THE ROLE OF ARTIFICIAL INTELLIGENCE IN SHAPING THE FUTURE OF PRIVACY IN INDIA

Sameera Ekhlaq*

ABSTRACT

Artificial intelligence (AI) technology is advancing quickly around the globe, with the internet becoming a commonplace presence and erasing geographical barriers to information flow. Data is now a vital component of our daily lives, with nearly every aspect of contemporary life being connected to AI in some way. Every aspect of our everyday lives, even social networking, banking etc. is closely connected to AI. It resulted in numerous new and intricate privacy and data protection issues. At the same time, it is imperative to guarantee that citizens should maintain and control their personal data by exercising their fundamental rights under Article 21 of the Constitution. The Indian government has adopted several laws in response to the growing concern over the protection of personal data and individual privacy rights. The preamble of the DPDP Act, 2023 seeks to offer a legislative viewpoint for safeguarding private data and individual rights in India's tremendously expanding technological advancements. This research attempts to examine the effectiveness of the legislation, and the difficulties associated with data protection laws in India, and to offer a solution for the beneficial applications of artificial intelligence.

Keywords: Artificial Intelligence, Technology Advancement, Personal Data, Fundamental Rights.

INTRODUCTION

Artificial intelligence is the simulation of human intelligence processes by machines, especially computer systems. Artificial intelligence (AI) is the intelligence that machines demonstrate, as opposed to natural intelligence that is exhibited by people or animals. AI is employing technology to automate processes that would typically call for human intelligence[1]. The theory and development of computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation

*BA LLB, FOURTH YEAR, UNIVERSITY OF ALLAHABAD.

[1] Artificial Intelligence, ENG. OXFORD LIVING DICTIONARIES, <https://en.oxforddictionaries.com/definition/artificial_intelligence> accessed 26, September 2024

between languages. The term 'Artificial Intelligence' for the very first time in 1956, when computer scientist Alan Turning attempted to decipher a section of code known as the "Enigma code," which the German forces employed for encrypted communication, machine learning was first applied during World War II. Turing claimed that a machine may be considered "intelligent" if it could converse with people while remaining hidden from them[2]. In the last few decades, the utilization of AI has tremendously increased due to its effortless access. With the use of AI technology, researchers have successfully automated a number of challenging jobs, like driving a car, playing chess, and interpreting between languages humans employ a wide range of cognitive abilities, including reasoning, planning, strategizing, and decision-making. Last but not least, driving entails using a few brain systems, including those related to vision, spatial perception, situational awareness, movement, consciousness, and judgment. However, this scientific fiction and futurological technology have also proposed that AI could threaten human survival due to its enormous potential and capability.

ACKNOWLEDGMENT OF THE PRIVACY RIGHT AS A FUNDAMENTAL RIGHT

The journey from the Supreme Court's denial[3] of the right to privacy to its acceptance[4] and subsequent recognition as a fundamental right changed dramatically.

The Right to Privacy was first introduced in the case MP Sharma and Others v Satish Chandra[5], just four years after the commencement of the Constitution, the Supreme Court while dealing with the question of the right to Privacy decided on the practice of search and seizure when contrasted with privacy. In the case of Kharak Singh v State of Uttar Pradesh[6], the Apex Court has not recognized the Right to Privacy as a part of Fundamental Right. However, in the case of Govind v. State of Madhya Pradesh,[7] the Court placed more emphasis on privacy rights by stating that an individual's right to privacy must be balanced against a compelling state interest. The scope of privacy has grown over time, and it now includes personal sensitive data such as medical records and biometrics.

[2] Simanta Shekhar Sarmah, 'Concept of Artificial Intelligence, its impact and Emerging Trends'(2019) 6(11) IRJET <https://www.irjet.net> accessed 26, September 2024
[3] Kharak Singh v. State of UP, 1963 AIR 1295
[4] Retd. Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1
[5] MP Sharma v Satish Chandra 1954 AIR 300, 1954 SCR 1077
[6] Kharak Singh v State of Uttar Pradesh, AIR 1963 SC 1295,
[7] Govind v. State of Madhya Pradesh, 1975 SCC(2) 148

In the case of R. Rajagopal v State of Tamil Nadu[8], the Supreme Court acknowledged the right to privacy as a fundamental component of individual freedom. The court ruled that the release of private, non-public data without permission may constitute a privacy invasion and that people's right to privacy must be respected. The concept of privacy, as a basic right, has evolved along with the inclusion of privacy regulations as established by the legislature in place of these rulings of the Court.

