International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0355
e ISSN: 2584-2854
Volume: 03
Issue:06 June 2025
Page No: 2256-2264

Safeguarding Privacy in the Age of Artificial Intelligence: Legal Implications and Challenges

Pankaj Sandhu[1], Dr. Madhu Bala[2], Kanika Singh[3], Mahima Suryavanshi[4], Nikhil Phour[5]
[1]Research Scholar, Department of Law, Maharishi Markandeshwar (Deemed to be University), Mullana, Haryana, India.
[2]Assistant Professor, Department of Law, Maharishi Markandeshwar (Deemed to be University), Mullana, Haryana, India.
[3]Assistant Professor, Swami Devi Dyal Law College, Golpura, Panchkula, Haryana, India.
[4]Research Scholar, Himachal Pradesh National Law University, Shimla, Himachal Pradesh, India.
[5]UG - Swami Devi Dyal Law College, Golpura, Panchkula, Haryana, India.
Email ID: *pankajsandhu9200@gmail.com[1], madhu.bala@mmumullana.org[2], rajputkanika4449@gmail.com[3], mahimasuryavanshi47@gmail.com[4], nikhilphour123@gmail.com[5]*

Abstract
The "Right to Privacy" is a fundamental right safeguarded by international agreements, the Indian Constitution, various legislations, and also ratified by the Supreme Court of India. The Supreme Court, in the case of K.S. Puttaswamy v. Union of India, adjudicated that the Constitution of India safeguards the "Right to Privacy" as a fundamental right under Part III. As far as, right to privacy and artificial intelligence are concerned both are intersecting. Artificial intelligence is quick in collecting personal information, processing and using the personal data without the owner's consent, and relies on the large database containing the sensitive personal information raises the serious threat to privacy breach. This paper delves into implications of Artificial intelligence and protecting personal data emphasizing at national and global context. The study relies on International Agreement, Reports, Treaties, Indian Legislations, rules, regulations, judicial pronouncements etc. Moreover, for a clearer and more fair presentation of the problem being studied, practical materials related to the topic shall be used. The approach adopted in this study is empirical research, involving the administration of a questionnaire to law students, professors, and advocates. Additionally, a doctrinal study will be employed to provide a theoretical framework for the findings.
Keywords: *Artificial Intelligence; Data protection laws; Fundamental right; Indian Constitution; Supreme Court of India.*

1. Introduction
Internet and computers have become a crucial part of our everyday life. The UNHRC in 2016 declared that internet access is a fundamental human right. However, every right is accompanied by a corresponding duty. In exercising their human rights, individuals must honor the rights of others. No individual has the authority to infringe upon the rights of another person. But some anti-socials use their right to use the internet to exploit others' rights by hacking others' devices, planting viruses in others' systems, cyber-bullying etc. Government has implemented various legislations to protect individuals from such abuses, including law aimed at preventing cyber-crime. However, now the cyber landscape has drastically evolved with the introduction of new technology called Artificial intelligence which, on the one hand, is helpful in various sectors such as education and healthcare, but on the other hand, is dangerous for the privacy of internet users. This paper aims to examine data

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0355
e ISSN: 2584-2854
Volume: 03
Issue:06 June 2025
Page No: 2256-2264

protection laws existing in India highlighting their implications and effectiveness and to explore the ethical concerns surrounding AI and Privacy. The research theoretically formulates and empirically evaluates the trade-offs between AI applications and the potential risks to individual privacy, aiming to identify effective strategies for mitigating privacy concerns. The approach that is adopted in this study is the quantitative approach that involves the questionnaire filled out by the law students, professors, advocates and common people. The objectives of the present study are to understand the impact of AI technology on personal privacy, ensure privacy and transparency in age of artificial intelligence, to discuss legal implications at national and international level, to critically analyses the laws available on data protection and to propose measures to safeguard privacy. The hypotheses of the present study include that online activities are tracked by AI technology, which may lead advertisements for products searched online, existing legislations do not adequately address the privacy concerns associated with AI, formulation of comprehensive national policies on AI ethics and regulations may give effective solutions for AI challenges, the companies may maintain user's reliance by ensuring transparency regarding how AI algorithms use their personal data.

