The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2024

Editor-in-Chief – Prof. (Dr.) Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

AI AND RIGHT TO PRIVACY: A COMPREHENSIVE ANALYSIS

AI abbreviates to Artificial Intelligence is the volatile technological advancement which is aiming to be effective than the human intelligence.

Artificial Intelligence (AI) is the replication of human intelligence in machines, where they are programmed to mimic human-like thinking and learning abilities. It involves the development of computer systems that can undertake tasks traditionally requiring human intelligence, including comprehension of natural language, pattern recognition, decision-making, problem-solving, and adaptability to new circumstances.[1]

In today's world the requirement necessary to get any IT job is to possess the Ai utilization skill. Although AI is proved to be helpful in many aspects it is still accused of violating the right to privacy. Right to Privacy is the crucial right which has been recognised by supreme court's nine Judge bench as the fundamental right within Article 21 of Indian Constitution in the year 2017. Privacy is the state of being free from unwanted or undue intrusion or disturbance in one's private life or affairs; freedom to be let alone:[2] The right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21and as a part of the freedoms guaranteed by Part III of the Constitution[3]

INFORMED CONSENT IN AI APPLICATION

[1] Diya Saraswat, Laws governing AI in India: Everything you should know, Legal Service India(e- journal).(Feb 1, 2024, 7:58pm), https://www.legalserviceindia.com/legal/article-13111-laws-governing-ai-in-india-everything-you-should-know.html

[2] Dictionary.com https://www.dictionary.com/browse/privacy (last visited Jan 30, 2024, 6:20am)

[3] Dristhi IAS https://www.drishtiias.com/daily-updates/daily-news-analysis/right-to-privacy-3 (last visited Feb 2, 2024, 8:32pm)

Generative AI needs vast amounts of data, and this data helps the model learn and generate new content. But where does this data come from? That is why it’s crucial to source this data ethically.[4]

Linchpin of privacy in AI is the consent. Although the concept of consent does not sound complex, it is in AI has much more significant than the generic “Accept all cookies” which we hit every time it pops up. Users of these AI applications voluntarily give consent for any use of their private data which they usually prefer to keep within their close family/friends circle or within themselves and in most of these cases, reason behind such provided consent is not that they have completely read and understood the terms and condition the application but simply hitting “Accept all terms and condition” without actually reading it and one main reason is that the smartness of the AI application owners who in the screen give “Read terms and conditions” which if you click then lead to another page where the terms and conditions are listed, rather than showing the actual terms in the first screen. The users with braveness or overconfidence along with their slothfulness rather choose to directly clicking the “Accept all terms and condition” and taking risk than taking time and reading the terms and conditions of the application. In this way they are willingly giving out their data. AI on the other hand to be fed with information and data to make it work masterfully and by giving out our data without reading the terms and conditions our information is fed to AI to facilitate in its working. Informed consent simply means the consent given by the person with his conscience.

"Nobody asks bystanders to sign a consent form before they get hit by a self-driving car. The car just hits them. The driver had to sign consent forms to purchase their car, letting the corporation off the hook for much of what goes wrong. However, the driver -- perhaps the most likely person to be killed by it -- never secures the consent of all the people exposed to that vehicle; these innocent bystanders get no say in whether they agree to be exposed to possible harm.[5]

Informed consent is a core concept holding together the rule-based international order. If you sign a contract, then you are legally bound to its terms. If you undergo a medical procedure,

[4] Shaip https://www.shaip.com/blog/the-role-of-consent-in-training-generative-ai/ (last visited Feb 1, 2024)

[5] SCU.Edu https://www.scu.edu/ethics/media-mentions/stories/should-ai-require-societal-informed-consent.html (last visited Feb 3, 2024)

you read the forms and sign your name, absolving medical practitioners from liability. If you get an app from the App Store, you sign a user license agreement that protects the app developer, not you."[6]

