AI MEMORY RETENTION: PRIVACY AND REGULATION CHALLENGES

Aayushi Kumari, BA LLB, Presidency University, Bangalore

ABSTRACT

Artificial intelligence is among the most significant developments in the modern world as far as technology is concerned. Some of the major areas where AI has played a key role includes decision making, communication and online transactions. One specific type of AI technology that has gained popularity includes chatbots in industries such as education, medicine, finance, customer services and entertainment. This is mainly attributed to the reflectiveness in providing personalized responses quickly and effectively. AI Chatbots depends on collecting, storing and analyzing vast amounts of user data. However, this process of collecting data comes with major data privacy challenges.

The current research paper seeks to evaluate the major privacy issues Posses by AI chatbots and other digital communication systems. Major topics for discussion will include profiling, surveillance, behavioral forecasting, emotional exploitation, security vulnerabilities, data breaches and abuse of sensitive personal information. Additionally, topics related to informed concern and transparency will be covered such as lack of proper consent from the user, misleading privacy policies, AI training methods an asymmetrical power dynamic between users and providers of technology.

This research is founded on the theories of privacy, data protection and ethical Artificial Intelligence governance. The research method adopted for the study is doctrinal and descriptive and the sources employed for the research include books, scholarly articles, legal documents and government reports. Additionally, this paper makes a comprehensive study of India Digital Personal Data Protection Act, 2023, the GDPR of the European Union and the US sectoral approach to privacy legislation to analyze their effectiveness in safeguarding the right to privacy of personal data. Judicial cases that are crucial to the study and highlight judicial acceptance of the privacy rights include K.S. Puttaswamy VS Union of India and Google's Spain SL VS AEBD.

I. INTRODUCTION

Artificial Intelligence has grown rapidly due to technological advancements. One of the most widely used tools of Artificial Intelligence is the AI Chatbots, which enables human to communicate with machines through text and voice interactions.

Initially, Chatbots were simple rule-based system that could only provide predefined responses. However, with the development of advanced AI models, modern chatbots are now capable of understanding human language, answering complex questions, generating content and assisting users in various tasks[1]. AI chatbots are now widely employed in sectors including education, Healthcare, customer Service, banking and many other industries because they can provide quick and efficient responses to user inquiries. These chatbots are designed using technologies such as machine learning and natural language processing to understand user queries and generate appropriate answers. In addition, AI systems can store user conversations to improve performance, provide personalized responses and enhance user experience[2]. Stored data may help developers to train AI models and provide better customer support services. However, this practice also raises concerns about privacy and data security.

AI has become an integral part of contemporary technology. However, at the same time several privacy concerns are associated with the technology. Firstly, AI gathers significant volumes of personal data related to user interactions, communication, browsing history and other activities. The gathered data is used by AI to enhance its efficiency and deliver personalized services. Nonetheless, when the data is mishandled, numerous privacy violations can occur and the security of personal information can be compromised. Users are worried that their confidential information and conversations might be misused and leaked without any permission[3]. Moreover, AI surveillance technology and face recognition software have raised numerous questions regarding user privacy and data security[4]. Consequently, it is critical to create privacy-related policies and legislation to prevent possible problems connected with the use of Artificial Intelligence technologies[5].

[1] Stuart Russell & Peter Norvig, *Artificial Intelligence: A Modern Approach* 1–28 (4th ed. 2020).
[2] Bernard Marr, *Artificial Intelligence in Practice* 45–60 (2019).
[3] European Parliament, Artificial Intelligence and Data Protection: Challenges and Possible Remedies, https://www.europarl.europa.eu (last visited June 8, 2026).
[4] UNESCO, Recommendation on the Ethics of Artificial Intelligence (2021), https://unesdoc.unesco.org (last visited June 8, 2026).
[5] General Data Protection Regulation, Regulation (EU) 2016/679, 2016 O.J. (L 119) 1.

One of the primary issues associated with the concept of AI is the lack of user awareness and legal certainty. It is quite common for users to be unaware of how their personal data are collected, stored and used through Artificial Intelligence applications[6]. Individuals commonly use AI applications without even bothering to read privacy policies or being aware of potential risk associated with the disclosure of personal data. In turn, it increases the likelihood of data misusing and privacy invasion. Apart from that, there is uncertainty as regards laws concerning the usage of AI technologies as different states have different laws and are unprepared for the problems brought by modern AI systems.[7]

II. RESEARCH QUESTIONS

Q1. What is the role of AI chatbots in modern technology and communications?

