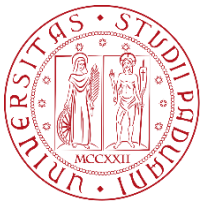
UNIVERSITÀ DEGLI STUDI DI PADOVA

DEPARTMENT OF POLITICAL SCIENCE,
LAW AND INTERNATIONAL STUDIES

Master's degree in
European and Global
Studies



AI and The European Union's Approach to Data Protection: The Case of ChatGPT

Supervisor: Prof. Daniele Ruggiu

Candidate: Amirreza Ahkami

Matriculation No. 2041202

A.Y. 2023/2024

Contents

Abstract

Artificial Intelligence (AI) is advancing rapidly, with generative models like ChatGPT revolutionizing numerous industries. However, these advancements present significant challenges in adhering to data protection regulations such as the General Data Protection Regulation (GDPR) in the European Union (EU). This thesis examines the complex relationship between AI and data protection within the EU, using ChatGPT as a case study to analyze the impact of GDPR on AI technologies.

The study explores the intricate dynamics between AI systems and data, focusing on the ethical, data collection and privacy issues inherent in AI-driven data utilization. It evaluates the implications of the GDPR framework on AI development, particularly in relation to provisions for user consent, data anonymization, and algorithmic transparency. Additionally, the research compares the EU's approach to AI regulation assessing the impact on international collaboration and AI innovation.

An aspect of this thesis is the examination of the January 2024 Garante della Privacy ruling, which underscores the necessity for stringent compliance mechanisms, transparency, and robust user consent procedures in AI operations. This ruling serves as a pivotal reference for future regulatory actions, highlighting the practical implications of GDPR enforcement on generative AI models like ChatGPT.

Through a comprehensive analysis of ChatGPT's GDPR compliance strategies and the associated challenges, this study provides insights for policymakers and AI developers. The findings advocate for a balanced regulatory approach that promotes innovation while safeguarding fundamental human rights. The thesis concludes with recommendations for enhancing transparency, user consent, and data privacy in AI systems, and suggests future research directions to address emerging challenges in the rapidly evolving field of AI.

Keywords: Artificial Intelligence (AI), General Data Protection Regulation (GDPR), Data Protection, EU Regulations, ChatGPT, AI Act

Introduction

The incoming Era of Artificial Intelligence

Throughout history, human progress has been marked by significant periods known as the Industrial Revolution. These transformative phases, from the mechanization of the first industrial revolution to the current decade, have reshaped societies, economies, and the fundamental aspects of human life.

As we stand at the give up of a brand new technology, the Fourth industrial Revolution, marked by using the convergence of virtual, physical, and biological realms, the landscape of innovation undergoes a seismic shift. At the heart of this transformation lies Artificial Intelligence (AI), that is at the centre of this thesis. Like its predecessors that altered the course of civilization, AI is quickly transitioning from a specialized technology to a universal mass innovation, reshaping industries and fundamentally redefining the boundaries of human potential. Understanding AI's trajectory necessitates viewing its ascendancy within the context of these historical industrial revolutions, unveiling its unmatched significance as the linchpin of this growing era of innovation and change (Britannica, 2024).

With the First Industrial Revolution of 1765 we can locate the proto-industrialization era when the mechanization of industries brought about the largest changes. In this period owing to mechanization, the industry began to supplant agriculture as the foundation of the society economy. The key innovation of the steam engine, which at the time enabled the rapid construction of railroads and, consequently, the acceleration of the economy, coincided with the vast extraction of coal from the earth (IED Team, 2023).

Nearly a century after the first Industrial Revolution, around 1870, we witness the Second Industrial Revolution taking place worldwide. The advent of a new energy source—oil, gas, and electricity—was aided by significant technological improvements in several industries around the end of the 19th century.

The internal combustion engine was created as a result of this revolution and it began to realize its full potential. Ultimately, the Second Industrial Revolution is still seen as the most significant one because of the creation of the vehicles and the airplanes at the start of the 20th century but the birth of the sector of telecommunication can be deemed the starting point of the advent of the computers (IED Team, 2023)

With the Third Industrial Revolution the main revolutionary step was due to the development of electronics, communications, and computers. Through the development of new technologies, the space travel, research, and biotechnology became possible. But it is the process of mechanisation that affected not only the industry but the whole society that we would like to underline. Two significant industrial inventions — robots and programmable logic controllers, or PLCs — helped usher in a high-level automation era (IED Team, 2023).

Though many continue to differ, Industry 4 is widely regarded as the fourth Industrial Revolution. We would have to acknowledge that Industry 4.0 is a revolution in progress if we were to regard it as such. It is something we live with on a daily basis, but its exact scope is unknown. Beginning with the one daily tool used by all, the Internet, Industry 4.0 got its start at the start of the third millennium. We can observe the shift from Industry 1.0, which was based on technological phenomena, to Industry 4.0, which creates virtual reality environments that let humans defy the rules of physics (IED Team, 2023).

Each era of human progress has been marked by major changes, from the mechanization of the First Industrial Revolution to the digitalization of the Third. As we approach the Fourth Industrial Revolution, which combines digital, physical, and biological domains, Artificial Intelligence (AI) is leading this upheaval. AI, which has quickly evolved from a niche technology, is transforming sectors and expanding human potential (Van De Ven, 2015).

AI as a vital participant in industry 4 is a human record-setting second. AI's growth is linked with past industrial revolutions, but its current rise as a mass invention portends a future where technology is ubiquitous. As AI permeates every aspect of life, from personal assistants to independent systems, its incorporation into business revolutions highlights its unprecedented role in guiding human growth and creativity (Nayak, 2023).

The Advent of the New Generative Artificial Intelligence

Generative intelligence stands as the pinnacle of AI evolution, promising an array of capabilities that extend far beyond the confines of conventional machine learning. It embodies the essence of creativity, allowing machines to not only process data but also generate new content autonomously. This transformative leap empowers AI systems to understand, interpret, and respond to individual preferences, behaviour, and nuances, tailoring experiences in ways previously unimaginable (Dwivedi et al., 2023).

However, the journey towards embracing generative intelligence is not without its challenges. One of the critical obstacles faced is the considerable demand for memory storage and computational power that these advanced systems necessitate. Overcoming these technical limitations remains a crucial milestone on the path to fully realizing the potential of generative intelligence (*How Generative AI Is Reshaping Education in Asia-Pacific*, 2023).

The rise of generative AI is also fuelling various concerns. These relate to the quality of results, potential for misuse and abuse, and the potential to disrupt existing business models. Here are some of the specific types of problematic issues posed by the current state of generative AI:

- It can provide inaccurate and misleading information.
- It is more difficult to trust without knowing the source and provenance of information.
- It can promote new kinds of plagiarism that ignore the rights of content creators and artists of original content.
- It might disrupt existing business models built around search engine optimization and advertising.
- It makes it easier to generate fake news.
- It makes it easier to claim that real photographic evidence of a wrongdoing was just an AI-generated fake.
- It could impersonate people for more effective social engineering cyber attacks.

The shift from traditional artificial intelligence (AI) to generative artificial intelligence represents a profound leap forward in the realm of technological advancement. This transition marks the onset of an era dominated by generative intelligence, a phase characterized by AI systems that possess unparalleled creativity, adaptability, and personalization. In this impending period, the landscape of technology will be fundamentally transformed, redefining the way we engage with and utilize devices, ranging from handheld mobile gadgets to classy computer systems (Dwivedi et al., 2023).

Once the barriers of memory storage and computational constraints are prevailed, the reliance on established tech giants such as Google and Amazon for search and information retrieval may undergo a substantial shift. Instead of depending on centralized platforms, individuals will harness the capabilities of their own personalized generative intelligence embedded within their devices. This shift will empower users to conduct searches, interact with information, and

navigate the digital realm in a manner that is uniquely tailored to their preferences, habits, and personality traits (Dwivedi et al., 2023).

The imminent era of generative intelligence not only signifies an expansion in the capabilities of AI systems but also heralds a significant societal shift. It emphasizes the widespread integration of personalized and adaptive technologies into our daily lives, fundamentally altering our interactions with and dependence on technology. As this era unfolds, it holds the promise of revolutionizing not just how we engage with devices, but how we perceive and navigate the world of information and innovation (*Henry a. Kissinger*, 2023).

A Question of Intelligence or a Question of Data?

The intelligence of smart machines hinges significantly on their adeptness in managing extensive volumes of data, fuelling their ability to extract patterns, make accurate predictions, and exhibit cognitive capabilities beyond traditional data processing. While the correlation between intelligence and vast data management is pivotal, it's imperative to recognize that intelligence isn't solely reliant on data processing ability but encompasses the capacity to learn, reason, and creatively solve problems (Rane et al., 2023).

Due to the quantity, quality, and diversity of data encountered during operation and training, smart machines can navigate massive databases, extract useful insights, and make predictions. They can generalize from experiences, make informed decisions, and perform difficult jobs like humans because they can comprehend billions of data points. They excel at natural language processing, picture recognition, recommendation systems, and autonomous operations by interpreting massive amounts of data. (Bandi et al., 2023).

Smart machines are intelligent beyond data handling—they learn, adapt, and solve problems. Combining algorithms and machine learning models allows these computers to gain insights, make informed decisions, and outperform humans in numerous fields. Scalability and parallelization make them essential in healthcare diagnostics, financial trading, robotics, and autonomous cars, revolutionizing industries and improving decision-making (Torabi, 2023).

Intelligence is more than data processing, yet the convergence of intelligence and enormous data management highlights smart machines' extraordinary powers. These robots are evolving

to drive unprecedented innovation, revolutionize industries, and improve decision-making as data volumes rise (Elahi et al., 2023).

In essence, the intelligence of smart machines is undeniably intertwined with their ability to manage and analyse immense data sets. This data-driven approach is revolutionizing industries and aspects of our lives, surpassing human capabilities in various domains. As data continues its exponential growth, the future promises even more ground-breaking advancements in smart machine intelligence, pushing the boundaries of what we perceive as achievable.

Research Problem and Objectives

This study seeks to better comprehend the complex relationship between AI, data protection, and ethics in the EU.

The thesis aims at understanding the problems that lie on the incredible huge ability of processing data by generative AI, and it make this starting from the case of ChatGPT.

The intersection of Artificial Intelligence (AI) and data protection has emerged as a pivotal area of inquiry, with profound implications for the European Union (EU) (Pinheiro & Battaglini, 2022). In this context, the rise of AI technologies, exemplified by systems like ChatGPT, necessitates a comprehensive examination of the existing link between AI and data. Specifically, this study seeks to explore how EU regulations, notably the General Data Protection Regulation (GDPR) (Sartor, 2020), impact the development and deployment of AI, focusing on ChatGPT as a case study. The complexity of AI technologies, coupled with the stringent data protection standards outlined in the GDPR, raises intricate questions about the ethical, legal, and societal dimensions of AI implementation within the EU framework. Understanding these nuances is crucial for fostering responsible AI innovation while safeguarding individual privacy and fundamental rights (Kuner et al., 2018).

This work has the following objectives:

1. **To Analyse the Interconnection between AI and Data:** Investigate the intricate relationship between AI systems, particularly ChatGPT, and the data they rely on. Explore the nuances of data collection, storage, and processing methods, emphasizing the ethical considerations associated with AI-driven data utilization.

2. **To Conduct a Comparative Analysis:** Compare and contrast the EU's approach to AI regulation, particularly through the GDPR. Assess the implications of these variations on AI development, innovation, and international collaboration.

3. **To Evaluate GDPR Provisions Relevant to AI Development:** Examine the specific GDPR provisions that intersect with AI technologies. Investigate how these regulations influence the design, implementation, and operation of AI systems, focusing on aspects such as user consent, data anonymization, and algorithmic transparency.

4. **To Assess Data Protection Challenges and Privacy Implications:** Delve into the challenges arising from data protection and privacy concerns in the context of AI, especially within the EU landscape. Evaluate the potential risks associated with AI systems like ChatGPT and their impact on individual privacy and data security.

5. **To Investigate ChatGPT as a Case Study:** Focus on ChatGPT as a representative case study to explore real-world applications of AI within the EU. Analyze how ChatGPT adheres to GDPR guidelines, examining the challenges faced and solutions implemented, thereby providing insights into the practical implementation of AI regulations in Europe.

Through a comprehensive exploration of these objectives, this research aims to shed light on the intricate dynamics between AI, data protection regulations, and ethical considerations within the EU context. By focusing on ChatGPT as a case study, this study aspires to provide nuanced insights that contribute to the ongoing discourse on responsible AI development, thereby informing future policies, practices, and scholarly endeavours in the field.

Significance of the Case Study: ChatGPT in Europe

- **Unravelling Complexities in AI and Data Integration:**

The significance of the ChatGPT case study in the European context extends far beyond its role as an AI model. It represents a microcosm of the intricate complexities embedded in the integration of Artificial Intelligence and data within the EU (Margoni & Kretschmer, 2022). AI systems like ChatGPT are not mere technological artifacts; they are engines powered by vast amounts of data (Margoni & Kretschmer, 2022). By closely examining ChatGPT's interaction with data – the lifeblood of AI – and the protocols in place to ensure GDPR compliance, this case study becomes a lens through which we can decipher the challenges and innovations within the realm of data-driven AI technologies (Lorè et al., 2023).

- **Ethical Considerations in Algorithmic Decision-Making:**

At its core, the case of ChatGPT delves into the ethical considerations intertwined with algorithmic decision-making (Pazzanese & Parsons, 2023). By studying how ChatGPT processes data while upholding the principles of user privacy, consent, and transparency mandated by the GDPR, we gain insights into the ethical dilemmas faced by AI developers (Tsamados et al., 2021). Ethical considerations are not abstract concepts but tangible challenges that emerge when AI algorithms interact with real-world data, especially within the stringent regulatory framework of the EU (Tsamados et al., 2021). This case study serves as a beacon, illuminating the path toward ethical AI development and guiding future endeavours in aligning technology with human values.

- **Navigating GDPR Compliance Challenges:**

The GDPR, with its robust data protection standards, represents a pioneering legislative initiative. However, translating these regulations into practice, especially in the dynamic landscape of AI, poses intricate challenges. ChatGPT's case study serves as a crucible where these challenges come to the fore. How does ChatGPT handle user data? What mechanisms are in place to ensure GDPR compliance across diverse contexts and user interactions? These questions are not merely theoretical; they encapsulate the real-world hurdles faced by AI developers. By dissecting ChatGPT's GDPR compliance

strategies, this research contributes actionable insights, guiding businesses and policymakers in navigating the complex terrain of data protection and AI development.

- **Fostering Cross-Disciplinary Dialogue:**

The case of ChatGPT transcends the boundaries of computer science and law, inviting a cross-disciplinary dialogue. Ethicists, legal experts, technologists, and policymakers converge around this case study, engaging in nuanced discussions about the future of AI in Europe (Brodin & Avery, 2020). The interdisciplinary nature of this discourse enriches the perspectives, ensuring a holistic understanding of the challenges and opportunities that lie at the intersection of AI and data protection (Brodin & Avery, 2020). Consequently, the case study becomes a catalyst for collaborative problem-solving, fostering an environment where diverse expertise converges to shape ethical AI policies and practices.

- **Shaping Global Narratives on AI Governance:**

As the EU sets standards in data protection and AI governance, the ChatGPT case study assumes global relevance (Tallberg et al., 2023). Europe's approach to regulating AI reverberates across international borders, influencing global conversations on ethical AI development. By meticulously analyzing ChatGPT within the EU's regulatory framework, this research contributes to shaping these narratives. It provides empirical data and nuanced insights that inform international deliberations, influencing how other regions conceptualize and implement data protection measures in the realm of AI (Schmitt, 2021). The case study, thus, becomes a cornerstone in the global discourse, guiding nations toward responsible AI governance in an interconnected world.

- **Empowering Informed Decision-Making:**

Ultimately, the significance of the ChatGPT case study lies in its potential to empower informed decision-making. By thoroughly understanding how AI systems like ChatGPT navigate the intricacies of data protection laws, stakeholders – ranging from policymakers and businesses to end-users – can make decisions rooted in knowledge. Informed businesses can develop AI technologies that respect user privacy, bolstering

consumer trust. Policymakers armed with empirical insights can craft regulations that strike the delicate balance between innovation and ethical standards (Angerschmid et al., 2022). Informed citizens, aware of the ethical considerations in AI, can actively engage with these technologies, fostering a symbiotic relationship between society and AI innovation.

In summary, the ChatGPT case study, when examined within the context of the EU's GDPR regulations, not only sheds light on the complexities of AI and data protection but also becomes a beacon guiding ethical AI development, fostering interdisciplinary dialogue, shaping global narratives, and empowering stakeholders to make decisions that resonate with the principles of responsible AI innovation and data privacy.

- **Integrating the Garante della Privacy Decision**

The decision by the Garante della Privacy in January 2024 represents a significant development in the regulatory landscape for AI in the EU. This decision specifically addresses the compliance issues faced by generative AI models like ChatGPT, underscoring the importance of adhering to GDPR standards. The Garante della Privacy's ruling highlights the critical need for transparency, user consent, and data protection in AI systems. By analyzing this decision, the research illustrates the practical implications of regulatory enforcement and provides a concrete example of how AI governance can be effectively implemented. This case study serves as a pivotal reference for future regulatory actions, reinforcing the need for robust compliance mechanisms and setting a benchmark for the ethical deployment of AI technologies.

The thesis highlights the critical significance of generative AI models like ChatGPT as it moves through a structured study of the intersections between AI and data protection inside the European Union.

The first chapter discusses artificial intelligence (AI) and generative AI, paying special emphasis to ChatGPT's evolution and ramifications. Setting the scene, this chapter looks at the generative AI's technological underpinnings and disruptive possibilities in today's digital environments.

The evolution of AI is traced in the second chapter, which emphasizes the vital significance of data. It investigates how the special qualities of generative AI both challenge and expand on

current data protection frameworks, laying the groundwork for a thorough analysis of the subtleties that exist between privacy concerns and AI capabilities.

