Page 407 - 424 **DOI:** *https://doij.org/10.10000/IJLSI.111916*

INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 6 | Issue 3

2024

Generative AI and Data Protection: The Regulatory Tapestry in India and EU

SHIVANGI GAUR[1] AND TANIMA BHATIA[2]

ABSTRACT

This research paper provides a comprehensive overview of the evolving landscape of Generative AI, examining its rising utilization, associated privacy concerns, and regulatory frameworks. It begins by delineating the tiers of AI systems, from Narrow AI to the theoretical realms of General AI and Super AI, focusing on the practical applications of Generative AI in content creation across various sectors. Amidst this surge in AI adoption, the abstract highlights the escalating privacy and security concerns, particularly regarding the potential misuse of personal data and the proliferation of deepfake content, which pose significant risks to individuals and societal stability. It discusses notable instances of privacy violations and deepfake-related scams, emphasizing the urgent need for robust governance structures and security protocols. In this context, the abstract explores the regulatory frameworks governing Generative AI, including the GDPR in the European Union and the Digital Personal Data Protection Act in India, outlining their provisions aimed at safeguarding personal data and ensuring compliance. It underscores the importance of transparency, data minimization, and rigorous security assessments in mitigating privacy risks and fostering ethical development and deployment of Generative AI technologies. Overall, the abstract calls for collaborative efforts among stakeholders to address privacy challenges effectively and establish ethical standards for the responsible use of Generative AI in the digital age.

Keywords*: generative AI, Data protection, GDPR, DPDP Act.*

I. INTRODUCTION

In recent years, there has been a notable surge in the advancement of Artificial Intelligence (AI), denoting machines, or robots capable of emulating various facets of human intelligence and cognitive processes like reasoning, comprehension, and problem-solving. The realization of AI hinges upon the refinement of algorithms facilitating tasks traditionally within the purview of human intellect. This technology is categorized into three distinct tires based on its operational scope: Narrow AI, also known as Artificial Narrow Intelligence (ANI), General

[1] Author is a LL.M. student at SRM University, India.
[2] Author is a LL.M. student at SRM University, India.

 [ISSN 2581-9453]

AI, or Artificial General Intelligence (AGI), and Super AI, also known as Artificial Super Intelligence (ASI).[3]

Narrow AI or Weak AI, also referred to as *Artificial Narrow Intelligence (ANI)*[4], pertains to systems capable of performing specific task as programmed. Examples include digital assistants and autonomous vehicles. *General Artificial Intelligence (AGI)*[5] or Strong AI, represent a category of intelligent computational systems capable of performing tasks at par with human abilities, exhibiting a cognitive capacity, similar to humans. Super AI, or *Artificial Super Intelligence (ASI)*[6], represents an advanced form of AI conceptualized to surpass human cognitive capabilities. Both AGI and ASI are a theoretical construct lacking real-world instance

Generative AI encompasses machines, capable of autonomously producing content across various mediums, such as text, images, audio, and videos. While the content generated appears novel and original, it relies on extensive data training. Generative AI systems have permeated various aspects of daily life, offering convenience in tasks ranging from content creation to professional applications. Widely utilized systems like ChatGPT[7], DALL-E[8], Google GEMINI[9], HeyGen[10], and XGROK[11] seamlessly respond to user prompts, providing diverse data output with minimal user intervention.

The potential for privacy and security concerns arises from the advanced capabilities of gene AI machines, to assimilate extensive data sets and produce novel content. Users must exercise caution when engaging with such platforms, particularly in supplying prompts, to mitigate the risk of inadvertent disclosure or retention of sensitive personal information.

Privacy violations perpetrated by Generative AI denotes an instance where the technology acquires or reviews confidential personal data, devoid of express authorization of Individuals. Generative AI, functioning as a subtype of Artificial Intelligence (AI), generates novel content by extrapolating from pre-existing data. Should this data encompass personal details, such as financial or medical records, the utilization of AI sans requisite permissions or robust security

[3] IBM, Artificial Intelligence, available at: https://www.ibm.com/topics/artificial-intelligence (last visited on Apr 12, 2024)
[4] DeepAI, Narrow AI Definition, available at: https://deepai.org/machine-learning-glossary-and-terms/narrow-ai (last visited on May 11, 2024)
[5] Tech Target, Artificial General Intelligence, available at: https://www.techtarget.com/searchenterpriseai/definition/artificial-general-intelligence-AGI (last visited on: May 11, 2024)
[6] IBM, what is Artificial Super Intelligence, available at: https://www.ibm.com/topics/artificial-superintelligence (last visited on: May 11, 2024)
[7] OpenAI, ChatGPT, available at: https://chat.OpenAI.com/
[8] OpenAI, DALL-E, available at: https://OpenAI.com/research/dall-e
[9] Google, GEMINI, available at: https://aistudio.google.com/app/prompts/new_chat
[10] HeyGen, available at: https://www.heygen.com/
[11] X, X Grok, available at: https://xgrok.icu/

 [ISSN 2581-9453]

protocols could result in breach of privacy. It encourages companies and individuals leveraging Generative AI Systems to comprehend the latent hazards to privacy, and Institute commensurate measures to alleviate them[12]. The study dives into the Privacy and Security risk posed by the generative AI.

II. RISING UTILIZATION OF GENERATIVE AI TOOLS

The field of Artificial Intelligence has risen exponentially over the past few years. From Narrow to General to thinking of Super AI, this world has witnessed everything.

