Is Artificial Intelligence a Boon or a Bane to the Privacy?

Ritwika mazumdar[1], Dr Md. Akbar Khan [2]
[1]*Ritwika Mazumdar, PHD Scholar, ICFAI Law School, IFHE, Hyderabad*
[2] *Dr Md.Akbar Khan, Associate Professor, ICFAI Law school, IFHE, Hyderabad*

***Abstract*— The purpose of artificial intelligence (AI), at its most basic level, is to develop computer systems that can carry out tasks that are typically done by humans. These activities, which can be categorized as intelligent, include the ability to perceive both sight and sound, to learn and adapt, to reason, to see patterns, and to make decisions. As well as most of the time, when utilizing technology like AI, we unintentionally or voluntarily divulge sensitive information like age, location, preferences, etc. where private information is gathered by tracking businesses, which then analyze it and use it to personalize on online experience. So this paper would discuss about how this Artificial intelligence would act as both boon and bane in our life in the aspect of privacy. And the issue of identifiability—whether or not a person's identity can be fairly determined from that data the concept of personal information.**

Keywords: Artificial intelligence, boon, bane, privacy, personal information.

I. INTRODUCTION

Artificial intelligence (AI)[1] is becoming a crucial and frequently employed technique in a variety of fields and sectors. Despite the very fact that artificial intelligence has existed for millennia, its true potential wasn't discovered until the 1950s. the thought of AI was conceived by a generation of scientists, physicists, and philosophers, but it wasn't until Turing , a British polymath, advocated that humans solve issues and make decisions supported available information and reason that it became a reality.

Computer complexity was an enormous stumbling factor to expansion. Before they might expand any further, they needed to adapt fundamentally. Orders might be executed by machines, but they couldn't be stored. Financing was also an issue until 1974.

Computers had become quite common by 1974. They were now faster and ready to store more information. The three "Vs" of massive data are widely used to describe its impact: volume, variety, and velocity. More data allows for more sophisticated and comprehensive analysis. Variety increases this power by with new and unexpected conclusions and predictions. Additionally, velocity allows for real-time analysis and sharing. Streams of knowledge from mobile phones and other online devices increase the volume, diversity, and velocity of knowledge about every aspect of our lives, making privacy a worldwide public policy concern.[2]

This trend will presumably be accelerated by artificial intelligence. Machine learning and algorithmic decisions underlie most of today's most privacy-sensitive data analysis, like search algorithms, recommendation engines, and adtech networks. As AI advances, it expands the likelihood to use personal data in ways that compromise privacy by bringing personal data analysis to new levels of power and speed.[3]

---

[1] Artificial Intelligence,MerriamWebster, https://www.merriam-webster.com/dictionary/artificial%20intelligence

[2] David Gewirtz,Volume, velocity, and variety: Understanding the three V's of big data,https://www.zdnet.com/article/volume-velocity-and-variety-understanding-the-three-vs-of-big-data/, March 21, 2018

[3] Cameron F. Kerry and Caitlin Chin, “Hitting refresh on privacy policies: Recommendations for notice and transparency,” The Brookings Institution, January 6, 2020.

As AI advances, it increases the likelihood to exploit personal information in ways that can infringe on privacy concerns by enhancing the strength and speed of personal data analysis. However, it also can provide the legal system a new method of operating and a rare opportunity to investigate new areas of law. AI poses many problems and has its risks.[4]

II. ORIGIN AND DEVELOPMENT

"During the 20th century a quick history of AI can be given as:

1. 1923 Karel Kapeks play named Rossum's University Robots (RUR) opens in London, the primary use of the word robot in English.

2. 1945 Asimov, alumni of Columbia University, invented the term Robotics.

3. 1950 Turing Test for evaluation of intelligence was introduced by Turing . Shannon published a detailed analysis of chess playing as a search.

4. 1956 John McCarthy coined the term AI.

5. 1958 John McCarthy invites its LISP programing language for AI.

6. 1964 Danny Bobrow's thesis at MIT showed that computers can understand tongue well enough to solve algebra word problems correctly.

7. 1979 the primary Computer-controlled autonomous vehicle, Stanford Cart was built.

8. 1984 Dennett discusses the frame problem and the way it relates to the difficulties arising from attempting to give robots common sense.