IMPACT OF AI ON PRIVACY

Although AI has vast benefits, it still possesses certain threat and one such concern is the privacy of an individual. All AI applications claim to be not a threat to privacy but the hidden reason behind how they collect data has been mentioned in the earlier paragraphs. The ways AI uses to collect data present serious privacy concerns, such as facial recognition software surveillance, possible data breaches that could result in identity theft, biased profiling and discrimination, a lack of informed consent, and the secondary use of data without user knowledge.[7]

AI presents a challenge to the privacy of individuals and organisations because of the complexity of the algorithms used in AI systems. As AI becomes more advanced, it can make decisions based on subtle patterns in data that are difficult for humans to discern. This means that individuals may not even be aware that their personal data is being used to make decisions that affect them.[8]

Not so long-ago AI was introduced in Snap Chat application also in the name of My Ai. As per my observation here, the users of snap chat can connect with Ai where it interacts with the users. When Ai was introduced in snap chat, it came on user's chat log as a normal snap chat's chat and the matter here is once you open the 'MyAIi" chat you cannot exit without accepting its terms and conditions without directly clearing the tab. There were many incidents reported pertaining to "My Ai" where snap chat claims to have no access to the personal data of the users yet it is found to be knowing everything. One of the distressing and questionable incidents is that a TikToker named evanpackardfinance displayed an exchange

[6] Ibid

[7] Kashish Maggo, Artificial Intelligence: Impact on Right to Privacy, Juris Centre, (Feb 1, 2024, 9:49pm) https://juriscentre.com/2023/09/12/artificial-intelligence-impact-on-right-to-privacy/#:~:text=AI%20privacy%20concerns%3A,of%20data%20without%20user%20knowledge.

[8] Dr Mark Van Rijmenam, CSP, Privacy in the age of AI: Risks, challenges, and solutions, The Digital Speaker, (Feb 1, 2024, 11:14pm) https://www.thedigitalspeaker.com/privacy-age-ai-risks-challenges-solutions/

with the bot about his location, in which My AI asked him where he liked to hike in his city. When asked directly, My AI denied knowing his location, but when asked again after changing the subject, the bot appeared to respond with the user's location.[9] Snap chat is just an example for the activities of Ai applications.

Artificial Intelligence (AI) indeed holds tremendous promise in enhancing our abilities, yet it's not without its pitfalls, especially in relation to privacy and security. The risk emerges from AI's proficiency in gathering, scrutinizing, and amalgamating vast volumes of data, a significant portion of which may be of a personal and sensitive nature. The Stanford Institute for Human-Centred AI (HAI) documented these concerns in a 2021 report, shedding light on the potential privacy and security challenges posed by AI.[10]

AI systems rely on extensive data collection to train and improve their algorithms. This data can include personal information, online activities, social media interactions, and more. While this enables AI to make accurate predictions and deliver personalized experiences, it also raises concerns about how this data is collected, stored, and used.[11] The increasing reliance on AI systems means that large volumes of sensitive data are being stored and processed. This presents an attractive target for cybercriminals who seek to exploit vulnerabilities and gain unauthorized access to personal information. Data breaches can have severe consequences, including identity theft, financial loss, and reputational damage.[12]

A survey of above 5000 people from different countries, conducted by Genpact in 2017 revealed that 63% of respondents prefer privacy over the customer experience and want companies to avoid using AI in case it invades their privacy, no matter how delightful customer experience it is delivering. About 71% of the respondents showed apprehensions

[9] Tuhin Das Mahapatra, Snapchat's My AI Chatbot Faces Criticism Over User Privacy and Accuracy Concerns, Hindustan Times (last visited 3Feb 3, 2024, 6:27am) https://www.hindustantimes.com/technology/snapchats-my-ai-chatbot-faces-criticism-over-user-privacy-and-accuracy-concerns-101682323903867.html

[10] Medium. Fentelics https://fintelics.medium.com/ai-and-its-impacts-on-privacy-and-security-57243e9d0b6f (last visited Feb 1, 2024, 4:16pm)