2. Meaning of Artificial Intelligence

Artificial intelligence (AI), signifies the capability of machines, especially computer systems, to replicate human cognitive functions. This includes processes such as problem-solving, reasoning, perception, learning, and understanding language. AI-systems are capable of analyzing data, make decisions, and recognize patterns, which allows them to perform tasks that typically need human intelligence. It consists of a series of technologies that enable computers to carry out various complex functions. These functions include the ability to perceive visual information, interpret and translate both spoken and written languages, analyze data, provide recommendations, and perform additional advanced operations. AI systems function by integrating vast amounts of data with intelligent, incremental algorithms that learn from the characteristics and patterns within the data they process. With every cycle of data analysis, an AI-system evaluates its self-performance and gains further knowledge. Since AI operates continuously without needing breaks, it can quickly execute hundreds, thousands, or even millions of tasks, promptly acquiring extensive knowledge and achieving high level of proficiency in the particular tasks for which it is being trained. However, the key to grasping how AI operates lies in recognizing that it is not merely a single software program or application; rather, it encompasses a broader field or scientific discipline.

3. Right to Privacy

The term privacy is originated from the Latin "privatus," meaning "personal and separate from public ownership," and "privo," which denotes "deprivation." The term privacy means "the condition of being isolated from others or not being observed." The "Right to Privacy" is a basic human right that shields individuals from arbitrary interference into their private concerns. It incorporates various aspects, including the right to maintain confidentiality of their private information, the right to make choices about one's own body and relationships, and the right to communicate without surveillance. This right is essential for maintaining dignity, autonomy, and freedom, allowing individuals to live without undue intrusion from the state, organizations, or other individuals. The "Right to Privacy" is enshrined in both national and international statutes and it often includes protections against unlawful searches and seizures, data breaches, and other forms of invasion into personal life. To protect this right of the world population, "The Universal Declaration of Human Rights 1948" under Article 12 provides that no person shall face any arbitrary interference with their privacy, family, domicile, or correspondence, nor shall they endure attacks on their honor and reputation. Each person is entitled to legal safeguards against such interferences or assaults. Moreover, Article 17 of "The Covenant on Civil and Political rights" also safeguards people

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0355
e ISSN: 2584-2854
Volume: 03
Issue:06 June 2025
Page No: 2256-2264

from unlawful interference with their privacy. The Indian Constitution does not explicitly affirm the "Right to Privacy" as a fundamental right but implies it. As decided in the case of Maneka Gandhi v. Union of India, that the "Right to life enshrined under Article 21 is not merely confined to physical existence but it includes within its ambit the right to live with human dignity." In R. Rajagopalv. State of Tamil Nadu, the Supreme Court has explicitly ruled that the "right to privacy" is safeguarded under Article 21 of the Constitution. A citizen has the right to preserve their own privacy, and also that of their family, marriage, motherhood, procreation, childbearing, and education, among other aspects. Nobody is allowed to publish any information regarding these matters without the individual's consent, regardless of whether the information is true or false, or whether it is positive or negative. If someone does publish such information, they would be infringing upon the rights of the individual involved. Moreover, in the landmark judgement of the case of Justice K.S. Puttaswamy v. Union of India, the Supreme Court determined that Privacy is a right that is constitutionally protected, mainly originating from the "Right to Life and Personal Liberty" outlined in Article 21. Aspects of privacy also emerge in different contexts from other elements of freedom and dignity acknowledged and secured by the fundamental rights under Part III. Justice Dr. D.Y. Chandrachud held "Privacy is concomitant of right of individual to exercise control over his or her personality. It finds an origin in the notion that there are certain rights which are natural to or inherent in human being. Natural rights are inalienable because they are inseparable from human personality. Human element in life is impossible to conceive without existence of natural rights and integrally founded on sanctity of life." The Supreme Court also decided that "Informational privacy is a facet of the Right to Privacy." In today's information-driven world, risk to privacy can arise not just from the state but also from private entities. Moreover, In the case of People's Union for Civil Liberties v. Union of India, the Supreme Court ruled that telephone-tapping is a significant violation of someone's privacy right which is incorporated in the "Right to Life and Personal Liberty" outlined in the Article 21. The State should only engage in such actions when there is a public emergency or a need for public safety.