9. 1990 Major advances altogether areas of AI

10. Significant demonstrations in Machine Learning

11. Case-based reasoning

12. Multi-agent planning

13. Scheduling

14. Data mining, web crawler

15. Tongue understanding and translation

16. Vision, computer game

17. Games

18. 1997 The Deep Blue Chess Program beats the planet Chess Champion, Gerry Kasparov

19. 2000 Interactive Robot Pets become commercially available. MIT displays a robot with a face-name Kismet that expresses emotions.

20. The two major approaches that have been developed for the regular AI system are the top-down approach which started with the higher-level functions and implemented those and the bottom-up approach which looked at the neuron level and worked up to create higher-level functions.

21. Within the year 1972, the primary full-scale intelligent humanoid robot, WABOT1, was created in Japan.

22. Within the year 1980, AI came with the evolution of Expert Systems. These systems are computer programs, which are designed to unravel complex problems.

23. Within the year 1997, IBM Deep Blue beat world chess champion Kasparov and became the first computer to defeat a world chess champion.

24. Within the year 2006, AI came into the business world. World's top companies like Facebook, Twitter, and Netflix also started using AI in their applications."[5]

Artificial intelligence (AI) is advancing at a snappy pace. Experimenters have developed software that uses Darwinian elaboration sundries, similar as" survival of the fittest," to produce AI programs that

[4] Cameron F. Kerry,Protecting privacy in an AI-driven world, February 10, 2020,https://www.brookings.edu/research/protecting-privacy-in-an-ai-driven-world/

[5] rojej Shrestha, artificial intelligence on humanity as a boon or bane, January 2022 https://www.researchgate.net/publication/358039327_artificial_intelligence_on_humanity_as_a_boon_or_bane

ameliorate generation after generation without the need for mortal intervention. The algorithm was suitable to duplicate decades of AI exploration in just a many days, and its generators believe that one day it'll be suitable to develop new AI approaches.

It takes time to develop an AI algorithm. Consider neural networks, a typical type of machine literacy used for effects like language restatement and independent driving. These networks are grounded on artificial neurons and learn from training data by conforming the strength of connections between them. Lower sub circuits of neurons do specific tasks for illustration, finding road signs and it can take months for experimenters to figure out how to connect them so they operate together seamlessly.

In recent times, scientists have automated some procedures to speed up the process. still, these programs still calculate on humans to put together pre-built circuits. That means that the outgrowth is still constrained by masterminds' imaginations and biases. So Quoc Le [6], a Google computer scientist, and associates created Auto ML- Zero[7], a program that could produce AI algorithms with nearly no mortal input, utilising only introductory fine principles that a high academy pupil would understand. The ultimate thing is to make unique machine learning[8] generalities that indeed scholars have not been suitable to identify. As artificial intelligence advances; it expands the possibility to use particular data in ways that compromise sequestration by bringing particular data analysis to new situations of power and speed.[9]

III. HOW AI GATHERS OUR PRIVATE DATA?

Our private data collecting is now much simpler than ever, thanks to contemporary technologies like surveillance cameras, smartphones, and the internet. In current digital age, it is quite simple to follow everything of a user's interests and actions, from their conversations while at home to their product searches to their restaurant visits. In addition to this unintentional disclosure of personal information, we also upload our own personal information to social media. When we go to a restaurant or a store, for instance, we may take a number of pictures of the food or merchandise we enjoy and upload them online. The majority of this data is moved to cloud computers, greatly increasing the likelihood that this sensitive data can be tracked.[10]

Let's examine how AI violates our privacy by gathering our personal information:

Persistent surveillance:

Governments and authorities can now study entire cities all at once thanks to persistent surveillance systems, a developing technology that uses unmanned aerial vehicles (UAVs) and drones. Persistent surveillance is the term used to describe ongoing observation of a person, place, or object. The military and police use this technique the most frequently to gather as much information as possible on a potential foe or suspect. AI is currently posing the same constant surveillance in our life with the help of the following innovations:

Digital Assistants

Persistent eavesdropping is now a characteristic of so-called AI assistants like Google Home and Amazon's Alexa. The parent company may easily access what individuals talk about while sitting at their houses thanks to these AI-driven devices that collect audio data from the user's home or any other area. After being saved and analyzed by the parent company, the data is then received via stream from these systems. As a result, without the users' knowledge, the parent

[6] https://www.crunchbase.com/person/quoc-le-2

[7] PureAI Editors,The AutoML-Zero System Automatically Generates Machine Learning Programs,https://pureai.com/articles/2020/08/03/automl-zero.aspx#:~:text=The%20AutoML%2DZero%20system%20uses,complex%2C%20hand%2Dcoded%20algorithms.

