

INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 6 | Issue 5

2024

© 2024 *International Journal of Legal Science and Innovation*

Follow this and additional works at: <https://www.ijlsi.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com>)

This Article is brought to you for free and open access by the International Journal of Legal Science and Innovation at VidhiAagaz. It has been accepted for inclusion in International Journal of Legal Science and Innovation after due review.

In case of **any suggestion or complaint**, please contact Gyan@vidhiaagaz.com.

To submit your Manuscript for Publication at International Journal of Legal Science and Innovation, kindly email your Manuscript at editor.ijlsi@gmail.com.

Challenges of Legal Regulation of Artificial Intelligence: A Study with Special Reference to Right to Privacy

APRAJITA SINGH¹ AND ROHIT SRIVASTAVA²

ABSTRACT

Modern democracies have recognised the right to privacy, also known as "the right to be let alone," as a fundamental component of human rights. With the development of artificial intelligence in particular, technological breakthroughs have brought about significant changes in society. In the contemporary digital era, where information is easily accessible and technology permeates every aspect of our lives, the right to privacy has emerged as one of the most significant and hotly contested human rights issues. Privacy infringement risks are rising as artificial intelligence (AI) technology become more integrated into daily life. Since artificial intelligence is a highly advanced technology, it cannot be regulated by global rules now in effect. Global regulation of this technology is desperately needed to protect people's rights, most notably their right to privacy. The contradiction between AI and privacy is discussed in the study. The study paper delves deeply into the fundamental ideas of privacy and the legal framework that supports it in various jurisdictions. In order to give people more control over their personal information and to strengthen the legal foundation—which includes mechanisms for clearly opting in and out of data collection and usage as well as access to, correction of, and erasure of data—the paper examines the global framework for data privacy and how data protection laws should be strengthened.

Keywords: Artificial Intelligence, Right to Privacy, European Union Artificial Intelligence Act, Indian laws, US regulations, Challenges in regulation of Artificial Intelligence.

I. INTRODUCTION

Artificial intelligence (AI) is a technology that employs algorithms that, through a system of prediction and adaptations, are capable of autonomous decisions.

John McCarthy initially used the term "artificial intelligence" in 1956. The term artificial intelligence is made of two words "artificial" and "intelligence". Artificial means "which copies something natural". Intelligence means "the ability to learn, understand, and make judgments or have opinions that are based on reason". Thus, artificial intelligence Artificial

¹ Author is a PhD Scholar at Banaras Hindu University, India.

² Author is a student at Jamia Millia Islamia, New Delhi, India.

intelligence is the term used to describe computer systems that simulate human intelligence processes by assimilating information and processing it. Artificial Intelligence has been defined by the European Commission in 2018 as “Artificial intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals.

AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of things applications).³

The European Commission updated the definition to “Artificial intelligence (AI) refers to systems designed by humans that, given a complex goal, act in the physical or digital world by perceiving their environment, interpreting the collected structured or unstructured data, reasoning on the knowledge derived from this data and deciding the best actions (according to pre-defined parameters) to achieve the given goal. AI systems can also be designed to learn to adapt their behaviour by analysing how the environment is affected by their previous actions. As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors, as well as the integration of all other techniques into cyber-physical systems). Artificial intelligence is a technology which possesses the following traits⁴

Artificial intelligence is a technology which possesses the following traits⁵

1. Ability to discover patterns to predict and adapt for desired outcome.
2. Ability to make autonomous decisions by augmenting human intelligence.
3. Ability of adaptation through constant learning by employing trial and error method for solving problems.

³ Azamat Abdoullev, “European AI Alliance - on the EC's Definition of AI, or How to Define Artificial Intelligence with Essence of Intelligence as Real and Conce” *2 Futurium* (2023), available at: <https://futurium.ec.europa.eu/en/european-ai-alliance/forum/ecs-definition-ai-or-how-define-artificial-intelligence-real-and-concerned-essence-intelligence?language=et>

⁴ Ziyadh Saleh, “Artificial Intelligence Definition, Ethics and Standards” *The British University in Egypt, ResearchGate* (2018-19), available at:

https://www.researchgate.net/publication/332548325_Artificial_Intelligence_Definition_Ethics_and_Standards

⁵ Ziyadh Saleh, “Artificial Intelligence Definition, Ethics and Standards” *The British University in Egypt, ResearchGate* (2018-19), available at:

https://www.researchgate.net/publication/332548325_Artificial_Intelligence_Definition_Ethics_and_Standards

4. Ability to analyze and integrate information to predict outcomes.

We will have the technological capacity to replace all human roles in organizations with machines in the very near future—much less than 25 years.⁶ The increasing use of artificial intelligence in daily life has created a critical need for regulation of artificial intelligence. The global community is becoming increasingly concerned about privacy as artificial intelligence becomes more advanced.