4. Data Protection and Artificial Intelligence

The Artificial Intelligence is a recent invention, and we can find it everywhere. It has integrated into various aspects of daily life, from personal assistants on our devices to advanced algorithms used in industries like healthcare, finance, and entertainment. Its presence is increasingly felt in technologies like chatbots, recommendation systems, and even self-driving cars, making it a significant part of modern technology. However, it is a universal fact that every innovation comes with its own share of drawbacks, and AI is no exception. AI can now endanger our privacy in ways we never thought possible before. "The IAPP Privacy and Consumer Trust Report 2023" indicates that 68% of global consumers are concerned about their online privacy. Complex privacy notices have made it hard for them to grasp how companies use their personal details. Data protection becomes a more crucial point in the world of Artificial Intelligence. Everything from automated assistants to personalized recommendations on our computers and mobile devices is powered by AI. AI uses our information without us even realizing it. Personalized recommendations on social media or online shopping platforms are generated through AI system. AI uses the data and preferences to suggest those items without explicitly informing the user. Additionally, AI analyzes browsing history to customize the advertisements seen online based on the interests and behavior of the user, all without user being directly aware of the process. The primary privacy concern associated with AI lies in the collection and dissemination of personal data. AI-algorithms necessitate extensive datasets for training and improvement, which may be sourced from diverse platforms, including social media, e-commerce, and personal devices such as smartphones and smart home technology. This process of collection of data for improvement is known as

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0355
e ISSN: 2584-2854
Volume: 03
Issue:06 June 2025
Page No: 2256-2264

Machine learning, which constitutes a subset of artificial intelligence, representing a computer technique that enables systems to autonomously acquire knowledge and improve performance (learn) through experience. AI-systems typically depend on large datasets to optimize their algorithms and improve their performance. This information might consist of personal details like names, addresses, and financial data, and also sensitive data, for instance, medical records and social security numbers. The gathering and handling of this information can lead to concerns pertaining to its usage and who is granted access to it. This data can be utilized to construct comprehensive profiles of individuals, facilitating targeted advertising, predictive analytics regarding future behavior, and even influencing political perspectives. The challenge surrounding data collection and sharing is that individuals frequently remain unaware of what data is being gathered, the identity of the collectors, and the intended uses of such data. For instance, numerous applications and websites collect information regarding users' locations, browsing histories, and search inquiries, which can contribute to a detailed profile encompassing interests, habits, and personality traits. This data may subsequently be shared with third-party entities, who may exploit it for purposes such as targeted marketing or market analysis. This is the key privacy concerns linked to AI include the potential for data violation and the unlawful access of personal information. Due to the vast amount of data being gathered and processed, it could potentially be compromised, either by hacking or other security incidents. Personal data constitute a significant asset and is often kept and used by companies that don't care much about privacy. A lot of the time, this data isn't well protected, which can lead to data leaks and stolen personal information. Even though Facebook is one of the biggest companies in the world, it had its fair share of data leaks and controversies. Facebook faced ongoing issues with security breaches involving user data. One of the largest breaches happened in April 2021, where information like names, contact numbers, Usernames, and passwords of more than 530 million individuals was leaked publicly. Facebook explained that the issue arose from a tool used for syncing contacts, with hackers taking advantage of a vulnerability to gather user profile data. "Cisco's 2021 Consumer Protection Survey" shows many consumers ended relationships with companies over data privacy issues, with 33% quitting social-media and 28% leaving Internet Service Providers. The major issue with data breaches is that when we download new apps, we usually just click "accept" on the terms and conditions without taking the time to read them. These agreements often contain a lot of legal jargon that can be confusing, and many people don't realize what they're agreeing to. Moreover, we often give apps permission to access sensitive features like our camera, microphone, and photos, as well as other personal data stored on our devices. In many cases, the app doesn't actually need this access to function properly, but it collects this information anyway. This can lead to serious privacy concerns. If the app experiences a data breach, all the personal information it has collected can be exposed, putting our privacy and security at risk. Additionally, a large number of users lack knowledge about the ways through which their data is being used or shared with third parties, which can lead to unwanted advertising or even identity theft. Just like this, users often find that to access certain websites, they need to accept some 'Cookies'.