Q2. How do AI chatbots collect, store and process user data?

Q3. What are the major privacy concerns associated with Artificial Intelligence?

Q4. How does the lack of user awareness affect the safe use of AI technologies?

Q5. What legal challenges arise from the use of AI chatbots and data storage systems?

Q6. Are existing privacy laws sufficient to regulate AI technologies effectively?

III. OBJECTIVES OF THE STUDY

1. To study the growth and development of AI chatbots.

2. To examine the functioning of AI chatbots and their use in different sectors.

3. To analyze the storage of user conversations and personal data in AI systems.

4. To identify privacy and security concerns related to Artificial Intelligence

5. To examine the issue of lack of user awareness regarding AI technologies.

[6] Frank Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information 3–18 (2015).
[7] National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework (2023), https://www.nist.gov (last visited June 8, 2026).

6. To evaluate existing legal frameworks and regulations related to AI and data protection.

7. To suggest measures for ensuring the ethical and responsible use of AI technologies.

IV. THEORETICAL FRAMEWORK

This study is based on the theories of privacy, data protection and ethical AI governance. Through the theories of privacy, data protection and ethical AI governance, analysis can be made about the ways in which AI chatbots gather, store and utilize the personal information[8]. The theory of privacy involves the protection of individual personal information. The data protection theories are concerned with the various legal measures that are required to protect data during its collection, storage and processing.[9] Ethical AI governance deals with the various principles such as transparency, accountability and responsible AI utilization[10]. This theoretical framework becomes necessary to analyze the issues related to privacy, storage and other legal and ethical aspects of AI technologies and digital communication systems.

Privacy theory is very important when looking at the effects that Artificial Intelligence technologies have on the lives of individual users. Many chatbots and virtual assistants make use of personal data in the form of interactions, browsing habits, preferences and behavior in order to offer customized service or to boost their efficiency. While this may help enhance their efficiency and convenience for users, it does raise questions about data security, unauthorized access to personal data, or the violation of an individuals' privacy rights. Privacy theory will help us understand if users are well-informed about how their data is being used by the AI system.

V. METHOLOGY

In terms of methodology, this study will employ a doctrinal and descriptive methodology. The research will be based upon the secondary sources, which include books, legislation, legal journals, research papers, government reports and official websites related to Artificial Intelligence and data privacy. A qualitative approach has been used to analyze privacy concerns, storage of conversations, legal uncertainty and user ignorance with respect to AI

[8] National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework (2023), https://www.nist.gov (last visited June 8, 2026).
[9] Creswell & Creswell, Research Design: Qualitative, Quantitative, and Mixed Methods Approaches 3–25 (5th ed. 2018).
[10] S.N. Jain, Legal Research and Methodology 45–60 (LexisNexis 2016).

technology. Existing legislations on data protection and ethical AI governance will be considered at national and international levels.

VI. UNDERSTANDING AI MEMORY

Artificial Intelligence memory refers to the capability of AI systems to retain and utilize information from previous interactions, datasets or experiences in order to improve future performance and responses. AI memory allows chatbots and virtual assistants to recognize user preferences, understand patterns of communication, and provide personalized services based on stored information. This feature enhances the efficiency, accuracy and adaptability of AI technologies in various sectors such as healthcare, education, banking and customer service. However, the storage and processing of user information through AI memory systems also create significant concerns relating to privacy, consent, surveillance and data security[11]. Therefore, effective legal regulations and ethical safeguards are necessary to ensure that AI memory systems operate responsibly and protect the rights of users.

TEMPORARY MEMORY AND **PERSISTENT MEMORY** – There are two kinds of memory which are important in AI, and those include **temporary memory** and **persistent memory**. As the name suggests, temporary memory which is used within one ongoing process or session. The purpose of the memory is to enable an AI system to remember previous inputs so that the conversation can continue uninterrupted. However, once the session is over, the data is normally discarded. On the other hand, persistent memory is a kind of long-term memory which keeps information to be used in future sessions. Through persistent memory, an AI system is able to recall user behavior and preferences to give personalized responses.