There is a dire need of regulation of artificial intelligence due to the following concerns: -

Data privacy concerns- large sets of data are frequently used in AI, which raises privacy and security issues. The possibility of data breaches and illegal access to personal information is the primary concern associated with artificial intelligence as there is so much data being gathered and processed.⁷ Standards for data collection, storage, and use can be established by regulations to safeguard people's right to privacy and stop the improper use of personal information.

1. **Right to be forgotten as a fundamental right**- The right to be forgotten encompasses a person's control over his data and its dissemination. It refers to the right of a person to get his data delinked or erased from all online and offline platforms so that his data cannot be accessed by third parties.⁸ In Europe, the data should be collected and processed accurately, fairly and lawfully for the legitimate purpose for which it has been collected, otherwise it shall be erased.⁹ This law has now been replaced by the General Data Protection Regulation which makes the processing unlawful if it is not in compliance for the consent or public interest.¹⁰ However the authority to decide the lawfulness of the processing is vested in the controller and shall be decided on a case to case basis which is a very tedious process. Thus, there is a need of a specialized authority designed to address such matters efficiently and promptly along with a law to decide the time limit till when such data can be processed. The right to be forgotten or right to be left alone has been recognized as a fundamental right in India.¹¹ In India

⁶ Simon H.A, "The Shape of Automation, Required in Various Forms" Weizenbaum J. 244-245 (1974).

⁷ AI and Privacy: The privacy concerns surrounding AI, its potential impact on personal data", The economic times, available at: <https://economictimes.indiatimes.com/news/how-to/ai-and-privacy-the-privacy-concerns-surrounding-ai-its-potential-impact-on-personal-data/articleshow/99738234.cms>

⁸ Prashant Mali, Privacy Law: Right to Be Forgotten in India, 7 NLIU Law Rev. 7-21 (2018)

⁹ European Union, Article 6 of "DIRECTIVE 95/46/EC of the EUROPEAN PARLIAMENT and of the COUNCIL of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data" Official Journal of the European Communities, available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=NL>

¹⁰ General Data Protection Regulation, Article 6, available at: <https://gdpr-info.eu/>

¹¹ Justice K.S.Puttaswamy(Retd) v. Union Of India 2019 (1) SCC 1

currently there is no explicit law there granting a “Right to be forgotten.”

2. **Artificial Intelligence and Surveillance-** Artificial intelligence technologies are now being employed to improve surveillance operations, like visual recognition and machine learning. As humans are getting technologically advanced each phone now has cameras and recorders, the images sounds and videos from them cannot be manually processed but with the help of artificial intelligence all this data can be easily processed and thus Artificial intelligence has made mass surveillance possible. AI technology is being extensively used in the private sector and is not just being used for government monitoring. Private entities use artificial intelligence for predicting pattern of individuals, use of unauthorized data etc. The use of artificial intelligence raises several issues like privacy concerns and ethical concerns.¹² The privacy concern includes the possibility of misuse, abuse, and illegal access to personal information. The ethical concerns relating to artificial intelligence include the bias in surveillance by artificial intelligence, use of artificial intelligence for political gains, consent, transparency, and accountability. Although artificial intelligence monitoring has many advantages for efficiency, security, and public safety, it also comes with serious concerns that must be handled by rigorous legislation and ethical considerations.
3. **Crimes and tort through artificial intelligence-** Artificial Intelligence can be of great help in detection of crime and prevention of crime by predicting human behaviour. However, there is need for legislation to balance the security of public with violations of privacy and ethics of individuals. AI-enabled crimes are crimes that use artificial intelligence tools or methods to accomplish malevolent goals. AI technologies have the potential to be used for a variety of illegal activities by criminals as they grow more advanced and accessible. These are a few instances of crimes enabled by AI are Deepfakes, Privacy violations, Audio/visual impersonation, Driverless vehicles as weapons, Tailored phishing, Disrupting AI-controlled systems, Large-scale blackmail, AI-authored fake news, offences related to child pornography, offences relate to copyright Autonomous attack drones, Tricking face recognition, AI-assisted stalking, forgery etc.¹³