[8] machine learning,https://www.techtarget.com/searchenterpriseai/definition/machine-learning-ML

[9] Andrej Kovacevic,AI is Having a Big Impact on Web Design, and it's Only the Beginning,https://medium.com/hackernoon/ai-is-having-a-big-impact-on-web-design-and-its-only-the-beginning-89bfa096bf2d

[10] Is Artificial Intelligence a Threat to Privacy,thinkmlteam,19sep2021 ,https://thinkml.ai/is-artificial-intelligence-a-threat-to-privacy/

company can easily keep an eye on what they are saying, doing, or preparing to do.
According to a 2018 Shields survey, consumers love the home security features of digital assistants but worry about privacy violations caused by these gadgets.

CitiWatch
In addition to the digital assistants that people choose to put in their homes, AI has made it possible for drone surveillance, which enables ongoing remote monitoring. This military technology has recently been used in non-military settings. In order to keep an eye on people in the city, Baltimore established Citi Watch in 2005. Citi Watch is a ground-level surveillance system with more than 700 cameras. Law enforcement officials in Baltimore claim that these actions have lessened crime. Privacy advocates argue in opposition that such programs violate their right to privacy and restrict their freedom.[11]

Contracts for Privacy Violations
The majority of people are not familiar with the terms and conditions that online service contracts include. They simply accept the terms and conditions without ever reading them because the contract is so lengthy and challenging to understand. However, they could have disastrous results. Facebook and Google own all contributed messages, images, and videos, and they have no qualms about selling your personal information to other companies.

Data de anonymization
Whether they are at home, at work, or anywhere else, anyone using a variety of gadgets can be recognized and watched by AI. Personal information that has been anonymized, for instance, is simple to de-anonymize using AI. People can also be found and followed using facial recognition powered by AI.

Inappropriate data masking
It may be easy to locate the person whose data has been disguised if the data masking is not done properly. Organizations must develop effective techniques and regulations for data masking in order to safeguard client privacy. IBM can help by providing the tools to provide guidance on appropriate data masking techniques.

AI-based Prediction
ML systems may easily infer sensitive information from non-sensitive data. For instance, using the keyboard's input, AI may predict a person's emotional states, such as concern, unease, and confidence.
Of course, Google has had a lot of success gathering private data. The main reason for its popularity is because when people conduct online information searches, they frequently are unable to hide their interests. Even if a person tries to hide sensitive personal information, he will not be able to look for information about his interests unless the search terms are entered. Our most private interests, whom we all want to keep that way, are now no longer private since they are collected online. Activity logs and a number of other measures can be used to predict political opinions, sexual orientation, ethnic identity, and general health.

IV. LEGAL FRAMEWORK IN INTERNATIONAL PERSPECTIVES:

CCPA by California

The "California Consumer Privacy Act" was passed into law in 2017 and is the most comprehensive law to prevent privacy violations. Since 2017, the CCPA has worked hard to prevent privacy abuses. It has established some guidelines to control privacy issues and emphasizes the need for users to give their consent before enterprises share their personal information with third parties.

GDPR by Europe
The privacy expectations of customers are of great importance to Europe, which is raising the bar to prevent privacy infringement. New criteria on an individual's right to his private information were introduced by Europe's GDPR in 2018 and raised expectations for digital privacy as a result. The goal of GDPR is to give customers more control over how their personal data is collected and used. In the event of violations, fines may be suggested. Organizations that violate the GDPR must pay a fine of at least €20 million, or 4% of their annual global turnover.

[11] Richard H. Wiggins III, Personal Digital Assistants,2004 Feb https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3043961/17,

Because of this, the EU's new privacy laws are taken seriously. The goal of GDPR is to make sure those business activities and policies comply with privacy regulations. Within the EU, a business using the personal data of the customers to offer services, to sell products, or to observe their behavior has to comply with these privacy regulations.

HIPPA Act

The HIPPA act was passed out of concern for patient health information security. This law requires businesses to reveal a patient's health information only with that person's consent.