The third chapter of the book switches to a thorough examination of the European Union's AI governance strategy, with a particular emphasis on the GDPR. This contains a detailed analysis of the privacy protection laws in the EU and the US, emphasizing the EU's unique strategy for striking a balance between innovation and strict data protection regulations. A case study of ChatGPT in Europe is presented in the third chapter, which looks at how it manages the complex regulatory environment. It describes the privacy and data protection issues that Italy and other European nations face, highlighting the real-world effects of GDPR on the application of AI.

The last chapter summarizes the key takeaways from each section and highlights their important contributions to comprehending the intricate interactions among AI, data protection, and EU laws. It draws on the in-depth analysis of ChatGPT to shed light on more general concerns in European AI policy and explores how the findings might affect future AI development and legislation in Europe.

This thesis not only demonstrates the European Union's dedication to strong AI governance, but it also identifies important areas that require further focus and flexible legislation. It highlights the difficult balance that must be struck in order to promote AI innovation and maintain strict data privacy; this balance will ultimately define how AI develops and is accepted by society in Europe. The demand for wise, knowledgeable, and adaptable regulation grows as AI technologies are progressively incorporated into more and more facets of societal operations. The analysis of ChatGPT in the EU provides a clear picture of the situation as it stands today and indicates future paths for practice and policy in the area of AI governance.

1. A Brief History of Artificial Intelligence

1.1 Introduction

By the middle of the 20th century, scientists, mathematicians, and philosophers had culturally adopted AI, partially due to science fiction. There were initially two fundamental obstacles to AI's advancement. Before 1949, computers could only execute commands, not store them. Even though they could be trained, computers could remember what they did. Computer leasing cost up to $200,000 a month in the early 1950s, making computing expensive. Only large IT companies and top institutions could afford to investigate these uncharted frontiers (Rockwell, 2017).

Weather forecasting, spam filters, and navigation systems use AI today. AI is crucial to daily life. AI development requires data protection legislation due to its growing computational capacity. Data collection is essential to artificial intelligence, thus AI systems must follow data privacy rules. Machines can now predict patterns and analyze vast datasets thanks to rapid advances in machine learning. AI systems must follow data privacy rules while using data to provide new and improved functionality due to their rising processing capacity (Rockwell, 2017).

AI is "a system's ability to interpret external data correctly, to learn from such data, and to use those learnings to achieve specific goals and tasks through flexible adaptation." AI enables image recognition, smart speakers, and self-driving automobiles. When AI was first studied, scientists ignored it, and it wasn't used in the actual world for over 50 years. Big data is becoming more ubiquitous in corporate and public discourse as processing capability grows (Haenlein & Kaplan, 2019).

Since the 1950s, experts have projected AGI will arrive in a few years. AGI systems have cognitive, emotional, and social intelligence and behave like humans. Simply wait and see whether this is true. To understand what is practically viable, AI can be approached from two angles: the one already traveled and the one still to be explored. This editorial aims to do that. To assess AI's progress, we use the four seasons (spring, summer, fall, and winter) to illustrate its technological growth (Haenlein & Kaplan, 2019).

1.2 The four AI Seasons of AI

AIS Spring: Artificial Intelligence's Inception

The 1940s, and specifically 1942, when American science fiction writer Isaac Asimov published his short story Runaround, are most likely the earliest known instances of artificial intelligence (AI). The Three Laws of Robotics are central to the tale of Runaround, a robot developed by engineers Gregory Powell and Mike Donavan. These laws state that: (1) a robot cannot cause harm to humans or allow humans to come to harm through inaction; (2) a robot must obey human commands unless doing so would be in violation of the First Law; and (3) a robot must defend its own existence unless doing so would be in violation of another law. Asimov's work has impacted numerous scientists in the computer science, robotics, and artificial intelligence domains. The American cognitive scientist Marvin Minsky is one such scientist who subsequently co-founded the MIT AI lab (Haenlein & Kaplan, 2019).

Alan Turing, an English mathematician, built the Bombe for the British government at the same time as he worked on less fantastical problems 3,000 miles away. The Bombe, the first electro-mechanical computer, weighed one ton and measured seven by six by two feet. Turing pondered if such computers could be sentient after The Bombe deciphered the Enigma code, which had stumped even the best mathematicians. In the groundbreaking paper "Computing Machinery and Intelligence" (Turing, 1950), he explained how to create and evaluate intelligent machines. The Turing Test is still used to test artificial system intelligence: computers are intelligent if they cannot be identified as machines while interacting with people.

The roughly eight-week-long Dartmouth Summer Research Project on Artificial Intelligence (DSRPAI) was arranged by Stanford computer scientists John McCarthy and Marvin Minsky. This workshop brought together the men who would later be considered the founding fathers of AI (Haenlein & Kaplan, 2019).

Summer and Winter of AI: The Highs and Lows of AI

Artificial intelligence saw significant breakthroughs for nearly two decades following the Dartmouth Conference. One famous example is the computer program known as ELIZA, which was created by Joseph Weizenbaum at MIT in 1964 and 1966. ELIZA, a natural language processing program that could simulate a conversation with a human, was among the first algorithms to attempt to pass the aforementioned Turing Test. Another early AI success story was the General Problem Solver program, developed by scientists Cliff Shaw and Allen

Newell of RAND Corporation, as well as Nobel Prize winner Herbert Simon. The allocation of substantial funds to AI research was prompted by these inspiring success stories, and this in turn gave rise to an expanding number of initiatives. Marvin Minsky estimated in a 1970 interview with Life Magazine that a machine with the general intellect of an average person could be created in three to eight years (Haenlein & Kaplan, 2019).

But regrettably, this was not accurate. Just three years later, in 1973, the US Congress started actively denouncing the substantial sums of money being spent on AI research. In a study commissioned by the British Science Research Council that same year, British mathematician James Lighthill questioned the upbeat viewpoint offered by AI specialists. According to Lighthill, machines could never be compared to a "experienced amateur" in games like chess since common sense reasoning will always be beyond their ability. Consequently, the British government withdrew funding for AI research from all universities save Edinburgh, Sussex, and Essex, and the American government swiftly followed suit. At this point, the AI Winter started. Even though the Japanese government began to aggressively fund AI research in the 1980s and the US DARPA increased spending in response, not much further progress was gained in the years that followed (Haenlein & Kaplan, 2019).

Fall of AI: The Harvest

The reason for the initial lack of progress in artificial intelligence and the sharp decline in reality compared to expectations can be attributed to the exact method that early systems such as ELIZA and the General Problem Solver tried to match human intelligence. Expert systems, which are essentially collections of rules based on the notion that human intellect can be boiled down to a series of "if-then" statements and then top-down formalized and reconstructed, are what all of them were. In domains where this type of formalization is appropriate, expert systems have outstanding performance capabilities. An instance of an expert system is the IBM *Deep Blue* chess software, which defied a statement made by James Lighthill more than 25 years earlier and defeated world champion Gary Kasparov in 1997. As per the reports, *Deep Blue* employed a tree search technique to evaluate 200 million possible moves per second and select the optimal move 20 moves in advance. (Campbell and associates, 2002)

Under the title of deep learning, artificial neural networks reappeared in 2015 when Google's *AlphaGo program* beat the world champion in the board game Go. Since there are 361 possible movements in Go at opening compared to just 20 in chess, it is significantly more intricate than chess, and it was long believed that computers would never be able to beat players in this game.

Deep learning, a specific type of artificial neural network, was used to enable *AlphaGo*'s remarkable performance. Twelve Artificial neural networks and deep learning are the basis of most applications that we currently identify as AI. They are the basis for the image recognition algorithms used by Facebook, as well as the speech and picture recognition algorithms driving autonomous vehicles and smart speakers. According to Silver et al. (2016), we are currently seeing the AI Fall, which is the result of past statistical successes being reaped.

1.3 The Generative Artificial Intelligence

Generative AI history

Early mathematicians and philosophers tried to automate reasoning, leading to AI. Modern AI was founded on George Boole's Boolean algebra and Alan Turing's thinking machines in the 19th and 20th centuries. In 1943, Warren McCulloch and Walter Pitts invented the mathematical neuron. Neural networks began here and power modern AI. In 1950, Alan Turing proposed a computer intelligence test in “Computing Machinery and Intelligence”. The Turing test is still used to evaluate AI. In 1956, the Dartmouth Summer Research Project introduced the term “artificial intelligence” and began AI research (Lambert, 2023)US Department of Defense funding for military uses and breakthroughs drove the 1960s AI boom. Herbert Simon and Marvin Minsky predicted a generation of human-like machine intelligence. AI proved harder than projected, reducing funding and development and generating the "AI winter". The 1980s saw AI interest reinvigorated once rule-based expert systems emulated human reasoning became commercially successful. Healthcare and finance used these systems. In 1987, another “AI winter” occurred despite this resurgence. In the 1990s and 2000s, ML ruled AI. The abundance of data made ML succeed. Unlike rule-based systems, ML algorithms directly recognize data patterns, enabling email spam filters, Netflix recommendations, and financial forecasts. ML makes AI data-driven, not rule-based. A major change occurred in 2012. Data, neural networks, and GPUs enabled deep learning, a kind of ML. Deep learning outperformed previous ML methods, lifting AI research, investment, and applications. Global AI investments reached $91 billion in 2022, providing many jobs and specialists. Spam filtering, driverless vehicles, and medical diagnostics use machine learning-based AI. A subset of ML, generative AI can create pictures, movies, sounds, and text, drawing attention (Lambert, 2023).

In the 1960s, Joseph Weizenbaum created the chatbot Eliza, the first generative AI. Early versions depended largely on patterns, had a tiny vocabulary, and were easily broken due to their rules-based approach. Early chatbots were hard to customize.

The ability of deep learning and neural networks to automatically learn how to transcribe voice, identify visual features, and evaluate written text revived the field in 2010 (Lawton, 2023).

GANs were introduced by Ian Goodfellow in 2014. This new deep learning technology arranged competitive neural networks to produce and rank distinct material. These might create realistic text, music, voices, and people. This raised concerns about generative AI's ability to create lifelike deepfakes that replicate video noises and people (Lawton, 2023). Since then, neural network topologies and methods have improved generative AI. Techniques include neural radiance fields, transformers, diffusion models, VAEs, and extended short-term memory.

How does generative AI work?

The generative AI process begins with a stimulus, which might be a word, image, video, design, musical notation, or other input. Following the instructions, AI algorithms return new content. Content includes essays, problem-solving methods, and lifelike fakes of real people. Early generative AI data submission required APIs or other cumbersome methods. Developers needed to learn Python and use specific tools (Lawton, 2023).

The advent of generative AI, epitomized by models like ChatGPT, heralds a new era in data collection and analysis capabilities, particularly concerning personal data. These advanced systems are not only adept at aggregating vast quantities of data but also possess creative capabilities that extend into the realm of profiling, such as generating new user profiles. This ability is especially potent when integrated into mobile devices, facilitating real-time data collection and enhanced microtargeting of users. A significant aspect of generative AI, often overlooked, is its default operational model where the collected data is routinely shared with third parties, including the AI developers, their clients, and an extended network of partners. This widespread sharing of data amplifies concerns regarding user privacy and data security, making the role of regulatory frameworks like the GDPR more crucial than ever in overseeing and safeguarding the ethical and responsible use of AI technologies in our increasingly data-driven world (Galič & Gellert, 2021).

Predictive engines were employed by the majority of AI applications until recently to correlate data or make choices. Despite the fact that generative AI has been around for decades, corporations have shown little interest in it because of its restricted capabilities. The ability to produce complex and well-spoken material at scale was showcased by ChatGPT's recent success, underscoring the potential benefits of generative AI for businesses of all sizes. Consequently, executives and business users are beginning to see complementing domains between predictive and generative AI (Dwivedi et al., 2023).

Generative AI can transform data into several formats and produce code, music, visuals, and marketing collateral. Predictive AI uses a variety of AI and machine learning (ML) approaches to produce predictions, recommendations, and decisions. In technical terms, generative AI frequently employs a variety of predictive procedures to gradually anticipate the following content unit within a result. The two realms of generative AI and predictive AI differ primarily in terms of use cases and ability to work with unstructured and structured data, respectively (Lawton, 2023).

The growing environment of generative AI offers impressive capabilities and raises important ethical concerns, particularly with data gathering, analysis, and utilization (Dwivedi et al., 2023).

Data Collection and Analysis: Generative AI, utilizing its complex algorithms, possesses an augmented capacity to gather and scrutinize extensive quantities of data, encompassing sensitive personal information. The capacity to analyze data extensively is crucial for comprehending and forecasting user behaviors and preferences. Nevertheless, it elicits apprehensions regarding privacy and the degree to which personal data is utilized without explicit agreement (Dwivedi et al., 2023).

Generative AI possesses the unique capability to generate fresh user profiles, which is known as creative profiling and microtargeting. Through the consolidation of various data sets, it has the capability to discern patterns and attributes that contribute to the development of comprehensive user profiles. This feature is especially powerful when incorporated into mobile devices, enabling the collection of data in real-time and precise targeting. Profiling of this nature can be employed for the purpose of focused advertising, exerting influence on user conduct, and even political campaigns, so giving rise to ethical concerns around manipulation and infringement of privacy (Dwivedi et al., 2023).

Generative AI has the capability to generate novel data aggregations, which in turn facilitates the creation of cutting-edge algorithms. These algorithms have the ability to detect nuanced user characteristics and behaviors, resulting in more precise profiling and microtargeting techniques. Although this ability is advantageous for customized experiences, it can also give rise to apprehensions over stereotyping, bias, and discrimination (Dwivedi et al., 2023).

Data sharing with third parties is an essential component of generative AI, particularly in products created by firms such as OpenAI. This involves sharing acquired data with other entities, including the AI developer, its clients, and subsequent parties in the hierarchy. The default data sharing technique presents substantial concerns regarding data privacy and security. Users frequently lack awareness regarding the sharing and utilization of their data by other entities, which can result in potential misuse or unwanted access (Dwivedi et al., 2023).

Important distinctions between generative and predictive AI

"In the field of artificial intelligence and machine learning, generative AI and predictive AI represent different paradigms," stated Bharath Thota, a partner in Kearney's advanced analytics practice, a worldwide strategy and management consulting firm.

The goal of generative AI is to exploit preexisting data patterns to learn and produce new and unique material, including text, graphics, and other media. It is beneficial in creative professions and innovative problem-solving, and it stimulates creativity.

Patterns found in past data are used by predictive AI to categorize or predict future events. It helps with strategy formulation and decision-making by offering practical insights.

"These approaches are not isolated and can prove to be symbiotic in developing an overarching business strategy," stated Thota. While predictive AI can predict customer demand or the market's reaction to these characteristics, generative AI can assist in the design of product features. A predictive model's training set can be improved by generative AI by creating realistic data, which will increase the predictive model's capacity (Lawton, 2023).

Predictive AI uses past data trends analysis to forecast future events by giving probability weights to the models. New data is produced by generative AI, and this data may take the shape of text or visuals. According to Inna Kuznetsova, CEO of ToolsGroup, a supply chain planning and optimization company, "think of the first [predictive AI] as a powerful analyst doing magic

with numbers, while the second [generative AI] is a creative kind -- a writer, an artist, or an assistant in research."

Generative AI is intended to produce original content in response to user input and the unstructured data that serves as its training set. These models could offer solutions, but they would be more like opinions supported by qualitative data. In the workplace, generative AI can work in tandem with predictive AI to extract value from both structured and unstructured data. Here, generative models are utilized to meet the content requirements of those processes, while predictive models are used to improve business processes and outcomes (Lawton, 2023). However, data privacy, security, and governance must be handled carefully. Furthermore, this combination could be applied to simulations, data augmentation, and synthetic data production forecasts.

Deep learning neural networks can learn complex correlations between unstructured texts and use these patterns to produce valuable outputs in response to specific text queries, which has driven the recent boom on large language models (LLMs) (Singhal, 2022). These LLMs enable generative artificial intelligence (AI) chatbots to provide a realistic and interactive user experience through text-based dialogue, unlike previous AI applications that have focused on single tasks (e.g., classification, segmentation, or prediction) with limited human-AI interaction (Aggarwal et al., 2021). ChatGPT uses LLM Generative Pretrained Transformer (GPT)-3.5 as its backend. Due to its cognitive abilities, including medical problem-solving, GPT-4 has garnered attention (Tan et al., 2023).

GPT-1: 2018 saw the release of GPT-1, which has about 117 million model parameters. 40GB of online data with an estimated word count of 600 billion were used to train GPT-1. It was feasible to translate languages, reword and create new content, and ask general queries using GPT-1. The model performed well when responding to requests for brief snippets or sentences, but it fell short of its successors in terms of understanding lengthy passages of text. (Sinha, 2023).

GPT-2: GPT-2 was designed to maintain the fundamental architectural features of its predecessor, the GPT-1 model. Compared to GPT-1, it was trained on a bigger corpus of textual data. GPT-2 was able to interpret more comprehensive textual samples efficiently since it could handle input that was twice as large as what GPT-1 could. With around 1.5 billion parameters, GPT-2 shows a significant improvement in language modelling performance. (Sinha, 2023).

GPT-2 underwent "Modified Objective Training," a procedure designed to enhance language models and guarantee that their answers retain coherence and relevance. This was accomplished by incorporating more contextual factors, such as the identification of subjects and objects and "Parts of Speech" like verbs and nouns. (Sinha, 2023).

GPT-3: When GPT-3 was released in 2020, it was praised for producing text that was more realistic and had a lot of depth. More than 570 GB of text data that was taken from the Internet were used to train it. Books of all genres, Wikipedia, BookCorpus, Common Crawl, and other resources were among the sources used. The GPT-3 model was a more developed version of the GPT-2 model, outperforming it in a number of areas. It has a maximum of 175 billion parameters and was trained on a far larger text dataset. For this reason, it was able to respond to a wide variety of prompts and inquiries and still can. But some of GPT-3's drawbacks were also emphasized heavily. It displayed a few examples of biases and errors. (Sinha, 2023).