5. Legal Provision Related to Privacy Breach by Artificial Intelligence

5.1. Information Technology Act, 2000

The provisions of this act that deals with AI are:
Section 43 provides that, unauthorized accesses to a computer, or network can result in serious consequences. This includes actions like downloading or copying data, damaging systems, disrupting services, or denying access to authorized users. Additionally, assisting someone in accessing a system illegally, altering or destroying information, or tampering with computer source code can also lead to liability. If any of these actions cause harm, the person responsible may have to compensate the

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0355
e ISSN: 2584-2854
Volume: 03
Issue:06 June 2025
Page No: 2256-2264

impacted individual. Section 43A provides that if a corporation that owns or operates sensitive personal data is careless in adhering to adequate security measures, and this negligence leads to wrongful loss or gain for someone, the corporation can be held liable and they may have to pay compensation to the affected person for the harm caused. Although this section has been omitted by "The Digital Personal Data Protection Act,2023." According to Section 72, if someone accesses electronic records or documents without the owner's consent and shares that information with others, the concerned person is subjected to imprisonment for maximum of 2 years, a fine of a maximum of 1 lakh rupees, or both. Section 72A of this act states that if a person, including an intermediary, discloses personal information accessed while offering services based on legal contract—without the approval of the concerned individual and with the aim of causing wrongful loss or gain—they can face severe penalties. The punishment can be imprisonment for maximum of three years, a fine of a maximum five lakh rupees, or both.

5.2. The Digital Personal Data Protection Act, 2023

In the case of Justice K.S. Puttaswamy v. Union of India, the Supreme Court while discussing the danger to privacy in the age of information technology suggested to the Union Government that they should review and establish a strong framework for data protection. Following this, the B.N. Shrikrishna committee was established to address concerns about the digitalization of personal data and suggest solutions. The committee prepared the draft "Personal Data Protection Bill, 2018," which was presented to the Lok Sabha. Later in 2019, this draft bill was submitted to a joint parliamentary committee for review and opened for public comments. Now, after five years of extensive submissions, discussions, recommendations, consultations, adjustments, and deliberations, a final draft of "The Digital Personal Data Protection Bill, 2023," was completed. After receiving approval from the cabinet, approved by both houses of Parliament and get President's assent on 11th August 2023. The principles of this Act are: This act states that the consent provided by the User must be voluntary, unambiguous, well-informed, specific, and explicit, indicating approval to the personal data processing for a specified objective. This consent should be limited to the personal data necessary for that purpose. If any part of the consent violates the law or regulations, it will be considered invalid. Consent requests must be communicated in simple language, allowing the user to obtain it in English or any language listed in the Constitution's 8th Schedule. Additionally, contact details for authorized person must be provided for any inquiries regarding the user's rights. If the user's consent is the foundation for operating personal data, she is entitled to revoke that consent at any time, and the process for doing so should be as easy as the initial consent process. If the user withdraw consent, it doesn't affect the legality of any personal data processing that took place while consent was still in place. For instance, if X uses an online shopping app administered by Y and gives consent for Y to process her personal data to fulfill her order, she can later withdraw that consent. However, if she withdraws her consent, Y can stop her from using the app for future orders, but they must still process the order that X has already placed and paid for. Any request for consent made to a user must be accompanied by a notice informing the user about the personal data that will be processed and the purpose for which it is intended. In the case of minor and disabled person, the Data Fiduciary must get clear permission from the minor's parents or the legal guardian of a person with a disability before processing their personal data. This should be done in a way that follows the rules set out. After consent is given and personal data is collected, its use must be limited to the specific purpose for which it was collected and for which consent was obtained from the individual. Any deviation from this agreed-upon purpose is not allowed under the proposed legislation. When seeking consent, the data fiduciary must ensure that the individual is fully aware of the purpose of acquiring their personal data. The users are entitled to request information from the Data-Fiduciary they

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0355
e ISSN: 2584-2854
Volume: 03
Issue:06 June 2025
Page No: 2256-2264

have consented to for processing personal data. This includes an overview of the personal data being operated and the related activities, the identities of other Data-Fiduciaries and Data-Processors that have received the personal data along with descriptions of the shared data, and any additional information concerning the personal data and its processing. Additionally, the Data Principal is entitled to modify, enhance, update, and delete their personal data they consented to. If a significant breach of the provisions of this Act is found during an inquiry, the person involved may be subjected to a monetary penalty after being given the opportunity of being heard.