[11] Medium. Alexender Stahl https://medium.com/@stahl950/the-impact-of-ai-on-data-privacy-safeguarding-our-digital-footprint-2974ee8221a6 (last visited Feb 1, 2024, 5:04pm)

[12] Ibid

that AI would be even making their main decisions without even their consent or knowledge.[13]

LEGAL FRAMEWORK (INDIA)

Currently, there are no specific laws in India regarding regulating AI. Ministry of Electronics and information Technology (MEITY), is the executive agency for AI-related strategies and had constituted committees to bring in a policy framework for AI.[14]

The Niti Ayog has developed a set of seven responsible Ai principles, which include safety & dependability, equality, inclusivity and non-discrimination, privacy and security, transparency, accountability and the protection and reinforcement of positive human values. The Supreme Court and high courts have a constitutional mandate to enforce fundamental rights including the right to privacy. In India, the primary legislation for data protection is the Information Technology Act and its associated rules. Additionally, the Digital Personal Data Protection Bill has been introduced by MEITY, although it is still awaiting formal enactment. If this bill becomes law, individuals will have the ability to inquire about the data collected from them by both private and government entities, as well as the methods utilized to process and store it.[15]

According to the Indian Constitution, encroachment on privacy stands in violation of the fundamental right to privacy which has been read into the right to life and personal liberty under Article 21. In 2012, a report by a group of experts, constituted under the government of India, talked about technological neutrality and conformity with data protection and international privacy policies, but it did not specifically talk about any policy changes that can be made with special reference to AI. However, in a recent report, the Ministry of

[13]ThinkML https://thinkml.ai/is-artificial-intelligence-a-threat-to-privacy/#google_vignette (last visited Feb 1, 2024, 3:32pm)

[14] Aditi Prabhu, Artificial intelligence in the context of the Indian Legal profession and judicial system, Bar and Bench, (last visited Feb 1, 2024, 11:19am) https://www.barandbench.com/columns/artificial-intelligence-in-context-of-legal-profession-and-indian-judicial-system

[15] Ibid

Electronics and Information Technology has proposed the use of an anonymization infrastructure for processing Big data in order to promote the privacy of individuals. [16]

AI developments are prompting a need for ethical guidelines and best practices to minimize privacy risks. Several industry leaders have already taken steps to address these concerns, such as Elon Musk's open letter in March calling for a six-month pause on AI development to assess the technology's societal impact. His unprecedented move served as a wake-up call for the industry to scrutinize AI's implications more closely.[17]

There has been a gross negligence on the part of various agencies and data breach which is constantly taking place in India. Through a report it has been recorded that around 3 lakh cybersecurity incidents were reported in 2019 alone, recorded by the Indian Computer Emergency Response Team (CERT-In)[18]. Some of the highly noted and high- profile data breach which took place in India are the Air India data breach which had an impact of 4.5 million, passenger personal data worldwide. There was also a story of data breach, where CAT burglar strikes again and exploited 2 lakh CAT applicant’s data. In a major fall back the entire customer base of Upstox had to reset their password due major data breach.[19]

The AI is a very magical model which can make human like decision at a very high range. It is estimated by International Data Corporation (IDC), that the Indian Market for AI will grow around $7.8 billion by 2025.[20] The Data Protection Bill could change the face of AI application in India and would also result in safeguarding people’s personal data. For any AI expansion data is the only major asset and if the government controls the regulation of such

[16] Parul Chaudhary, policy improvisation: addressing vulnerability caused by intrusion of AI in privacy of individuals, iPleaders, (last visited Jan 31, 2024, 3: 32pm) https://blog.ipleaders.in/policy-improvisation-addressing-vulnerability-caused-intrusionaiprivacyindividuals/#Corroborating_data_privacy_compliance_by_AI

[17] Gai Sher and Ariela Benchlouch, The privacy paradox with AI, Reuters, (last visited Feb 4, 2024, 5:21am) https://www.reuters.com/legal/legalindustry/privacy-paradox-with-ai-2023-10-31/#:~:text=The%20technology's%20potential%20to%20infer,that%20demand%20immediate%20proactive%20solutions

