VOLUME 6 | ISSUE 1

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

AI AND ITS EFFECT ON PRIVACY LAWS

- Ayask Pandey[1]

Abstract

AI is changing the world as we know it; along with it come several challenges, suchasuser privacy. Current privacy laws are ill-equipped to protect user privacy as new things like automated decision-making are introduced, which current privacy laws are not able to protect.

In this research paper,I am going to talk about AI and how it affects privacy and what laws need to be changed to ensure the confidentiality of the user is not affected by it, along with all current privacy laws like the DPDP Act and GDPR and their shortcomings when it comes to AI.

Also, all upcoming acts that are being passed or already passed for AI by different organisations in the world. Along with proposals that can be made to ensure user privacy is protected inchanging times.

Keywords

AI, Privacy, Legal Right, Doctrinal Gaps.

Introduction

Recently, Denmark announced new laws to protect the faces of its citizens from AI by granting them the right to copyright their faces. This comes after numerous instances of people using AI to create deepfakes of others, including making a complete copy of their voice. There has been a significant rise in AI in our everyday lives, and it is being used for various purposes, including research, image generation, and many applications that now utilise AI to augment and create work.

[1] Student at New Law College, BVDU, Pune

This raises concerns among people about the right to privacy and whether they can protect their identity from AI and deepfakes. The right to privacy is a human right that is provided to everyone. It should be protected, but is it really possible in this era of AI, where generative software that feeds on data is constantly being used to create fake or morphed images without the consent of that person, these constant worry comes from the fact that AI constantly uses data to keep updated about current issues and data is always fed to AI and people have no idea from where that data comes from and whether these AI company have taken consent of people while training their AI from the data that is available. There is very little known about AI and how it is taught, and whether the data fed to AI is reliable without any bias.This paper examines the interplay between AI and privacy laws, analysing risks, limitations of current legal systems, and global efforts to regulate AI.

Understanding AI and its dependence on data

[2]'AI system' means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments;

AI in modern times is based on machine learning andis dependent on data that is constantly being fed to it.

It requires a pre-existing set of data to create something using a machine learning algorithm; the origin of that data is crucial to ensure privacy protection of the data owner, as the AI may be trained on other people's data without their knowledge or consent, resulting in privacy infringement.

There are many ways this data can be obtained from many devices that are used in our daily lives, like smartphones, watches, AI voice assistants, etc. The data obtained from these devices can be used to train AI.

Privacy as a legal right

[2]https://artificialintelligenceact.eu/article/3/#:~:text=An%20AI%20system%20is%20a,places%20it%20on%20the%20market.

"Privacy, once understood as the 'right to be let alone,[3]' must now be reimagined in the AI era to protect not only individual autonomy but also informational integrity in an environment driven by data and algorithmic decision-making."

Privacy has always been a tricky subject, as the interest of the nation comes above the privacy of an individual. This argument always comes up when it comes to the national security of a country. This issue was resolved in the landmark judgement of K.S. Puttaswamy v. Union of India (2017)

Privacy has been a legal right for a long time in India. The right to privacy has been declared a fundamental right in the case of Puttaswamy v. Union of India (2017). This 9-judge bench decision ensured that the right to privacy is a fundamental right under Article 21 of the Constitution.

This judgment fundamentally changed privacy laws in India and changed the legal landscape by establishing a constitutional basis for the Right to Privacy.

This judgment opened the door for other government privacy laws to be enacted, ensuring citizen privacy, such as the DPDP Act 2023, which sets rules to regulate, store, and process digital personal data for organisations handling personal data.

It is evident that AI uses personal data to train its model and stores data for its training purposes.[4]. However, it's challenging to determine whether the source of this data was obtained with consent or with the user's knowledge.

Most of the countries in the world either have outdated or don't have any laws to protect user privacy from AI that collects user data, but some countries are now making laws against AI collecting personal data without the consent or Knowledge of the user. These laws need to be updated accordingly, as AI is developing rapidly and may find new ways to collect user data, so laws need to be updated at the same pace.

Statutory Privacy Frameworks: Comparative Overview

The statutory framework regarding AI has been developed in a few countries, including the EU, the U.S and India, with Acts like the DPDP Act and the GDPR, etc.