GPT-3.5: Similar to its most recent predecessor, GPT-3.5 was trained using more than 570 GB of data from a variety of sources, including Wikipedia, the Internet, and e-books. With the same number of characteristics as GPT-3, it was published in 2022. GPT-3.5 is unique in that it complies with certain principles that were developed with consideration for the human value system. A method known as Reinforcement Learning with Human Feedback (RLHF) was used to incorporate it. GPT-3.5 was changed to guarantee correctness and veracity while also conforming to human purpose. (Sinha, 2023).

GPT-4: GPT-4, the next generation of advanced language models, is a masterwork by OpenAI. It can support ideas and thoughts, co-relate to prompts beautifully, and convert concepts into text format. Unlike its predecessors, GPT-4 is able to recognize objects in an image and provide a succinct analysis of the image's topic or theme.

Although OpenAI hasn't released a detailed study outlining GPT-4's architecture, the fact that it can produce contextually meaningful text from visual inputs implies that GPT-4 has been trained using both textual and visual data. GPT-4 processes text and images at the same time because it uses dual-stream converters. This consists of a decoder model to produce text-based outputs and a visual encoder to analyze visual input. As such, GPT-4 is particularly good at interpreting texts that include pictures, schematics, infographics, and diagrams (Sinha, 2023).

GPT-4 uses the Reinforcement Learning with Human Feedback (RLHF) method in its training process, just like earlier models. It is plausible to presume that OpenAI has amassed a broad

and substantial dataset from multiple web sites and digital sources to improve the model's knowledge base, even though they have not published the actual size and sources of the data used to train GPT-4.

The GPT-4 model has been trained and exposed to a wide variety of textual and visual data by OpenAI. As a result, it can generate polished text samples and react to cues in a human-like manner. Among its many other abilities are the following:

• Completing sentence fragments and anticipating the appropriate combination of options when given insufficient input.

• Agreeably showcasing the photographs' main notion and perfectly expressing them.

• Generally understanding jokes accurately.

• Using several programming languages to write code.

• Creating lengthy, conversational email texts and legal document provisions.

Over the past five years, OpenAI and its team of engineers and AI scientists have worked to transform GPT models into tools that can support human success in a variety of domains and problem-solving. The significant progress can be attributed to continuous enhancements in multiple areas, including as the volume and caliber of training data, the variety of data sources, the quantity of parameters, and training approaches (Sinha, 2023).

Expectations on ChatGPT-5

Undoubtedly, ChatGPT-5 will possess more size, speed, and strength. Notable Enhancements and Characteristics

• The papers generated by ChatGPT-5 are anticipated to exhibit superior quality compared to its previous versions, characterized by enhanced coherence, inventiveness, and accuracy.

• Enhancing the memory model will empower ChatGPT-5 to effectively handle and analyze various discussion threads, enabling it to get a deeper comprehension of user inputs and uphold coherence.

• Enhanced input capabilities: ChatGPT-5 possesses the capacity to handle and scrutinize different inputs, such as diverse articles or tales. Consequently, it will produce material that is more precise and pertinent by leveraging the offered information.

• Bias elimination - The problem of biased AI, which has been a worry in past models, is likely to be resolved as a more diverse group of people train the AI and it continues to learn from many sources (catapult creative media, 2023).

ChatGPT-5 could potentially be a major advancement in the development of artificial intelligence with the ability to learn autonomously and adjust to unfamiliar circumstances. The ramifications of such an advancement are extensive and have the potential to impact all facets of civilization, ranging from technology to the realm of science fiction (catapult creative media, 2023).

1.4 The Role of Data in AI Systems: Collection, Storage, and Processing

Artificial intelligence (AI) systems are heavily dependent on data because their goals include imitating human intelligence, learning from mistakes, and carrying out activities that have historically required human thought. The amount, nature, and processing of data have a critical role in the effectiveness and success of AI systems. This section explores how important data is to AI, with a particular emphasis on the gathering, storing, and processing of data. It takes into account findings from scholarly research, business practices, and technology breakthroughs (Xu et al., 2021).

In AI systems, data gathering is the initial phase of the data lifecycle. In order to train and test AI models, it entails obtaining data from many sources (MIT Sloan Management, 2022). The kind and caliber of data gathered have a big impact on how well AI systems operate (Luan et al., 2020).

Large volumes of data are necessary for AI systems to learn and develop precise predictions (MIT Sloan Management, 2022). Text documents, photos, videos, social media posts, and sensor data from Internet of Things devices are just a few of the many sources from which this data may originate (Luan et al., 2020). To ensure that the AI system can generalize successfully to new, unseen data, the data must be indicative of the problem domain the system is intended to work in (Luan et al., 2020). Data collecting in AI systems is not without difficulties, though.

Assuring the caliber of the data gathered is one of the primary concerns (Javaid, 2023). Inaccurate forecasts and biases in AI systems might result from low-quality data (Javaid, 2023). As a result, it's critical to use strong data cleaning and validation procedures when gathering data (Luan et al., 2020).

Data scientists and engineers clean and validate data. These specialists use various methods to find, fix, or remove erroneous, incomplete, or irrelevant data. Data scientists ensure data quality with their domain knowledge and analytical skills. Data anomalies and inconsistencies are found using statistical approaches and algorithms. Data engineers concentrate on data cleaning technology. They provide methods and pipelines to automatically cleanse big datasets, providing high-quality and reliable AI model data. Organizations may also use automated data cleaning technologies that leverage machine learning algorithms, although human monitoring is still necessary to preserve data quality and relevance for AI applications (Stedman, 2022).

Managing the ethical and privacy implications of data acquisition presents another difficulty because AI systems frequently need sensitive or personal data to work properly, user privacy and data protection are raised (Luan et al., 2020). As such, it is imperative to implement strict data governance rules and adhere to pertinent data protection laws (Luan et al., 2020).

In AI systems, data collection is an essential procedure. It gives AI algorithms the raw data they need to learn from, but it also poses several issues that must be resolved to guarantee the efficiency and moral conduct of these systems.

Difficulties in Gathering Data

A number of obstacles prevent AI systems from collecting data effectively.

• Data Volume and Variety: Managing a variety of datasets is made more difficult by the exponential growth of data in various formats. Complex processing and interpretation methods are needed when working with unstructured data, such as text, audio, and photographs (Sivarajah et al., 2017).

• Data Labeling and Annotation: Accurate labelling is necessary for supervised learning, which uses labelled datasets. This process can be labour-intensive and time-consuming (Label Studio, 2023).

• Data Privacy and Security: It can be difficult to collect and use data while upholding people's right to privacy and making sure that data security is compliant with laws like the General Data Protection Regulation (GDPR) (Your Europe, 2022).

• Data Collection Bias: Inaccurate or biased models may result from biases introduced during the data collection process (2022).

Techniques and Optimal Strategies

Effective techniques for gathering data are essential for developing AI systems.

• A Variety of Data Sources: Having access to data from multiple sources guarantees thorough understandings and a wider perspective of real-world situations (Aldoseri et al., 2023).

Thorough data labelling and cleaning procedures guarantee the elimination of noise and irregularities, augmenting the caliber of datasets (Aldoseri et al., 2023).

• Ethical Considerations: Following moral standards and legal frameworks (such as the GDPR) when gathering data guarantees ethical and legal procedures (Aldoseri et al., 2023).

• Continuous Iteration and Improvement: To increase the caliber and applicability of datasets, the data gathering process is iterative and necessitates ongoing assessment, feedback assimilation, and improvement (Aldoseri et al., 2023).

Scientific research, notably behavioral studies and machine learning, increasingly uses microwork platforms like Amazon Mechanical Turk for data cleaning and processing. Microworkers in countries like the US and India provide important Human Intelligence Tasks (HITs) for data gathering and processing. Compensation and informed consent are major ethical concerns when using microworkers for research. Microwork platforms include advantages including low-cost broad sampling and good project management. For instance, microworkers may experience pressure to finish tasks and overlook informed consent documentation (Molina et al., 2023).

Fair compensation for micro workers is debated. Not all platforms, like Click worker, propose paying close to the country's minimum wage. Many microworkers do these jobs to make ends meet or augment other income, sometimes for modest salaries. Under pressure, less experienced workers may avoid assignments, which might impact their success score and eligibility for higher-paying duties (Molina et al., 2023).

Fair compensation is complicated since individuals with better organization and technology typically take on well-paying jobs and drive out less skilled ones. Researchers using microwork platforms should understand these dynamics and pay microworkers at least the minimum wage, serving as temporary employers. This strategy recognizes the financial demands of microworkers and the ethical responsibilities of researchers (Molina et al., 2023).

In AI systems, data collection is more than just accumulation—it serves as the foundation for AI models. The difficulties, procedures, and moral issues around data collection play a significant role in determining how efficient, just, and trustworthy AI systems are. Research from academia and business emphasizes how important it is to have thorough, varied, and morally sound data collection procedures in order to support the creation of accountable and effective AI systems.

Data storage

In AI systems, this is the second phase of the data lifecycle. It entails keeping the gathered data in a way that makes efficient access and retrieval possible. The performance of AI systems can be greatly impacted by the data storage option selected. Large data volumes are frequently processed by AI systems, which makes the adoption of scalable and effective data storage solutions necessary. To meet the high data throughput demands of AI workloads, these solutions must facilitate quick read and write operations (Mazumdar et al., 2019).

Data security and integrity must also be guaranteed by data storage solutions for AI systems. This entails putting policies in place to shield data against corruption and unwanted access. Furthermore, data storage systems must abide by data protection laws, especially when handling sensitive or personal data (Mazumdar et al., 2019).

Importance of AI Data Storage

AI systems require effective data storage for a number of reasons.

Scalability: In order to train and learn continuously, AI models need large amounts of data. Good storage options enable the scalability required to handle the data's exponential expansion (Barmer & Dzombak, 2021).

Accessibility and Retrieval: AI systems can quickly retrieve data during the training and inference phases thanks to storage techniques that facilitate rapid and easy access to datasets (Barmer & Dzombak, 2021).

Data Versioning and Management: Reproducibility, validation, and refinement of models depend on the maintenance of many dataset versions and the lifecycle management of those versions (Talia, 2019).

Real-Time Processing: AI systems that need to make decisions quickly must have storage options that allow for real-time access to data (Talia, 2019).

Techniques for AI System Storage

AI systems use a range of storage techniques adapted to certain needs:

• Databases and Data Warehouses: Data warehouses and relational and non-relational databases store and organize structured and semi-structured data and offer powerful analytics and querying features (Younus, 2023).

• Distributed File Systems: Often utilized in big data scenarios, systems such as Amazon S3 and the Hadoop Distributed File System (HDFS) provide scalable storage alternatives for large-scale data processing and storing (Talia, 2019).

• Object Storage: Offering flexibility and scalability, object-based storage—like Amazon S3 or Azure Blob Storage—accommodates unstructured data, including documents, videos, and photographs (Talia, 2019).

• In-Memory Databases: These databases improve performance for AI applications that require real-time processing by optimizing data retrieval speeds by storing datasets in memory (Younus, 2023).

Difficulties with AI Data Storage

There are still a number of issues with data storage for AI systems.

• Scalability and Performance: Managing and processing massive amounts of data while guaranteeing prompt access and processing power presents formidable obstacles (Barmer & Dzombak, 2021).

• Data Security and Privacy: Preserving data integrity, protecting stored information from unwanted access, and making sure laws like GDPR are followed are important issues (Talia, 2019).

• Cost and Resource Allocation: According to Younus (2023), effective data storage systems necessitate large expenditures for infrastructure, upkeep, and resource allocation.

• Data Redundancy and Backup: To avoid data loss and preserve continuity, it's critical to ensure data redundancy and to put strong backup plans in place (Younus, 2023).

New Developments and Prospects

A number of significant trends are starting to emerge regarding the future of data storage in AI systems. To cut latency and allow real-time processing at the network edge, one of these strategies involves using edge computing and storage for AI applications (Deng et al., 2020; Carvalho et al., 2021). This strategy reduces the quantity of data that needs to be transported across the network and improves performance by moving computation and storage closer to the data source (Deng et al., 2020; Carvalho et al., 2021).

The creation of a hybrid infrastructure through the combination of cloud-based services with on-premises data storage is another noteworthy trend (Khan et al., 2021). Organizations can take advantage of the advantages of both on-premises and cloud storage with this strategy's scalability, flexibility, and affordability (Khan et al., 2021).

Furthermore, an increasing emphasis is being placed on putting advanced encryption techniques and security measures in place to safeguard stored data from cyber-attacks and

guarantee adherence to data protection laws (Zhang et al., 2021; Sarker et al., 2021). This is especially crucial in light of the growing number of cyberthreats and the strict data protection laws that are in place in many countries (Zhang et al., 2021; Sarker et al., 2021).

For AI systems to operate and execute well, effective data storage is essential. To develop resilient, scalable, and secure storage systems that serve the changing needs of AI applications, it is essential to comprehend the significance of storage approaches, difficulties, and upcoming trends (MIT Sloan Management, 2022). Organizations may guarantee that their AI systems are prepared to handle the data-intensive jobs of the future by keeping up with these trends and implementing them into their data storage strategies (Luan et al., 2020).

Data processing

Data processing is the third phase of the data lifecycle in AI systems. It involves formatting raw data so that artificial intelligence (AI) systems can understand and use it. Often, this involves several steps, including dimensionality reduction, feature extraction, data cleaning, and normalization (Chubb et al., 2021). Data cleaning includes addressing missing numbers, removing or correcting erroneous data, and managing outliers. This is crucial since inaccurate data can lead to biases and incorrect predictions in artificial intelligence systems (Hosseinzadeh et al., 2021).

Scaling numerical characteristics to a standard range such that no feature's scale governs the learning process is known as normalization. This is important since it makes sure certain features don't unduly alter the model's predictions because of how big they are (Seo et al., 2021). Unprocessed data is transformed into a set of features during feature extraction, which may then be used to represent the data in a useful way. Finding characteristics or patterns in the data that are relevant to the ongoing activity is usually required for this. For example, color histograms, edges, and corners could be characteristics in picture identification tasks (Zhang et al., 2022).

Dimensionality reduction is the process of reducing the number of features in the dataset in order to mitigate the negative impacts of dimensionality. This could improve AI systems' functionality and efficacy. Principal Component Analysis (PCA) and t-Distributed Stochastic Neighbor Embedding (t-SNE) are two common techniques used to do this (Scicluna et al., 2023).

Data processing is fundamental to artificial intelligence systems and is significant in many respects. It makes it simpler to extract relevant information from raw data in order to discover patterns, correlations, and insights that are essential for training AI models. This process is known as information extraction, per Artificial Intelligence (AI): What It Is and Why It Matters (n.d.).

Furthermore, data processing is involved in feature engineering, which is the process of transforming and selecting attributes from unprocessed data that significantly influence the effectiveness and predictive capacity of models (Artificial Intelligence (AI): What It Is and Why It Matters, n.d.). Furthermore, progressively enhances the models' performance by preparing datasets for model validation and training (Artificial Intelligence (AI): What It Is and Why It Matters, n.d.). AI applications that need to make judgments quickly might benefit from data processing's speed and agility since it processes data in real-time (Artificial Intelligence (AI): What It Is and Why It Matters, n.d.).

AI systems process data effectively using a range of techniques. They comprise data cleaning and preprocessing. Microworkers, mainly from third countries, frequently participate in this labor under circumstances marked by meager salaries and restricted entitlements, devoid of the advantages of vacations, labor unions, or other types of worker safeguards. (i.e., removing noise, filling in missing values, normalization, and transformation) in order to ensure the quality of the data before training the model. Principal Component Analysis (PCA) and t-Distributed Stochastic Neighbor Embedding (t-SNE) are two dimensionality reduction methods that maintain relevant information. Depending on the needs of the AI application, both batch processing—which processes data in fixed-size batches—and stream processing—which processes continuous input in real-time—are employed. Large datasets are processed efficiently over distributed systems using parallel computing paradigms like Spark or MapReduce (Tandon, n.d.).

There are still a lot of challenges with data processing for AI systems, though. Ensuring data quality across the processing pipeline, avoiding bias, and maintaining integrity face numerous challenges. To effectively manage computational complexity, processing large-scale datasets requires a strong computational infrastructure and the right techniques. If memory, processing power, or computational resources are limited, data processing tasks might not be as scalable or efficient. The handling of ethical concerns and ensuring compliance with regulations (such

as GDPR) concerning data usage and privacy further complicates data processing (Tandon, n.d.).

Novel Patterns and Opportunities for the Future

The future of Generative AI is its incorporation into a diverse range of devices, such as mobiles, to greatly enhance user interaction and accessibility. This expansion is anticipated to transform the way we engage with AI systems, facilitating more accessibility to advanced AI capabilities in our everyday activities. The practice of eliminating the tedious, repeated steps required in creating machine learning models is known as automated machine learning, or AutoML. For data scientists, analysts, and developers, it allows the creation of machine learning models at scale, with high productivity and efficiency, all the while preserving model quality (Express Analytics, 2022).

Federated Learning is a machine learning technique that enables the training of an algorithm across multiple decentralized data sources without requiring data exchange. It enables security, privacy, and heterogeneous data access (Federated Learning, 2023).

XAI, or explainable AI: Applications and techniques of artificial intelligence (AI) that enable people to understand the results of the solution are referred to as XAI. Businesses use it to increase people's comprehension of the workings of a model (IBM, n.d.).

Data processing is a crucial step in artificial intelligence systems that significantly affects the system's operation. Therefore, it is essential to use appropriate data processing techniques that align with the requirements of the specific AI task. By managing these processes well, we can build AI systems that are more accurate, efficient, and fair.