Currently, there is no legal structure that specifically addresses AI-crimes. The current criminal

¹² Coby Mendoza, “The Rise of AI Surveillance: Exploring Ethical Considerations and Global Implications” AI Canvass of Intelligence (2024) available at: <https://www.linkedin.com/newsletters/ai-cavass-of-intelligence-7017713226087858176/>

¹³ Nyman Gibson Muralis, “AI-Enabled Future Crime: Study Reveals 20 Disturbing Possibilities” Lexology, available at: <https://www.lexology.com/library/detail.aspx?g=93ff642e-0026-4f99-ba79-0fae4114ded5>

liability system is insufficient in dealing with AI enabled crimes. The primary questions which arise here is that who will be responsible for the criminal act or the cases where intent is sine qua non for the crime but no mens rea can be attributed to AI or what will be the jurisdiction for crime committed with help of AI.¹⁴ Given the speed at which AI technology is developing, legislation addressing the intricate questions of jurisdiction and culpability in the context of AI-enabled crime is desperately needed.

4. **Artificial Intelligence and Copyright** – With the use of Artificial Intelligence in all spheres of human life, now the issues relating to authorship of works and infringement of copyright and fair use of works has gained importance. In cases where any work is generated by an AI following the command of a human being, the primary question arises is who shall be considered the author of the work? The programmer or the AI or the AI system or the person giving commands. According to the copyrights law in India the author in relation to any literary, dramatic, musical or artistic work which is computer-generated, the person who causes the work to be created.¹⁵ Indian copyright law does not explicitly recognise AI as an author, making ownership of content produced by AI tools a complex and evolving issue.¹⁶ This also raises a serious concern that if the author of computer generated work is the person giving commands then this would imply that the author of work generated by applications like ChatGpt will be the person giving command , whereas the application itself copies the works already existing and produces before the user.

II. RIGHT TO PRIVACY AND ARTIFICIAL INTELLIGENCE

It derives from the Latin phrase "Privatus," which meaning "isolated from the entire world." Personal privacy is essential for maintaining human dignity and freedom of association and freedom of speech. The right to one's privacy is a basic human right. It is well-known around the globe, in a variety of cultures and locales. According to Dean Prosser, "privacy is not an individual value at all but a composite interest in reputation, emotional tranquillity and intangible property."¹⁷

According to Warren and Brandeis, the idea that every individual is entitled to total protection

¹⁴ Kamshad Mohshin, "Regulation of AI and AI Crime". available at SSRN 8-9(2020) : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3552140

¹⁵ The Copy Right Act (1957), s.2.

¹⁶ Srishti Ojha, "Who Owns the Generated Work? Here's What the Laws Say on Copywriyth Issues", India Today, Sept. 22, 2023, available at: <https://www.indiatoday.in/law/story/chatgpt-ai-generated-content-copyright-ownership-complexities-india-2439165-2023-09-22> (last visited on Apr. 28, 2024).

¹⁷ S.K Sharma, Privacy Law: A Comparative Studies 78 (Atlantic Publisher and Dist. 1994, India).

for their person and property is as ancient as common law. But with time, it has become necessary to reevaluate the precise scope and nature of this protection. Changes in the political, social, and economic spheres necessitate the recognition of new rights. New technologies and corporate strategies draw attention to need to ensure people's safety and to defend their "right to be let alone," as defined by Judge Cooley.¹⁸

The tort of privacy can be categorized as follows:¹⁹

1. Intrusion in the plaintiff's privacy, or personal space.
2. Public revelation of humiliating private details about the plaintiff.
3. Publicity that presents the plaintiff falsely and presents them in an unfavourable manner to the general public.
4. Unapproved use of the plaintiff's identity or image for the defendant's gain.