[3]https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html
[4]https://forums.theregister.com/forum/all/2021/03/18/openai_gpt3_data/

A comparative overview of the privacy framework concerning AI and its potential misuse of user privacy.

European Union – GDPR & AI Act

The E.U. is one of the few organisations that has passed a law called the General Data Protection Regulation 2018, which is one of the first Acts to protect user privacy from AI.While not specifically mentioning AI, it does ensure that users have the right not to be subjected to automated decision-making.[5]. This act also gives the user the right to object, rectify, erase and restrict processing of user data, even if they operate outside the E.U. but still hold and process E.U. citizens' data.

The EU also introduced the AI Act in 2024, which restricts and regulates AI by banning AI systems that infringe on users' fundamental right of privacy and also regulates AI to ensure transparency and data storage of the user.[6] The AI acts in line with GDPR to prevent AI systems from exploiting user privacy without restricting the way AI works and trains.

These act gives us the idea of regulating AI and ensuring user privacy while for the development and use of AI.

United States – CCPA/CRPA

The U.S currently lacks any specific federal law to protect privacy,but they do have state laws and some laws that have the concept of privacy in them, but they are not specifically made for privacy; rather, privacy is a part of that law. One of the state laws is the California Consumer Privacy Act (CCPA), which gives the consumer the right to know, delete, modify or limit the use of their personal data. [7]This act ensures that consumers' right to privacy is protected under state law,but it does not mention AI or misuse of data by AI, as the law needs reform to include AI and data gathered through AI.

India – Digital Personal Data Protection Act (DPDP Act)

The DPDP Act was enacted in August 2023 to govern the processing of personal data. It was formed after the KS Puttaswamy judgment declared privacy as a fundamental right, which paved the way for parliament to make a law to protect the privacy of Indian citizens from

[5]https://gdpr-info.eu/
[6]https://artificialintelligenceact.eu/
[7]https://oag.ca.gov/privacy/ccpa

companies using their data without any restrictions. This law gave the user the right to access, correct, erase their data. This act also allowed the users to nominate someone else to exercise these rights.

This act also created an obligation for companies to obtain consent of the user and use it lawfully, also inform the government of any data breach and the individuals affected by it, and use measures to prevent data breaches.[8]

These are all the measures taken by the Indian government to ensure the privacy rights of its citizens are protected by this law.

These are the privacy laws created by countries to ensure the privacy of their citizens, but none of these laws are made specifically for AI to prevent privacy violations. Although DPDP act as well as GDPR act, both have some provisions that can be applied to AI, but these laws still lackthe right against automated decision-making or data transparency, which are needed to ensure data protection in the age of AI.

Doctrinal Gaps in Applying Privacy Law to AI

- **Consent and Autonomy**- Data obtained for AI training and use may come from sources that have not consented to it or may not know about it.
- **Limited scope but wide use-** Some data with limited scope can be used out of its scope, like personal data of an individual can be used outside its scope or allowed limit.
- **Data Minimisation** - governments worldwide promote minimal data collection, but AI's entire model relies on data gathering.
- **Accountability and Liability –** Most privacy laws around the world are ill-fitted for AI use,as AI is not held accountable for privacy failure like other companies are.
- **Cross-border data transfer**- AI use cross-border data that undermines local jurisdiction,which needs to be addressed

AI Specific Privacy Concerns in Law

1. Automated decision making- automated decision making is an AI-specific privacy concern, as AI may use personal data without users' consent and may

[8]https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

even share it with people, as it might not follow regulations set in local regulations. Some acts are in place to stop it, but they are obsolete, and new laws need to be made against it.

2. Profiling and discrimination – since AI use data to give a specific response, it may cause profiling and discrimination based on the data that has been used to train it. So, laws need to be made to ensure that neutral data is used to train AI.
3. Opacity and Explainability- due process requires reasons for adverse decisions. AI lacks the explainability of where it gets data from, whether the sources are legitimate or illegitimate, which makes these decisions riskier and causes privacy concerns for users.
4. Re-identification of data- even though sources of data may be anonymous, AI can infer data to identify the individual through different data sets provided to it, which violates the privacy rights of that individual.
5. Right to erase data- usually, when it comes to data used by a corporation, there exists a right of the user to delete that data, but when it comes to AI, even if the user deletes the data, as AI already incorporates data that has been deleted.