1.5 Rise of ChatGPT: a New Turn?

The emergence of ChatGPT represents a giant milestone inside the realm of conversational AI, signalling a new era in human-pc interplay. ChatGPT, advanced through OpenAI, is an advanced language model primarily based on the GPT (Generative Pre-trained Transformer) structure. Its upward push indicates a transformative shift in how we understand and engage with AI-powered conversational structures. ChatGPT's skills lie in its capability to understand,

system, and generate human-like text responses, enabling it to preserve contextually applicable conversations throughout diverse topics and domains. It leverages a full-size amount of pre-existing text records to examine patterns, context, and language nuances, allowing it to generate coherent and contextually suitable responses to user queries or prompts (Marr, 2023).

The arrival of ChatGPT and similar language fashions has added forth numerous opportunities and applications throughout various fields, which includes customer service, content technology, language translation, education, and extra. Its capability to realise and generate human-like textual content has redefined human-computer interaction, supplying greater herbal and intuitive interfaces for customers to have interaction with AI systems. However, the rise of ChatGPT also raises discussions around moral concerns, statistics privateness, and the responsible deployment of such powerful AI models. As these systems end up more familiar in various packages, ensuring they are used ethically and responsibly will become crucial (Dwivedi et al., 2023).

In essence, the ascent of ChatGPT represents a turning point in the evolution of conversational AI, marking a shift in the direction of extra superior and human-like interactions between people and machines. As this technology continues to conform, its effect on various elements of our lives and society as a whole is expected to develop, starting new horizons for innovation and collaboration at the same time as necessitating a careful method in the direction of their moral and responsible use.

Something happened in December 2022 that completely changed the way we search for, use, and store information. The release of ChatGPT was well received right away. Though many were taken aback by it, ChatGPT is the outcome of several advancements in the application of chatbots, often known as chat robots, or computer programs that mimic and process written and spoken human conversations. This is coupled with Large Language Models (LLMs), which gather copious amounts of data from multiple sources, such as Wikipedia, open forums, and websites devoted to programming, such as tutorials and Q&A pages. LLMs use this massive quantity of data to improve their responses (Balch, 2023).

ChatGPT has advantages as well as disadvantages. These tools are viewed as a shortcut and a threat to the entire learning spectrum by several academics. Furthermore, it's possible that children won't acquire the abilities needed for critical thinking and unique thought. Nonetheless, some educators are excited about the potential for brainstorming, overcoming

writing obstacles, and producing first drafts—basically getting pupils ready for a future in which these tools are now commonplace. Above all, the one thing academics cannot afford to do is to turn a blind eye to what's going on (Balch, 2023).

It is true that word processors, spell checks, grammar checkers, autocompletion, and predictive text software are logical predecessors of ChatGPT. But there's a crucial distinction between AI-generated writing and machine learning (ML), and predictive text systems. A subset of artificial intelligence (AI) programs, predictive text programs are typically more focused on one task, whereas AI programs can do a larger range of activities. The quality of the input, or what has been previously referred to as "GIGO," or garbage in-garbage out, is the crucial factor, though (Balch, 2023).

Like every new development, there are frequently drawbacks in addition to benefits. In a study headlined "Professors published a paper on AI with a 'plot twist' — ChatGPT wrote it," Wu (2023) brought this to light. Three peer reviewers who said they thought the manuscript was written by a person approved the submission. They discovered other mistakes after it was discovered that ChatGPT was the source of the document. According to research, 32% of the academic abstracts written by ChatGPT made it past the peer review process, despite the reviewers being informed that some of the abstracts were fraudulent (Balch, 2023).

Numerous tools can lessen the effort of proofreading material for grammatical, spelling, and citation problems; nevertheless, these applications differ from ChatGPT in that ChatGPT generates entire texts. According to the most current study, ChatGPT deceived scientists over one-third of the time. But recently, AI detection features are included in AI detection programs such as Turnitin and GPT-2 Output Detector (Balch, 2023).

1.6 Importance of Data Processing in Automated Decision-Making

The process of employing computer systems or algorithms to make decisions without direct human interaction in each decision is known as automated decision-making. These choices are made using predetermined guidelines, reasoning, or computer models that evaluate information and data to make judgments or take action (Lukács & Váradi, 2023).

In this situation, automation seeks to expedite the process of making decisions by employing algorithms and computing power to quickly examine vast amounts of data. Systems for automated decision-making are present in many different sectors and industries, such as manufacturing, transportation, healthcare, and finance. They are used to improve decision-making processes' effectiveness, precision, and consistency (Ali et al., 2023).

An essential component of automated decision-making is data processing. It entails gathering, modifying, and analysing data in order to get insightful knowledge that can guide decision-making. Decision-makers are able to decrease ambiguity and base judgments on certain insights and facts thanks to this procedure (MSI-NET, 2016).

Furthermore, by producing precise decisions and accurate predictions, data processing aids in risk management. This can assist in seeing possible problems early on and taking action to mitigate them. Because efficient data processing increases production and efficiency, cost savings might also result from it. It can also assist in locating places where cost-saving resource optimization is possible. Decisions can be based on facts thanks to data processing, which lessens the need for conjecture. Decision-making as a result may become more precise and efficient. Decision-makers can be more pro-active by using data processing to spot patterns and anticipate outcomes. Proactive decision-making is made possible by this, and improved results may result (Soori et al., 2023).

Decision-making bias can be lessened with the aid of data processing. Decisions can be made based on facts rather than preconceived notions by using data. Strategic decision-making is made possible by data processing, which offers insights into patterns and trends. Making strategic decisions that support the objectives of the company can be aided by this. Decision evaluation and tracking are made simple with the help of data processing. This can assist in determining the success of decisions and making the required corrections. Decision-making becomes fluid and nimble with the help of data processing. Decisions made using it can be made more quickly and adaptably using real-time data (Analytics, 2023).

Decision-making is empowered by data processing, which delivers precise and fast information. Better control over decisions and their results is made possible by this. Statistics and patterns produced by data processing can offer insightful information. Making wise decisions can be aided by these observations.

Analytics, which can offer deeper insights and support in making better decisions in the future, is made possible by data processing. Decision-making becomes more objective and transparent

as a result of data processing. Decisions can be made transparently and impartially by using data (Calzon, 2023).

Data processing is a key component of automated decision-making and is essential to the effectiveness and functionality of these systems in order to give the user the sensation of interacting with a real human person. Data processing is crucial for automated decision-making in a number of important ways.

• Insight Generation: When raw data is handled well, insightful information is produced. Systems are able to identify patterns, correlations, and trends thanks to data processing, which converts large and frequently complicated datasets into intelligible and useful information. These realizations are essential for directing and educating automated systems' decision-making processes.

• Enhanced Accuracy: Data processing entails cleaning up errors, removing redundant information, and reducing noise in datasets. This curation guarantees the accuracy and dependability of the data that automated systems utilize to make decisions. Consequently, these systems produce more accurate and reliable decisions (Dhanashree, 2023).

• Decision-Making Models: The creation of decision-making models heavily relies on data processing. For these models to work well, processed data is necessary, regardless of whether they are rule-based or use sophisticated machine learning algorithms. By using data processing to optimize and fine-tune these models, it is ensured that they are capable of making well-informed decisions (Dhanashree, 2023).

• Adaptability and Learning: Machine learning techniques, which require constant data processing, are commonly included into automated systems. Over time, these systems can adjust and enhance their decision-making abilities by examining fresh data and trends. Systems can improve their predictive abilities and learn from previous experiences through the iterative process of data processing.

• Speed and Efficiency: Quickly turning raw data into useful insights, efficient data processing expedites the decision-making process. Large volumes of data can be processed quickly by automated systems, allowing for prompt action depending on the information gathered (AppleTech, 2023).

• Risk Mitigation: Identification and mitigation of potential dangers associated with automated decision-making are facilitated by comprehensive data processing. These systems reduce the

risks associated with erroneous or defective data by thoroughly evaluating the data in order to identify errors, biases, or abnormalities prior to making choices (AppleTech, 2023).

• Customization and Personalization: By analyzing various datasets, automated systems are able to produce solutions that are both specialized and unique. For example, data processing in marketing makes it easier to create personalized suggestions based on particular customer interests and habits.

• Governance and Compliance: Data processing makes sure automated systems abide by applicable laws and regulations. Data processing include procedures like data anonymization, encryption, and compliance with privacy laws like GDPR, which guarantee that systems function within the bounds of the law.

In conclusion, data processing is the cornerstone that supports the development of dependable and effective automated decision-making systems. It turns unprocessed data into insightful knowledge that helps these systems make quick, precise, and well-informed judgments. Robust data processing is essential to the efficient operation of automated decision-making systems because it reduces risks, facilitates compliance, and improves overall performance (Dhanashree, 2023).

2. GDPR and EU Data Protection

2.1 The EU Approach to Artificial Intelligence Governance

The main focuses of the EU's approach to AI governance are the social, legal, and economic facets. The EU wants to foster AI development and use within its borders, transforming the region into a hub for AI from the lab to the marketplace. Additionally, the EU wants to make sure AI benefits people and advances society. The European Union is trying to develop a strategic leadership in industries with a significant impact (European Approach to Artificial Intelligence, 2024). A national and European governance framework has been proposed by the EU. The European Union seeks to guarantee that AI is created and applied in a manner that upholds essential principles and rights, such as confidentiality, equality, and openness (European Commission, 2023).

A number of legislative actions that the EU has introduced will help develop reliable AI. These include a civil liability framework that adjusts liability laws to the digital age and artificial intelligence, a European legal framework for AI that addresses fundamental rights and safety risks unique to AI systems, and an update to sector-specific safety laws (such as the Machinery Regulation and General Product Safety Directive) (European Commission, 2023).

Furthermore, the EU is creating initiatives to improve access to high-quality data, which is essential for creating dependable, effective AI systems. The EU Cybersecurity Strategy, the Digital Services Act, the Digital Markets Act, and the Data Governance Act (European Commission, 2023) provide the framework required to construct such systems.

The EU is making significant investments in AI R&D. The EU intends to invest €1 billion annually on artificial intelligence through the Horizon Europe and Digital Europe projects. Over the course of the digital decade, it will mobilize more capital from both the private sector and the Member States to reach a yearly investment volume of €20 billion (European Commission, 2023).

The EU Approach to Artificial Intelligence Governance: Fostering Excellence and Trust

As artificial intelligence (AI) rapidly transforms industries and society, the European Union (EU) is trying to regulating this sector in advance compared to all the other nations. Therefore, EU has developed an overall strategy for AI and it is discussing a proposal of regulation (AI Act). With regard to the first, it has taken a proactive approach for ensuring responsible and

trustworthy AI development and deployment. The EU's strategy to govern AI is centered on striking a balance between promoting innovation and safeguarding fundamental rights, ethics, and human values (European Commission, 2023).

Key Principles of EU AI Governance

The EU's AI governance framework should be guided by a set of core principles that aim to ensure the ethical and responsible development and use of AI. These are:

Human-centricity: AI should be designed to benefit society and individuals, fostering human autonomy, dignity, and well-being.

Safety: AI systems should be developed and deployed in a safe and secure manner, minimizing the risk of harm to individuals, society, and the environment.

Transparency: AI systems should be transparent and understandable to both users and regulators, allowing for accountability and informed decision-making (Antonini, 2023).

Accountability: Organizations developing and deploying AI systems should be accountable for their actions, ensuring that AI systems comply with applicable laws and ethical norms.

Non-discrimination: AI systems should not discriminate on the basis of protected characteristics such as race, gender, religion, or sexual orientation.

Robustness: AI systems should be robust and resistant to adversarial manipulation, ensuring that they behave as intended and do not produce unintended consequences.

Privacy and data protection: AI systems should comply with relevant data protection and privacy regulations, respecting individuals' right to privacy and data protection.

Explainability and interpretability: AI systems should be explainable and interpretable to a reasonable extent, allowing for the understanding of their decision-making processes and the identification of potential biases or risks (Madiega, 2019).

A Risk-Based Approach

The AI Act is a regulation of the European Union on artificial intelligence (AI) that is it is final stage approval. It is the first comprehensive law on AI by a major regulator at the worldwide level. The EU AI Act is intended to ensure the safety of AI systems on the EU market and provide legal certainty for investments and innovation in AI, while minimizing associated risks to consumers as well as compliance cost for providers. The EU AI Act prominently features a risk-based approach, defining four different risk classes, each of which covering different use cases of AI systems: minimum or no risk, severe risk, limited risk, and unacceptable risk. While some AI systems are banned entirely, barring narrow exceptions, the EU AI Act imposes specific obligations on the providers and deployers of so-called high-risk AI systems, including testing, documentation, transparency, and notification duties (Hainsdorf et al., 2023).

In the marathon trilogue negotiations between the EU Commission, Parliament and Council leading to political agreement, the list of prohibited and high-risk AI systems, including the classification of and exceptions for biometric identification systems, as well as the enforcement structure and mechanisms of the EU AI Act were amongst the most contentious issues. Furthermore, the regulation of so-called general purpose AI models, like foundation models and generative AI, which was first introduced in the EU Parliament's negotiating position from June 2023, was fiercely debated in the final stages of the trilogue and deemed particularly controversial due to fears that excessive regulation could hinder innovation and harm European companies (Hainsdorf et al., 2023).

Following the political agreement between the Commission, Parliament and Council, the EU AI Act will shortly be officially adopted and published in the EU's Official Journal to enter into force. The majority of the Act's provisions will apply after a two-year grace period for compliance. However, the regulation's prohibitions will already apply after six months and the obligations for GPAI models will become effective after 12 months. By joining to the AI Pact, which will be launched by the European Commission, AI developers can commit to

implementing key provisions of the EU AI Act voluntarily prior to the respective deadlines. During the grace period, much work will need to be done at both Member State and Union levels to establish effective oversight structures and publish guidance on the implementation of the EU AI Act (Hainsdorf et al., 2023).

With the imminent entry into force of the landmark EU AI Act, the EU seeks to position itself at the forefront of responsible AI development and to ensure that governance keeps pace with innovation in this rapidly evolving sector. Given the stated aim of the EU AI Act in ensuring that AI systems in the EU are "safe, transparent, traceable, non-discriminatory and environmentally friendly", 44 the efficacy of the EU AI Act will no doubt be compared to and measured against approaches adopted in other leading AI nations such as the UK and the US, and international efforts to set out guardrails for AI such as at the G7, G20, OECD, Council of Europe, and the UN (Hainsdorf et al., 2023).

The core premise of the EU, which informs the AI Act, is that Europe will adopt AI globally as long as reliable technologies are developed. According to the European Commission, fostering trust necessitates appropriately safeguarding individuals' safety and fundamental rights, which can be accomplished by setting limits on the applications and motivations for AI systems. But these restrictions shouldn't be so onerous that they prevent the very innovation they are meant to encourage. (Gaumond, 2021).

Ensuring an ideal balance between safeguarding individuals' safety and fundamental rights, while minimizing obstacles to the progress of artificial intelligence, is a significant challenge. The AI Act has adopted a risk-based strategy in order to find a compromise. The policy restricts specific impermissible applications of AI, imposes stringent regulations on certain uses that pose substantial hazards, and remains silent on low-risk or risk-free applications, except for promoting the implementation of norms of conduct. (Gaumond, 2021).

The European Union seeks to guarantee that AI is created and applied in a manner that upholds essential principles and rights, such as confidentiality, equality, and openness (European Commission, 2023). Therefore, as said, four categories of risk are identified by the AI Act that represent the main novelty of the European regulation proposal. These levels address a minimum or no risk, a severe risk, a limited risk, and an unacceptable risk.

These four levels make up the pyramid that is used to symbolize the gradation of hazards.

Minimal Risk: the technologies at the base of the pyramid pose little to no risk. This includes any current AI systems that aren't specifically covered in the proposal. It includes "the vast majority of AI systems currently used in the EU," according to the Commission.

Artificial intelligence (AI)-powered video games and spam filters, for example, are not going to be subject to additional legal restrictions. But even though the act won't explicitly govern these AI systems, Article 69 may nonetheless have an impact on how they grow. The creation of rules of behaviour to govern these technologies is particularly encouraged by this clause. The Commission believes that by implementing these soft-law regimes, it may encourage the voluntary adoption of standards like robustness, openness, and human oversight—principles that would otherwise only apply to extremely dangerous artificial intelligence systems.

Limited Risk: both high-risk and low-risk technologies are included in this porous layer. This type of AI systems is distinguished by the fact that they provide particular transparency challenges, necessitating additional disclosure requirements.

These particular transparency requirements apply to three sorts of technologies: deepfakes, AI systems designed for human-to-human interaction, and AI-enabled emotion recognition/biometric classification systems (Gaumond, 2021).

People living in the European Union have the right, according to Article 52 of the AI Act, to know whether the video they are watching is a deep fake, whether the person they are speaking with is a chatbot or voice assistant, and whether their biometric data is being used by an AI system for emotion recognition analysis or biometric categorization. As a result, limited-risk AI systems need to be open about being artificial. (Gaumond, 2021).

There are a few exclusions, though. Artificial intelligence (AI) systems that are legally permitted to identify, stop, look into, or prosecute criminal offenses are exempt from the transparency requirements. However, emotion recognition technologies are not exempt, and it is always required to disclose their use. Many observers believe that emotion systems should be outlawed outright since they are based on poor research; simply requiring them to maintain transparency is insufficient (Gaumond, 2021).

High-Risk: this group of technologies will be subject to a number of novel and onerous requirements.

High-risk AI systems come in two varieties. Under sectoral regulation, the first group includes those that are integrated into products and act as safety components for those products that are

already subject to third-party inspection. This covers safety elements for toys, medical equipment, and machinery. Sector-specific laws governing these systems will be modified to incorporate the responsibilities outlined in the proposed regulation. Therefore, compliance with the AI Act will be necessary for an AI system to be in conformity with sectoral regulations (Gaumond, 2021).