5.3. Drawbacks of the Act

Section 3(c)(ii) of this act specifies that it doesn't pertain to personal data that users have shared publicly. This exemption includes data that is provided directly by data principals or data that is shared by individuals who are legally required to make it public. However, the law does not specify what constitutes "publicly available" data. For instance, the act explains that if someone shares her personal information on social media while expressing her opinions in a blog, the processing of that information will not fall under this act. This provision enables companies to handle personal data available publicly without requiring consent or complying with other regulations in the Act. Furthermore, this emphasizes the potential for facial-recognition technologies to utilize publicly accessible profile images for its training purposes. Despite the lack of clarity, this exemption encourages extensive data scraping while failing to impose necessary obligations on businesses to protect scraped personal data, report breaches, or ensure accountability. Guidance from the government on the definition of publicly available data would be beneficial. The DPDP Act mandates that companies implement "reasonable security safeguards" to avoid personal data breaches, with non-compliance potentially leading to penalties amounting to Rs.250 crores. However, there is a lack of certainty regarding the specific provisions that need to be taken and what qualifies as "reasonable" safeguards. Even though the Data Protection Board can levy fines for violating personal data, none of the penalties benefit the victims, who are the users affected by the breach. Moreover, the act eliminates "section 43A of the IT Act, 2000," which used to offer reimbursement to these individuals. The DPDP Act gives the Data Protection Board the power to levy a fine extendable to ₹10,000 if any user doesn't meet the obligations as specified in the Act. For instance, one of these obligations is that users should avoid submitting false or trivial complaints to the Board. This rule could discourage individuals from submitting complaints initially due to the concern of incurring the fine. An act focused on protecting users' privacy rights should not penalize them in this way. The act puts forth provisions for protecting children's data, such as requiring parental consent. However, there are still hurdles to overcome, particularly in terms of verifying age and determining what exactly qualifies as harmful to children. Additionally, establishing a reliable connection between a child and their parents presents its own set of challenges. When seeking consent, a company is not obligated to reveal the identities of all parties with whom the data will be shared or the specific purposes for sharing it. The notice provided to users during the consent process only needs to indicate what personal data will be obtained and the purpose for which it will be used. This is a change from the previous bill, which mandated that companies disclose how long they would retain the data, whether it would be shared with third parties, the source of the data, and details regarding any cross-border data transfers. Furthermore, companies are no longer obligated to provide privacy policies on their websites as was stipulated in the earlier bill.

6. Result of Hypotheses

Researchers have conducted a survey through Google Forms responded by 45 respondents involving advocates, law professors, and law students to gather insights on the topic "Safeguarding Privacy in the Age of Artificial Intelligence: Legal Implications and Challenges." The survey revealed that a significant percentage of participants expressed concerns about

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0355
e ISSN: 2584-2854
Volume: 03
Issue:06 June 2025
Page No: 2256-2264

AI-technology's impact on their privacy. The responses from the survey support the given hypotheses and the results of the hypotheses are drawn based on the questions asked of the respondents. The following figure is based on the collected data, with the Y-axis showing values from 0 to 45, representing the number of respondents, and the X-axis showing the hypotheses. (Figure 1)

H1: The online activities are tracked by AI technology, which leads to advertisements for products that individuals have discussed or searched for online. Out of 45 respondents 77.8% of respondents feel that their online activities are being watched or tracked by AI technology and they favored first option 'Yes,' while 22.2% negatively responded and do not share this concern. 82.2% of respondents believe their conversations are monitored for targeted advertising, while 17.8% did not experience such advertisements. 88.9% of respondents notice advertisements on social media related to products they searched for on shopping apps, while 11.1% do not notice any such advertisements. This statistic reveals a significant level of concern among participants regarding their privacy in the digital landscape. The high percentage of affirmative responses suggests that many individuals are increasingly aware of the implications of AI technology on their personal data. Moreover, this phenomenon highlights the growing concern over how companies utilize data and the extent to which AI and algorithms track user behavior to deliver personalized content. Companies are successfully utilizing algorithms to track user behavior across different platforms, creating a seamless experience where online searches and social media interactions are interconnected.

H2: The existing legislations do not adequately address the privacy concerns associated with AI.