An AI training system is a term used for the methods and techniques that involve the learning process of an Artificial Intelligence model using data over time. Such AI systems are trained on big volumes of data such as text, pictures, sound or other types of data. Using machine learning techniques, AI training enables systems to recognize patterns, analyze data, and such as chatbots, recommendations, face recognition software and automated decision-making programs[12]. Nevertheless, big volumes of training data bring along various issues such as

[11] Margaret A. Boden, Artificial Intelligence: A Very Short Introduction 72–89 (Oxford Univ. Press 2018); Frank Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information 3–18 (Harvard Univ. Press 2015).

[12] Pedro Domingos, The Master Algorithm: How the Quest for the Ultimate Learning Machine Will Remake Our World 25–48 (Basic Books 2015); Kate Crawford, Atlas of AI: Power, Politics, and the Planetary Costs of

privacy issues, biases, data copyright infringement and ethical utilization of data.

Data storage in Artificial Intelligence is defined as the activity of collecting, organizing, maintaining and storing the information utilized by Artificial Intelligence systems during their operation.AI systems use a huge amount of data such as user chats, behavioral data, images and other digital data to store them in databases or cloud storage systems. The stored data plays an important role in increasing accuracy and learning from previous experiences. Data storage usually consists of activities such as data collection, classification, processing, encrypting and retrieving the data for further usage. Nevertheless, incorrect data storage or its management can result in privacy concerns, data leakage and misuse of data. That is why safe data storage is critical for effective functioning of Artificial Intelligence.[13]

VII. PRIVACY RISKS IN AI CHAT STORAGE

In particular, the development of AI technologies has brought significant changes to communications, operations of companies and internet interactions. Modern chatbots, virtual assistants, recommendation systems and automation are used extensively for educational, healthcare, banking, commerce, entertainment and social networking purposes. As AI-driven technologies need to operate properly, they collect, store and analyze large amounts of user data[14]. Despite all the benefits provided by AI, the mentioned technologies have created numerous concerns related to profiling, surveillance, predictive behavioral analysis, emotion manipulation, hacking, data breaches and use of confidential personal data. It should be noted that the issues above raise several legal, ethical and social questions related to user privacy and personal information.

PROFILING

One of the most widespread practices implemented in AI technologies and digital platforms is profiling. Profiling implies the collection and analysis of information about an individual and his or her categorization based on their behavior, interests, habits, preferences and other

Artificial Intelligence 15–37 (Yale Univ. Press 2021)

[13] Viktor Mayer-Schönberger & Kenneth Cukier, Big Data: A Revolution That Will Transform How We Live, Work, and Think 97–120 (Houghton Mifflin Harcourt 2013); Shoshana Zuboff, The Age of Surveillance Capitalism 93–117 (PublicAffairs 2019).

[14] Klaus Schwab, The Fourth Industrial Revolution 7–25 (Crown Bus. 2017); Nick Bostrom, Superintelligence: Paths, Dangers, Strategies 1–18 (Oxford Univ. Press 2014)

characteristics revealed via user interaction with technology or website[15]. To implement profiling, AI technology needs to gather data from user conversation, browsing history, search engine records, social media interactions, purchase history and any online activities that reveal the user. Such profiles help in predicting interests, offering recommendations for products and services, personalizing advertising and affecting decision- making. Although the use of profiling helps improve user experience and make business operations more efficient, It also raises questions about the possibility of discrimination, invasion of privacy and absence of informed consent. The individual does not know how much personal data is collected by AI algorithms[16].

SURVEILLANCE

Surveillance can be viewed as another crucial issue that is related to Artificial Intelligence. Today, a variety of technologies such as facial recognition and biometrics Identification tools, monitoring systems, location tracking technologies and others allow monitoring and observing users' actions. Although some people may argue that monitoring systems provide an opportunity to ensure security, prevent any type of crime and enhance operational efficiency[17]. They may limit some basic human rights such as the right for privacy, free speech, personal autonomy and others. Digital surveillance tools may lead to a condition when users feel permanently monitored. Therefore, they will change their behavior and act accordingly to new circumstances.