Countries started enacting wide privacy protection legislation in the early 1970s, with the goal of ensuring that individuals' personal information was protected. There is a global effort toward the implementation of extensive privacy laws that provide a platform for protection of individual information. With the advent of new technology, the possibility of intrusion into an individual's privacy has increased, and eavesdroppers have gained access to new instruments to use against them. Individual privacy is now more important than it has ever been before. Social media and the internet have the potential to accumulate vast amounts of data on individuals, profile them in a variety of ways, commodify them, and deal with them in a manner that might infringe an individual's right to privacy.

III. REGULATION OF ARTIFICIAL INTELLIGENCE (AI) TO SAFEGUARD THE RIGHT TO PRIVACY IN EUROPE AND INDIA

(A) Europe-

In Europe, the idea of protecting personal data or information has a long history. After World War II, the right to be free from "arbitrary interference with... privacy, family, home, or correspondence" was enshrined in the 1948 Universal Declaration of Human Rights, and the right to respect for private and family life was included in the 1950 European Convention on Human Rights. The first data protection law in Europe was passed by the German state of Hessen in 1970. National data protection laws were subsequently enacted in Sweden in 1973,

¹⁸ Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy" 4 *Harvard Law Review* 193-195 (1890).

¹⁹ Neil M. Richards and Daniel J. Solove, "Prosser's Privacy LAW: A Mixed Legacy" 98 *California Law Review* 6

Germany in 1977, and France in 1978. These legislative actions emerged partly in response to a strong privacy culture (France and Sweden) as well as state-imposed monitoring regimes (Germany). The European Parliament further underscored the significance of data protection rights by adopting a resolution in May 1975, affirming that safeguarding these rights was a duty of the Member States.²⁰

In the 1980s, the OECD guidelines were published and the Council of Europe adopted a convention in 1981 in an attempt to bring the increasing number of state legislation on personal data protection closer together. The latter, also known as Convention 108, was the first legally binding international agreement to safeguard people against any violations of their rights that may occur during the processing of their data.²¹

In 1995 Data Protection Directive 95/46/EC (DPD), became the primary EU legislative framework for protecting personal data. Data Protection Directive 95/46/EC (DPD) was repealed by the General data protection regulation in 2016.

The General Data Protection Regulation (GDPR)²² is regarded as the most stringent data protection regulations globally. It limits the processing of personal data by organizations and improves individuals' access to information about themselves.²³

The aim of GDPR is to harmonize the rules relating to data protection of the member states of the European Union. This legislation applies to all organizations that collect, analyze, and use such data, regardless of its origin or regardless of whether the processing takes place in the Union or not.²⁴ This Regulation covers the processing of personal data either through automated means or manually.²⁵

The GDPR covers a wide range of rights like: -

1. Rectification of inaccurate personal data.²⁶
2. Right to know purposes of the processing for which the personal data intended as well as

²⁰ Understanding EU Data Protection Policy, European Union, available at: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651923/EPRS_BRI\(2020\)651923_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651923/EPRS_BRI(2020)651923_EN.pdf) (last visited on 24TH April 2024)

²¹ *Ibid.*

²² Regulation (Eu) 2016/679 of the European Parliament and of the Council (27 April 2016), available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679> (last visited on 24th April 2024)

²³ "What is GDPR? the Summary Guide to GDPR Compliance in the UK", Wired, Mar. 24, 2020, available at: <https://www.wired.com/story/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018/> (last visited on Apr. 28, 2024).

²⁴ *Supra Note 22*, art 6.

²⁵ *Id.*, art 2.

²⁶ *Id.*, art 16.

the legal basis for the processing.²⁷

3. The data subject shall have the right to obtain access to the personal data being processed.²⁸
4. Right to erasure of personal data in case of withdrawal of consent, data is no longer necessary for purposes for which it was collected, data was unlawfully processed or compliance with a legal obligation.²⁹
5. Right to restriction of processing in case of inaccuracy, unlawfulness or processing no longer necessary.³⁰

The data subject for enforcement of his rights under the GDPR has to lodge a complaint with a supervisory authority, in particular in the Member State.³¹ The supervisory authority has the power to handle complaints, investigate and inform the complainant of the progress and the outcome of the investigation.³²

Although the GDPR is a comprehensive law to protect the right to data privacy in European Union, yet it is not well equipped to deal with the challenges brought on by the Artificial Intelligence. The enforcement of rights under the GDPR is done on a case-to-case basis and each request is processed separately. The artificial intelligence works with huge loads of data and thus in cases of violation of rights of data subject by the Artificial intelligence, the authority will not be sufficient to deal such huge number of cases. Thus, the artificial intelligence is likely to over whelm the enforcement of the regulation making such regulation futile.