Subsequently, in the case of PUCL v Union of India[9] also known as the Telephone Tapping Case, the Supreme Court determined that individuals had a privacy right in the content of their phone conversations. Thus, a succession of instances demonstrates that the right to privacy was accepted, but its limitations were also given careful consideration.

In the second decade of the 21st century, privacy concerns have concentrated on Aadhaar, a government system that provides people with a unique ID based on biometrics like fingerprints and iris scans demographic information. The Aadhaar was challenged in the Supreme Court on the basis of violation of the Right to privacy.

In a historic decision delivered on August 24th 2017, the Bench unanimously recognized a fundamental right to privacy of every individual guaranteed by the Constitution, within Article 21 in particular and Part III on the whole. The decisions of *M.P.* Sharma and Kharak Singh were overruled[10].

PRIVACY REGULATIONS IN INDIA

Through its "Digital India" plan, the Indian government lately envisioned a digital world during the global "Digital Revolution" of the twenty-first century. But the real question is: Will this initiative be successful in a developing country like India, which does not have a particular data protection statute? This brings us to the significance of data protection. Every nation that aspires to be fully digitalized and has a digital economy needs to have strong, transparent, and accountable data protection regulations of its own. Since the right to privacy, which includes the protection of personal data, is a fundamental right in India, our Supreme Court on August 24, 2017, in its landmark judgment in the case of Justice K.S. Puttaswamy and Anr. v. Union

[8] R. Rajgopal v State of Tamil Nadu, 1995 AIR 264, 1994 SCC (6) 632
[9] PUCL v Union of India, AIR 1997 SC 568 / (1997) 1 SSC
[10] Supreme Court Observer, 'Fundamental Right to Privacy'< https://www.scobserver.in/cases/puttaswamy-v-union-of-india-fundamental-right-to-privacy-case-background/> accessed 24, September 2024

of India And Ors[11].("Right to Privacy Case"). After this Judgment, the legislation was urgently required to protect the personal data and privacy of individuals. As a result, in August 2017, the Central Government of India appointed a Data Protection Committee under the chairmanship of retired Supreme Court judge, Justice Srikrishna and on July 27, 2018, the committee headed by him released an extensive white paper showing the importance and need of data protection law in the country. Consequently, in July 2018, the committee released the final draft of the Personal Data Protection Bill, 2018. Later the Personal Data Protection Bill, 2019 ("PDP Bill") was introduced in the Loksabha with few modifications.

Subsequently, on December 12, 2019, the PDP Bill was referred to a Joint Parliamentary Committee ("JPC") for further debate and examination. After around 2 years, the committee submitted its report with various recommendations and changes. The Digital Personal Data Protection Act got the assent of the President of India in August 2023 but it has to have come into force with the notification of the Central Government. August 2024, marks the end of one year under India's new data protection law, But even after a year, it is essentially useless because the clauses are still unenforceable in the lack of specific regulations that have not yet been announced.[12]

This legislation provides the protection of all digital personal data, whether it is kept online or was first kept offline before being converted to digital form, is covered by the DPDP Act. It also covers the processing of digital personal data that takes place outside of India, especially when it comes to providing products or services to people who are physically present in India. Under the DPDP Act, individuals possess several rights, including the ability to access information about how their data is processed, rectify incomplete or inaccurate data, remove data that is no longer needed for processing, file a complaint in the event of a data breach, and designate another person to exercise these rights in the event of incapacity or death.

Targeting the growing concerns about misinformation propagated by Artificial Intelligence such as Deep fakes etc. the Ministry of Electronics and Information Technology ('MeitY') released an advisory to all intermediaries to ensure compliance with the existing Information

[11] Retd. Justice K.S. Puttaswamy and Ans. v. Union of India and Ors., (2017) 10 SCC 1

[12] Business Standard,'One year of DPDP Act: Firms in a fix over delayed implementation of rules'(Monday, September 23, 2024) <https://www.business-standard.com/economy/news/one-year-of-dpdp-act-delayed-rules-hamper-india-s-data-protection-law-124081100299_1.html > accessed 23, September 2024

Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023 (the "IT Rules").[13]

AI CAN ASSIST IN DATA PROTECTION

Everything has two fundamental aspects; similarly, Artificial Intelligence is used to provide both opportunities for stronger protection and challenges that need to be tackled and surveillance as well. The equilibrium needs to be maintained and it can be achieved by effective privacy legislation that safeguards individual rights while fostering innovation.

Artificial intelligence (AI) and machine learning (ML) are becoming crucial to information security because of their ability to swiftly and expeditiously evaluate millions of data sets and detect a variety of cyber threats, from malware to questionable behaviour that might indicate a phishing attempt. The ideal choice for businesses looking to thrive in the contemporary online marketplace is AI cyber security. Security experts need strong support from intelligent machines and cutting-edge technology like artificial intelligence (AI) in order to defend their enterprises against cyber-attacks.