BEHAVIORAL PREDICTION

Behavioral prediction is directly linked with profiling and surveillance. AI uses data in order to make predictions concerning users' behavior, preferences, interests and so on. Machine learning technologies use various algorithms to analyze user behavior in order to identify how a certain user can respond to advertisements, political messages, new products and other elements. Corporations and online platforms apply behavioral prediction in order to promote their product and improve user interaction with the platform[18]. Predictive technologies can also

[15] David Lyon, Surveillance Society: Monitoring Everyday Life 19–42 (Open Univ. Press 2001); Oscar H. Gandy Jr., The Panoptic Sort: A Political Economy of Personal Information 53–79 (Westview Press 1993)
[16] Cass R. Sunstein, #Republic: Divided Democracy in the Age of Social Media 45–70 (Princeton Univ. Press 2017); Shoshana Zuboff, The Age of Surveillance Capitalism 199–232 (PublicAffairs 2019)
[17] Sandra Wachter, Brent Mittelstadt & Luciano Floridi, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, 7 Int'l Data Privacy L. 76 (2017)
[18] Bruce Schneier, Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World 85–112

be used in order to manipulate people and modify their behavior.

EMOTIONAL MANIPULATION

Yet another potential problem related to AI is the possibility of emotional manipulation. Highly sophisticated AI is capable of analyzing the emotion and behavior of the user based on his/her facial expression, voice intonation and other factors. This feature is actively used in the work of social networks, marketing campaigns and customer care systems. Emotion analysis allows manipulating people by showing advertisements and contents that can trigger a certain reaction on the part of users. In such cases, it becomes possible for the system to exploit an individual emotionally.

UNAUTHORIZED ACCESS

Another major threat that comes from Artificial Intelligence technology and digitalization is the risk of unauthorized access to personal data. Many AI- powered technologies are capable of storing huge amounts of personal data, ranging from conversations, financial information, biometrics, password credentials and behavioral patterns. The lack of necessary security measures can enable hackers, cybercriminals and other unauthorized parties to access such confidential information. As a result, individuals may become victims of identity theft, financial scams, cyber harassment, blackmailing and any other use of the confidential data. The widespread usage of cloud-based information storage has contributed significantly to the risks of cyber-attacks and accessing confidential personal information[19]. Thus, companies should implement necessary cybersecurity measures, encryption techniques and other protective measures to secure personal user data.

DATA BREACHES

In connection with the aforementioned threat, another considerable risk faced by the world due to digitalization and Artificial Intelligence involves data breaches. It is defined as the exposure, stealing, leaking and unapproved access to confidential or sensitive information. Personal data is type of data that attracts most cybercriminals and hackers since AI-Powered technologies

(W.W. Norton & Co. 2015); Daniel J. Solove, Nothing to Hide: The False Tradeoff Between Privacy and Security 98–126 (Yale Univ. Press 2011)

[19] Paul M. Schwartz & Daniel J. Solove, The PII Problem: Privacy and a New Concept of Personally Identifiable Information, 86 N.Y.U. L. Rev. 1814 (2011); Helen Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life 127–156 (Stanford Univ. Press 2010)

collect huge amounts of personal data belonging to millions of users. These types of occurrences can lead to serious financial, emotional and reputational harm and even a violation of privacy rights[20]. It should be noted that in most cases, a used will not even realize that their private information was used before some serious harm is done to them. These data breaches show us the need for new laws regarding data regulation, proper cybersecurity measures and proper management of data.

SENSITIVE PERSONAL DATA

An important topic that must be discussed when speaking about personal data concerns sensitive personal data. Personal data considered to be sensitive includes health records, biometrics data, financial data, religious beliefs, political opinions, personal communication and sexual orientation. Sensitive personal data is used by AI algorithms to provide a personal approach to its customer. However, using sensitive personal data without consent or for inappropriate purposes might have a significant effect on the life of the individual whose information was obtained. For example, this data could be used to exclude one person from society, steal their identity, harm their reputation, violate their privacy and discriminate against them.

Due to these rising concerns, many nations and organizations worldwide have come up with laws, rules and policies concerning data protection and AI governance. There are laws and regulations covering issues of privacy, cybersecurity and ethical AI that govern the processing, storage and utilization of data collected by AI. Such laws underscore important values like transparency, accountability, consent, equity and the security of data[21]. However, technological advancements have raised further issues that the existing legal frameworks cannot cover. In addition, many consumers are unaware of how data about themselves is collected and processed by AI applications.