The European Parliament has passed the Artificial Intelligence act on 13 March 2024 to effectively tackle the problems arising from the fast-developing artificial technology. The act is binding on all members of the European Union; however, the member states need to adapt their laws and incorporate the act in their national legislation.

The objective of Artificial Intelligence act is “to promote the uptake of human centric and trustworthy artificial intelligence (AI) while ensuring a high level of protection of health, safety, fundamental rights as enshrined in the Charter of fundamental rights of the European Union (the ‘Charter’), including democracy, the rule of law and environmental protection, against the harmful effects of AI systems in the Union, and to support innovation”.³³

²⁷ *Id.*, art 13.

²⁸ *Id.*, art 15.

²⁹ *Id.*, art 17.

³⁰ *Id.*, art 18.

³¹ *Id.*, art 77.

³² *Id.*, art 55.

³³ Artificial Intelligence Act (2024), art. 1 available at: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf

The fundamental right to the protection of personal data is safeguarded in particular by GDPR³⁴ and the regulation on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data³⁵ and Directive on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.³⁶ The Artificial intelligence act does not affect the application of these laws governing the processing of personal data.³⁷

The EU AI Act emphasizes on accountability and transparency in the application of AI. It requires developers to give users clear information about the potential and limitations of AI systems so they may make educated judgments. Developers must also keep up-to-date documentation in order to support regulatory oversight.³⁸

The principles of transparency, privacy and data governance, non-discrimination, fairness, accountability, environmentally friendly and diversity should be used in designing and using AI models.³⁹ Market surveillance authorities have the power to guarantee the proper and efficient implementation of the duties and responsibilities set out by this act. The Market Surveillance authority may also take action against any AI system that poses a risk.⁴⁰

The AI Act represents a significant milestone globally in the regulation of artificial intelligence. However, the act does not define Artificial intelligence and as the technology is growing very fast lack of precise definition might pose difficulty in implementation of this act

(B) United States

Although the right to privacy is not expressly mentioned in the US Constitution, the Supreme Court has on several occasions construed different amendments to declare the existence of this right. The United States Supreme Court held that the right to privacy is fundamental and a general "right to privacy" that cannot be unreasonably violated is created by the "spirit" of the following amendments: the First Amendment (freedom of speech), the Third Amendment

³⁴ *Supra Note 22.*

³⁵ REGULATION (EU) 2018/1725 of the EUROPEAN PARLIAMENT and of the COUNCIL of 23 October 2018 Available at :<https://eurlex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1725>(last visited on 24th April 2024)

³⁶ *Supra Note 31*, art.10.

³⁷ Sanhita Cjauriha, "An Overview of the European Union's Artificial Intelligence Act", *The Hindu*, Dec. 18, 2023, available at: <https://www.thehindu.com/sci-tech/technology/an-overview-of-the-european-unions-artificial-intelligence-act/article67648550.ece> (last visited on Apr. 28, 2024).

³⁸ *Supra Note 33*, art. 27.

³⁹ *Id.*, art.156.

⁴⁰ *Griswold v. Connecticut*, 381 U.S 479(1965)

(prohibition on the forced quartering of troops), the Fourth Amendment (freedom from searches and seizures), the Fifth Amendment (freedom from self-incrimination), the Ninth Amendment (other rights), and the Fourteenth Amendment (right to life, liberty, or property and equal protection of laws).⁴¹

The Privacy Act 1974 establishes a set of fair information standards that regulates how federal agencies collect, store, use, and share personal data. Although the United States is leading the way in the worldwide race for artificial intelligence, yet it does not have a specific federal legislation to regulate the AI. The White House has released a blue print for AI bill of rights which deals with data privacy, algorithm discrimination protections, safe and effective AI, notice of use of AI and its extent on the data provided by individuals.⁴² This blue print is not legally enforceable. The federal government passed the Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence according to which if the safety test results indicate that an AI system could be dangerous to national security, then makers of AI systems must notify the US government. Various states within the United States have enacted legislation to regulate the use of artificial intelligence (AI) within their jurisdictions.