Narrow Artificial Intelligence, also known as Weak AI, is a specialized form of AI designed for tasks, lacking the capacity to emulate Human-like intelligence. Currently prevalent, Narrow AI, leverages, Machine Learning and Deep Learning techniques, surpassing human accuracy in designated domains. However, its capabilities are confined to predefined functions, devoid of abstract thinking or emotional Intelligence. Notable instances include voice assistance such as Amazon Alexa, Google Assistant, and Apple Siri, adept at tasks like weather updates, location interpretation, reminders, and music. Autonomous self-driving cars, streaming platforms like Netflix employing Narrow AI for user preference predictions, and conversational agents like ChatGPT exemplify its practical applications.

General Artificial Intelligence, also known as strong AI, emulates human intelligence and exhibits responses beyond predefined instructions. Machines powered by strong AI are virtually indistinguishable from humans, capable of nuance responses based on input data. Generative AI, a subset of General AI, focuses on generating novel data. Prominent examples include tools like DALL-E 3 and Google Gemini, which demonstrate human-like functions such as reasoning, learning, problem-solving, and creativity. These advancements represent a significant stride towards achieving a comprehensive understanding of and replication of human intelligence in artificial systems.

The theoretical concept of ***Super Artificial Intelligence*** envisions an advanced form of AI capable of executing not only all tasks performed by humans but also those beyond human capabilities. This level of intelligence is anticipated to transcend human actions and encompasses diverse functions such as scientific discovery, social skills, and wisdom. While examples of Super AI remain speculative, ongoing research by futurists and scholars explores potential implications in various domains.

In the realm of Artificial Intelligence, prominent technology entities, such as OpenAI, Google,

[12] ET Online, "AI and Privacy: The privacy concerns surrounding AI, its potential impact on personal data", Economic Times, (Apr 25, 2023)

and Microsoft have spearheaded the development of diverse Generative AI tools. Among OpenAI's, innovative contributions is ChatGPT, a text-based tool, proficient in generating original content spanning narratives, essays, lyrics, and code, which seamlessly integrates with DALL-E 3 – an image creation software capable of producing high-quality images. Additionally, OpenAI has introduced tools like Codex and Stable Diffusion to further augment its AI portfolio. Google, on the other hand, has introduced transformative tools, such as Gemini, Vertex AI, and the Generative AI App Builder, exemplifying their commitment to advancing the capabilities of Generative Artificial Intelligence.

(A) Trends

In a survey by McKinsey Co.[13], the report states that at least 1/3rd of their respondents used Generative AI tool for business. Generative AI possesses the potential to fuel a 7% increase in global GDP, or almost $7 trillion, over the next decade, according to Goldman Sachs research. The McKinsey Technology Trends Outlook report for 2023[14] highlights a remarkable surge of 425% in venture capital investments in Generative AI since 2020. Noteworthy advancements in use cases for Generative AI have been observed across diverse industries, including financial and life sciences. The recent incorporation of a Search Generative and a new Large Language Model (LLM) named PaLM 2, Empowering tools such as BARD, underscores the industry's commitment to innovation. Similarly, Salesforce has made substantial investments in integrating Generative AI models into its existing products. The global market size of Generative AI reached $ 13.0 billion in 2023, with an anticipated Compound Annual Growth Rate (CAGR) of 36.5% from 2024 to 2030. This growth is attributed to factors like text-to-image and text-to-video conversion, as well as workflow modernization, as indicated by a Grand View Research Report. Goldman Sachs predicts that global investments in Generative AI could reach an evaluation of $200 billion by 2025. This surge in investment and diverse applications underscores the profound impact and potential of Generative AI and shaping the future landscape of technology.

The research conducted by Infosys foresees a substantial surge in investments within the Generative AI sector, particularly in the North American region, where a remarkable 67% increase is anticipated, amounting to $5.6 billion by the year 2024. In the European continent, encompassing 11 survey countries, the report projects a collective expenditure of $2.8 billion

[13] McKinsey and Co, The State of AI in 2023, available at: https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2023-generative-ais-breakout-year (las visited on Apr 12, 2024)
[14] McKinsey & Co., Technology Trends Outlooks Report 2023, available at: https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/mckinsey%20technology%20trends%20outlook%202023/mckinsey-technology-trends-outlook-2023-v5.pdf (last visited on Apr 12, 2024)

on Generative AI initiatives by 2024. Conversely, the Asia Pacific region has demonstrated comparatively lower spending and investment levels than Europe and North America with China leading with an investment of $800 million. Nonetheless, the report suggests a prospective upswing in investments, with companies in the APAC[15] region Planning to collectively invest $3.1 billion in 2024. This underscores the evolving landscape of Generative AI and the dynamic investment patterns across different global regions.

In various sectors, including business, legal, professional services, consumer goods/retail, healthcare, pharma, financial services, and technology, Generative AI tools have found widespread application. A survey conducted by McKenzie and Company across APAC, Europe, and North America revealed that the technology industry exhibits the highest adoption of these tools, with 16% of legal professionals and other professional service personnel, incorporating them into their routine of work and personal activities. Notably, the greater China region leads in extensive utilization of these tools, with an impressive 83% engagement rate according to the report. This is the pervasive influence and strategy, implementation of generated tools across diverse global industries.