This is why it is vital to come up with stricter laws, regulations and policies for the use and governance of AI systems. It is the responsibility of both governments and organizations to see

[20] European Commission, Ethics Guidelines for Trustworthy AI (2019), https://digital-strategy.ec.europa.eu (last visited June 8, 2026); Organisation for Economic Co-operation and Development (OECD), OECD Principles on Artificial Intelligence (2019), https://oecd.ai (last visited June 8, 2026)

[21] European Commission, Ethics Guidelines for Trustworthy AI (2019), https://digital-strategy.ec.europa.eu (last visited June 8, 2026); Organisation for Economic Co-operation and Development (OECD), OECD Principles on Artificial Intelligence (2019), https://oecd.ai (last visited June 8, 2026)

that technologies work in a fair, secure, accountable and transparent manner and do not violate the privacy rights of individual.

VIII. CONSENT AND TRANSPARENCY ISSUES

Consent and transparency are the two core aspects of regulating the usage of AI technologies from both the ethical and legal perspectives. The operation of AI chatbots, virtual assistants and other digital platforms depends on vast amounts of private data[22]. As a result, collecting, storing and processing personal information necessitates obtaining consent and ensuring that users know how their information will be handled. Still, there are multiple problems associated with informed consent, inadequate and opaque privacy policies, training processes that remain invisible for users and unequal negotiations between tech companies and customers.

INFORMED CONSENT

Firstly, a major problem that arises when considering regulating AI systems is the problem of informed consent. Informed consent means that people understand what kind of data is being collected, how it will be used, by whom it will be used and what will happen as a result of it[23]. Thus, when using an AI service, people need to be provided with a chance to give informed consent for their personal information being used. However, many people cannot provide it because they do not understand the amount of data AI uses.

VAGUE PRIVACY POLICIES

The problem associated with opaque and hard to understand privacy policies also exit. Many AI systems have policies concerning privacy issues where users get familiar with data collecting procedures. Nonetheless, the mentioned documents are usually long, sophisticated and unclear to typical consumers. Crucial details related to the strong and processing of data, as well as training may be hidden in intricate legalese. As a result, people tend to accept the policy terms without reading them carefully or fully understanding them. Thus, the mentioned issues undermine transparency and prevent users from having any control over their data since

[22] Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* 43–67 (Harvard Univ. Press 2018)
[23] Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* 127–156 (Stanford Univ. Press 2010).

transparency presupposes clear communication of the matter[24].

HIDDEN TRAINING PRACTICES

The hidden processes related to data utilization for training algorithms represent another major problem. It is common practice for companies to collect vast amounts of data via user interactions, online activity etc. to train their AI systems[25]. Users are usually not informed that their interactions, prompts and other data may be utilized for algorithm training purposes. Even if companies disclose their data use practices in their privacy policy, the process still remains unclear and inaccessible. Unclear communication about the use of data brings into focus issues related to fairness, transparency and autonomy of individuals whose data can be unwittingly used to train AI systems, without any knowledge about the storage, analysis and reuse of personal data.

UNEQUAL BARGAINING POWER

The issue of inequality in power also presents difficulties when discussing issues related to consent and transparency in AI systems. Digital companies and technology providers have an abundance of knowledge and control regarding data practices compared to the end users of their services. Usually, most users do not have much negotiating power, especially since the standards terms and conditions of using a certain service are non-negotiable. Instead, users are left with the option to either agree or not. In many cases, consent to collect data cannot be regarded as a voluntary decision, since in order to gain access to a certain service, one needs to agree to collect personal data – a situation which occurs quite often, since most people rely on digital platforms for communication, learning, working and leisure[26].

These examples illustrate the idea that consent and transparency go beyond the mere action of having a user agree by clicking a button or checking a box. To guarantee privacy, there needs to be communication, comprehensible policies, user empowerment and accountability when it comes to collecting and using personal information. With the constant evolution of AI, lawmakers need to make sure that companies and other organizations follow transparent

[24] Ryan Calo, Digital Market Manipulation, 82 Geo. Wash. L. Rev. 995 (2014)
[25] Michèle Finck & Frank Pallas, They Who Must Not Be Identified—Distinguishing Personal from Non-Personal Data Under the GDPR, 10 Int'l Data Privacy L. 11 (2020)
[26] Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 Harv. L. Rev. 1880 (2013)

policies and show respect towards the users about AI data management.