(C) India

The right to privacy has been in constant debates in India since 1954.⁴¹ The Right to privacy was directly or indirectly in issue in a large number of cases.⁴² Until it was finally recognized as a fundamental right. The Hon'ble Supreme Court of India has recognized right to privacy as a fundamental right and is protected under Article 14, 19 and 21 on the Constitution of India. However it was held that this right is not absolute if there exists a legal system, provisional safeguards against intrusion and the interference is necessary and proportional to the purpose to be achieved.⁴³ The Right to privacy was directly or indirectly in issue in a large number of cases.⁴⁴ Until it was finally recognized as a fundamental right. The Hon'ble Supreme Court of India has recognized right to privacy as a fundamental right and is protected under Article 14, 19 and 21 on the Constitution of India. However it was held that this right is not absolute if there exists a legal system, provisional safeguards against intrusion and the interference is necessary and proportional to the purpose to be achieved.⁴⁵ The proclamation of privacy as a

⁴¹ The Privacy Act (1974), ss. 5 U.S.C. § 552a (2012)

⁴² 17 U.S.C. §105(2022), U.S.A, available at: <https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf> (last visited on 20th April 2024)

⁴³ Kharak Singh v. State of Uttar Pradesh (1954) SCR 1077

⁴⁴ MP. Sharma v. Satish Chandra, (1954) SCR 1077, Gobind v. State of Madhya Pradesh 1 SCR 332 (1964). Union for Civil Liberties (PUCL) v. Union of India, AIR 1997 SC 568, X v. Hospital Z (1998) 1 SCR 723, Suchitra Srivastava and another v. Chandigarh Administration' (2009) 14 SCR 989, (2009) 9 SCC, Smt. Selvi & Ors. v. State of Karnataka (2009) 14 SCR 989, (2009) 9 SCC 1

⁴⁵ Justice K. S. Puttaswamy (Retd.) and others v. Union of India n others ((2017) 10 SCC 1)

fundamental right prompted the government to initiate efforts toward enacting a new data protection law for the nation. The government constituted a committee chaired by retired Supreme Court Justice BN Srikrishna. The committee submitted a report on Data Protection Framework.⁴⁶ Following the suggestions of the report the Personal Data Protection Bill 2019⁴⁷ was framed. However, the Joint Parliamentary Committee in its report⁴⁸ proposed several amendments to the personal data protection bill. The bill was finally withdrawn by the government due to the following reasons: - 1. The parliamentary committee proposed several amendments to the bill. 2. Tech companies: They thought that rules like data localization—which stores Indian data in India were overly restrictive. 3. Privacy activists: They believed that the bill offered the government an excessive amount of power for surveillance. 4. Startups: They were concerned that there would be too much compliance work. The government finally passes the Digital Personal Data Protection Act⁴⁹ on 9, August 2023, which is currently the umbrella law dealing with privacy in India. This act is applicable on processing “personal data” in India which was collected online or offline in India or, processing of “personal data” outside India where processing is in connection with any profiling of, or activity of offering goods or services.⁵⁰ “Personal” does not always imply extreme sensitivity in this instance. Rather than that, it refers to a connection between the information and a person, meaning that the information, whether important or trivial, may be linked to an individual in some way.