[18] Soumik Ghosh, *The biggest data breaches in India*, CSO (Feb 1 2024) https://www.csoonline.com/article/569325/the-biggest-data-breaches-in-india.html

[19] Ibid

[20] Aishwarya Srinivasan, *India’s Data Protection Bill in the light of Responsible AI*, LinkedIn, (last visited Feb 1,2024,10:19am) https://www.linkedin.com/pulse/indias-data-protection-bill-light-responsible-ai-aishwarya-srinivasan/

data, then the entire nation could be secured from all types of hidden data exploitation which takes place in the lure of innovation and development.

The key highlights of the Personal Data Protection (PDP) bill of India, which is still hunting for its light from the legislature is a great base which have been established and if the government works on it with right vision, then it can really turn out to be one of the greatest assets for the nation. The following are the bill's main highlights[21]

- Purpose-based data collection and usage – The bill requires organisations to only gather specified categories of users' personal data that are deemed necessary for the goals the organisation has set. Data collection by the organisation must not go beyond what is necessary for the usage and the data must only be utilised for the defined use and not be transferred to other use-cases.
- Consent for data collection: Under the bill, organisations must present a consent that users can accept or reject. Users' data should only be gathered from those who have given their agreement to share it.
- Individuals' Data Rights – The bill gives people the right to access and examine the data that is being gathered on them, the right to ask for the data's deletion if it is inaccurate, and the right to recommend changes.
- Data Localization: According to the statute, "Critical data" must be processed locally in India. A copy of "sensitive personal data"[22] (such as biometric data, government identifiers, and financial information) must be kept in India even if it is moved outside of the country.
- Data Protection Authority: The proposed legislation calls for the establishment of a central body to oversee and enforce the laws outlined in the Data Protection Bill.

A major concern that revolves around the corner of Data Protection Bill is, "Will the data Protection bill cause a disruption or stoppage to the AI advancements and innovations ", the answer to this is a big NO, because the Data Protection bill will prevent the unethical use of data and which would further build a responsible AI application which knows its boundaries

[21] Ibid

[22] Ibid

of expansion and will be conducive to sustained use of technology which would be built on human touch and will be very much human-centric in approach.[23]

HERE ARE SOME PROVISIONS THAT DEALS WITH AI:

- Information Technology Act, 2000:

  The Information Technology Act, 2000 (IT Act) serves as the fundamental legislation governing electronic transactions and digital governance. Although it does not explicitly mention AI, specific provisions within the Act are applicable to AI-related activities. Section 43A of the IT Act enables compensation in case of a breach of data privacy resulting from negligent handling of sensitive personal information. This provision is particularly relevant in the context of AI systems that process user data. Another provision is Section 73A of this act.[24]

- Personal Data Protection Bill, 2019:

  The Personal Data Protection Bill, 2019 (PDP Bill) is currently under consideration and aims to establish a comprehensive framework for protecting personal data. The bill introduces principles and obligations for entities processing personal data, including consent, purpose limitation, data localization, and accountability.
  Additionally, it proposes the creation of a Data Protection Authority to oversee and enforce the provisions of the bill.The PDP Bill includes provisions addressing profiling and automated decision-making. It mandates explicit consent from individuals when processing personal data using AI algorithms that significantly impact their rights and interests.[25]

- Indian Copyright Act, 1957:

[23] Ibid

[24] Diya Saraswat, Laws governing AI in India: Everything you should know, Legal Service India(e- journal).(Feb 1, 2024, 7:58pm), https://www.legalserviceindia.com/legal/article-13111-laws-governing-ai-in-india-everything-you-should-know.html

[25] Ibid

The Indian Copyright Act, 1957 safeguards original literary, artistic, musical, and dramatic works, granting exclusive rights to creators and prohibiting unauthorized use or reproduction. The rise of AI-generated content has prompted discussions regarding copyright ownership and infringement liability[26]

- AIRAWAT: Recently, Niti Ayog (planning commission of India) also launched AIRAWAT, which stands for AI Research, Analytics, and Knowledge Assimilation platform. It considers all the necessary requirements of AI in India.[27]

CASELAWS

Justice K.S. Puttaswamy (Retd.) v. Union of India[28]

The Supreme Court of India recognized the right to privacy as a fundamental right under the Indian Constitution. This ruling emphasizes the need to safeguard personal data from AI-based systems.