IX. COMPARATIVE LEGAL ANALYSIS

DIGITAL PERSONAL DATA PROTECTION ACT,2023 (DPDP)

The growth of Artificial Intelligence and the communication system, data protection has become one of the essential legal issues worldwide. With respect to the AI technology, a vast amount of personal data is collected, stored and processed by the same technology. Thus, there emerge many problems like privacy, profiling, surveillance and misuse of information. To manage all these legal concerns, various legislative regimes regarding data protection have been formed by India, the European Union and the USA[27].

The Indian Digital Personal Data Protection Act, 2023 is a principal law dealing with the issue of personal digital data. According to section 4, personal data should be processed for any legitimate purpose only and on the condition of consent or legitimate uses. In turn, section 6 sets the rules for the consent stating requirements that consent is free, specific, informed and clear. Moreover, section 11, 12 and 13 provide the data principles with the right to access, correct and erase personal data respectively. Meanwhile, Section 8 imposes obligations on data fiduciaries regarding ensuring data accuracy And security safeguards. At the same time, Section 17 exempts the state from many responsibilities for several reasons[28].

Although the Act puts into place a consent-based system. These exceptions pose questions regarding surveillance by the government as well as poor privacy protection measures.

GENERAL DATA PROTECTION REGULATION (GDPR)

The GDPR of the European Union can be stated as the most effective privacy law throughout the world. The principle set by Article 5, which include the lawfulness, fairness, transparency, purpose limitation and data minimization. Lawful basis of processing are described in Article 6, whereas Article 7 states the condition for obtaining valid consent. Access, rectification and the right to be forgotten are provided in articles 15, 16 and 17. Article 22 provides protection from any decisions taken only using automated process and profiling. Article 32 and 71 explain

[27] Paul M. Schwartz & Daniel J. Solove, The PII Problem: Privacy and a New Concept of Personally Identifiable Information, 86 N.Y.U. L. Rev. 1814 (2011)
[28] Digital Personal Data Protection Act, No. 22 of 2023, §§ 4, 6, 8, 11–13, 17 (India).

how concerns should be made through a deliberate action and how to guard against profiling and discrimination[29]. GDPR provides more protections and imposes greater accountability compared to DPDP act. Under Cal. Civ. Code §§ 1798.100 and 1798.105, Known as the California consumer Privacy Act[30], consumers have a right to know and delete their personal information. However, the lack of a federal privacy law causes inconsistencies and make consumers unprotected in some cases.

A comparative analysis of these frameworks demonstrates that GDPR has a rights-based approach, ensuring the highest level of privacy, consent and profiling protection. The DPDP act employs many rights-based elements similar to GDPR, yet it fails to offer maximum protection due to a more extensive number of exemptions provided by state legislation in section 17. "The United States follows a sectoral regulatory model, which gives businesses comparatively greater freedom[31].

In general, GDPR is still the most stringent standard worldwide regarding privacy protection. Despite being one of the most important steps in regulating digital privacy, the Indian DPDP Act still requires stronger protection from misuse and governmental overreach. In turn, the framework of the United States is effective but inconsistent. Considering the growing importance of Artificial Intelligence, stricter privacy laws are needed.

X. JUDICIAL PERSPECTIVE

Privacy and data security in the context of artificial intelligence can be well explained by important judicial decisions on the matter. Two Landmark decisions related to privacy and protection of personal data from violations include - K.S. Puttaswamy v. Union of India[32] in India and Google Spain SL v. Agencia Española de Protección de Datos in the European Union. They have been playing a crucial role in the development of modern privacy laws and ensuring the safety of personal data in the digital age. Specifically, in the K.S. Puttaswamy V. Union of India, the Supreme Court of India declared the right to privacy as one of the fundamental rights guaranteed by Article 21 of the Constitution of India. It was recognized that privacy is an integral part of the right to life and personal liberty. Importantly, This decision became a

[29] General Data Protection Regulation, Regulation (EU) 2016/679, arts. 5–7, 15–17, 22, recitals 32 & 71, 2016 O.J. (L 119) 1
[30] California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100, 1798.105 (2018)
[31] Health Insurance Portability and Accountability Act, 45 C.F.R. § 164.502 (2024).
[32] *K.S. Puttaswamy v. Union of India*, (2017) 10 S.C.C. 1 (India)

landmark in Indian constitutional law in which the right to privacy and personal information is considered a key right protected by the government. The court decision is highly pertinent to AI because of the extensive collection of personal information from chatbot users. These principles established by the Puttaswamy case support the collection of personal data in accordance with the proper rules and regulations. These principles further helped to lay the foundation stone for passing the Digital Personal Data Protection Act, 2023 in India.

