University Research Resource Journal

ISSN : 2581-3730

JAYOTI VIDYAPEETH WOMEN'S UNIVERSITY, JAIPUR

Volume 6, Issue 2 (April-June, 2023)

Artifical Intelligence & Privacy:Its Significance & Risk

JV'n DEEPANSHI GARG, BA LLB X SEM

JV'n Ms. Tanushi Sahni, Assistant Professor

Abstract :

The development in science and technology gives rise to the new concept of artificial intelligence. This is the concept in which technology uses the information and generates the results even in those conditions where human intelligence is needed. It is commonly used in various sectors like healthcare, transportation, personalized services.

As the information is shared it is very important to understand the relation between privacy & AI because if at one time it helps the human beings then on the other side it also leads to privacy risks.

This abstract highlights the complicated relationship between AI & privacy, determining the need to maintain a balance between using the AI benefits & protecting privacy of individuals at the same time. The abstract talks about different opportunities that are created by the integration of AI systems in our daily life.

On one side, AI provides number of chances for protecting privacy. The AI driven encryption techniques provide strong data protection, preserving confidentiality of sensitive information. There are various privacy mechanisms that permits the organization to separate valuable information while maintaining privacy at the same time. The AI uses algorithms that enable the users to control the transmission & sharing of their personalized information.

On the other side, AI raises significant privacy risks. The whole AI system works by collecting, processing & analyzing the large amount of data so this many times leads to violation of privacy of an individual. There are instances when the governments of different countries uses AI for surveillance this will also leads to violation of right to privacy of different individuals provided by international instruments & constitutions of different democratic countries.

Conclusion : The Privacy &AI are interlinked & striking balance between them is important to increase benefits of AI while protecting privacy.

Keywords : Artificial Intelligence, Privacy, Information, Algorithms

Introduction : Artificial intelligence (AI) is a disruptive technology that is quickly changing many facets of our existence. AI has the ability to significantly improve our day-to-day experiences through voice assistants, driverless driving, and personalised suggestions. The expanding use of AI, however, also prompts questions about data security and privacy.

A number of difficulties are presented by the privacy and AI interaction. The gathering and holding of personal data is one issue. Companies that create AI applications must make sure that data is gathered ethically, transparently, and with individuals' explicit agreement. They also need to take precautions against breaches, unauthorised access and improper use of data.

The possibility for AI machine systems to draw conclusions or anticipate the future based on specific facts is another difficulty. Even without explicit disclosure, AI systems can find hidden connections and patterns that could disclose sensitive information. In this system the data is shared even to third parties like cloud service providers so, this increased the risk of data leakage. The organizations are working over legal framework for regulating AI & privacy.

Meaning of Artificial Intelligence :

The AI concept refers to the creation of smart machines that can carry out activities that traditionally need human intellect is the emphasis of this large area of computer science. AI is the process of creating algorithms and models that give computers the ability to think, reason, learn, and act in ways that are comparable to those of humans. The best example of AI system is Google Location Tracker. It is of two types-

- Weak AI (Narrow AI)-These are the systems that are designed to perform the specific tasks like Alexa.
- Strong AI (General Intelligence)- These are the systems that are designed to understand ,learn the complex tasks at a time.

Utility Areas of Artificial intelligence

- Detect diseases - It is commonly used to detect serious diseases like heart disease in patients by analysing blood vessels in a retina scan; detect cancerous tumours by examining CT scans; diagnose pneumonia by examining chest x-rays; and identify adult-onset diabetes by looking for patterns of retina damage.
- Visual & Hearing impaired persons-Helping visually impaired people comprehend pictures or better grasp their surroundings by describing them as text, or assisting hearing-impaired people in communicating by converting spoken words into text on a screen, is another application of computer vision. Face recognition is perhaps the most widely utilized daily use of computer vision. It also includes search images, tag friends' photos on internet, and unlock smartphones. The use of computer vision in sports has also been demonstrated in the improvement of driver safety in auto racing, player experience and analysis in golf, and the International Gymnastics Federation's intention to utilize it to aid judges in the 2020 Summer Olympics in Tokyo.

Meaning of Privacy & Data Protection -

The term privacy is made from a term privitas and is coined by Louise warren & Brandeis in their article written for a Haward law journal. It is very difficult to define it has its own meanings according to the individual interpretation but these scholars try to define it as "to be left alone" meaning thereby there is no interference of an individual within the life of individual without his consent.

The question of privacy & data protection is of great importance as we are surrounded by the machines which works like humans only. The terms privacy & data protection looks identical to each other. The term data protection refers to protection of private or public data by the use of legal framework and data protection is the mechanism for protection of privacy.

Importance of Privacy in Digital World- Personal data has become a very valuable asset in the digital age. The vast amount of data generated and shared online every day has enabled businesses, governments and organizations to gain new insights and make better decisions. However, this data also contains sensitive information that individuals may not want to share or that organizations may have used without their consent. Privacy becomes important here.

Reasons for privacy as significant factor

Privacy is important for many reasons. One is to protect individuals from harm such as identity theft and fraud. It also helps you maintain personal autonomy and control over personal data, which is essential for personal dignity and respect. Additionally, privacy allows individuals to maintain personal and professional relationships without fear of surveillance or interference. Last but not least, it protects our free will. If all of our data is public, harmful recommendation engines can analyze our data and use it to manipulate individuals into making certain (purchasing) decisions.