Standalone artificial intelligence systems belong to the second type. According to the draft legislation, the use of stand-alone systems in some locations is regarded to be high-risk. Article 7 permits modifications in the subsequent domains: biometric identification and classification of individuals.

• Oversight and administration of vital infrastructure (e.g., water, gas, heating, and electricity supply)

• Provision of education and vocational training

• Facilitation of employment, workers' management, and opportunities for self-employment

• Ensuring access to and enjoyment of essential private services, public services, and benefits (e.g., credit and emergency first response services)

• Maintenance of law and order

• Management of migration, asylum, and border control

• Administration of justice and democratic procedures

The proposal establishes a Conformité Européenne (CE) marking procedure to lessen the risk posed by these systems. Many products sold in Europe bear the CE mark, a badge that indicates that the product satisfies strict safety, health, and environmental protection standards set by the EU. This certification will be necessary for high-risk AI systems to reach the European market. They will also need to adhere to five requirements, which are strongly influenced by the main ideas from the previously described ethics rules, in order to receive that mark.

These responsibilities are summarised below (Gaumond, 2021).

Data and data governance: high-risk AI systems need to be created with high-quality datasets, including those that are utilized for algorithm testing, validation, and training. This quality requirement in practice means that the data must be comprehensive, accurate, representative,

and relevant. Additionally, it is essential to follow sound data management procedures, which include paying close attention to biases, data gaps, and data deficiencies.

Transparency for Users: To guarantee appropriate usage of AI systems, those that build high-risk AI systems (referred to as "providers" under the proposed law) are required to disclose specific kinds of information. For instance, suppliers are required to submit details regarding the features, capacities, and restrictions of the AI system, the reason for which it is being used, and the data required for its upkeep and management.

Human oversight: high-risk AI systems have to be built with human oversight in mind. Crucially, it does not imply that people have to fully comprehend the process by which AI systems — often referred to as "black boxes" — arrive at a judgment. Rather, the emphasis lies on a person's ability to comprehend the primary constraints of AI systems and recognize these flaws in a specific system. Monitoring for automation bias issues, identifying abnormalities or dysfunctional indicators, and determining whether to overrule an AI system's judgment or to activate the "kill switch" in the event that a system endangers people's safety or fundamental rights are all part of the supervisory responsibilities.

Accuracy, robustness and cybersecurity: a level of accuracy, resilience, and cybersecurity appropriate to their intended use must be attained by high-risk AI systems. AI system providers will have a duty to share accuracy figures with users of their services. Technical solutions to stop cybersecurity problems like data poisoning will also be necessary, as will back up or fail-safe procedures to guarantee enough robustness.

Traceability and auditability: high-risk AI system providers need to create technical documentation with the data needed to evaluate whether or not their products meet the other aforementioned requirements. Annex IV of the AI Act has a comprehensive list of items that need to be documented, including risk management plans and data management procedures. Furthermore, the plan mandates that occurrences (logs) be automatically recorded.

Providers are able to fulfill these requirements by self-evaluating; however, there is a more rigorous approach for remote biometric identification systems. The supplier of an AI system completes an EU declaration of conformance after the compliance assessment is finished, at which point it can apply the CE marking of conformity and join the European market (Gaumond, 2021).

Unacceptable risk: Article 5 governs systems in this category. It forbids the use of AI in specific contexts and domains. This category includes four different sorts of technologies: real-time biometric identification systems, dark-pattern AI, manipulation, and social scoring (Gaumond, 2021).

The ban on social score appears to be a direct challenge to China-style AI systems that are allegedly used to track nearly every element of people's lives in order to determine their reliability, from their purchasing history to their tendency of jaywalking. As Jamie P. Horsley the social credit system in China has not been accurately portrayed by Western countries since the technology in use today are "nowhere close to Black Mirror fantasies." However, this is unimportant. This prohibition has symbolic intent. The EU has made it plain that its view of AI is one that preserves fundamental rights by declaring that public authorities cannot use AI to judge people's reliability (Gaumond, 2021).

Another total ban targets a few AI systems that exhibit black patterns. According to the plan, gadgets that use subliminal techniques that work outside of a person's conscious knowledge to materially affect their behaviour in a way that could jeopardize their physical or psychological well-being will be prohibited by the EU. Article 5(1)(a) prohibits, for example, making an inaudible sound in a truck driver's cabin in order to induce him to travel farther than is safe and healthy (Gaumond, 2021).

Furthermore, prohibited under the proposal is "manipulation." According to the proposal, this involves AI systems that "exploit any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, in order to materially distort a person's behavior within that group in a way that causes or is likely to cause that person or another person physical or psychological harm." Under Article 5(1), a doll with an integrated voice assistant that invites a juvenile to participate in more risky activity would be forbidden (b) (Gaumond, 2021).

Finally, Article 5 forbids law enforcement from using real-time remote biometric identification systems, or facial recognition technology used for identification, in areas that are open to the public. Even though it falls into the unacceptable risk category, there isn't a complete ban. Instead, it's a component of a larger political agreement that's covered in the section below. However, the rules are anticipated to have a big impact on American IT developers because the current legislation applies to all high-risk AI systems that are placed on the European market and all high-risk AI systems whose output is used in the union (Gaumond, 2021).

In fact, American tech developers will frequently have to abide by European regulations because of the Brussels effect—a phenomena where the European Union tries to impose its own legislation to foreign actors through extraterritoriality measures. If you don't, you risk facing severe financial consequences. Failing to comply with the unacceptable risk prohibitions or data governance criteria can result in fines of up to 30 million euros or the equivalent to 6% of a company's global annual turnover. Penalties for breaking other AI Act rules can reach 20 million euros, or 4% of worldwide sales annually (Gaumond, 2021).

The Role of Ethics in AI Governance

The EU has a dynamic approach to AI governance, which will develop further as the technology advances and its effects on society become more profound. In order to shape a future where AI helps society and individuals while respecting fundamental rights and ethical principles, the EU must remain committed to guaranteeing responsible and trustworthy AI development and deployment (Montgomery, 2023).

The EU will have to modify its governance structure as AI develops in order to meet new issues and make sure that AI deployment and development are consistent with its ideals. In this regard, important difficulties consist of:

i) Addressing algorithmic bias and discrimination - According to Chen (2023), AI systems have the potential to reinforce or magnify preexisting biases in data or algorithms, resulting in unjust or discriminating outputs.

ii) Improving interpretability and explainability - Building accountability, transparency, and trust in AI systems requires providing insightful justifications for AI judgments.

iii) Cyber threat protection - AI systems are susceptible to cyberattacks, which can result in data leaks, tampering, or abuse (Center for Security and Emerging Technology, 2023).

iv) Ethically handling AI in delicate domains - privacy, autonomy, and social justice are among the sensitive areas where AI is being used, including healthcare, education, and criminal justice.

The EU is addressing these challenges through the implementation of the AI Act that has just been approved by EU and the development of ethical guidelines and supporting initiatives. The EU's approach to AI governance emphasizes transparency, accountability, and human oversight, ensuring that AI systems are developed and deployed in a way that benefits society

and individuals while respecting fundamental rights and ethical principles (European Parliament, 2023)

2.2 Overview of General Data Protection Regulation (GDPR)

The fact that AI, especially in its ultimate version (generative Artificial Intelligence), largely bases its effectiveness on an uncommon ability of collecting and processing a huge amount of data in real time, makes the regulation on data strategic in the development of AI. This fact makes the GDPR, the General Data Protection Regulation (2016/679), that regulates data privacy of the European citizens in the EU, a crucial tool of governance together with the AI Act in the field of artificial intelligence.

The GDPR was adopted on April 14, 2016 and entered into force on May 25, 2018. Basically, it implements the right to data protection established by Article 8(1) of the EU Charter of Fundamental Rights, with an articulated net of rights and principles all centred on a basic idea: the principle of "Privacy by design" which is a framework that advocates for integrating privacy features into the design and development of products, services, and systems that process data. It thus emphasizes proactive measures to anticipate and address privacy concerns from the outset rather than reacting to them later. This approach ensures that privacy protections are built into the construction of the design, making it easier to protect the individuals' privacy and comply with regulations throughout the lifecycle of the product or service. By prioritizing privacy in the design process can also enhance user trust, mitigate risks, and demonstrate their commitment to respecting individuals' privacy rights. It regulates personal data beyond the EEA and EU. The GDPR aims to improve data privacy and streamline global business laws.

The nomenclature is streamlined and the Data Protection Directive 95/46/EC is replaced by introducing a common unique regulation among Member States in order to protect the Internal European Market and the rights of the European citizens. The aim was to i) ensure a single market of the circulation of data able to foster the data-based business in Europe and ii) avoid the the phenomenon of elusion of the stricter regulations of privacy, and iii) protect the rights of the European citizens in Europe and, due to extraterritoriality force, abroad.

The GDPR is an extensive change of data protection laws that seeks to ensure the necessary level of protection for the rights of individuals whose data is being processed (The European

Data Protection Supervisor, 2023). It had advantages for both enterprises and individuals. Individuals have been granted special rights, like the right to consent, to information, to access, the right to be forgotten etc. These rights empower individuals to have greater control over their personal data (The European Data Protection Supervisor, 2023). The GDPR has played a crucial role in influencing the worldwide discourse on data privacy and has served as a catalyst for the enactment of comparable laws in other nations. The General Data Protection Regulation (GDPR) is a significant measure aimed at empowering individuals to exercise greater authority over their personal data, while also imposing responsibility on enterprises for the collection and handling of such data.

The GDPR is based on seven fundamental principles that are aimed to implement a right that is the heart of the whole regulation: the principle of "Privacy by design", namely the data controller must conform to the principle of data protection through the implementation of design and default settings (principle of "Privacy by design"). These seven principles are:

1. Lawfulness, fairness, and transparenc - The collection and the processing of data must be lawful, namely it must comply with the provisions of the GDPR such as the consent of the natural person.

In general, a processing of data becomes illegal whenever there was no consent for personal data, when the data are processed for a purpose different from that communicated by the controller, data are not destroyed at the end of the processing, data are shared with a unlimited number of third parties, if the rights of the natural persons granted by the GDPR are violated, thus, whenever the provisions of the GDPR are violated. Apart from the requirements of the GDPR, there is always a need to make sure that personal data is not utilized in a way that would be deemed illegal. It would also be illegal if a criminal offense were to be committed as a result of the data processing. This covers offenses including violating someone else's copyright or violating a duty of confidentiality. All of these matters for compliance as well as a business's offline and online reputation (Rana & Rana, 2023).

2. Purpose limitation -This GDPR principle ensures that individuals possess reasonable anticipations regarding the organization's handling of their personal information and are cognizant of the underlying motivations for providing it. The GDPR considers this as a way to ensure responsibility and prevent the misuse of data for purposes that the individual has not been told about. This grants individuals a degree of authority in dictating the future utilization

of their personal data and allows them to decide whether or not they are willing to reveal it. Although GDPR does not universally forbid future use for other purposes, this concept does.

3. Data minimization - Data controllers should consider the minimum information needed to achieve organizational goals. Thus the data that can be collected are only those that are necessary for achieve the purposes for which a given system of data processing is devised. It is wrong to collect more data from a data subject if only a small fraction is needed for the processing. Moreover, data can be shared only with a limited number of third parties (Rana & Rana, 2023).

4. Storage limitation - Data may only be retained for the amount of time specified in the initial specifications (duration). Data cannot be retained for longer than is necessary. This means that once data are processed for a given legitimate purpose and the collected data must be destroyed. The business bears the responsibility of providing justification for the timeline they have set. It is reasonable to expect that the likelihood of erroneous or outdated data increases with its age (Rana & Rana, 2023).

5. Integrity and confidentiality - This is also referred to as the "principle of security," addresses the safe processing of data to prevent data breaches. The data controller must implement all the security measures of technical and organisational nature for ensuring the protection of personal data (including encryption, limited access, passwords, labour organisation etc.) (Rana & Rana, 2023).

Only individuals with the proper authorization may access and manage data, according to the Data Protection Regulation (GDPR). The GDPR does not specify the security precautions that must be taken, Rather, it mandates the implementation of a security level that is "appropriate" to the risks involved in the data processing (Rana & Rana, 2023).

6. Accountability - Those who process personal data must accept accountability for their dealings with it and for abiding by the other standards. Measures and records must be in place in order to verify compliance across special categories, which is a necessity. This not only indicates to clients and suppliers that the organization processes data legally, but it also displays to them that data protection is a major concern and that an individual's rights and freedoms are respected. It also implies that in the event of a problem—like a data breach or unauthorised disclosure, for example—it will be possible to show that precautions and protections were taken to lessen the likelihood of the incident. This could imply that there is protection from any legal action being taken (Rana & Rana, 2023).

These principles are applied throughout the GDPR and are designed to ensure that personal data is processed fairly, transparently, and securely. They also give individuals more control over their personal data and require companies to be accountable for the data they collect and process (ICO, 2023).

Rights of the Data Subject

Under the GDPR, individuals (data subjects) have several rights that they can exercise. These rights include:

a) Right to consent: In general, the basic rule is that the personal data need the consent of the natural person (right to consent). Moreover, the data subject has the right to withdraw the consent at any time (art. 7). This means that personal data are related to a *natural person* not a firm. The GDPR outlines six distinct justifications for processing personal data in order to comply with the requirements of specific grounds (art. 6). To abide by the GDPR's guidelines for data protection, at least one must apply.

1. The person whose data is being collected has given consent.

2. processing is necessary to carry out the terms of a contract with a certain person or for particular tasks prior to the beginning of the contract.

3. processing is necessary for compliance with a legal obligation to which the controller is subject.

4. processing is necessary in order to protect the vital interests of the data subject or of another person (e.g. hospitalisation).

5. 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.

6. when there is a legitimate interest pursued by the controller or by a third party.

In particular, the consent is necessary for particular categories of data, that are considered sensitive. These are data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited, criminal records (art. 9). Given their special importance and the related risks, for genetic data the consent is not sufficient, it is also necessary a specific authorisation of the national Data Protection Authority.

b) Right to information: The data controller is required to provide specific information to the data subject. These are:

The identity (and contact details) of the controller, its representatives, and the data protection officer responsible what data is processed and why, as well as any legal basis for processing the data;

The purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

Where the data is processed and if there'll be any transfer to a third party, such as external processors or joint controllers;

The type of data collected, and the measures used for the processing;

How long the data is stored in your system (duration);

Their right and how to demand for those rights, including the right to restriction, erasure, and rectification, the right to lodge a complaint to the supervisory authority;

The technical and organisational measures used for the protection of personal data;

Furthermore, the information notice must be given in a clear, comprehensible, and accessible manner.

c) Right to Access: The data subject has the right to know whether a given processing is pursued by the data controller and, where that is the case, access to the personal data and the whole information about the processing.

d) Right to Rectification: The right to correction allows individuals whose data they deem to be erroneous or outdated to have it updated. In addition, you must have a backup plan in case this fails, such as phone numbers, web forms, or live chat help for changing their information.

e) Right to Erasure (Right to be Forgotten): It is precisely what it sounds like—the right to be forgotten, or the right to erasure. A data subject may ask for their information to be permanently removed from your database.

The right to erasure can be ensure whenever:

(i) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(ii) the data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing;

(iii) the data subject objects to the processing;

(iv) the personal data have been unlawfully processed;

(v) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

However, there are certain circumstances that make this right null and void. The data controller has the right to reject a request for erasure if:

- The data is necessary for the exercise of freedom of expression and information.

- The data is necessary to fulfil a legal obligation.

- The data is necessary for the establishment, exercise, or defense of legal claims.

- there are legitimate reasons based on public interest, scientific or historical research, or statistical purposes.

f) Right to Object to Processing: The data subject have the right to obtain from the controller restriction of processing where: (a) the accuracy of the personal data is contested by the data subject; (b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; (c) the controller no longer needs the personal data for the purposes of the processing; (d) the data subject has objected to processing pending the verification whether the legitimate grounds of the controller override those of the data subject.

g) Right to Data Portability: If technically feasible, the data subject has the right to request their data in a machine-readable, standard format and have the right to transmit those data to another controller without hindrance from the controller.

h) Right to Object to Processing: Subjects to data processing have the right to object to the processing. In this case the controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject. The right to object does not apply only when data processing is required for the public interest (EDPS, 2023).

i) The right to not be subject to automated decision-making: Additionally, people must to be informed that they have the option to refuse the automated decision-making process that will be applied to their data that could have an impact on their legal situation. This situation occurs whenever there is a procee of profilying. Profiling refers to the automated processing of personal data to assess various aspects of an individual, such as their work performance, economic status, health, personal preferences or interests, reliability or behaviour, and location or movements. This involves analysing and predicting these aspects using the collected data.

Nonetheless, there are a few justifiable reasons overcoming the right to not to be subjected to automated decision making, specifically:

If automated decision-making is required to enter into or complete a contract;

If you have explicit consent from the data subject;

If you're authorized by the EU or member state law to process the data and have provided sufficient protection of the data subject's rights, freedoms, and interests (EDPS, 2023).

Privacy by Design and Privacy by Default

The GDPR is entirely articulated around the principle of "Privacy by design", namely on the right to privacy of the European citizens (art. 7 and 8 EU Charter). This means that privacy must be protected from the time a given system of data processing is projected. "Privacy by design" is in its turn articulated in the principle of *data protection by design* and *data protection by default*.

The principle of Data Protection by Design requires data controllers to implement appropriate technical and organizational measures to ensure that data protection principles are integrated into the processing of personal data from the outset. This involves considering data protection issues at the initial design stage of a system, service, or product, and throughout its entire lifecycle.

The principle of Data Protection by Default requires data controllers to implement measures to ensure that, by default, only personal data necessary for each specific purpose of the processing is processed. Additionally, this principle requires that the personal data is not made accessible to an indefinite number of individuals without the data subject's intervention.