As a confidential advisor, AI has advanced endpoint security protocols by promptly identifying, analyzing, and thwarting intrusions through a comprehensive behavioural analysis. Patterns are typically used to identify cyber-attacks. AI can be highly beneficial in examining current data to detect similar and recognizable patterns in fresh data.[14]

When an application or service in the system or network exhibits anomalous or unexpected behaviour, artificial intelligence and machine learning can notify the user or network administrator. Additionally, it has the ability to immediately stop unauthorized data transactions, suspicious activity, and harmful websites before they are carried out. In addition, AI can assist in swiftly rolling back to a previous secure endpoint in the event of a security compromise.

Envision a technologically advanced digital protector that constantly monitors your emails to look for any dangers. AI-driven data security tools are like a watchful watchtower; they spot

[13] Deeksha, 'MeitY issues advisory against AI-Deepfakes on social media and other platforms' SCC Online(2023) <https://www.scconline.com/blog/post/2023/12/28/meity-issues-advisory-against-ai-deepfakes-on-social-media-legal-news/> accessed 23, September 2024

[14] How AI Can Help in Personal Data Protection and Privacy<https://10xds.com/blog/ai-for-personal-data-protection-and-privacy/?hl=en-IN> accessed 23, September 2024

phishing emails' dubious links and possibly dangerous attachments right away. These sophisticated technologies examine every aspect of the communication, including the sender's personal information and the finer points of the text. Like a detective putting together clues, they are doing more than simply data analysis; they are also interpreting context and making connections between the message's body and subject line. Real-time notifications are triggered by the AI when it detects a possible danger, keeping you and your network one step ahead of hackers. Businesses can turn the tables on would-be invaders and strengthen their defences like never before by utilizing these cutting-edge behavioural analysis technologies to revolutionize how they handle phishing and social engineering assaults.[15]

HOW THE GOVERNMENT CAN USE AI IN ADMINISTRATION

Artificial intelligence has the potential to revolutionize and improve governmental operations by enhancing decision-making processes, improving public service delivery, and fostering greater transparency and efficiency. The most evident and advantageous opportunities are those where AI can lessen administrative burdens, assist in resolving resource allocation issues, and take on noticeably complex tasks. Future use cases of AI in government will still be limited by government resources, human creativity, and public trust. Today, there are five main areas in which AI case studies in citizen services are found: responding to enquiries, completing and finding paperwork, routing requests, translating, and document draughting. With the help of these apps, government workers may be able to work more productively and spend more time fostering stronger bonds with the public[16]. Artificial Intelligence might be one approach to close the gap between citizen happiness and digital government products, which leaves much to be desired, while also enhancing citizen participation and service delivery.

Artificial intelligence is an area of opportunity that government agencies can actively anticipate and plan for when upgrading their legacy systems.[17]

[15] ibid
[16] Hila Mehr, 'Artificial Intelligence for Citizen Services and Government' , Harvard Ash Center for Democratic Governance and Innovation 2017 <https://ash.harvard.edu/wpcontent/uploads/2024/02/artificial_intelligence_for_citizen_services.pdf> accessed 25, September 2024
[17] ibid

LEGAL CHALLENGES AND ETHICAL CONSIDERATION IN THE AGE OF AI

India, a rising centre of the technology industry, is positioned to successfully negotiate the complex terrain that lies at the intersection of innovation and data protection. The necessity to comply with international privacy standards, handle new issues, and defend people's fundamental right to privacy has led to notable changes in India's data protection regulatory environment.

This Supreme Court decision significantly changed the judicial to see the Right to Privacy along with personal data protection. The ruling was very important because it set the stage for India to create a more comprehensive and strong data protection law that recognized the changing issues brought about by the introduction of the digital era in the twentieth century.

The court emphasised the role of privacy as a necessary component for the meaningful enjoyment of life with dignity and personal liberty under Article 21[18] of the Constitution, affirming that it is vital for the exercise of other rights and freedoms. A complicated and multidimensional journey spanning centuries, societal, technological, and legal advances have affected the growth of privacy legislation in India.

The judiciary has broadened its interpretation of the Right to Privacy to include informational privacy, which protects individuals from unwarranted surveillance, data collection, and dissemination. Individuals have the right to control their personal information, including who can access it and for what purposes.

Even if AI technologies contribute to many of these problems, they also hold the potential to be the answer since they offer new means of elucidating the actions taken with respect to an individual's data at every stage of processing or because they allow for customized platforms where consent may be exercised by individuals.