To protect consumer privacy, all of these rules and regulations are still in the early stages of development. They are not yet perfect and will continue to change as privacy laws are expanded. Additionally, compliance and legal teams are currently manually addressing the difficulties relating to data privacy rules. Businesses utilize a manual method that takes a lot of time and effort to assure privacy protection. A technological gap prevents lawyers from defining and managing privacy policies in a creative manner. . To ensure secure data sharing and prevent privacy abuses, a company by the name of "Cape Privacy" offers practical and cutting-edge privacy approaches. This company provides software that can be integrated into the data science and machine learning infrastructure of the business to enable data privacy more easily.

V.LEGAL FRAMEWORK IN NATIONAL PERSPECTIVE

Although there are no particular data protection rules in India, Sections 43A and 72A of the Information Technology Act protect personal data. Similar to GDPR, it provides a right to compensation for unauthorized disclosure of personal information. The right to privacy was deemed a fundamental right protected by the Indian Constitution in 2017 by the Supreme Court.

SECTION 43A OF THE IT ACT, 2000-Under Section 43A of the (Indian) Information Technology Act, 2000, a body corporate that is in charge of, dealing with, or handling any sensitive personal data or information and is negligent in establishing and maintaining reasonable security practices that result in wrongful loss or wrongful gain to any person may be held liable to pay damages to the person so affected. It is important to highlight that in these situations, the impacted party may ask for an unlimited sum of compensation.

SECTION 72A of IT ACT,2000-Information disclosure committed intentionally and willfully without the subject's consent and in breach of a legal contract is punishable under Section 72A of the (Indian) Information Technology Act, 2000 by up to three years in prison and a fine of INR 5,00,000.

The Personal Data Protection Bill, 2019-

The Personal Data Protection Bill, 2019 was tabled in the Lok Sabha on December 11 by Mr. Ravi Shankar Prasad, Minister of Electronics and Information Technology. To guarantee the protection of people's personal information, the Bill creates a Data Protection Authority.

The Joint Parliamentary Committee eventually presented its eagerly awaited report to the Indian Parliament on December 16, 2021, following two years of debates on the Personal Data Protection Bill, 2019. It is hoped that this will bring an end to the extensions that have been granted and pave the way for a strong data protection law in the largest democracy on earth.

The National Strategy for Artificial Intelligence, a policy document from the NITI Ayog, was released in 2018 and explored the significance of AI and its possible uses across several Indian businesses. Additionally, it was recommended that a national AI initiative be launched in the 2019 Budget. India still lacks sufficient legislation to control and regulate the AI industry, despite all of these scientific advancements.

IV. CHALLENGES

The main application-related difficulties center on the development of a framework that enables us to address the problems caused by the quick development of AI. However, the results may be used in the following areas:

Government Responsibility:

It is up to Parliament to pass privacy laws that protect individuals from any unfavorable effects of the use of their personal data in AI without unduly restricting research or getting entangled in complex social and political quagmires. When discussing AI in the context of the privacy debate, the shortcomings and failures of AI systems are frequently brought up, such as the

potential disparate impact of predictive policing on minorities or Amazon's unsuccessful experiment with a hiring algorithm that replicated the company's current disproportionately male workforce. Both of these raise significant difficulties, but regulating privacy is difficult enough without taking into account all the possible social and political repercussions of information uses. It is critical to distinguish between generic and specific data challenges. In order to evaluate the influence of AI on privacy, it is necessary to consider both issues that are common to all AI, such as the prevalence of false positives and negatives or overfitting to patterns and those that are specific to the use of personal information. To increase openness between these internet companies and the consumers, many nations have now developed their own data regulation regulations. Most of these rules are designed to provide consumers more control over the information they can share and to notify them of how the platform will utilize it. The GDPR law, which became operative for the EU countries a few years ago, is a fairly well-known example of this. More control over their personal data and how it is used for EU citizens.

Company Responsibility:

Most social data on users is literally owned by big firms like Google, Facebook, Amazon, Twitter, YouTube, Instagram, and LinkedIn. Due to their reputation as industry titans, companies should take extra precautions to prevent any data leaks, whether deliberate or accidental.

AI Community Responsibility:

The responsibility of the AI community is to speak out against the unethical use of AI on users' personal data without their permission. This responsibility falls particularly on thought leaders in the community. They should also spread the word that this behavior can have such terrible social repercussions. Already, a lot of institutions offer courses in AI ethics and educate the subject.