Transfer to the Third States

To ensure continued protection where personal data is transferred to countries outside the European Economic Area (EEA) (Third States), the GDPR imposes strict conditions on international data transfers. Such transfers must be based on one of the instruments provided for by the GDPR, including Commission adequacy decisions and Standard Contractual Clauses (SCCs). GDPR Article 43a regulates Third-State's access to personal data of the European citizens. It should prevent third nations from getting EU controller or processor data through judgments or administrative decisions. An EU controller or processor receiving such an order must notify the applicable supervisory authority, which can authorize the transfer or disclosure if necessary and permitted by the GDPR (Article 44) (Boehm, 2015). Supervisory authorities shall use consistency where applicable.

The Mechanism of Sanctions

A crucial aspect of this framework is its mechanism for sanctions, designed to enforce compliance and penalize violations. Article 83 of the GDPR, specifically paragraphs 4 and 6, outlines the fines applicable for certain types of infringements.

Paragraph 4 of Article 83 addresses infringements that, while significant, are considered less severe compared to those in paragraph 5. These include violations pertaining to:

Integrating Data Protection by Design and by Default: Non-compliance with obligations related to data protection by design and by default.

Records of Processing Activities: Failure to maintain a record of processing activities under the responsibility of the data controller or data processor.

Cooperation with the Supervisory Authority: Non-cooperation with the supervisory authority in the performance of its tasks.

Security of Processing: Infringements related to the security of processing personal data.

For such infringements, GDPR sets a maximum fine of up to 10 million EUR, or, in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Paragraph 6 of Art. 83 deals with non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority. This category is viewed as a serious non-compliance issue because it directly challenges the authority's decision-making and oversight capabilities.

The fines for such non-compliance are substantial: up to **20 million** EUR, or, in the case of an undertaking, up to **4%** of the total worldwide annual turnover of the preceding financial year, whichever is greater. This level of fine underscores the importance the GDPR places on compliance with the directives of the supervisory authority.

Enforcement and Discretion

While the GDPR sets out maximum fines, it also provides discretion to supervisory authorities in determining the appropriate sanction for a specific case. Factors considered in this determination include:

- Nature, Gravity, and Duration: Considering the nature, gravity, and duration of the infringement.
- Intentional or Negligent Character: Determining whether the infringement was intentional or negligent.
- Mitigating Actions: Assessing any action taken by the data controller or processor to mitigate the damage.
- Preventive Measures: Evaluating the degree of responsibility of the data controller or processor, taking into account the technical and organizational measures they have implemented.

The sanction mechanism under Article 83, particularly paragraphs 4 and 6, reflects the GDPR's commitment to ensuring compliance through a structured penalty system. This system is not only punitive but also serves as a deterrent, encouraging organizations to proactively align with GDPR's data protection standards. The flexibility in sanctioning allows for a balanced approach, considering the specifics of each case while upholding the overarching principles of data protection and privacy within the EU.

2. 3 Relevant GDPR Provisions for AI Development

On June 25, 2020, the European Parliament published a paper about the connection between AI and the GDPR and its effects on it. The study looked at how the GDPR impacts AI with its provisions and how well it fits into the conceptual framework of the law. It is expected that the GDPR will have a significant impact on the creation, application, and use of AI technologies. The study's conclusions highlight that although the GDPR can be used to manage AI, its guidelines need to be stronger and more specific (Baig, 2023).

With the introduction of its proposal of the EU AI Act, the EU started the process of developing AI regulations in response to the European Parliament's initial investigation. One of the first comprehensive global regulations pertaining to AI that was proposed to control the creation and application of AI systems is the AI Act. The goal of the proposed rule is to guarantee that AI systems used in the EU uphold fundamental rights and values and are transparent, dependable, and safe (Baig, 2023).

The Confluence between AI and GDPR

Since AI systems need to analyse vast volumes of data, including personal data, in order to learn and improve their performance, GDPR principles, rights, and provisions become essential when developing and putting into use AI systems:

Lawful Basis for Data Processing

Businesses that are creating or utilizing AI should ascertain whether they process personal data and, if so, under what legal authority. They ought to abide by all rules concerning the legal foundation they use. For instance, they have to make sure that consent is given freely, knowingly, expressly, and without ambiguity (Baig, 2023).

Data minimization

Organizations must follow data minimization guidelines, processing personal information only when necessary to fulfil defined goals and retaining it for the shortest amount of time. Additional guidance is provided by GDPR Article 5(1), which states that companies must take three considerations into account whenever they process personal information. (Velázquez, 2022). With regard to the data processing by AI systems, there is a number of questions to be considered.

Adequacy: is the personal data that's been processed sufficiently to fulfil your stated purpose?

Relevance: does the information have a clear link to that purpose?

Necessity: do you have more information than you need to fulfil that purpose?

Businesses that possess unrestricted access to keep and handle consumer data put their privacy and security at risk. The main advantages of adopting data minimization in a company are listed below (Data Security Plus, 2023).

1. Reduces data storage costs

Organizations can handle the rapid expansion of data by managing undesired data within data warehouses. Regularly purge and handle data that has no business value to free up your tier 1 storage for information that is essential to your operations (DataSecurityPlus, 2023).

2. Strengthens data security posture

A firm may become the target of targeted assaults if large amounts of unnecessary personally identifiable information and electronic protected health information are stored across several data repositories When a firm retains extensive volumes of personally identifiable information (PII) and electronic protected health information (ePHI) across multiple data repositories, it potentially increases its vulnerability to targeted cyber-attacks. However, it is crucial to recognize that the quantity of data stored does not necessarily correlate with ease of protection. Contrary to the initial assertion that securing less data simplifies the prevention of undesired exposure, theft, and loss, a more nuanced understanding is required. In reality, the complexity and robustness of security measures, along with adherence to data protection protocols, play a more pivotal role in safeguarding data. Effective data management and stringent security protocols are essential, irrespective of the data volume, to mitigate the risks of hacking and unauthorized access" (DataSecurityPlus, 2023).

3. Fortifies data privacy measures

Unrestricted collection of personal information has resulted in far too many negative effects, such as intrusive consumer behavior modeling and targeted advertising. Data privacy is ensured by deleting personal information after it has served its purpose. (DataSecurityPlus, 2023).

4. Smooths business operations

When users need to locate and process important business information from data repositories, optimizing data junk is essential. With less data to process, it is simpler to control data availability and integrity. (DataSecurityPlus, 2023).

5. Maintains compliance with data regulations

Organizations are required by a number of regulatory authorities, like as the GDPR, HIPAA, CCPA, and others, to gather and keep just the data required to deliver pertinent goods and services. Data reduction techniques assist firms in adhering to these regulatory requirements. (DataSecurityPlus, 2023).

In addition to the GDPR's assessment and strengthening of the data minimization principle and the new requirements it imposes on personal data, it also serves as best practice for preserving consumer confidence and lowering the risk of unauthorized access and other security threats. (DataSecurityPlus, 2023).

Anonymization and Pseudonymization

The GDPR places a strong emphasis on the use of anonymization and pseudonymization methods to protect personal information and improve an individual's privacy. Anonymized data is not considered personal data under the GDPR. Re-identifying personal data is less likely when pseudonymized. Pseudonymized material is still regarded as personal data, nevertheless. Pseudonymization and anonymization are crucial methods for the functioning of AI systems that handle personal data (Baig, 2023).

Accuracy and Storage Limitation

AI systems handling people's personal data are required to keep accurate and current records of that data and not keep it longer than is necessary (Baig, 2023).

Right to Information regarding Automated Decision-Making

Organizations that base their decisions exclusively on automated processing that results in legal or similarly significant effects are required by GDPR to notify data subjects of such activity, give them meaningful information about the reasoning behind the processing, and explain the significance and expected outcomes of the processing. The data must be easily obtainable and precise (Baig, 2023).

Data Protection Impact Assessments (DPIAs)

Organizations are required by Article 35 of the GDPR to conduct DPIAs for AI applications that seriously jeopardize the rights and liberties of individuals. These assessments help identify and mitigate potential data protection risks prior to the deployment of AI systems (Baig, 2023). This means that whenever there is a processing by an AI system at play the producer has to nominate a Data Protection Officer for the evaluation of the potential risks for privacy through the above mentioned DPIA.

Security and Accountability

Companies need to take accountability for the data that their AI systems process and make sure that any AI apps that handle personal data have security algorithms in place to protect that data. In addition, these entities ought to implement suitable technical and organizational protocols that align with the type of risk associated with their processing operations (Baig, 2023).

Cross-Border Data Transfers

One of the primary focuses of the General Data Protection Regulation (GDPR) is to guarantee appropriate safeguards for the movement of personal data across international borders. As a consequence of this, companies that develop and utilize artificial intelligence systems are obligated to ensure that they have suitable safeguards in place, such as Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs), prior to transferring any personal data to a foreign country (Baig, 2023).

Rights of Individuals

As seen, the GDPR grants data subjects several rights, including the right to access, rectification, erasure, restriction of processing, portability of data, and objection. AI systems are required to respect and abide by these rights. The General Data Protection Regulation (GDPR) forbids the use of automated decision-making on persons unless one of the listed exceptions—namely, express, contractual consent or legal authorization—applies (Baig, 2023).

Since AI is developing quickly, it is crucial for businesses to comprehend how using AI may affect data processing while still adhering to GDPR regulations.

Consent for Data Processing

Organizations are required by GDPR Articles 6 and 7 to establish a legitimate basis before processing personal data. One of the legal justifications for processing personal data is consent. Free, explicit, informed, and a clear expression of the data subject's desires is required for consent. Organizations should also provide people the option to withdraw their consent at any moment (Baig, 2023).

If an organization engages in the development or utilization of AI, it must ensure that it obtains legitimate consent and provides data subjects with sufficient information regarding the processing of personal data, in compliance with GDPR regulations. This is particularly important when the business relies on consent as the legal basis for such processing (Baig, 2023).

Transparency

Businesses are required by GDPR's Articles 12, 13, and 14 to provide individuals with clear, comprehensible, and freely accessible information about how their personal data is processed. These provisions pertain to transparency and the right to information. This includes explaining to data subjects how automated decision-making processes, including profiling, are used and the reasoning behind them. Organizations ought to be forthright and truthful about the application of AI, the handling of personal data, the significance of AI-driven decision-making, and any potential risks or negative impacts (Baig, 2023).

The Complexity of AI Algorithms

In example, deep learning algorithms are often very complex and operate as "black boxes." Giving people an intelligible explanation of the intricate layers of calculations and transformations that occur within these algorithms is a challenging task (Baig, 2023).

AI models are always learning and updating, adjusting to new settings and information. The dynamic nature of the model makes explanations challenging because it can behave differently over time and older explanations may become out of date (Baig, 2023).

Certain AI models and algorithms are created using proprietary techniques and are shielded from infringement by intellectual property laws (trade secret). If the inner workings of these models are made public, there may be worries about losing competitive edge (Baig, 2023).

AI systems are capable of learning from biased input and thus coming to biased conclusions. Making decisions based on skewed facts can give rise to ethical dilemmas. This process needs to be handled cautiously as a result. Organizations should take into account the aforementioned aspects when informing data subjects about how AI systems manage their personal data and make sure the information is clear and correct (Baig, 2023).

Decisions that are made exclusively on the basis of automated processing that have legal ramifications for the data subject or otherwise have a substantial impact on them are generally prohibited by GDPR. This restriction is not applicable if the ruling is:

• is required to establish or fulfil a contractual agreement between the individual providing the data and the entity controlling the data,

• is permitted by European Union's or Member State's legislation that applies to the data controller and includes appropriate safeguards to protect the individual's rights, freedoms, and legitimate interests, or

• is based on the explicit consent of the individual providing the data.

It is essential to note that the individual or organization responsible for managing the data must ensure that they take necessary measures to safeguard the rights, freedoms, and lawful interests of the individual whose data is being processed. This includes granting the individual the right to request human involvement from the data controller, express their concerns, and contest any decision made based on consent or legal requirements (Baig, 2023).

Using sensitive personal data to make automated decisions is not allowed, unless it is necessary for significant public interests, the individual explicitly agrees, it follows the laws of the European Union or Member States, and there are measures in place to protect the individual's rights, freedoms, and legitimate interests (Baig, 2023).

Data Security and Privacy by Design

Organizations must put in place the proper organizational and technical protections in accordance with Article 32 of the GDPR to ensure a level of security appropriate for the risk posed by any processing operations. This entails implementing security measures to prevent personal data from being transferred, stored, or processed in any other way being accidentally or illegally destroyed, lost, altered, disclosed, or accessed (Baig, 2023). AI apps that process

personal data are required to adhere to the necessary security protocols in order to safeguard the data they process.

As seen, the GDPR provides that these security protocols are implemented at the design stage ("data protection by design and default"). According to this principle, businesses must take privacy and data security into account from the very beginning of AI system construction and continue to do so. It also necessitates making sure that privacy settings are always set to the strictest possible options and integrating privacy aspects into the architecture of AI apps (Baig, 2023).

3. Case Study: ChatGPT in Europe

3.1 ChatGPT and Its Implementation in Europe

ChatGPT is a large language model (LLM) created by OpenAI and made available to the general public through a research preview in November 2022. Natural language processing (NLP) and language models (LLMs) are specialized domains within the science of artificial intelligence (AI) that rely on deep learning methodologies and the training of neural networks using substantial datasets. LLMs possess the ability to comprehend and produce text in a manner that resembles human language (Ray, 2023).

In recent years, the artificial intelligence has experienced notable progresses, partly attributed to the rapid advancements in supercomputer construction and deep-learning algorithms. Simultaneously, the abundance of data currently accessible has enabled researchers to effectively train their models using the extensive input of information required (Ray, 2023)

ChatGPT needs to be trained to perform the tasks that users request.

The training of ChatGPT consisted of two phases: The initial phase encompassed unsupervised training, when ChatGPT was trained to anticipate missing words in a provided text, enabling it to grasp the structure and patterns of human language. After the initial pre-training, the second phase involved fine-tuning ChatGPT using Reinforcement Learning from Human Feedback (RLHF). RLHF is a supervised learning method where human input is used to help the model alter its parameters and improve its task performance (Europol, 2023).

In early 2023, shortly after ChatGPT was introduced to America It seems a commercial by OpenAI. Change source (that cannot be OpenAI itself), it quickly piqued the interest of European viewers as well. ChatGPT is gaining popularity throughout Europe. Several European nations possess well-educated and technologically proficient citizens who promptly grasped the vast potential of ChatGPT (chatgpt4admin, 2024).

Each nation adopts distinct positions when incorporating new technologies into society, influenced by local values and interests. Interest in ChatGPT remains significant throughout the area, but European countries have differing opinions on suitable applications of the technology (chatgpt4admin, 2024). Typical commercial uses in Europe include:

- Customer service and sales chatbots
- Content creation automation

- Software coding and testing assistance
- Data analysis and business intelligence
- Personalization and recommendations

Employees can devote more time to high-value, creative projects by outsourcing repetitive duties to ChatGPT. Businesses can significantly increase output without just hiring more employees thanks to the corporate productivity multiplier effect (chatgpt4admin, 2024).

For instance, a digital agency based in Europe might use ChatGPT to automatically produce comprehensive reports on keyword analysis for SEO. Account strategists then just evaluate AI results and spend time creating original link-building outreach instead of manually compiling recommendations (chatgpt4admin, 2024). Any new technology, such as ChatGPT, must be carefully evaluated in terms of security and regulatory compliance before being integrated into crucial business processes.

- Confidential data leakage
- Intellectual property theft
- Violations of sector regulations
- Spread of misinformation by a faulty AI

As conversational systems become more networked and have access to more internal platforms, these risks become increasingly serious (chatgpt4admin, 2024). Establishing governance and proactively recognizing vulnerabilities are critical. Strong cybersecurity measures including DNS filtering infrastructure, endpoint monitoring, and multi-factor authentication. Policies for preventing data loss keep sensitive information flows under control. In order to prevent undiscovered flaws, ongoing audits evaluate AI behavior for stability across time and training data changes (chatgpt4admin, 2024).

Furthermore, avoiding responsibility dilution even when utilizing AI tools is possible by maintaining transparency and human accountability. This maintains compliance under stringent regulatory oversight in industries like financial services, healthcare, and

communications, among others. when such innovation is applied to public areas like education, the picture becomes much more nuanced (chatgpt4admin, 2024).

Unlike commercial players, academics have more difficult issues when it comes to AI helpers. Institutions are under pressure on two fronts: one is to rank globally for research excellence while maintaining a focus on development. Students themselves take to new devices and applications with enthusiasm. Thus, numerous requests for access to ChatGPT are already handled by university IT departments. Scholars are understandably concerned about undermining the integrity of research, though. Over-reliance on AI algorithms runs the risk of impeding cognitive development. It might potentially make cheating easier, lowering the validity of assessments (chatgpt4admin, 2024).

Privacy & Data Considerations for European ChatGPT Users

Data governance becomes increasingly important as AI capabilities develop, since they are partially dependent on processing people's information. With laws like GDPR, Europe in particular enshrines high privacy standards with regard to technology. Therefore, it makes sense that there is some ambiguity regarding the personal information that ChatGPT collects about its customers. Individuals are guaranteed agency over related dangers, such as profiling, through transparency (chatgpt4admin, 2024).

Anthropic has so far disclosed stringent guidelines that restrict data acquisition to essentials like invoicing or product performance. They allow most tracking to be opted out of. Furthermore, no user content should enter ChatGPT training without permission.

These options are in opposition to the advertising strategies used by consumer tech giants who are always pleasing algorithms. They represent for doubters how AI that upholds rights might flourish in marketplaces. While users are assured of ethical management, they submit data more voluntarily while using services like ChatGPT. (chatgpt4admin, 2024).

Such AI ideas are being codified into law through ongoing EU legislation, which covers anything from values-based design standards to documentation procedures. Proactive policymaking can facilitate swift integration with cultures by anticipating and resolving anxieties. Additionally, societies continue to have opportunity to influence results by actively participating (chatgpt4admin, 2024).

