International Journal of Law, Policy and Social Review
www.lawjournals.net
Online ISSN: 2664-6838, Print ISSN: 2664-682X
Received: 03-03-2024, Accepted: 27-03-2024, Published: 18-04-2024
Volume 6, Issue 2, 2024, Page No. 30-33

The Era of AI- the ultimate breach of privacy

Dev Kanwar, Khushboo Malik
Department of Law, Christ University Delhi-Ncr, Delhi, India

Abstract
The rapid development and the widespread of artificial intelligence (AI) technology is raising a significant concern about the potential breach of privacy. This research is aimed to explore and analyze the impact of the AI on an individual's privacy right. this research will investigate how the increasing use of AI systems, such as recommendation systems, virtual assistants and surveillance technologies may infringe upon personal privacy. This research will try to examine the legal framework regarding privacy and data protection, with the focus on relevant acts and sections in the jurisdiction of the court. additionally, case studies and expert opinions will also be analyzed to assess the impact of AI on an individual privacy right. This research will consider various aspect of the issue including the surveillance systems', constant monitoring and data collection in public spaces without proper consent. It will also examine the nature of AI driven recommendation systems and personalized advertising algorithms that rely on extensive personal data analysis. This research will analyze the risks which can arise due to the breach of privacy in AI decision making systems in critical sectors, such as finance, healthcare, and criminal justice, which may compromise privacy due to lack of transparency. The findings of this research will contribute to the existing body of knowledge surrounding AI and privacy concerns which will. Allow us for a vast understanding of the potential risks and implications which can arise due to the breach of privacy.

Keywords: Artificial intelligence (AI), legal implication, data protection, privacy laws, privacy risks, security breaches

Introduction

In previous years, we saw the growth of Artificial Intelligence (AI) and its increasing involvement into many aspects of our lives. AI has brought about many positive benefits and improvements, revolutionizing industries such as healthcare, finance, transportation, and even governing systems. However, the growth of AI also raises many concerns about privacy breaches which can cause in loss of personal information.AI, by its very nature, involves the collection and processing of vast amounts of data. So therefore, This can raise concerns about the unauthorized access, security breaches, and misuse of personal information. Machine learning algorithms used in AI systems have the ability to analyze individuals behavior, preferences, and habits based on the data collected. This creates a significant risk of potential exploitation.

AI Development in India

AI has been growing rapidly in India and has been introduced in various sectors and industries in India for providing more easy and efficient work in those sectors.

Many government initiatives are taken by government to provide more development in AI in India. The national institution for transforming India also known as NITI Aayog recently released a national strategy for AI, which aims to provide more systematic development to AI as well as it aims to provide India as a Global leader.

India's growing semiconductor industry will be the backbone of the Indian AI market and by 2025, the Indian AI market will be worth $ 7.8 bn. 60% of AI's Gross

3 Value Added (GVA) in India's GDP by 2025 is expected to be driven by four end user sectors – Industrials & Automotive, Healthcare, Retail and CPG [1].

Many major Indian corporation in India are investing in AI for its research and development. Companies in sectors like IT sectors, Healthcare, and finance are merging AI technologies into their day-to-day operations for more effective and efficient work.

AI is used and developed heavily in healthcare sector as in healthcare sector it can be applied in various things such as diagnostics, personalized medicines and managing health records.

With growing demand for AI Professionals, there is a focus on developing AI education and AI skill development in India. Many types of workshops, training programs and courses are being offered to acquire individuals with required AI skills.

Relationship between AI and Privacy in India

In India AI and Privacy is a very complicated topic, particularly in the context of digital personal data protection bill. The bill which is proposed directly challenge the processing of personal data enabled by it as it gives a clear indication of issues which can arise due to the full deployment of AI power to the principle of data protection. As the motive of data protection laws are not intended to cause issue in the AI ecosystem so therefore, there is a need to find the right balance between compliance and data usage to be able to work more efficiently so that it can provide maximize output in society The introduction of AI has revolutionized Various aspects of life but because of the this the issue of data privacy has become more critical than ever especially to ensure that AI systems are not used to exploit individuals or to discriminate anyone based on their personal data.

Cooperation from various stakeholder like government, industry and civil society can help to develop and promote privacy and security while with the understanding the benefits of AI in an ethical, responsible, and sustainable manner.

Review of Literature

As we know artificial intelligence has become such important in area of research in many fields like education, medicine, engineering, military etc which contribute in development of our nation. AI development can benefit everyone across all ages but the only issue which can arise due to using AI id mostly associated with the exploitation to the data breach which can arise privacy concern. The growth of AI being used would be the reason of threat towards national security and major concern will be the threat of exploitation of data which can occur to all the people who are accessing everything on digital Platform where all their personal information is being stored. The paper has major finding from the sources Listed

Below

1. The information about the Australian Act was taken from the official website of the office of the information commissioner, Australian Government and this source give in dept detail about the rights and responsibilities which. The citizen hold over their personal Information.
2. International Comparative Legal Guide is also a very important source which recorded the key finding about the Us sector specific Laws on privacy and data protection and how in world US is said to be the safest cyber secure country.