(B) ChatGPT and DALL-E 3

The exponential growth in user adoption of open AI's cutting-edge AI platforms has been prominently featured in recent publications. According to reports from Reuters, ChatGPT, an advanced AI platform, achieved a significant milestone in January 2023, surpassing a user base of hundred million and setting a record for unprecedented growth. Forbes, further underscores the widespread acclaim of ChatGPT, noting that platform Garnered over 1 million users within just five days of its launch in November 2022. In a survey discussed by Insider Intelligence, 83% of global executives identified chatbots, such as ChatGPT, as the most relevant application of generating AI for their businesses. Additionally, 75% express optimism about generative AI rule in data, while 71% showed interest in its text capabilities. The adoption rate of Generative AI in business reached 54% by November 2023, merely one year after the release of ChatGPT.[16]

Geographically, the majority of ChatGPT users are situated in the United States, constituting 15.22% of the user base, with India closely following at 6.32%, and Japan at 4.01%. This surge in global adoption underscores the pervasive impact and widespread appeal of ChatGPT in the field of artificial intelligence. Open AI's image generating platform, DALL-E, boasts an active

[15] Infosys, "Generative AI Radar 2023: APAC", 2023

[16] PWC, "AI and generative AI in 2023: Four top questions answered", available at: https://www.pwc.com/us/en/tech-effect/ai-analytics/artificial-intelligence.html (last visited on Apr 12 2024)

user base of 1.5 million, generating over 2 million images daily, as reported by OpenAI. This data driven approach reflects the platform's integral role in various industries, demonstrating its impact in significance in the landscape.[17]

III. ISSUE OF PRIVACY WITH GENERATIVE AI SYSTEMS

The landmark decision by the Supreme Court in the case of Justice *KS Puttaswamy Swamy v. Union of India*[18] has unequivocally affirmed the status of the right to privacy as a fundamental right safeguarded under articles, 14, 19, and 21 of the Indian constitution.

Instances of privacy violations by Generative AI occur when the technology accesses or examines confidential personal information without explicit authorization from individuals. Generative AI, as a subset of Artificial Intelligence (AI), produces new content by extrapolating from existing data. If this data includes personal details like financial or medical records, the use of AI without necessary permissions or strong security measures could lead to privacy breaches. This is important for companies and individuals utilizing Generative AI systems to understand the potential risks to privacy and implement appropriate measures to mitigate them.[19] In recent years, there has been a significant Sergen exploration, limitations, and ubiquity of Generative AI models, including Large Language Models (LLMs) and image generation systems. While these technologies offer numerous benefits, they also pose significant challenges in terms of privacy and security. As a result, there is a pressing need for thorough examination and careful consideration of these issues.

The advent of Generative AI technology poses a notable privacy threat, given its ability to produce remarkable authentic synthetic content across diverse mediums, including text, images, audio, and video, commonly referred to as " Deepfake" technology. This capability introduces substantial risk, including dissemination of false information, impersonation of individuals, and the creation of inappropriate or harmful content. These concerns, transcend individual privacy, impacting the integrity of online information and discourse. A survey conducted by cyber security firm. McAfee found that over 75% of survey internet users in India encountered some form of Deepfake content and approximately 38% of respondents reported encountering Deepfake-related scams between 2023 and 2024.[20]

[17] NikolaRoza, DALL-E Statistics Facts and Trends for 2024- All the Crucial Stats You Must Know!, available at: https://nikolaroza.com/dall-e-statistics-facts-trends/ (last visited on Apr 12 2024)
[18] (2017) 10 SSC 1
[19] ET Online, "AI and Privacy: The privacy concerns surrounding AI, its potential impact on personal data", Economic Times, (Apr 25, 2023)
[20] ET, "75% Indians have viewed some deepfake content in last 12 months, says McAfee survey", Economic Times, (Apr 25, 2024)

In the development of Generative AI systems, the compilation of training datasets typically encompasses vast repositories containing personal data, User-Generated Content (UGC), and copyrighted material. Notwithstanding efforts towards anonymization, the employment of such data engenders substantial concerns pertaining to data privacy and the conceivable risks of exposure or improper use of sensitive information.

In a recent report conducted by Menlo Security[21], an examination of the impact of Generative AI on organizational security postures was undertaken. This investigation focused on analyzing employee utilization patterns and associated risks. Notably, within a 30-day observation period, findings revealed that 55% of incidents related to data loss protection were attributed to employees attempting to input personally identified information into Generative AI platforms. This trend raise concerns regarding the inadvertent exposure of confidential documentation, with personally identified data accounting for 40% of such incidents. Subsequently, NOYB, a european privacy rights organisation, filed a complaint with the Australian data protection authority against AI, alleging violations of the European Union's general data protection regulation.[22] Furthermore, in response to growing apprehension surrounding data security, the White House in the United States implemented a ban on the usage of Generative AI systems, including chat, GPT, and Microsoft copilot, by staff members for official work purposes. This decision reflects the administration's efforts to mitigate potential risks associated with the utilization of such a technology in sensitive context.[23]

In a recent study conducted by cyber security defenders, a notable 400 million instances of malware were detected across a network, encompassing 8.5 million endpoints. This highlights the considerable challenge posed by cyber threats and the contemporary digital environment. The prevalence of Malware discoveries remains strikingly elevated, with more than 5,00,000 new occurrences identified daily, thereby augmenting an already extensive reservoir of 1 million circulated Malware programs, as reported by the Data Security Council of India (DSCI), a leading authority in the data protection industry.[24]