Changes and additions

The European Parliament's proposed amendments seek to guarantee the safety, transparency, traceability, non-discrimination, and environmental friendliness of AI systems. In order to accommodate evolving types of artificial intelligence, they also aim to incorporate a standard definition of AI that is independent of technology (Fernhout & Rad, 2023).

The use of AI systems that present an intolerable risk is forbidden by the AI Act. In part to broaden the prohibition on the use of AI systems for discriminatory purposes, the European Parliament made significant changes to the list of AI kinds that are considered to pose an intolerable danger. One instance is the application of AI systems for social scoring, which involves assessing or categorizing people according to their social behavior, socioeconomic standing, or known or anticipated personality qualities. The untargeted internet or CCTV image scraping of faces for the purpose of building or expanding facial recognition databases, biometric categorization systems that use sensitive data to classify natural persons, and AI systems that infer an individual's emotions for use in law enforcement, border management, the workplace, and educational institutions are just a few of the AI applications that the European Parliament added to the list (Fernhout & Rad, 2023).

Furthermore, depending on its intended use, an AI system was originally deemed to have high risk. The criteria that a system must also seriously jeopardize people's health, safety, or fundamental rights in order to qualify as high risk has been added to this definition. The list of high-risk AI systems now includes recommender systems from social media companies that the Digital Services Act (DSA) designates as extremely significant online platforms (Fernhout & Rad, 2023).

General Purpose AI

The European Parliament's changes closed a generative AI-related gap that was beginning to show up in the draft legal framework. The legislative proposal for the professional use of AI systems has been reexamined by European politicians in response to the widespread use of ChatGPT and other generative AI. Consumer-focused generative AI is frequently implemented extensively and in a variety of industries, which is not totally consistent with the risk-based strategy outlined in the AI Act's initial draft, which determines risk based on variables like purpose and industry. Because of its tiered structure, the initial plan did not address generative

AI models intended for widespread application. These models are now categorized as high-risk AI systems under the compromised amendments, and as a result, they will be subject to more stringent disclosure obligations. One of the prerequisites is to make it obvious whether content was created using artificial intelligence. One other noteworthy change is that any copyrighted data used to train generative AI systems must be recorded and its use must be disclosed in a comprehensive overview (Fernhout & Rad, 2023).

3.2 ChatGPT Data Protection Challenges and Privacy Implications

ChatGPT under the GDPR

Evaluating ChatGPT's compliance with the GDPR is challenging. Enormous volumes of text used to train ChatGPT contain information on natural beings, and that this is still included in the dataset it works with, even though the extent to which ChatGPT's source data contains personal information is unknown. OpenAI states that all of its training data has been anonymized and cleansed to eliminate any identification when questioned about this. Even for experienced users, it is nearly impossible to confirm this (Suarez, 2023).

Moreover, artificial intelligence programs have trouble forgetting the knowledge that has been taught to them. ChatGPT's neural network will have adjusted to the input by giving distinct "weights" to each data point in succeeding layers once it has learned from specific personal data points. As a result, even if the original data is removed from the base layer, the system will retain what it has learned. This creates a challenge for the exercise of the right to erasure, as guaranteed by Article 17 of the GDPR, and it's not apparent how to address it technically short of retraining the machine entirely, which would require a significant investment of resources (Suarez, 2023).

Lastly, interactions give the computer access to a tonne of personal data. "The types of content that you view or engage with" is among the "personal information we receive automatically from your use of the service," according to OpenAI's privacy policy, which is collected through interactions. Based on the specific words and spellings used, the algorithm may be able to predict the user's hidden attributes, including gender, age, socioeconomic status, and degree of education. For instance, a youthful user is more likely to speak using internet slang, whereas someone with a high level of education may correctly distinguish between "their" and "they're" (Suarez, 2023).

Sensitive information may also be gathered through user contact. For example, if a user asked the bot frequently about gender identity, health-related issues, or symptoms of pregnancy. Interactions that don't seem important can yet reveal unique data categories. The user may indicate to the machine that they are a vegetarian or that they have left-wing political views, for example. The totality of these data points can be utilized to create a thorough profile of a user, even if they have never voluntarily given any information and might not be aware that their information is being gathered (Suarez, 2023).

According to OpenAI's privacy statement, the information gathered is utilized for a variety of purposes, including service upkeep, legal compliance, research, communication, and the creation of new products. However, businesses might be enticed to monetize all the data acquired through personalized advertising, including political campaigns, as the service's popularity increases and Microsoft and OpenAI enter into a multibillion dollar alliance. What's more concerning is that users may not even realize they are the subject of sponsored PR if this monetisation occurs through informal chats with the computer (Suarez, 2023).

Evaluating ChatGPT's User Data Handling, Storage, and Data Collection In accordance with OpenAI's data usage policy, ChatGPT undergoes pre-training on a sizable corpus of text that is freely accessible on the internet. However, it is not aware of the precise documents that comprised its training set and is not permitted to access any proprietary, classified, or private data. The model is trained using a dataset created with the assistance of human reviewers in accordance with the criteria supplied by OpenAI during the fine-tuning stage. OpenAI keeps track of user interactions for a period of 30 days. Instead of being used to customize user experiences, the information that users submit while engaging with models such as ChatGPT is utilized to enhance the models. OpenAI's most recent data usage policy should be the primary source of more precise and up-to-date information (Sebastian, 2023).

Though it's crucial to remember that the model itself doesn't have access to personal data, LLM-based chatbots like ChatGPT may raise privacy issues because they generate text based on substantial training data. This might be especially problematic if the bot produces responses that seem to divulge sensitive information. Furthermore, if privacy protocols for user interactions using ChatGPT are not sufficiently implemented or understood, concerns may also surface regarding the possible misuse of these interactions. Some of the most frequent privacy and data leakage problems with these AI-based chatbots are mentioned below. The trust that users place in AI systems may be greatly impacted if any of these problems arise. Users must

have faith that the system will protect their privacy and that their data is safe. Users may lose trust in AI systems as a result of privacy and data security violations, which would be detrimental to the tools' usefulness and reputation (Sebastian, 2023).

I. Intentional Data Collection: Large Language Models (LLMs) such as ChatGPT are trained on diverse datasets, which include data collected intentionally during interactions with users. This collection process can be problematic, particularly when users are unaware that their data will be used for such purposes or if the data handling practices are not transparent. This data, while used to improve model accuracy and response relevance, raises concerns about user consent and data minimization principles (Sebastian, 2023).

II. Data from Microworkers: The employment of data generated by microworkers—individuals who perform tasks to train, tune, and validate the AI models—is another critical area of concern. These contributions can include sensitive or personally identifiable information that microworkers may not realize is used to train AI systems. The ethical implications of using such data, including consent and fair compensation, must be carefully managed to avoid exploitation and privacy violations (Sebastian, 2023).

III. Unintentional Disclosure of Sensitive Information: This happens when a user gives the AI system access to private or sensitive information without realizing it. For example, a consumer may divulge their credit card details, thinking the AI will keep it safe. Even while ChatGPT and other non-PII AI models can't remember or store this kind of data — they only temporarily store it for 30 days in order to enhance performance — the data may still be intercepted during transmission if the communication channel isn't secure (Sebastian, 2023).

IV. Data Leakage through Model Outputs: Although LLM models, such as ChatGPT, are trained on anonymous data, they may occasionally produce outputs that appear to allude to particular data or disclose private information. These outputs, however, are not indicative of the access to any particular data sources or private databases. Rather, they are produced based on patterns discovered during training. Responses from the AI might "hallucinate" certain, delicate features. The program is concocting stories based on the patterns it discovered, without disclosing sensitive real-world data that it was trained on (Sebastian, 2023).

V. Adversarial Attacks: In these attacks, malevolent individuals try to coerce or influence AI into acting in a particular way, usually for negative ends. An adversarial assault, for example, would entail feeding in carefully constructed data meant to trick the AI into producing

offensive or dangerous content. LLM Chatbots may be vulnerable to evasion assaults, trojan horse attacks, and fake review attacks, among other cybersecurity threats (Sebastian, 2023).

VI. Model extraction: In this technique, an attacker makes a duplicate of a machine learning model without having access to the original training data by utilizing the model's outputs. If successful, the attacker might compromise the security and integrity of the original system by using the extracted model for nefarious reasons (Sebastian, 2023).

VII. Data Poisoning: In order to affect a model's future predictions or behavior, an attacker can insert malicious data into the model's training set. It poses a serious risk to systems that get continuous learning from user interactions (Sebastian, 2023).

Cybercrime and fake news

Criminals may also become more accustomed to using ChatGPT. Because ChatGPT can be used to create false news and other deceptive content, cybercriminals may utilize the platform to harm the gullible. The technology can readily be used to spread evil intent or misleading information because it is not intended to discern between fact and fiction. When this technology is misused, it might result in the creation of offensive or defamatory information in addition to copyright violations. The program might be used, for instance, to create spam messages, phishing emails, or even bots that disseminate malware automatically (Almeida, 2023).

Because ChatGPT is based on real-world interactions, it is possible that the text that is created contains discriminatory, prejudiced, or otherwise offensive words. Therefore, when utilizing the technology, ethical issues need to be taken into mind. Because the database is based on texts that have previously been produced, it is possible that some facts and details have changed over time or do not directly relate to the scenario you had in mind when you generated the text. Therefore, when creating text using this database, extreme caution and attention are recommended (Almeida, 2023).

Many businesses are now adopting ChatGPT and other generative AI models to produce original content, as their popularity has surged in recent years. However, there are a lot of moral and legal issues with this application, mostly related to data privacy. One such concern is whether OpenAI can abide with GDPR Article 17 and remove a person's personal information entirely from the model upon request (Hillemann, 2023).

The right to be forgotten

People can ask for the removal of their personal data from an organization's records under the GDPR. This means that people have more control over their personal data and is referred to as the "right to be forgotten" or "right to erasure."

A person may ask for their data to be deleted if they are no longer comfortable with their personal information being processed, if there are major errors in the information, or if it is determined that the data is no longer required (Hillemann, 2023).

However, this right is not unqualified, and companies are not required to comply with the request at all times. Individuals have the right to the erasure of their personal data under GDPR Article 17. This covers any information that is no longer needed for the reason it was gathered or processed in the first place (Hillemann, 2023).

The controller shall take adequate measures to ensure that any other processing controllers are informed that all links to the personal data, along with any copies or replicas of the personal data that may already exist, must be removed if the controller has illegally processed the personal data of an individual. A person has the right to request that their personal data be deleted if they no longer consent to its processing. If this is the case, the organization has an obligation to remove the data. Likewise, if someone believes that their personal data is being kept longer than necessary, they have the right to request that it be deleted (Hillemann, 2023).

When it impedes on the freedom of expression and knowledge, the right to be forgotten is restricted. Should an individual request the removal of inaccurate personal information while maintaining the correctness of the data, the organization may not be required to do so. A crucial component of the GDPR that offers people more control over their personal data is the right to be forgotten. According to Hillemann (2023), individuals have the ability to request that their data be deleted if it is no longer required for the original purpose of collection or processing, or if they no longer consent to its use.

That being said, organizations might not always uphold the right to be forgotten because it is not a given. One of the main and most important tenets of the EU's General Data Protection Regulation is the right of oblivion (Hillemann, 2023).

Because of the permanent nature of the data generated by generative AI systems like ChatGPT, it is challenging to enforce the right to be forgotten as stated in Article 17 EU-GDPR. Since

replies are generated from the gathered data using natural language processing, it is practically hard to eradicate all traces of a person's personal information (Hillemann, 2023).

Businesses using generative AI now need to realize how difficult it might be to erase data upon request because it involves a deep understanding of how their AI systems interpret and produce answers. For enterprises to adhere to the right to be forgotten, they must understand the data that is utilized to generate these responses (Hillemann, 2023).

According to ChatGPT, AI systems — like neural networks — don't forget the same way people do. Rather, the network modifies its weights to better fit fresh data, producing distinct results for the same input. The network is simply concentrating more on the fresh data it is gathering, it is not forgetting in the traditional sense. It still retains all of the data. Thus, it is evident that the requirements of Art. 17 EU-GDPR are not satisfied (Hillemann, 2023).

According to OpenAI's Privacy Guidelines, all data will be kept private and used only for the purposes specified in the terms of the agreement. Additionally, they hold that no personal information gathered and handled will be disclosed to outside parties. However, it's unclear if this holds true for information kept in ChatGPT and other artificial intelligence models (Hillemann, 2023).

A member of the European Data Protection Board (EDPB), Alexander Hanff, raises concerns about OpenAI's purported data gathering for ChatGPT. He thinks it is against the terms of the contract to collect billions or trillions of data points from websites whose terms and conditions prohibit third parties from scraping them. Furthermore, according to Hanff, ChatGPT is a commercial product, hence fair usage is not applicable (Hillemann, 2023).

Currently, it is unclear if ChatGPT or other generative AI models will be able to adhere to the GDPR's Article 17's "right to erasure." To ensure that people's rights to data privacy are upheld, a thorough inquiry must be conducted to determine and implement the laws pertaining to the use of AI models. However, this specific AI model does not fulfill the standards outlined in Article 17 of the EU-GDPR (Hillemann, 2023).

3.3 Italian Case Study: ChatGPT in Italy

The use of the ChatGPT chatbot was stopped on March 30, 2023 by the Italian data protection authority (Garante per la protezione dei dati personali), for the violation of privacy of the Italian users. The General Data Protection Regulation (GDPR) compliance of OpenAI has been the subject of a probe declared by the Italian watchdog. Authorities have specifically said that there is no legal justification for the extensive gathering and archiving of personal data in order to train the algorithms that power the platform (Kreitmeir & Raschky, 2023).

Contrary to popular belief, the Garante's examination into ChatGPT did not begin as a generic inquiry into the service's GDPR compliance. Rather, it was brought on by a personal data breach that was reported to Garante on March 20, 2023. The incident affected the conversations that users of ChatGPT had as well as the details of payments made by service customers. But the Garante also used the breach notification as a chance to evaluate OpenAI's GDPR compliance, specifically with regard to ChatGPT's handling of personal data (Barcelo et al., 2023).

Several problems about GDPR compliance were highlighted in the Garante's March 30 decision.

First, the Garante della privacy discovered that data subjects whose data is collected and further processed by OpenAI through ChatGPT were not given the information required under Articles 13 (information to be provided where personal data is collected from the data subject) and 14 (information to be provided where personal data has not been obtained from the data subject) of the GDPR (Barcelo et al., 2023).

Furthermore, the ChatGPT service did not incorporate an age verification method into its registration procedure, despite its stated age restriction of 13 and above. Considering the children's level of development and self-awareness, the Garante reasoned that ChatGPT might expose minors utilizing the service to inappropriate answers (Barcelo et al., 2023).

Furthermore, the Garante claimed that ChatGPT's processing of personal data probably does not comply with Article 5(1)(d) of the GDPR, which requires accuracy. Since the information made available by the service does not always match the factual circumstances, this Article requires that personal data be accurate and, where necessary, kept up to date. It also requires that every reasonable step be taken to ensure that personal data that is inaccurate, having regard

to the purposes for which it is processed, is erased or rectified without delay (Barcelo et al., 2023).

Ultimately, the Garante della privacy concluded that there was insufficient and unclear clarification of the legal foundation for OpenAI's collection and processing of personal data in order to train the underlying algorithms.

The Italian data protection authority (Garante della privacy) has established a clear framework for lifting the temporary restriction on the use of ChatGPT in Italy. According to the authority's judgment, OpenAI must execute a set of actions by April 30 to ensure GDPR compliance. These efforts include increased transparency in the handling of personal data for both users and non-users, as well as the establishment of a legally permissible basis for algorithmic training using user data. OpenAI is planned to alter its information notices to make them more accessible and visible to users at important contact points, such as before registration and during service renewal. Furthermore, the corporation is required to eliminate any claims of contractual need from its legal basis for data processing, instead opting for permission or legitimate interest. This change is critical for the resumption of ChatGPT services in Italy, pending the resolution of the urgency that caused the initial ban. Furthermore, OpenAI must build an age gating system to prevent minor users from using the service without proper consent, with a full implementation plan due by May 31 and a thorough age verification system in place by September 30, 2023. OpenAI will also launch a public information campaign in cooperation with Garante to educate the public about how their personal data is used to train algorithms. This campaign is scheduled to debut on May 15 and will use a variety of media venues. The Italian SA is continuing to investigate and may alter its measures based on the findings (ChatGPT: Garante Privacy)

The Garante’s Decision does not include all the GDPR compliance concerns others have raised with these types of technologies. For instance, privacy advocates have questioned if and how OpenAI would abide by the rights of data subjects under the GDPR, including the right of access, rectification, and forgetting. The DPAs in France and Spain have both said they will look into it. The European Data Protection Board recently announced the formation of a task group to examine ChatGPT's GDPR compliance in the interest of harmonization (Barcelo et al., 2023).

The Court of Justice of the EU has emphasized the enforcement role of EU Member State DPAs since the July 2020 Schrems II ruling where the Court of Justice declared the European

Commission's Privacy Shield Decision invalid on account of invasive US surveillance programmes. These agencies have been more active in fining GDPR violations per se and closely examining commonly used and developing digital technologies to ensure they comply with fundamental EU data privacy principles (Barcelo et al., 2023).

Indeed, in May 2022, the Garante fined US-based Clearview AI with 20,000,000 € for illegally obtaining facial photographs from public web sources and matching them with its biometrics database, in accordance with hefty fines levied by the Greek, French, and UK DPAs. A few months later, in July 2022, the China-based social network TikTok announced its intention to serve ads to users aged 18 and over based on legitimate interest rather than informed consent. This announcement prompted the Garante, in accordance with the Spanish DPA, to issue a warning to TikTok regarding its handling of personal data used for targeted advertising (Barcelo et al., 2023).

