunities combined with significant risks, especially in the realm of human rights, most importantly, privacy. The massive capabilities of AI in processing and analyzing large chunks of data have really made it a necessity in various sectors; however, they also expose individuals to dangers of surveillance, profiling, and exploitation. Therefore, it is significant to ensure that AI is used responsibly and ethically as a way to protect fundamental human rights.

Protecting data privacy in an AI-powered world will require business, government, and individual responsibility. Business will have to adopt ethical AI practices and invest in cyber security, while governments will have to pass comprehensive data protection laws and actively collaborate on an international basis to establish uniform standards. Individuals will also be responsible and vigilant about their rights to privacy while making use of privacy-enhancing tools and advocating for ethical AI policies. Critical steps towards regulating AI and ensuring responsible personal data handling come in the form of global frameworks such as "GDPR" and the "CCPA" and the trends that emerge from algorithmic accountability and harsher penalties. Finally, the efforts of India in strengthening its data protection framework by way of initiatives such as the "Personal Data Protection Bill" and the "Puttaswamy Judgment" reflect a call to treat privacy as a fundamental right in the digital era.

In conclusion, the future of AI cannot be at the expense of human autonomy and privacy. Society will benefit from the advantages of this revolutionary technology by being transparent, fair, and accountable in the design of AI systems. Thus, the ongoing development of legal frameworks, technological safeguards, and ethical guidelines will build a future in which AI increases human dignity and freedom instead of diminishing it.

Observation

In my observation, the rise of Artificial Intelligence (AI) brings with it both immense potential and significant challenges, particularly regarding the protection of human rights and data privacy. AI's ability to process vast amounts of data opens up opportunities for innovation in various fields, such as healthcare, education, and governance. This increases surveillance and unauthorized access, as well as the probability of biases in decision-making. Privacy is being eroded more and more because large amounts of one's personal information are constantly collected, analyzed, and sometimes misused without his or her knowledge or consent. What stands out here is the adoption of ethical AI practices and ensuring that businesses, governments, and others take responsibility to protect privacy. The creation of regulations such as "GDPR" and the "CCPA" and India's "Personal Data Protection Bill" reveals that there is growing recognition worldwide to strengthen data protection mechanisms. Still, this is not all; rather, it is just the start. We need to focus on transparent

collection practices, consent, and we must encourage businesses to take robust cyber security measures for the data they collect. In conclusion, while AI holds great promise, the ethical implications and privacy risks cannot be ignored. It is crucial to continue strengthening regulatory frameworks, creating awareness, and fostering collaborations between stakeholders to protect fundamental human rights in an AI-driven world.

Reference

1. https://www.gp-digital.org/what-would-a-human-rights-based-approach-to-ai-governance-look-like/
2. https://gdpr-info.eu/
3. https://www.entrust.com/resources/learn/what-ccpa#:~:text=The%20California%20Consumer%20Privacy%20Act,%C3%97
4. https://www.dataprivacyframework.gov/Program-Overview
5. https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf
6. https://indiankanoon.org/doc/127517806/
7. http://privacylibrary.ccgnlud.org/case/spain-sl-vs-agencia-espaola-de-proteccin-de-datos-aepd