In response to potential threats posed by privacy and security concerns, researchers, policymakers, and industry participants must collaborate in formulating, comprehensive

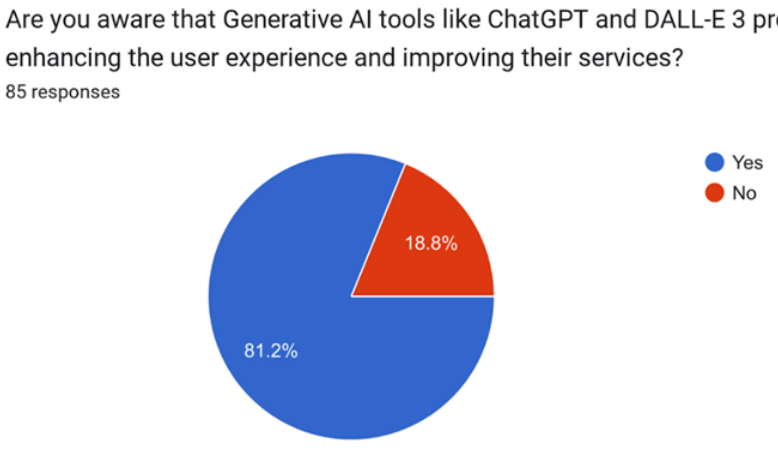
[21] Security magazine, "55% of generative AI inputs comprised personally identifiable data", available at: https://www.securitymagazine.com/articles/100400-55-of-generative-ai-inputs-comprised-personally-identifiable-data (last visited on: May 8, 2024)
[22] CIO, "data protection activists accuse ChatGPT of GDPR Breach" available at: https://www.cio.com/article/2096414/data-protection-activists-accuse-chatgpt-of-gdpr-breach.html
[23] TOI, After ChatGPT, US Congress bans Microsoft's Copilot AI chatbots on official devices; here's why, Times of India, (Mar 30, 2024)
[24] K V KURMANATH, "2024: Generative AI — the new battlefield for cyberspace", The Hindu Businessline, (December 29, 2023)

governance structures, security protocols, and ethical standards for the advancement and implementation of Generative AI technologies. This endeavor encompasses the establishment of a regulatory framework Concerning data privacy, formulation of policies for content, moderation, and imposition of transparency standards for both training and utilization of AI models. By proactively tackling these obstacles, we can capitalize on the advantages of Generative AI while concurrently minimizing the prospective has to personal privacy and societal stability.

(A) Empirical study

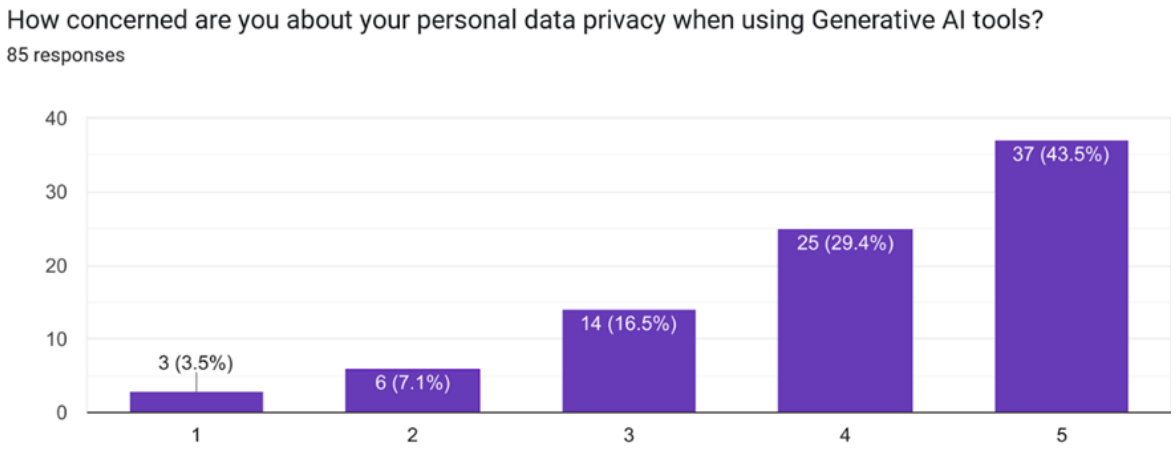
The empirical investigation undertaken by the study involved a sample size of 85 participants represent representing diverse occupational backgrounds. The cohort and compass individuals from various demographics, including students, professionals, legal practitioners, and homemakers. The survey instruments comprised a comprehensive questionnaire addressing multiple facets of participants' encounters and attitudes toward Generative AI systems. Initially, demographic data such as age groups were collected, followed by inquiries into participants, and utilization of Generative AI platforms like ChatGPT and DALL-E. Privacy apprehensions and awareness regarding data sharing and storage practices were also probed. The study will discuss the privacy-related issues faced by the respondents related to Generative AI systems, such as ChatGPT and DALL-E.