The responses regarding the Indian Constitution's safeguards for the right to privacy in the digital era are mixed. Approximately 41.2% of respondents believe it provides adequate protection and affirmatively selected option 'Yes,' while 20.6% believe it does not address the privacy issue and negatively selected option 'No.' Meanwhile, 38.2% of respondents are unsure about its effectiveness. The responses regarding "The Information Technology Act, 2000" and its address of the ethical use of AI in handling personal data show varied opinions. Approximately 31.1% believe it offers sufficient guidance and favors option 'Yes,' while 28.9% think it lacks coverage of moral implications related to privacy and security and favors option 'No.' Additionally, 40% are uncertain about the Act's effectiveness. The respondents ranked "The Digital Personal Data Protection Act, 2023" regarding its efficiency in dealing with data protection from AI. The results showed that the lowest ranking grade, option 1, received 22.2%, followed by option 2 at 24.4%. Option 3, which is considered fairly effective, received 33.3%, while option 4 had 15.6%. Lastly, option 5, viewed as the highest grade of efficiency, received only 4.4% responses.

H3: The formulation of comprehensive national policies on AI ethics and regulations may give effective solutions for AI Challenges. The result of third hypothesis shows a strong need for more national AI policy in India. Out of total 45 respondents, 70.6% positively believe that enhanced policies are essential for ethical use and data protection. 5.9% respondents are in favour of option second 'No.' A few thinks current regulations are enough or that rapid AI growth complicates policy-making. 23.5% respondents are in favour of third option (may be). Some are uncertain, seeing value but concerned about implementation.

H4: The companies may maintain user's reliance by ensuring transparency regarding how AI algorithms use their personal data. The result of third hypothesis is that as out of 45 respondents, total of 84.4% of respondent's express concern about the security of their personal information when using AI-powered services and responded affirmatively to option one Yes,' while 15.6% respondents negatively answered. This thumbing majority indicates a clear desire among individuals for greater transparency regarding how their personal data is being utilized by companies. Many individuals feel that they are not

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0355
e ISSN: 2584-2854
Volume: 03
Issue:06 June 2025
Page No: 2256-2264

adequately informed about how their information is collected, stored, and used, especially concerning AI-algorithms that drive targeted advertising and other personalized services. The demand for transparency suggests that consumers are increasingly seeking accountability from companies regarding their data practices.

Suggestions

- The Companies that collect user data need to be transparent about what data is being gathered, how long it's being kept, and which third parties will have access to that data.
- The mechanism for filing complaints in data breach cases should be easily accessible and ensure faster disposal of cases.
- The users whose data has been violated shall be provided with the compensation.
- The legislature needs to establish rules for DPDPA, 2023 for greater clarity with specific subjects.
- There should be more AI-oriented laws and legal provisions, along with an increase in experts to address the situation.
- Only the data that users have consented to should be collected, and the consent should be obtained in simple terms.

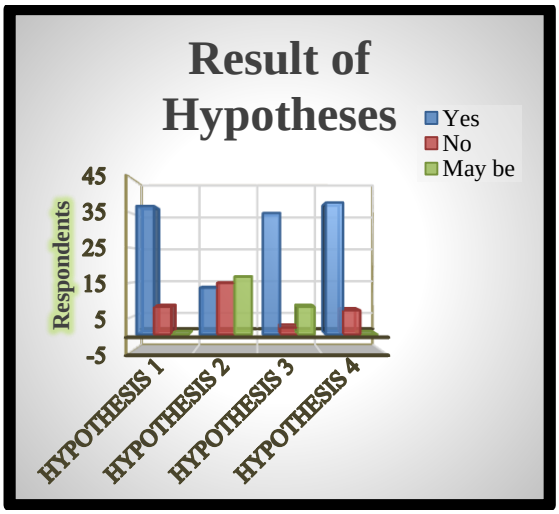

Figure 1 Graph

Conclusion

Artificial Intelligence has become an incredible tool in the cyber-world, but it comes with its own set of drawbacks, primarily concerning privacy. The privacy of internet users is at significant risk due to AI-algorithms, which collect user data for improvement. According to the empirical data gathered for this article, users are also worried about receiving ads on social media platforms for products they have discussed or searched for on shopping sites. Implementing stricter laws could help address this issue. Although the new "Digital Personal Data Protection Act, 2023" seeks to secure user data from misuse, it still has several shortcomings. Enhancing legal frameworks to tackle the unique privacy concerns posed by AI is essential for protecting individual rights in our increasingly digital world. By establishing regulations that emphasize transparency, accountability, and user control over personal data, we can create a safer environment for AI-technologies. Ultimately, a collaborative approach that involves stakeholders from various sectors will be essential in creating effective legal frameworks that can adapt to the fast-paced advancements in AI-technology while prioritizing the privacy and rights of individuals.