Gramophone Company of India Ltd. v. Super Cassettes Industries Ltd.[29] *(2011),*
the Delhi High Court determined that AI-generated music produced by a computer program lacks human creativity and, therefore, is ineligible for copyright protection. This case clarifies the copyrightability of AI-generated content in India.

R v. Spencer (2014),[30] The Canadian Supreme Court recognized informational privacy in the online space. It also talked about anonymity as an element of informational privacy. Thus, if AI technologies are used to de-anonymize individuals and re-identify them by collecting data

[26] Diya Saraswat, Laws governing AI in India: Everything you should know, Legal Service India(e- journal).(Feb 1, 2024, 7:58pm), https://www.legalserviceindia.com/legal/article-13111-laws-governing-ai-in-india-everything-you-should-know.html

[27] Ibid

[28] (2017) 10 SCC 1; AIR 2017 SC 4161

[29] 1995(33)DRJ333

[30] 2014 SCC 43

from multiple sources, then it will cause a breach of the informational privacy of an individual.[31]

SUGGESTIONS FOR PRIVACY PROTECTION FROM AI

Here are some best practices to significantly mitigate the data privacy risks associated with using AI in customer service.[32]

1. Anonymize your data

Data anonymization involves removing or modifying personal identifiers in your datasets. This prohibits identifying or associating individuals with data. When you use this data AI model training, you have useful data without the risk of compromising customer privacy. Even if there is a breach, there is no way to trace the leaked data back to specific customers.

2. Involve human oversight

This means incorporating human judgment into your AI decision-making processes. A human supervisor should review and validate the decisions made by your AI systems, providing a crucial layer of oversight. Practicing human oversight helps you catch errors or biases that the AI might overlook.

3. Implement data retention policies

You probably do not need to keep your customer data forever. In fact, you should keep it only for as long as you need it in your processes, then delete it once it's no longer necessary. By limiting how long you keep your customer data, you reduce the risks of unauthorized access or data breaches.

[31] Parul Chaudhary, policy improvisation: addressing vulnerability caused by intrusion of AI in privacy of individuals, iPleaders, (last visited Jan 31, 2024, 3: 32pm) https://blog.ipleaders.in/policy-improvisation-addressing-vulnerability-caused-intrusion-ai-privacy-individuals/#Corroborating_data_privacy_compliance_by_AI

[32] Alvin Lee, How to protect data privacy when using AI, twillo, (last visited Feb 3, 2024, 7:409pm) https://www.twilio.com/en-us/blog/ai-data-privacy

Data retention policies dictate how long to store data and when to delete it. Establish these policies, then enforce them. This not only enhances privacy but also ensures compliance with various data protection laws—such as GDPR, HIPAA, CCPA, and more.

4. Be transparent with your customers

Transparency with your customers is essential to building their trust. Your customers have the right to know how you use their data.

The AI should offer a clear and concise overview of how an AI model uses data, along with its level of data privacy. Because so much of modern AI usage is opaque, providing a high level of transparency to your customers will be a welcomed change and foster a tremendous amount of trust.[33]

CONCLUSION

AI has now made its place in all the fields; medical science is also not an exception. It is said that some day AI will take over the world and dominate humans and on the other hand AI camera misunderstood bald head as a ball and followed him throughout the match. It cannot be said that AI violates the right to privacy but the present models of AI is not concerned about the Right to Privacy, with proper enforcement of laws and rules the AI applications can be designed in such a way that it can be helpful for the users without violating their privacy.

[33] Ibid