Personal information includes the following:

- (i) Information that establishes an ownership relationship with an individual;
 - (ii) Information that establishes a descriptive relationship with a person; and
 - (iii) Information that establishes an instrumental mapping relationship with an individual.
- Under the Act the data may be processed only by express or implied consent of the data principle.⁵¹ The data fiduciary shall give the data principle a notice of the

⁴⁶ Government of India, “White Paper on Data Protection Framework for India,” (Ministry of Electronic and Information Technology, 2028) , available at: <https://www.meity.gov.in/white-paper-dataprotection-framework-india-public-comments-invited> (last visited on March 12, 2024)

⁴⁷ Government of India, “Personal Data Protection Bill” (Ministry of Electronics and Information Technology, 2018) available at: <https://www.meity.gov.in/content/personal-data-protection-bill-2018> (last visited on March 20, 2024)

⁴⁸ Government of India, “Report of The Joint Committee on personal data protection bill”, 2019, available at: http://loksabhaph.nic.in/Committee/CommitteeInformation.aspx?comm_code=73&tab=1 (last visited on 16 March, 2024)

⁴⁹ Digital Personal Data Protection Act, 2023 available at https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Potection%20Bill%2C%202022_0.pdf

⁵⁰ Digital Personal Data Protection Act (2023), s. 4

⁵¹ *Id.*,s.5.

description of the data collected and purpose of the collection.⁵²

The act makes clear provision for informed consent and withdrawal of consent.⁵³ However, the legality of processing personal data that was based on consent prior to its withdrawal is unaffected by the withdrawal of consent. The act enumerates several rights of data principle: -

1. Right to information about personal data.⁵⁴
2. Right to correction and erasure of personal data.⁵⁵
3. Right of grievance redressal.⁵⁶
4. Right to nominate.⁵⁷

The act enumerates several duties of data principle⁵⁸:-

1. Comply with the provisions of law.
2. Not register a false or frivolous grievance or complaint.
3. Furnish any false particulars or suppress any material information or impersonate another person. Furnish only such information as is verifiably authentic.

The act provides for the Obligations of data fiduciary⁵⁹ :-

- (i) Ensure accuracy of data.
- (ii) In the event of a data breach, notify the Data Protection Board of India and the affected parties.
- (iii) Create adequate security measures to prevent a data breach.
- (iv) Erase personal data as soon as the purpose has been fulfilled and retention is not required for legal purposes (storage limitation). However, Governmental organizations are exempt from storage restrictions and the data principal's right to erasure.
- (v) Create adequate security measures to prevent a data breach.
- (vi) Erase personal data as soon as the purpose has been fulfilled and retention is not required for legal purposes (storage limitation). However, Governmental organizations are exempt from storage restrictions and the data principal's right to erasure.

⁵² *Id.*,s.6.

⁵³ *Id.*,s.7.

⁵⁴ *Id.*,s.12.

⁵⁵ *Id.*, s.13.

⁵⁶ *Id.* s.14.

⁵⁷ *Id.* s.15.

⁵⁸ *Id.*,s.16.

⁵⁹ *Id.* s.9,10,11.

- (vii) Create adequate security measures to prevent a data breach.
- (viii) Erase personal data as soon as the purpose has been fulfilled and retention is not required for legal purposes (storage limitation). However, Governmental organizations are exempt from storage restrictions and the data principal's right to erasure. The Act also provides for several exemptions where the personal data may be processed without express consent.⁶⁰

The primary concerns which arise out of this act are⁶¹:-

1. It deals only with personal data which may be linked to an individual. Non personal data is not covered by this act. There is a need for protection of non-personal data as well as it plays an important role in economics and politics.
2. Exemptions to government in processing personal data may give rise to excessive misuse of personal data by government. The act does not require the government to delete the data after it is no longer useful may lead to creation of a huge data base by the government.
3. The act does not provide for a general right to be forgotten. The right to be forgotten is available only in the following circumstances: -
 - (a) The act provides option to the data fiduciary to either cease to retain personal data, or remove the means by which the personal data can be associated with particular Data Principal in case the purpose of collection has been served or retention is no longer necessary for legal and business purposes.⁶²
 - (b) The right to erasure of personal data is given only when data is no longer necessary for the purpose for which it was processed unless retention is necessary for a legal purpose. In cases where the consent is withdrawn, the withdrawal of consent shall not affect the lawfulness of processing of the personal data based on consent before its withdrawal.⁶³

Currently the Artificial Intelligence is dealt under the Information Technology Act, 2000⁶⁴. Despite being a fundamental piece of legislation, the Information Technology Act (IT Act) is

⁶⁰ *Id.* s.8.

⁶¹ *Id.*, s.9.

⁶² *Supra Note 57.*

⁶³ *Supra Note 55.*

⁶⁴ The Information Technology Act(2000)

unable to fully regulate AI in India for a number of reasons.