Endnote

[1]. Utkarshshara. (n.d.) Right to Internet and Fundamental Rights. LegalserviceIndia. Retrieved fromhttps:// www.legalserviceindia. com/legal/article-2967-right-to- internet-and-fundamental-rights.html#:~:text=Right%20To%20Internet%20A%20Basic,to%20live%20life%20with%20ease. Craig, L., Laskowski N., & Tucci L. (2024, october 1).

[2]. What is AI? Artificial Intelligence explained. TechTarget. Retrieved from https://www.techtarget.com/searchenterpriseai/definition/AI-Artificial-Intelligence. Google cloud. Retrieved from https://cloud.google.com/learn/what-is-artificial-intelligence.

[3]. CSU Global. (2024, October 23). Colorado

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0355
e ISSN: 2584-2854
Volume: 03
Issue:06 June 2025
Page No: 2256-2264

State University Global. https://csuglobal.edu/blog/how-does-ai-actually.

[4]. Gautam, V. (n.d.) Right to Privacy in Cyber World. legalserviceindia. Retrieved from https://www.legalserviceindia.com/legal/article-11477-right-to-privacy-in-cyber-world.html.

[5]. UDHR. (1948). Article 12 Universal Declaration of Human Rights. ICCPR. (1966). Article 17 The International Covenant on Civil and Political Rights. Maneka Gandhi v. Union of India, AIR 1978 SC 597.

[6]. Pandey, J.N. (2019). Constitutional Law of India. (56th ed.). Allahabad: Central Law Agency. R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.

[7]. Justice K.S. Puttaswamy v. Union of India, AIR 2017 SC 4161. People's Union for Civil Liberties v. Union of India, AIR 1997 SC 568. IAPP-Survey. (2023). Privacy and Consumer Trust. Retrieved from IAPP.https:// iapp.org/resources/article/privacy-and-consumer-trust-summary/.

[8]. Tyagi, N. (2023, March 16). Protecting privacy in an AI driven World. ipleader. Retrieved from https:// blog. ipleaders.in /protecting-privacy-in-an-ai-driven-world/ Data_collection_and_sharing.

[9]. OVIC- Office of the Victorial information Commissioner. (n.d.). Artificial Intelligence and Privacy – Issues and Challenges. Retrieved from https:// ovic.vic .gov.au/ privacy/resources-for organisations/artificial-intelligence-and-privacy-issues-and-challenges/.

[10]. EconomicTimes. (2023, April 25). AI and Privacy:. AI and Privacy: The privacy concerns surrounding AI, its potential impact on personal data. Retrieved from https://economictimes.indiatimes.com/news/ how-to/ai-and-privacy-the-privacy-concerns-surrounding-ai-its-potential-impact-on-personaldata/articleshow/99738234.cms?fro

[11]. CHin, K. (2024, September 16). Biggest Data Breaches in US History (Updated 2024). Upguard. Retrieved from https://www.upguard.com/blog/biggest-data-breaches-us.

[12]. Cisco-Survey. (2021). Building Consumer Confidence Through Transparency and Control. Cisco. Retrieved from chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-cybersecurity-series-2021-cps.pdf.

[13]. Priyanka. (2024, May 21). Digital Personal Data Protection Act, (DPDPA), 2023. ipleader. Retrieved from https://blog.ipleaders.in/digital-personal-data-protection-act-dpdpa-2023/#:~:text=The%20DPDP%20Act%2C%202023%20establishes,measures%20provided%20in%20the%20Act.

[14]. Chacko, M., Misra, M., & Shaharbanu, A. (2023, November 13). Beyond the hype: Shortcomings of new data law. Indian Business Law Journal. Retrieved from https://law.asia/new-data-law-shortcomings/.

[15]. Mathi, S. (2023, August 4). Fifteen major concerns with India's Digital Personal Data Protection Bill, 2023. Medianama. Retrieved fromhttps://www.medianama.com/2023/08/223-major-concerns-india-data-protection-bill-2023-2/.Ibid.

[16]. DrishtiIAS. (2024, July 19). DPSP Act 2023 and the issues of Parental Control. Retrieved from https://www.drishtiias.com/daily-updates/daily-news-analysis/dpdp-act-2023-and-the-isssue-of-parental-consent.