Australian federal privacy Act

The Australian model has well extended legislative framework which covers every possible sector of Australia and geographics. The very important personal information in Australia is controlled and supervised under the privacy act, By giving an individual. To have major control of the personal information is handled. The key feature of this act is that an individual can have the right to know why the person personal information is being collected and how this personal information will be used and where finally it would be disclosed to fulfil the task. The individuals or also have the right to opt for an option of not identifying themselves and disabling this right from the host party who is trying to have the access of the information. The party involved in receiving information are bound to give access to the individuals who are giving their information and also have right to access health information [2]. In Australia the people have the control to stop any unwanted 5 direct marketing message. There is no room for any scam or forgery by asking individual to change the personal information that is incorrect to be corrected in Australia any incident or activity which proves that any organisation which is registered is mishandling or exploiting the personal information given to them then an individual can file a complaint to the competent authority.

Who is responsible under the privacy act

In Australia, the government and registered organizations with an annual turnover of more than $3 million have responsibilities in managing data under the Privacy Act, subject to some exceptions. The Privacy Act also defines the role of various organisation which may comprise of an individual, including a sole trader, a corporate body which is registered under different heads alongside a partnership, any other unincorporated association or well recognised trust functioning in the territory of Australia [3].Under the Privacy Act in Australia, certain exceptions are given to state or territory government agencies, state and territory public hospitals, universities that are not private, the Australian National University, and public cantered schools. Media houses that are committed to observing published privacy standards are also provided with relief.

The Australian Federal Privacy Act also go along with the Information Privacy Act 2014 (ACT), which is directly used to Australian Capital Territory for the agencies registered under public sector circle. The Territory Privacy Principles (TPPs) covers the collection, storage, mode of usage, personal information [4].

How Australian legislative framework be useful to India

Drawing from the Australian legislative framework could be beneficial for a country like India, known as the world's largest democracy, where freedom of speech and expression is largely unrestricted. This openness makes India a conducive environment for user-friendly data usage and collection. Both India and Australia are in the process of reforming their data protection laws to address various concerns, with India making strides in AI regulation and the proposed Digital India Act aiming to bring AI under its scope. The Act also provides exemptions for certain entities, and the Indian government is actively participating in the conversation on AI adoption and regulation

Sector Specific Data Protection in United States

India is currently working on establishing a single data protection and privacy law to address the challenges posed by artificial intelligence in data usage. In contrast, the United States has implemented a more comprehensive approach, with a mix of federal and state-level data protection laws. The Federal Trade Commission (FTC) enforces consumer protection regulations, ensuring that companies adhere to their published privacy promises and take necessary precautions. This approach, which combines sector-specific legislation with a broader umbrella framework, has proven effective in data protection. Like there is Driver's Privacy Protection Act of 1994 (DPPA) [5], which supervise over personal data protection and privacy when information is collected and used by the Departments of Motor Vehicles. Next sector specific legislation is of the children who are governed under the Children's Online Privacy Protection Act (COPPA) [6] The Children's Online Privacy Protection Act (COPPA) in the United States places strict limits on the collection of data about children under the age of 13. The law requires websites and online services directed to children under 13 to post a clear and comprehensive online privacy policy and obtain verifiable parental consent before collecting any personal information from children. If a child's information must be collected, the company must follow specific guidelines to ensure the protection of children's privacy. This approach, which combines sector-specific legislation with a broader umbrella framework, has proven effective in data protection.

In the United States, there is a diverse set of regulations and guidelines that apply to specific sectors, such as distinct privacy rules and data protection laws for areas like credit banking, insurance, and health information probability. This sector-specific approach is a prominent feature of the United States' data protection framework. In the United States, there are various agencies responsible for regulating data protection through sector-specific laws. These include the

Comptroller of Currency (OCC), the Securities and Exchange Commission, and the Office of Health and Human Services Commission (HHS). The US has a patchwork of hundreds of laws enacted on both the federal and state levels that cover different aspects of data privacy, such as health data, financial information, or data collected from children. While some states have passed their own comprehensive data privacy laws, most data privacy protections are at the state level, and there is no central enforcement agency responsible for compliance. However, the Federal Trade Commission (FTC) enforces consumer protection regulations and takes action against companies that breach their published privacy promises.

Legal provisions for Governing AI in India

In India there is no specific legal provisions that directly deals with AI but the competent authority is expressing concerns regarding this issue which is non availability of a law that can directly deal with AI in India.

Here are some legal provisions that nearly deals with AI in India

Information Technology Act, 2000

The Information Technology Act, 2000 in India has been updated to address digital threats and cyber-crime. While it does not explicitly mention AI, certain provisions within the Act are relevant to AI-related activities. For example, Section 43A of the IT Act allows for compensation in cases of data privacy breaches resulting from the negligent handling of sensitive personal information, which is pertinent to AI systems processing user data. Another provision, Section 73A, is also applicable. The Act plays a crucial role in regulating data protection and privacy in the context of AI in India.