The study conducted by the author proves the concerns and level of awareness amongst the respondents, findings below:

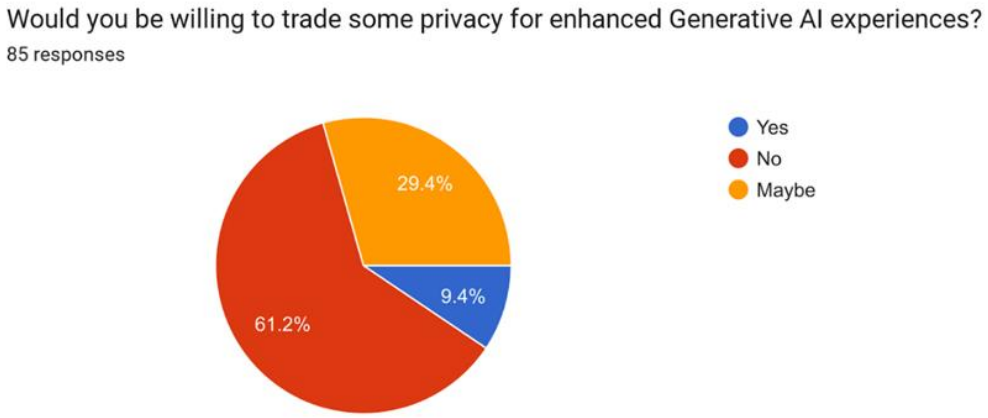


The study examines respondents' awareness and apprehensions regarding privacy ramifications linked with the utilization of Generative AI systems such as ChatGBT and DALL-E. Concerning their awareness regarding the processing of personal data by these

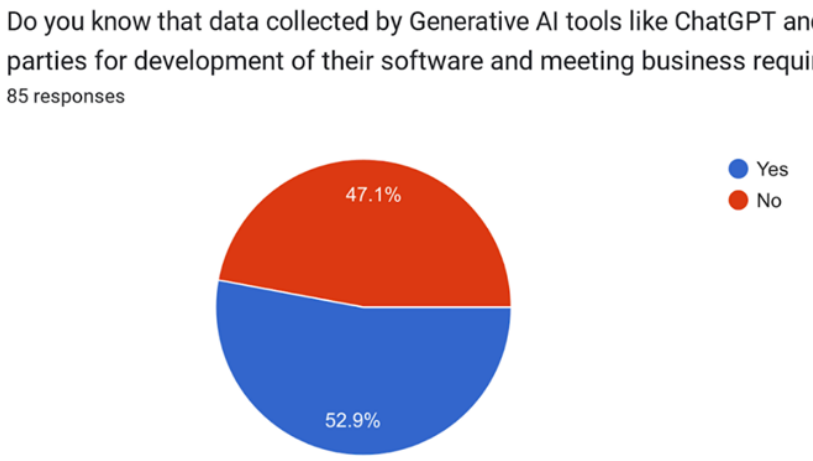
systems, a significant majority of participants at 81.2%, affirm their cognizance of such practices. Conversely, a minority subset of respondents at 18.8% indicated a lack of awareness regarding this facet.



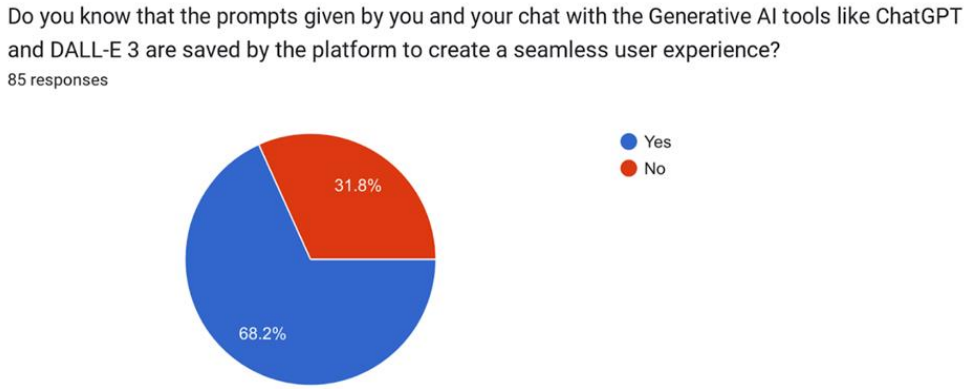
Respondents were requested to assess their degree of apprehension regarding the privacy of personal data while utilizing Generative AI systems. The findings revealed a diverse range of responses, with 27.1% reporting minimal concern and 72.9%, indicating heightened levels of apprehension.



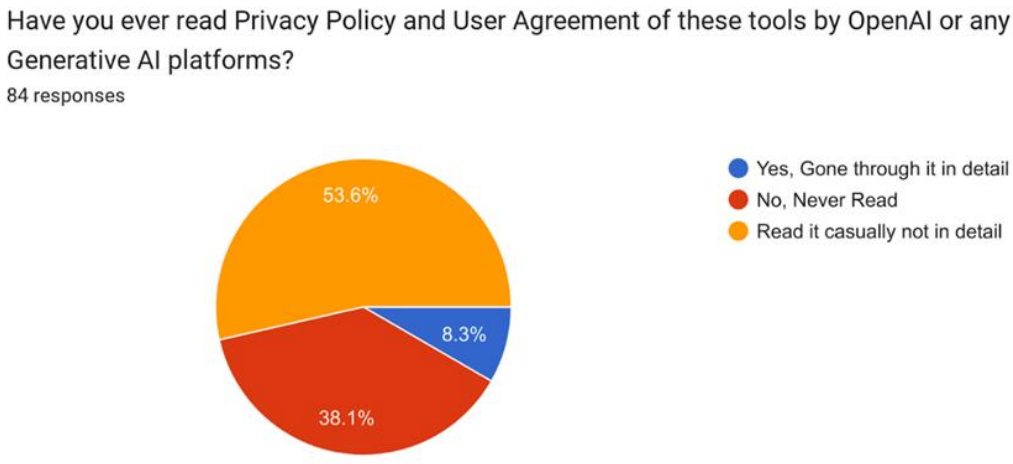
In the context of trade-offs between privacy and enhanced generative experiences, findings revealed a fragmented response among participants. Specifically, 9.4% of respondents demonstrated receptivity towards such exchanges, while a major majority of 61.2% exhibited hesitant or outright opposition. The meaning of remaining respondents expresses uncertainty regarding their stance on the matter.