In the recent case of Arijit Singh v Codible Ventures LLP[19] by using tI the voice of famous Indian singer Arijit Singh was generated without his consent and knowledge. The Bombay High Court held in favour of the plaintiff by stating that protection of his personality rights viz. his own name, voice, signatures, photograph, image, caricature, likeness, persona, and various

[18] Constitution of India 1947, art 21
[19] Arijit Singh v. Codible Ventures LLP 2024 SCC OnLine Bom 2445

other attributes of his personality against unauthorized is the violation of his moral rights in his performances conferred upon him by virtue of Section 38-B of the Copyright Act, 1957[20].

ACTIONS TAKEN BY GOVERNMENT TO DRIVE PROGRESS

The Nirbhaya Fund Scheme: The Indian government to guarantee the security and safety of women and children established this fund. Furthermore, the Ministry of Home Affairs has established a single phone to manage the problem. This is located under the Emergency Response Support System (ERSS).[21]

National Database on Sexual Offenders (NDSO): It was developed to help with monitoring and investigating sexual offences. The NDSO portal will only be used by law enforcement Organizations in order to efficiently monitor and look into sexual offence cases.[22]

Cybercrime Coordination Centre Scheme: This approach focuses mostly on the problems and victims that women and children face in online media. It also increases young people's awareness of cybercrime. It covers every kind of cybercrime in detail. National Cybercrime Training Center, National Cybercrime Forensic Laboratory Ecosystem, National Cybercrime Training Portal, National Cybercrime Threat, Analytics Unit, Joint Cybercrime Investigative Team Group, National Cybercrime Training Center, Management Unit of Cybercrime Ecosystem, and National Cyber Research and Innovation Centre.

RECOMMENDATIONS

Currently, many agencies may not have the substantial quantity of data required to train and begin employing AI, and many will not be at the level of data management required for AI applications. However, best practices on the kind of data that will be utilized and gathered will be crucial for usage with AI in the future as government offices improve their data gathering and management. Governments have to consider the kind of information they require, its expiration date, and the way it will be combined to provide a particular person's context. People need to know where their data is going and be able to trust the technologies they use to connect with.“ Governments should allow individuals to choose whether or not their personal data will

[20] The Copyright Act 1957, sec 38-B
[21] Shobita, ‘Overview of concept of cyber bullying in India’ (iPleaders, 29 April 2023) <https://blog.ipleaders.in/overview-of-concept-of-cyber-bullying-in-india/#Section_66_A_of_the_Information_Technology_Act_2000> accessed 25, September 2024
[22] Chhavi, ‘Online Laws against Cyberbullying and Online Harassment in India’ (2023) 4(1) JCLJ <http://doi-ds.org/doilink/12.2023-27624836/juscorpuslawjournal/v4/i1/364373> > accessed 26, September 2024

be utilized, and they should be very upfront about the data they acquire. If the only data being utilized is already being given to the government, privacy issues could be reduced by individuals.

There should be a harmonious balance between the utilization of AI technologies and privacy rights concerning individuals. On the one hand, AI can enhance efficiency, advancement and decision-making in government, on the other hand, it must not compromise the privacy of the citizen. The enforcement of strict laws with regard to AI technology, open data practices, and moral standards will make it easier to guarantee that AI systems respect individuals' right to privacy. Including the public in conversations about the application of AI promotes responsibility and trust, which encourages innovation while preserving fundamental rights. In the end, governments may use AI to their advantage without sacrificing people's privacy or dignity if they take a cautious approach.

In order to maintain transparency and accountability, the people should have the right to an explanation so that people would be able to know where their personal data is being used and can challenge any infringement of this right in a competent court of law. Many influential members of the AI community believe that the 'ability to explain,' or the openness of choices, is essential to fostering and preserving confidence in the dynamic connection between AI technology and peoples' rights, even in the face of existing technological obstacles.

CONCLUSION

AI has the ability to significantly change how people see and communicate with their government. While AI is a potent tool to improve government efficiency, it is not a diacatholicon for issues faced by the government in every case. AI adoption and utilization in citizen services may also serve as a barometer for other new digital technologies that the public sector might employ to its advantage. AI brings up concerns about privacy, the increasing use of digital technologies, and whether or not people can keep up with the rate of automation in the long run. Prioritizing citizen feedback and involvement on these and other issues with developing digital technologies should be facilitated by the deployment of AI earlier on, beginning with low-risk applications in service delivery.

A thorough framework for data security, responsible AI development, and cooperative efforts from the government, business community, academic institutions, and civil society is also an essential component for India's success in the AI age. India can foster a flourishing AI

ecosystem and protect the basic right to privacy for its citizens by adopting a proactive approach to data privacy.