In the same way, in Google Spain SL v. Agencia Española de Protección de Datos[33], The Court of Justice of the European Union identified the "Right to be Forgotten". In this landmark decision, the court stated that individuals have the right to ask for search engines to erase their personal information in case it has become outdated and unnecessary. This landmark Decision increased the level of privacy rights for individuals and led to the inclusion of Article 17 in GDPR. This acknowledges the right to erasure. This case study is relevant to the topic of AI as AI based system store personal information for prolonged periods and make use of it for profiling purposes.

Both the cases highlight the increasing significance of protecting privacy in the digital age. While the case of Puttaswamy has set a precedent for the establishment of privacy as a basic right under the Indian Constitution, the case of Google Spain provides an edge to individuals in exercising the rights over their own data in the EU region.

XI. REGULATORY CHALLENGES AND RECOMMENDATIONS

The advent of Artificial Intelligence is associated with various regulatory issues in areas like privacy and Data Protection. The absence of an overarching regulatory regime that applies uniformly across different countries poses a critical challenge. For instance, while the European Union has GDPR[34] as its privacy law, other nations such as the United States, have various scattered laws applicable to particular sectors, while India just passed its law on Digital Personal Data Protection[35] in 2023. This presents some problems when transferring data across borders for use by AI applications.

Lack of transparency is another challenge presented by AI applications. Some AI technologies

[33] *Google Spain SL v. Agencia Española de Protección de Datos (AEPD)*, Case C-131/12, ECLI:EU:C:2014:317 (C.J.E.U. May 13, 2014)
[34] General Data Protection Regulation, Regulation (EU) 2016/679, 2016 O.J. (L 119) 1.
[35] Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023)

rely on black box technologies in which there are opaque mechanisms of decision making[36]. This raises concerns about accountability and risk associated with misusing the technology.

One of the challenges of AI and privacy is also consent management. Consent is expected to be informed however people tend to agree to terms of service and lengthy privacy policy without really comprehending what is happening to their personal data, especially regarding its use training AI models. Hidden data training is another source of lack of transparency since users do not know that their data is being used to train AI models. Moreover, cyber security threats and data breaches become critical issues in this aspect as Artificial Intelligence stores huge volumes of personal data and hence is open to cyber threats. Law usually does not provide enough protection against the above dangers.

It is necessary to create more efficient regulations regarding AI use. Governments have to adopt certain standards for regulating Artificial Intelligence with the help of laws on transparency, accountability and proper data handling. Simplification of privacy policies will make it easier for users to understand what is happening to their data. Mechanisms for users' consent need to be developed properly. Finally, auditing of Artificial Intelligence applications has to be carried out regularly in order to detect cases of bias data misuse and violation of privacy.

XII. CONCLUSION

Artificial intelligence is now an essential part of contemporary living and communication, as well as obtaining information. Chatbots and digital platforms that utilize Artificial Intelligence technology offer fast and tailored solutions because of the acquisition and analysis of consumer data. But the expansion of their operations poses significant threats to consumers including privacy issues, monitoring problems, data misuse and abuse, surveillance as well as breaches in security. This study demonstrates the problem of privacy violations, which include, among other things, the lack of informed consent from users, ambiguous terms of privacy policy and even hidden procedure for collecting user data without consent[37].

The Comparative Evaluation of Privacy Regulations Under the DPDP act, GDPR and the US

[36] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* 15–30 (Harvard Univ. Press 2015).
[37] Ministry of Electronics & Information Technology, Government of India, Report of the Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (2018).
(Foundation for India's Data Protection framework)

Privacy Act also proves the importance of adopting Stricter measures and better legal frameworks. In addition, judicial decisions such as K.S. Puttaswamy and Google Spain support the relevance of privacy. Hence it is evident that strict regulation of Data Protection and awareness are crucial.