Moreover, when questioned regarding their familiarity with the data-sharing protocols involving Generative AI systems and third-party entities, 52.9% of respondents acknowledged of awareness of such engagements. Conversely, a majority of participants, 47.1% indicated a lack of awareness regarding these practices.



In a parallel manner, participants were questioned regarding their knowledge of retention of prompts and engagements with Generative AI systems by platforms for the enhancement of user experiences. Findings unveiled that 68.2% of respondents were conscious of this procedure, but 31.8% demonstrated an absence of awareness.



Enquiries were made regarding participants' acquaintance with the privacy policy and user agreements of OpenAI under study. It revealed a diverse range of responses: 8.3% acknowledged having thoroughly pursued the policies, whereas 38.1% admitted to not having done so, and 53.8% stated having only casually reviewed them. These findings underscore the significance of transparency, education, and informed decision-making in navigating the evolving landscape of privacy, awareness, concerns, and attitudes among users of Generative AI systems.

IV. DATA PRIVACY REGULATIONS AND THEIR IMPACT ON GENERATIVE AI

(A) European union

a. GDPR (General Data Protection Regulation)

Generative AI tools represent a significant advancement in technology, leveraging algorithms to create new content such as images, text, and music. However, the use of these tools raises important considerations regarding compliance with the GDPR (General Data Protection Regulation)[25], particularly concerning the collection and processing of personal data.

Generative AI tools often rely on large datasets to train their algorithms effectively. These datasets may contain personal data, such as images or text, which can directly or indirectly identify individuals. Under the GDPR, any information that relates to an identified or identifiable natural person constitutes personal data. Therefore, organizations using generative AI tools must carefully consider the implications of collecting and processing such data.

Although, GDPR does not mention the word AI but it has various provisions regarding the data processing and storage that can be applied to the basic concept of AI. Article 6, Para 1 of GDPR[26].

[25] EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016

[26] "Processing shall be lawful only if and to the extent that at least one of the following applies:

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

c) processing is necessary for compliance with a legal obligation to which the controller is subject;

d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks."

The legality of processing personal data hinges on several conditions outlined within data protection regulations. The processing is legitimate when it serves the legitimate interests of the controller or a third party, except when these interests clash with the rights and freedoms of the data subject, particularly if the data subject is a child. However, it's important to note that this provision does not extend to processing conducted by public authorities in the execution of their official duties. These criteria establish the framework for determining the lawfulness of processing personal data, ensuring that such activities are conducted within defined parameters that respect individuals' rights and interests.

The provisions outlined in *Articles 13 and 14* of the GDPR place responsibilities on the controller concerning the disclosure of crucial information to data subjects during the collection of personal data. It is imperative to recognize the intricacy involved in furnishing such details, particularly in scenarios where the processing constitutes Automated Decision-Making (ADM) according to *Article 22* of the GDPR. This is significant because ADM can lead to legal ramifications or have significant impacts on individuals. When dealing with automated decision-making and acknowledging the opacity inherent in AI models, users of AI systems are required to:

a) notify the data subject about their inclusion in automated decision-making processes.

b) offer comprehensive explanations regarding the underlying logic.

c) clarify the extent and anticipated consequences of the processing.

One of the fundamental principles of the GDPR is that personal data must be processed lawfully, fairly, and transparently. This requires organizations to have a lawful basis for processing personal data, such as obtaining explicit consent from individuals or demonstrating that the processing is necessary for the performance of a contract or compliance with a legal obligation. When using generative AI tools, organizations must ensure that they have a valid lawful basis for collecting and processing personal data and that individuals are informed about how their data will be used.

Moreover, the GDPR emphasizes the importance of purpose limitation, which means that personal data should only be collected for specified, explicit, and legitimate purposes. Generative AI tools must adhere to this principle by ensuring that the personal data they collect is only used for the intended purposes, such as training the AI model or generating content.[27] Any additional uses of personal data must be compatible with the original purposes and

[27] Dr. Nils Lölfing, "Generative AI and GDPR Part 1: Privacy Considerations for Implementing GenAI Use Cases into Organizations," BIRD & BIRD (Oct. 06, 2023).

supported by a valid lawful basis. Data minimization is another key principle of the GDPR, requiring organizations to limit the collection and processing of personal data to what is necessary for the specified purposes. Generative AI tools should be designed to minimize the amount of personal data they collect and use, and organizations should implement measures to anonymize or pseudonymize data whenever possible to reduce the risk of privacy breaches. Additionally, the GDPR grants individuals' certain rights regarding their personal data, such as the right to access, rectification, erasure, and portability. Organizations using generative AI tools must be prepared to fulfil these rights and provide individuals with mechanisms to exercise them. This may include implementing processes for individuals to request access to their data, correct inaccuracies, or delete their data altogether.