Artificial intelligence & privacy- It shares a very complicated relationship with each other .Some researcher are of the view that AI is the threat to privacy & data protection but some opined that AI technology is helping the humans in a broader way.

AI may assist businesses in limiting or monitoring who has access to a person's data and responding in real-time to stop misuse or data theft. Companies are creating AI-based privacy solutions like privacy policy scanners, which aim to explain and simplify privacy policies so users can comprehend them more easily, and privacy bots, which try to remember privacy preferences and try to keep them consistent across multiple sites. In order to "read a privacy policy it has never seen before and extract a readable brief, displayed in a graphic representations like diagrams, of what kind of data a service collects, where that data may be sent, and whether a user can opt out of that," Polisis, which stands for "privacy policy analysis," is an AI, uses machine learning.

Everything has pros & cons it also has some disadvantages like large amount of data sharing leads to breach of privacy and even data can be used for unethical purposes in a common parlance companies try to maintain privacy systems but the hackers may access the personalized data & use it for illegal purposes.

International law on AI & privacy

The AI technology has developed rapidly and very widely used by the humans across the globe so it create issues globally also.

It has effected various spheres internationally-

- **Human Rights -** AI systems have the potential to have an influence on human rights, such as the right to privacy, freedom of speech, and nondiscrimination. International human rights legislation offers a framework for addressing these problems, and nations must guarantee that artificial intelligence (AI) technologies are created and utilized in accordance with human rights commitments.
- **Data protection and privacy -** AI relies on large amount of personal data, raising questions about data security and privacy. International regulations, such as the European Union's General Data

Protection Regulation (GDPR), create principles and standards to protect personal data and control how personal data is processed, including AI applications.

- **Autonomous Weapon Systems (AWS) :** The development and installation of Autonomous Weapon System (AWS), also known as "killer robots, "has sparked international humanitarian law debate. Discussions are underway to develop standards, laws, and limits to ensure that AWS isused in accordance with ideals of excellence, impartiality, and military necessity.
- **Cyber security :** AI systems are vulnerable to attacks over the internet and their use could compromise global cyber security. International legal frameworks, such as the Tallinn Manual on International Law Applicable to Cyber warfare, provide advice on the applicability of existing international law to cyber operations, especially those using AI.

National Law on AI-India does not have specific data protection laws but personal data is protected under Section 43A and 72A of the Information Technology Act. Similar to GDPR, you have the right to seek compensation for improper disclosure of your personal data. In 2017, the Supreme Court declared the right to privacy to be a fundamental right protected by the Indian Constitution. AI is expected to contribute $957 billion, equivalent to about 15% of India's current total value in 2035. AI could impact everyone's life in some way or another to come. In 2018, NITI Aayog (Policy Committee) launched various programs on AI applications.

The Ministry of Electronics and Information Technology has set up four committees to focus on and analyze several AI ethical issues. The Parliamentary Joint Committee is currently considering the PDP Bill - Personal Data Protection Act 2019 under the Data Protection Bill. If approved by both houses, the bill becomes law. In India, the speed of AI adoption is faster than the rules enacted to regulate AI. The industry is now beginning to leverage AI technology to up skill its workforce.

Challenges to Privacy in AI

- **The Tech Giants over Data -** The large entrepreneur business like Google, Amazon, Meta these are playing a greater role in shaping the global economy &are also actively involved in politics & policy making by influencing public opinion. They are creating such a virtual environment in which they can easily mould the choices & earn handsome amounts. These giants use data 20 times more than internet. It is clearly the violation of privacy.
- **Collection of Information & its use by AI systems -** One of the significant feature of AI systems is the collection of data &working on it. The data collection rises it increases concern for privacy also. The data used by AI systems is not always transparent it may be complex moreover individual is unable to understand how the collected data is used so it creates distrust among the people.
- **Use of AI in surveillance -** Altogether Ai in surveillance is very helpful as it collects different data from different sources like social media accounts & help to moniter a person & prevent crime but at the same time it violates civil liberties also. It is not transparent as individual does not know when he is to be monitored & for what.

Conclusion :

After all the research we came to the conclusion that AI play a very important role but there are other serious issues that individual is facing while using it .It may be a good decision maker in the situation where human intellect is required but not always because its decision making & complex working is based on the data entered by the user it solely depends on data received now if the data is biased then, decision must not be transparent.

There are many AI systems that have our personal information & use it without our consent we even not known that our information is being used it creates serious privacy issues.

Moreover, the AI as makes the life of human being comfortable but this has increased unemployment as the work which is in past years being done by humans now being performed by machines.

There are different legal framework that are enacted to use AI efficiently while maintaining privacy at the same time.

References :

https://www.thedigitalspeaker.com/privacy-age-ai-risks-challenges-solutions/#:~:text=AI%20presents%20a%20challenge%20to,difficult%20for%20humans%20to%20discern.

https://singhania.in/blog/assessing-the-intelligence-of-the-artificial-intelligence-in-law-prospects-in-india-

https://bmcmedethics.biomedcentral.com/articles/10.1186/s12910-021-00687-3