User's Responsibility

Last but not least, we must keep in mind that despite government rules, these are merely policies, and that it is our own responsibility to abide by them. We must be cautious about the information we post on social media sites and mobile applications, and we must always check the permissions we grant them to view and use our data. We should not just "accept" whatever is stated in the "terms and conditions" that are presented to us on these online platforms.

V. AI AS A BOON

Better health care, safer cars and other modes of transportation, and customised, more affordable, and long-lasting goods and services are just a few ways that AI may help people. It may also improve access to knowledge, instruction, and training. The Covid-19 pandemic increased the need of distance learning. Additionally, AI may assist companies in developing new products and services, especially in sectors where European companies already hold dominating positions, such as equipment, farming, healthcare, fashion, and tourism, as well as green and circular economies, as well as fashion and tourism. Sales can be boosted while also improving customer service, maintaining equipment better, increasing production productivity and quality, and conserving energy.

VI. AI AS A BANE

Since there is no explicit definition of artificial intelligence's legal personality elsewhere in modern law, it is hard to predict how generally accepted laws and customs would deal with them. There will inevitably be misunderstandings surrounding the rights and obligations of AI-driven tools and gadgets because an AI is not now subject to legal culpability for its own actions or omissions. And the majority of people are not aware of the terms and conditions that are included in online service contracts. They simply accept the terms and conditions without ever reading them because the contract is so lengthy and challenging to understand. However, they could have disastrous results. Facebook and Google control every word, image, or video that is submitted, and they don't believe.

VII. CONCLUSION

The legal industry's outlook has undoubtedly changed as a result of technological advancements, and it can be concluded that AI in the legal field has many advantages: it has aided legal professionals in quick research; it can support judges in decision-making processes with its predictive technology; it is useful for law firms for due diligence work, data collection, and other tasks that all make their work more efficient; and it is useful for law firms for due diligence work,

data collection, and other tasks that all make it easier for judges to make decisions. Despite its many advantages, AI cannot take the position of lawyers. While it can help people in some capacities, artificial intelligence (AI) lacks human-level strategic thinking and creativity. Robots can't improvise in front of a court since they lack emotional intelligence, empathy, and both. It is necessary to develop a thorough legal framework to manage Artificial Intelligence and stop it from exploiting the data of its clients since integrating AI into the legal industry has several issues, including the fact that it is still exposed to a number of dangers. We won't be able to fully benefit from AI until there is a legal framework governing its behavior to minimize the risks involved.

VIII. RECOMMENDATION AND SUGGESTIONS:

A balanced strategy must be adopted to make sure AI is included. Here are some suggestions:

1. Different laws must be adopted at the municipal, state and union levels to prevent privacy infringement. The goal of these rules is to make sure that compliance management must include privacy as a mandatory consideration.
2. It is essential to have stringent legal framework outlining the responsibilities and liabilities of this intelligent machine.
3. The legislation must be clear about the liability with regard to any conduct through AI. There shall be the provision for the penalties and fines imposed on the violation of any provision and the sufferer must be rewarded with compensation

IX. LIMITATION OF THE STUDY:

The methodology adopted in this regard is doctrinal and dependable on secondary sources. It is not possible and feasible enough to find out the exactly found about the implication of AI in the field of law within the country.

X.IMPLICATIONS AND FUTURE SCOPE OF THE STUDY

The study is to find out the transformation in society with the taking overt AI in the field of law as privacy. People's ways of living, working, and communicating have already been altered by the digital revolution. Furthermore, it has just begun.

REFERENCE

[1] Harry Surden, Artificial Intelligence and Law: An Overview, Georgia State University Law Review, Vol. 35, 2019, Available in https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3411869
[2] The Information Technology Act, 2000
[3] The Personal Data Protection Bill, 2019
[4] Tyagi, Amit and Tyagi, Amit, Artificial Intelligence: Boon or Bane? (August 15, 2016). Available at SSRN: https://ssrn.com/abstract =2836438 or http://dx.doi.org/10.2139/ssrn. 2836438
[5] Pradeep Kumar U, Artificial Intelligence In Smart Phones: A Boon Or Bane, Available in https://www.psychosocial.com/article/PR270041/139