The GDPR requires organizations to implement appropriate technical and organizational measures to ensure the security of personal data. Generative AI tools should be subject to rigorous security assessments to identify and address any vulnerabilities that could compromise the confidentiality, integrity, or availability of personal data. By adhering to the principles and requirements of the GDPR, organizations can mitigate the risks associated with the use of generative AI tools and ensure that personal data is handled responsibly and ethically.

b. EU AI Act

The European Union Artificial Intelligence Act (EU AI Act) addresses the concept of privacy in relation to generative AI systems by introducing specific regulations and guidelines. The Act aims to ensure that AI systems, including generative AI, are developed and deployed in a way that respects and protects the privacy of individuals. Here are some key aspects of the EU AI Act's approach to privacy and generative AI:

1. Definition of Generative AI: The EU AI Act defines generative AI as a type of AI system that can generate content, such as text, images, or videos, without human intervention. This definition is crucial in understanding how the Act applies to these systems[28].

2. Risk-Based Approach: The EU AI Act takes a risk-based approach to regulating AI systems, including generative AI. This means that the level of regulation depends on the potential risks associated with the system. For example, high-risk AI systems, including those that can manipulate human behavior or exploit vulnerabilities, are subject to stricter controls.[29]

[28] https://www.stibbe.com/publications-and-insights/the-eu-artificial-intelligence-act-our-16-key-takeaways
[29] https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20240314-the-european-parliament-adopts-the-ai-act

3. Data Protection: The EU AI Act emphasizes the importance of data protection in the development and deployment of AI systems. It requires that high-risk AI systems ensure data governance that is consistent with data protection law priorities, ensuring that personal data is processed in a way that is transparent, secure, and respects the rights of individuals.[30]

4. Transparency and User Awareness: The Act also highlights the need for transparency and user awareness in the use of AI systems, including generative AI. This includes ensuring that users understand when they are interacting with an AI system and that the system is not deceiving or manipulating them.[31]

5. National Security Carve-Out: The EU AI Act includes an exemption for AI systems deployed for national security purposes. This exemption has raised concerns about the potential for intrusive and unethical technologies to be created and deployed under the guise of national security[32]

Overall, the EU AI Act aims to strike a balance between promoting innovation in AI and protecting the privacy and fundamental rights of individuals. By introducing specific regulations and guidelines for generative AI systems, the Act aims to ensure that these technologies are developed and deployed in a way that respects the values of the European Union.

(B) India

a. DPDP ACT

In accordance with Section 3 of the Digital Personal Data Protection Act, 2023[33], publicly accessible data will not fall within the purview of its provisions. This implies that activities such as social media postings or generating prompts for AI tools are exempt from regulation under this Act in India, unlike in Western nations and Europe. Notably, the Act confers certain powers akin to those of a civil court upon the Data Protection Board[34]. Additionally, orders issued by the Appellate Tribunal[35] under this Act are enforceable as civil decrees, highlighting the predominantly commercial and civil law nature of most data protection matters. Unlike in other jurisdictions where considerations of public duty rooted in public law come into play, India's regulatory stance on governing the use of artificial intelligence technologies remains

[30] https://cdt.org/insights/eu-ai-act-brief-pt-2-privacy-surveillance/
[31] https://secureprivacy.ai/blog/eu-ai-act-compliance
[32] https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence
[33] Act No. 22 of 2023
[34] Chapter V of DPDP Act, 2023
[35] Chapter VII of DPDP Act, 2023

primarily focused on commercial and civil legal frameworks. However, it is anticipated that this approach will evolve, particularly concerning the regulation of high-risk and low-risk AI systems under the Digital India Act that is already in the process of formation.

The omission of provisions pertaining to artificial intelligence, particularly generative AI, in the latest iteration of the Digital Personal Data Protection (DPDP) Act has sparked concern among experts, who fear it will create a gap in privacy regulation. This absence not only raises apprehensions about the adequacy of the law in keeping pace with rapidly evolving technologies but also introduces ambiguity regarding their governance. However, the absence of regulations addressing generative AI has drawn criticism, particularly in light of the increasing prevalence of deep fakes generated by such tools. Experts emphasize the urgent need for the DPDP to address this issue, especially given the impending elections in two major democracies, India and the US. The potential misuse of generative AI to create manipulated images or videos of public figures for malicious intent underscores the importance of regulatory intervention. Consequently, there is a growing call for the DPDP to incorporate provisions specifically targeting deep fakes and similar AI-generated content. Notably, platforms like ChatGPT and Google's Bard may face restrictions on processing personal data of Indian citizens sourced from the public domain under the proposed legislation.

Where, it lacks to address AI in particular but if talked about personal data, it lays down various provisions where and how the personal data maybe collected and if there is a certain breach, then what is the correct procedure under this act to regulate it. Section 4(1)[36] mentions the grounds for a person in which the personal data can be processed personal data of the data principal.

Moreover, the DPDP Act prohibits search engine giants such as Google, Microsoft (or OpenAI), and others from indiscriminately scraping vast amounts of publicly available data from the internet. This restriction is intended to safeguard individuals' privacy and prevent unauthorized exploitation of their personal information by AI platforms and tech companies. However, the absence of explicit guidelines on regulating generative AI raises concerns about potential loopholes in the legislation, leaving room for further debate and refinement to ensure comprehensive protection of personal data in the digital age.[37]

[36] *"4. (1) A person may process the personal data of a Data Principal only in accordance with the provisions of this Act and for a lawful purpose,—*
(a) for which the Data Principal has given her consent; or
(b) for certain legitimate uses."