Emerging Legislative and Policy Responses

European Union- AI Act

The EU introduced the AI Act in 2024[9],allowingthe EU to classify AI into 4 categories: unacceptable risk, high risk, limited risk and minimal risk. These categories classify AI that are to be banned, monitored and regulated to follow certain restrictions to carry out their operations or to be banned completely to protect the citizens and country alike.

- **Unacceptable/ Banned AI Systems - Banned** AI systems include social scoring, biometric recognition in public, and AI manipulating children are completely banned. This was made to ensure privacy and protection for the vulnerable groups from AI misuse.
- **High Risk AI Systems-** High-risk AI includes credit scoring AI, healthcare, recruitment, and law AI; all these are allowed only after fulfilling a list of regulatory

[9]https://artificialintelligenceact.eu/

and compliance processes, including cybersecurity, transparency, human oversight, quality data sets, etc.

- **Limited risk AI systems-** these systems are used in our daily lives, like chatbots, generative AI, etc.This system needs to be transparent and disclose important information. To the user, like they are talking to a chatbot or the content is AI-generated, etc.
- **Minimal risk AI system-** the risk associated with these is pretty low, so that they can work without any regulation. These are AI spam filters or AI used in games, etc
- **Special rules for general-purpose AI-** these are special rules set for large language models like ChatGPT, Gemini, etc. These rules include publishing technical documentation, safeguarding against misuse and disclosing copyrighted data.

These are some of the rules made by the EU to regulate this, making the EU one of the first organisations to make laws to regulate AI and ensure the protection of the privacy of its citizens.

United States- As of now, there is no federal U.S. act that acts on AI, but there are some laws that are close to being enacted, such as the Take it Down Act[10], introduced in 2025. This act is passed to curb deepfakes of individuals without their consent, made from AI or an authentic method, both of which are to be taken down immediately.

There is also a state act, the Colorado AI Law, that may be passed in 2026, which might setthestage for other laws that protect user privacy from AI to be passed.

India – India does not have a law to control and regulate AI, but India does have laws that protect user privacy, like the DPDP Act, since it ensures that personal data, as mentioned in the act, that "any system that processes personal data, partially or wholly automated, must comply with the DPDP Act "[11]

So, AI also comes under the ambit of this act; other than this, there are no provisions made to protect user privacy from AI. Also, this act has many issues, as it does not cover a lot of things like automated decision-making,which makes this not as effective in protecting privacy when it comes to AI.

[10]https://www.congress.gov/bill/119th-congress/senate-bill/146
[11]https://www.meity.gov.in/documents/act-and-policies?page=1

These are all the policies that government organisations of the world have made or are in the process of making. Many policy suggestions can ensure that the privacy rights of the user are protected.

Reform Proposals: Towards AI-Responsive Privacy Laws

- **Strengthening consent model-** As AI is moving toward automated decision making, moving toward a dynamic consent model allows the user to adapt to continuous changes in AI, so laws need to be made to ensure a proper consent model to protect user privacy.
- **Expanding Definition of Personal Data- The** Definition of personal data needs to be expanded to include pseudonym data, as it can be inferred by AI to form a pattern that can identify the person.
- **Cross-Border Treaty-** Cross-border treaties need to be signed so that the privacy of the user can be protected even if data is moved to a different country with a different jurisdiction.
- **Institutional Reform-** institutions that are solely made for AI monitoring needs to be made as AI is integrating into our daily lives, as well as constantly evolving, we need these institutions to constantly monitor and regulate AI so privacy can be protected.
- **Embedding Privacy Design-** Privacy laws need to be embedded in the AI system as a statutory requirement, which ensures privacy at the core of AI. This move will protect user privacy.

These are all policy proposals that the government organisation of the world can make to ensure the privacy rights of the user.

Conclusion

The use of AI in recent times in many different fields has increased manyfold, and privacy concerns from this are beyond the scope of current privacy laws. This raises concern for the privacy rights of the individual, which can be addressed if the laws are made for AI that protect user privacy. The privacy laws must evolve in three directions — conceptual

(redefining privacy), institutional (empowered regulators), and transnational (harmonised global norms).

This way, the laws can not only ensure the data of the user but also the dignity, privacy and autonomy of the user are protected.

The challenge of law in the AI era is not only protecting personal data but also making laws that keep evolving to keep up with constantly evolving AI.