1. Law of the Pre-AI Era: The IT Act was drafted in 2000, before to the general use of AI. It lacks clauses created especially to deal with the particular difficulties presented by AI systems.
2. Pay Attention to Data, Not AI: The IT Act mainly addresses intermediary liability and data protection. These are significant features of AI, but they don't deal with problems like algorithmic bias, the explainability of AI judgments, or possible safety hazards.
3. Restricted Scope: Electronic communication and online activities are the primary areas covered by the IT Act. Artificial Intelligence is quickly moving beyond the digital sphere, and the IT Act does not address these situations.
4. Though India has passed a personal data protection bill, still there is a need of law to protect data other than personal data, further there is a need of amendment in the existing laws to safeguard the protection of data privacy especially against the government agencies. India also needs a specific law to deal with the artificial intelligence as the current information technology act is obsolete and no longer sufficient to regulate the current advanced technology like the Artificial Intelligence.

Despite being a fundamental piece of legislation, the Information Technology Act (IT Act) is unable to fully regulate AI in India for a number of reasons.

1. Law of the Pre-AI Era: The IT Act was drafted in 2000, before to the general use of AI. It lacks clauses created especially to deal with the particular difficulties presented by AI systems.
2. Pay Attention to Data, Not AI: The IT Act mainly addresses intermediary liability and data protection. These are significant features of AI, but they don't deal with problems like algorithmic bias, the explainability of AI judgments, or possible safety hazards.
3. Restricted Scope: Electronic communication and online activities are the primary areas covered by the IT Act. Artificial Intelligence is quickly moving beyond the digital sphere, and the IT Act does not address these situations.
4. Though India has passed a personal data protection bill, still there is a need of law to protect data other than personal data, further there is a need of amendment in the existing laws to safeguard the protection of data privacy especially against the government agencies. India also needs a specific law to deal with the artificial intelligence as the current information technology act is obsolete and no longer

sufficient to regulate the current advanced technology like the Artificial Intelligence. Though India has passed a personal data protection bill, still there is a need of law to protect data other than personal data, further there is a need of amendment in the existing laws to safeguard the protection of data privacy especially against the government agencies. India also needs a specific law to deal with the artificial intelligence as the current information technology act is obsolete and no longer sufficient to regulate the current advanced technology like the Artificial Intelligence.

IV. CONCLUSION

Artificial Intelligence has enormous potential to improve lives in the future. The artificial intelligence technology is growing at a very rapid pace and it is likely to take replace all human activity in a very near future. The paper has analysed the various threats involved in the use of Artificial Intelligence. As artificial intelligence (AI) technologies become more pervasive in everyday life, there is an increasing risk of privacy infringement. The artificial intelligence is a very sophisticated technology which cannot be governed by the existing laws all around the world. An urgent need has arisen around the globe to regulate this technology to save the various rights of the people especially the right to privacy. The European Union is the first institution which has passed a legislation. However, the members of European Union are yet to implement this Act. Though this act has tried to regulate and the individuals can file case when their rights are violated. The author is of the view that the law should fix the number of years till the information can be stored and processed from the date of the collection. The author is also of the view that the number of times a data can be processed must also be limited by the law so that the AI does not perpetually and infinitely predict human response from a given set of data. Countries like US and India do not currently have a specific law to regulate Artificial intelligence. As artificial intelligence is taking huge technological leaps day by day. The whole world including India and US need to frame laws to regulate artificial intelligence as soon as possible, so that they can adapt these laws with the growth of technology to protect the rights of the people. The right to privacy has been recognised as a fundamental right in India and across the globe. However, India currently has framework only to protect personal data. Even this legislation has its flaws like it provides exemption to government in processing and storing data and non-recognition of right to be forgotten as a general rule. India needs to adapt its current legislation and incorporate data privacy in case of both personal and non-personal data. In the era when the technology is taking such giant leaps, countries where the data privacy is not sufficiently secured the Artificial Intelligence is likely to pose a great threat and might even crumble the existing society and the legal system. Thus, there is a great need to firstly, frame

and strengthen data privacy laws and secondly, to frame and continuously adapt the specific laws to regulate Artificial intelligence.