[37] "Indic Pacific," The Digital Personal Data Protection Act: Shaping AI Regulation in India (accessed Feb. 25, 2024), https://www.indicpacific.com/post/the-digital-personal-data-protection-act-shaping-ai-regulation-in india.

Regarding the transnational flow of data and efforts to foster digital connectivity between India and other nations, the Act grants unilateral authority to the Government to restrict data flow as deemed necessary. Presently, the absence of specific measures delineated by the Government can be attributed to ongoing trade negotiations concerning the information economy involving India and key stakeholders such as the UK and the European Union, which have encountered challenges. This predicament is not unique and is emblematic of a broader issue faced by companies and governments worldwide. Firstly, the trans-border flow of data intersects with trade law, necessitating diplomatic negotiations that often fail to yield consensus due to its transactional nature. Secondly, data protection law, rooted in the historical context of telecommunications law, complicates matters further, as contractual and commercial aspects of trans-border data flow remain intertwined with telecommunications regulations. This echoes the broader discussion on moratoriums on digital goods and services within the framework of WTO Law, which is slated for deliberation in forthcoming WTO Ministerial Conferences. An excerpt from the joint submissions of India and South Africa on 'E-commerce Moratoriums' underscores the significance of this issue.

In conclusion, effective regulations are imperative to govern the use of generative AI technologies in a manner that balances innovation with ethical considerations and safeguards individuals' rights to privacy and security.[38] Such regulations should encompass various aspects, including but not limited to, the detection and mitigation of deep fakes, transparency in the deployment of AI algorithms, accountability mechanisms for AI creators and users, and robust data protection measures. Furthermore, a collaborative approach involving policymakers, technologists, ethicists, and other stakeholders is essential to develop comprehensive regulatory frameworks that anticipate and address the challenges posed by generative AI while fostering responsible innovation and societal benefit. By implementing thoughtful and forward-thinking regulations, we can harness the transformative potential of generative AI while mitigating its risks and ensuring its alignment with broader societal values and interests.[39] India has seen significant governmental efforts aimed at harnessing the potential of artificial intelligence (AI) while ensuring its ethical and responsible use. These initiatives, spearheaded primarily by the AI Task Force and NITI Aayog, have resulted in a series of crucial documents and reports that have deeply influenced the country's AI strategy.

[38] "The Hindu," Should generative artificial intelligence be regulated? (Feb. 25, 2024), https://www.thehindu.com/opinion/op-ed/should-generative-artificial-intelligence-be-regulated/article67356695.ece.

[39] "The Economic Times," Experts flag revised data bill's silence on generative AI tools (accessed Feb. 24, 2024), https://economictimes.indiatimes.com/tech/technology/experts-flag-revised-data-bills-silence-on-generative-ai-tools/articleshow/102480170.cms.

 [ISSN 2581-9453]

The journey towards leveraging AI capabilities in India began in 2018 with the publication of the "India: The AI Century" report by the AI Task Force, setting the foundation for India's AI ambitions. Following this, NITI Aayog introduced a discussion paper titled "National Strategy for Artificial Intelligence #AIFORALL," aimed at formulating comprehensive strategies to democratize AI access across various sectors. The momentum continued to build in 2021 with NITI Aayog's release of the "Approach Document for India Part 1 – Principles for Responsible AI," signaling a notable shift towards prioritizing responsible AI practices. This was followed by the publication of the "Approach Document For India: Part 2 – Operationalizing Principles For Responsible AI" in August 2021, which provided practical insights into implementing responsible AI principles.

In November 2022, NITI Aayog unveiled the "Responsible AI for All: Adopting the Framework – A use case approach on Facial Recognition Technology," focusing on specific AI applications, particularly facial recognition technology, and outlining guidelines for its responsible deployment. The culmination of these legislative and policy efforts came in October 2023 with the inaugural release of the IndiaAI Report by IndiAI, offering valuable insights into the trajectory and potential of AI in India.

V. CONCLUSION AND SUGGESTIONS

In conclusion, the ascent of generative AI tools marks a significant leap forward in technological innovation, offering unprecedented capabilities across various sectors. However, this progress is accompanied by pressing concerns surrounding privacy and security, necessitating proactive measures to address potential risks. Collaboration among researchers, policymakers, and industry stakeholders is vital to establish robust governance structures and ethical standards that safeguard personal privacy and societal stability. Regulatory frameworks such as the GDPR and the EU AI Act provide important guidelines for responsible development and deployment, emphasizing principles of transparency, data protection, and user awareness. Yet, the absence of specific provisions addressing generative AI in some jurisdictions, notably India, underscores the need for adaptive regulation to keep pace with technological advancements.

Moreover, the complex interplay of data privacy regulations, trade law, and telecommunications regulations highlights the challenges in managing transnational data flows and fostering digital connectivity. Ongoing dialogue and cooperation among nations are essential to navigate these complexities and ensure the responsible and ethical use of generative AI technologies. By prioritizing the development and implementation of comprehensive

governance frameworks, stakeholders can harness the transformative potential of generative AI while upholding ethical principles and safeguarding the interests of society.

*****

 [ISSN 2581-9453]