Indian Copyright Act, 1957

The Indian Copyright Act of 1957 safeguards original literary, artistic, musical, and dramatic works, providing exclusive rights to creators and prohibiting unauthorized use or reproduction. The emergence of AI-generated content has sparked discussions regarding copyright ownership and infringement liability. In the case of Gramophone Company of India Ltd. v. Super Cassettes Industries Ltd. (2011), the Delhi High Court ruled that AI-generated music lacks human creativity and is therefore ineligible for copyright protection, thereby clarifying the copyrightability of AI generated content in India. This case has significant implications for the copyright protection of AI-generated works, as it highlights the challenges in determining the eligibility of AI-generated content for copyright protection under existing laws. The legal landscape surrounding AI-generated content and copyright ownership in India is complex, and it requires careful consideration and potential revisions to intellectual property laws to address the unique challenges posed by AI-generated content and ensure fair and effective copyright protection.

India's Data Protection Bill

The proposed Digital Personal Data Protection Bill in India could have a significant impact on the use of AI and the protection of personal data. By regulating the use of AI and ensuring data protection, the bill could prevent hidden data exploitation that occurs in the pursuit of innovation and development. The bill does not explicitly regulate the use of AI, but its provisions directly challenge the processing of personal data enabled by AI, creating a clear rift between its data protection principles and the full deployment of AI's power. The bill's provisions, such as Section 18(2)(b), may have far-reaching consequences for AI-based industries, as they engage in profiling, which is prohibited by the bill. Balancing the benefits of AI with the protection of personal data and privacy is a critical challenge that the Indian government must address to ensure a sustainable and ethical digital future.

The following are the bill's main highlights [7]

- **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" (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.

Suggestion

The paper, through its comparative study, suggests that India should establish a legislative framework to address the dual aspects of AI advancements and the cyber threats arising from data breaches and unethical data usage. It proposes adopting a sector-specific approach similar to the United States for framing data protection laws and establishing a Data Governing Council to oversee and regulate data breaches. This council would act as a central authority for monitoring and regulating large-scale data breaches. The study emphasizes the need for India to reconcile laws around data protection and privacy before creating responsible AI laws and regulations. This is in line with the European Union's approach, which first laid a strong foundation of data protection cantered around the rights of its people before moving towards a responsible and safe AI Act. The upcoming Digital Personal Data Protection Bill in India is expected to set the tone for the country's AI governance.

Conclusion

The paper, through its comparative study, suggests that India should adopt a proactive approach to data protection as AI has the potential to benefit as well as harm society and all forms of life. It highlights the importance of considering the data protection aspect before creating responsible AI laws and regulations. The paper draws inspiration from various international data protection models, such as the Australian Federal Privacy Act of 1988 and the United States' sector-specific approach, which could help India address the challenges of data protection and privacy in the context of AI development and innovation. The paper also 10 emphasizes the need for India to establish a Data Governing Council to monitor and regulate large-scale data breaches and ensure compliance with data protection laws.

References

1. h#ps://www.inves.ndia.gov.in/team-india-blogs/ar.ficial-intelligence-powering-indias-growth story#:~:text=India's%20growing%20semiconductor%20industry%20will,%2C%20Healthcare%2C%20Retail%20and% 2 0CPG.
2. *rights and Responsibili1es*, Office of Australian Informa.on Commissioner, AUSTRALIAN GOVERNMENT, h#ps://www.oaic.gov.au/privacy/privacy-legisla.on/the-privacy-act/rights-and responsibili.es#:~:text=The%20Privacy%20Act%20allows%20you,informa.on%20(including%20your%20health%20in forma.on)
3. *Rights and Responsibili1es*, Office of Australian Informa.on Commissioner, AUSTRALIAN GOVERNMENT, h#ps://www.oaic.gov.au/privacy/privacy-legisla.on/the-privacy-act/rights-and responsibili.es#:~:text=The%20Privacy%20Act%20allows%20you,informa.on%20(including%20your%20health%20in forma.on)
4. *Rights and Responsibili1es*, Office of Australian Informa.on Commissioner, AUSTRALIAN GOVERNMENT, h#ps://www.oaic.gov.au/privacy/privacy-legisla.on/the-privacy-act/rights-and responsibili.es#:~:text=The%20Privacy%20Act%20allows%20you,informa.on%20(including%20your%20health%20in forma.on)
5. *Data Protec1on Laws and Regula1on USA* (2022-2023), ICLG, h#ps://iclg.com/prac.ce-areas/data-protec.on-laws and-regula.ons/usa#:~:text=There%20is%20no%20single%20principal,Code%20§%2041%20et%20seq
6. *Data Protec1on Laws and Regula1on USA* (2022-2023), ICLG, h#ps://iclg.com/prac.ce-areas/data-protec.on-laws and-regula.ons/usa#:~:text=There%20is%20no%20single%20principal,Code%20§%2041%20et%20seq
7. Aishwarya Srinivasan, *India's Data Protec1on Bill in the light of Responsible AI*, h#ps://www.linkedin.com/pulse/indias-data-protec.on-bill-light-responsible-ai-aishwarya-srinivasan/