By April 30, 2023, OpenAI has to abide with the regulations outlined by the Italian DPA with regard to openness, the rights of data subjects (including users and non-users), and the legitimacy of processing user data for algorithmic training (GPDP, 2023).

Consequently, the corporation was required to put into effect a number of specific measures in compliance with the GDPR and the Garante della privacy’s decision . The requested measures are:

Information

First, an information notice outlining the arrangements and reasoning behind the data processing necessary for ChatGPT's functioning, as well as the rights granted to data subjects (users and non-users), must be drafted by OpenAI and posted on its website. Before registering for the service, the information notice must be published in a viewable and easily accessible location (GPDP, 2023).

Before completing their registration, users from Italy will need to be shown this notification and confirm that they are older than eighteen (GPDP, 2023).

When the service is reactivated, registered users will need to show the notification when attempting to access it. They will also need to go through an age gate that will filter out users who are younger than the specified age based on their age (GPDP, 2023).

Legal basis

The Italian DPA ordered OpenAI to remove all references to contractual performance and to rely, in accordance with the accountability principle, on either consent or legitimate interest as the applicable legal basis for the processing of users' personal data for the purpose of training algorithms. This will not affect the DPA's ability to conduct investigations or take enforcement action in this regard (GPDP, 2023).

Enabling data subjects to exercise their rights

A further set of measures relates to the provision of instruments that allow data subjects, including non-users, to request the rectification of inaccurate personal data created by the service or, in the event that rectification is deemed to be technically impractical, the erasure of said data (GPDP, 2023).

In order to enable non-users to exercise their right to object to the processing of their personal data, which is necessary for the algorithms to function, OpenAI will need to make readily accessible tools available. If users' legitimate interests are selected as the legal justification for data processing, they will need to be granted the same rights (GPDP, 2023).

Measures safeguarding minors

In regards to age verification measures, the Italian DPA ordered OpenAI to put in place an age gating system for the purpose of registering for the service immediately and to submit by May 31st, 2023, a plan for implementing, by September 30th, 2023, an age verification system to weed out users under the age of 13 and users between the ages of 13 and 18 for whom the holders of parental authority are unable to grant consent (GPDP, 2023).

Campaign to raise awareness

By May 15th, OpenAI must, in accordance with the Garante della privacy, launch an informational campaign via radio, television, newspapers, and the internet to educate people about the use of their personal data for algorithm training (GPDP, 2023).

Following the conclusion of the ongoing fact-finding investigation, the Italian DPA will continue its investigations to determine any potential violations of the applicable laws and may choose to take further or different actions if appropriate (GPDP, 2023).

New settings for ChatGPT improve data privacy

Up until recently, the bot's interactions with private users might be utilized to train the algorithm, which meant that user input could potentially be used by the machine to generate responses for the public in the future. Due to the possibility of another user discovering the personal information entered into the system, this presented one of the software's largest data protection risks. It was also a warning sign for confidential data that can unintentionally become public, such as company secrets and code. Even though OpenAI was aware of this issue and asked users not to divulge "any sensitive information" in talks, many users continued to do so, sparking debates at Amazon and Samsung, among other businesses (Suarez, 2023).

OpenAI made these announcements on April 25. It is now possible for users to modify their privacy preferences and disable the "Chat History and Training" feature. The user's and the bot's chats will not be utilized to train the algorithm and will not show up in the chat history when this setting is turned off. This lessens the possibility that chat data would inadvertently be disclosed to uninvited parties (Suarez, 2023).

Additionally, OpenAI released a revised privacy statement, which is available to new users directly from the registration page. Additionally, the company launched a "welcome back" page in Italy with links to the updated privacy statement and notices about processing personal data for algorithm training (Suarez, 2023).

The corporation developed a method that enables data subjects to seek the correction of inaccurate or misleading information that the bot disseminates about them in response to concerns regarding the accuracy of the data provided by the bot about natural beings. Data subjects may also ask for their data to be deleted from ChatGPT's output if fixing the issue is not technically viable (Suarez, 2023).

In conclusion, OpenAI has introduced an Age Gate that requires users to verify that they are either 18 years of age or older, or that they are between the ages of 13 and 17 and have acquired permission from their parents to use the service. The purpose of this precaution is to prevent mionors from using the bot to access inappropriate content (Suarez, 2023).

Despite the changes, concerns remain

Although improvements in data protection compliance have been made, the situation is still difficult. OpenAI staff members can still view user discussions for moderating purposes, even

if they off the "Chat History and Training" option to stop their conversations from being used to train the algorithm (Suarez, 2023).

Besides, all of OpenAI's servers are situated in the US, which does not grant the same level of privacy protection as the GDPR. As a result, each time personal information is submitted into the ChatGPT system, it is transferred internationally to a jurisdiction whose data security regulations may be less stringent, endangering the security of the information (Suarez, 2023).

The Further decision of the Garante della Privacy

In a significant development, the Italian Data Protection Authority (DPA), the Garante della privacy, has notified OpenAI of breaches in data protection law concerning its ChatGPT platform. This notification follows the temporary processing ban imposed on OpenAI on March 30 of the previous year. The conclusion was drawn from a comprehensive fact-finding activity conducted by the Garante, which revealed evidence of violations of the European Union's General Data Protection Regulation (GDPR) (GPDP, 2024).

OpenAI has been granted a period of 30 days to respond to these allegations and submit any counterclaims regarding the cited breaches. This period allows OpenAI to present its defenses and clarify its data handling practices in an effort to address the concerns raised by the Italian authority.

Furthermore, in its final determination on the case, the Italian Garante will consider the ongoing efforts (EDPB). This task force is specifically focused on examining the broader implications of AI and machine learning platforms like ChatGPT under the GDPR framework. The integration of insights from the task force's work reflects the Garante's commitment to a thorough and informed decision-making process that aligns with broader European data protection efforts.

This stage in the regulatory process underscores the critical importance of compliance with GDPR provisions and the potential repercussions for global technology companies operating in Europe. The outcome of this case will likely have far-reaching implications for the privacy practices of AI platforms and the regulatory landscape of data protection (GPDP, 2024).

4. Conclusion

This thesis focuses on the two-fold potential and substantial obstacles related to incorporating ChatGPT and comparable generative AI models within the regulatory framework of the General Data Protection Regulation (GDPR) in the European Union. Although ChatGPT is a significant breakthrough in human-computer interaction, its implementation brings attention to significant issues in compliance, namely in safeguarding data privacy, upholding transparency, and preventing the unauthorized use of personal data. The thesis conducted a thorough examination of the relationship between AI and data protection in the European Union. It also identified crucial aspects that have a direct influence on AI technologies. The report analyzed the regulatory compliance challenges faced by ChatGPT and the techniques used to tackle these concerns.

The results of this study emphasize the crucial requirement for a well-balanced regulatory strategy that promotes creativity while protecting essential human rights. The preservation of this delicate equilibrium is crucial not just for the responsible implementation of ChatGPT but also for the wider regulatory approaches pertaining to AI technology. The issues mentioned, such as guaranteeing data accuracy, acquiring informed user consent, and upholding transparency in AI operations, are essential for the ethical utilization of AI. It is crucial to incorporate these concepts into any legislative framework in order to guarantee the responsible and efficient development of AI technologies.

The ruling made by the Garante della Privacy in January 2024 highlights the need for strict data protection measures. This pivotal ruling emphasizes the rigorous regulatory examination that generative AI models such as ChatGPT must undergo in order to adhere to GDPR. It is a significant illustration of the regulatory obstacles and reactions in the EU, highlighting the significance of strong compliance systems. This decision is not just a legislative milestone, but also a significant standard that will influence future regulatory actions and stimulate the improvement of AI governance frameworks throughout the EU.

To tackle these difficulties, it is crucial for AI developers to prioritize improved transparency and strong user consent methods. Enhancing transparency can be achieved by enhancing the comprehensibility of AI decision-making processes for users and ensuring they are fully informed about data usage policies. It is essential to establish user consent procedures to empower users with control over their data and ensure their active participation in decisions regarding their personal information.

Future research should prioritize the development of sophisticated techniques to guarantee data

privacy and the ethical deployment of artificial intelligence. This encompasses developing innovative approaches for anonymizing data, enhancing ways for ensuring transparency in algorithms, and establishing flexible ethical frameworks that can effectively adapt to the swift advancement of AI technologies. Policymakers must consistently modify legislation to align with the rapid rate of technological breakthroughs, creating a regulatory framework that is both protective and supportive of innovation. The continuous exchange of ideas between AI developers, legislators, and the public is essential in order to create policies that are both successful and adaptable to technological advancements.

In conclusion the convergence of artificial intelligence (AI) and data protection in the European Union (EU) creates a multifaceted environment with both advantageous prospects and intricate obstacles. The EU can establish worldwide leadership in ethical and responsible AI development by creating a conducive climate that promotes innovation and enforces strict data protection measures. The thesis offers valuable insights that enhance our understanding of these dynamics, providing a solid basis for future policy-making and research in this crucial sector. Striking a balance between innovation and regulation is difficult but necessary, necessitating cooperation from all parties involved to guarantee the development and implementation of AI technology in a way that honors and safeguards basic human rights.

Bibliography

Aggarwal, R., Sounderajah, V., Martin, G., Ting, D. S. W., Karthikesalingam, A., King, D., Ashrafian, H., & Darzi, A. (2021, April 7). Diagnostic accuracy of deep learning in medical imaging: a systematic review and meta-analysis. Npj Digital Medicine, 4(1). https://doi.org/10.1038/s41746-021-00438-z

Ali, S., Abuhmed, T., El-Sappagh, S., Muhammad, K., Alonso-Moral, J. M., Confalonieri, R., Guidotti, R., Del Ser, J., Díaz-Rodríguez, N., & Herrera, F. (2023, November). Explainable Artificial Intelligence (XAI): What we know and what is left to attain Trustworthy Artificial Intelligence. Information Fusion, 99, 101805. https://doi.org/10.1016/j.inffus.2023.101805

Almeida. (2023). The legal status of ChatGPT - Privacy. Retrieved February 1, 2024, from https://heydata.eu/en/magazine/the-legal-status-of-chat-gpt

Arnbak, & Goldberg. (2015). Loopholes for Circumventing the Constitution: Unrestrained Bulk Surveillance on Americans by Collecting Network Traffic Abroad. Retrieved January 8, 2024, from https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1204&context=mttlr

Artificial Intelligence (AI): What it is and why it matters. (n.d.). SAS. https://www.sas.com/en_us/insights/analytics/what-is-artificial-intelligence.html

Barcelo, Mechelli , Perray, Arzuaga, Maisnier-Boché, & Perin. (2023, April 21). ChatGPT: A GDPR-Ready Path Forward? - McDermott Will & Emery. McDermott Will & Emery. Retrieved February 1, 2024, from https://www.mwe.com/insights/chatgpt-a-gdpr-ready-path-forward/

Barmer, & Dzombak. (2021). National AI Engineering Initiative Scalable AI. Carnegie Mellon University. https://insights.sei.cmu.edu/documents/608/2021_019_001_735330.pdf

Bertollo, A. G., De Carvalho Braga, G., Tonin, P. T., Luzardo, A. R., Bagatini, M. D., & Ignácio, Z. M. (2023, October 5). The Impact of Stress from Social Isolation during the COVID-19 Pandemic on Psychiatric Disorders: An Analysis from the Scientific Literature. Brain Sciences. https://doi.org/10.3390/brainsci13101414

Bignami. (2015). "The US legal system on data protection in the field of law enforcement - Safeguards, rights and remedies for EU citizens".. Retrieved January 8, 2024, from https://www.europarl.europa.eu/RegData/etudes/STUD/2015/519215/IPOL_STU(2015)519215_EN.pdf

Boehm. (2015). A comparison between US and EU data protection legislation for law enforcement purposes. Retrieved January 6, 2024, from https://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU(2015)536459_EN.pdf

Carvalho, G., Cabral, B., Pereira, V., & Bernardino, J. (2021, January 18). Edge computing: current trends, research challenges and future directions. Computing, 103(5), 993–1023. https://doi.org/10.1007/s00607-020-00896-5

Catanzariti. (2020). Handbook on the Techniques of Judicial Interactions in the Application of the EU Charter DATA PROTECTION. Retrieved January 8, 2024, from https://cjc.eui.eu/wp-content/uploads/2020/05/eNACT_Handbook_data-protection-compresso.pdf

ChatGPT Heralds an Intellectual Revolution | Henry A. Kissinger. (2023, February 27). Henry a. Kissinger. https://www.henryakissinger.com/articles/chatgpt-heralds-an-intellectual-revolution/

ChatGPT: Garante privacy, limitazione provvisoria sospesa se OpenAI adotterà le misure richieste. L'Autorità ha dato tempo alla società fino al 30 aprile per mettersi in regola. (n.d.). Retrieved May 13, 2024, from https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9874751

ChatGPT: Garante privacy, notificato a OpenAI l'atto di contestazione per le violazioni alla normativa privacy. (n.d.). https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9978020

Committee of experts on internet intermediaries (MSI-NET). (2016). STUDY ON THE HUMAN RIGHTS DIMENSIONS OF AUTOMATED DATA PROCESSING TECHNIQUES (IN PARTICULAR ALGORITHMS) AND POSSIBLE REGULATORY IMPLICATIONS. Committee of Europe. https://rm.coe.int/study-on-algorithmes-final-version/1680770cbc

Data Protection Commissioner v Facebook and Max Schrems. (2017). EPIC - Electronic Privacy Information Center. Retrieved January 8, 2024, from https://epic.org/documents/data-protection-commissioner-v-facebook-and-max-schrems-standard-contractual-clauses/

Deng, S., Zhao, H., Fang, W., Yin, J., Dustdar, S., & Zomaya, A. Y. (2020, August). Edge Intelligence: The Confluence of Edge Computing and Artificial Intelligence. IEEE Internet of Things Journal, 7(8), 7457–7469. https://doi.org/10.1109/jiot.2020.2984887

Dwivedi, Y. K., Kshetri, N., Hughes, L., Slade, E. L., Jeyaraj, A., Kar, A. K., Baabdullah, A. M., Koohang, A., Raghavan, V., Ahuja, M., Albanna, H., Albashrawi, M. A., Al-Busaidi, A. S., Balakrishnan, J., Barlette, Y., Basu, S., Bose, I., Brooks, L., Buhalis, D., . . . Wright, R. (2023, August). Opinion Paper: "So what if ChatGPT wrote it?" Multidisciplinary perspectives on opportunities, challenges and implications of generative conversational AI for research, practice and policy. International Journal of Information Management, 71, 102642. https://doi.org/10.1016/j.ijinfomgt.2023.102642

Dwivedi, Y. K., Kshetri, N., Hughes, L., Slade, E. L., Jeyaraj, A., Kar, A. K., Baabdullah, A. M., Koohang, A., Raghavan, V., Ahuja, M., Albanna, H., Albashrawi, M. A., Al-Busaidi, A. S., Balakrishnan, J., Barlette, Y., Basu, S., Bose, I., Brooks, L., Buhalis, D., . . . Wright, R. (2023, August). Opinion Paper: "So what if ChatGPT wrote it?" Multidisciplinary perspectives on opportunities, challenges and implications of generative conversational AI for research, practice and policy. International Journal of Information Management, 71, 102642. https://doi.org/10.1016/j.ijinfomgt.2023.102642

Dwivedi, Y. K., Kshetri, N., Hughes, L., Slade, E., Jeyaraj, A., Kar, A. K., Baabdullah, A. M., Koohang, A., Raghavan, V., Ahuja, M., Albanna, H., Albashrawi, M. A., Al-Busaidi, A. S., Balakrishnan, J., Barlette, Y., Basu, S., Bose, I., Brooks, L., Buhalis, D., . . . Wright, R. (2023, August 1). Opinion Paper: "So what if ChatGPT wrote it?" Multidisciplinary perspectives on opportunities, challenges and implications of generative conversational AI for research, practice and policy. International Journal of Information Management. https://doi.org/10.1016/j.ijinfomgt.2023.102642

Dwivedi, Y. K., Kshetri, N., Hughes, L., Slade, E., Jeyaraj, A., Kar, A. K., Baabdullah, A. M., Koohang, A., Raghavan, V., Ahuja, M., Albanna, H., Albashrawi, M. A., Al-Busaidi, A. S., Balakrishnan, J., Barlette, Y., Basu, S., Bose, I., Brooks, L., Buhalis, D., . . . Wright, R. (2023, August 1). Opinion Paper: "So what if ChatGPT wrote it?" Multidisciplinary perspectives on

opportunities, challenges and implications of generative conversational AI for research, practice and policy. International Journal of Information Management. https://doi.org/10.1016/j.ijinfomgt.2023.102642

Elahi, M., Afolaranmi, S. O., Martinez Lastra, J. L., & Perez Garcia, J. A. (2023, December 7). A comprehensive literature review of the applications of AI techniques through the lifecycle of industrial equipment. Discover Artificial Intelligence, 3(1). https://doi.org/10.1007/s44163-023-00089-x

EUR-Lex - 62010CO0617 - EN - EUR-Lex. (n.d.). https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62010CO0617

Fernhout, & Rad. (2023). Artificial Intelligence Act: an update. Stibbe. Retrieved January 31, 2024, from https://www.stibbe.com/publications-and-insights/artificial-intelligence-act-an-update

Hosseinzadeh, M., Azhir, E., Ahmed, O. H., Ghafour, M. Y., Ahmed, S. H., Rahmani, A. M., & Vo, B. (2021, November 17). Data cleansing mechanisms and approaches for big data analytics: a systematic study. Journal of Ambient Intelligence and Humanized Computing, 14(1), 99–111. https://doi.org/10.1007/s12652-021-03590-2

How AI Is Improving Data Management | MIT Sloan Management Review. (2022, December 20). MIT Sloan Management Review. https://sloanreview.mit.edu/article/how-ai-is-improving-data-management/

How generative AI is reshaping education in Asia-Pacific. (2023, November 30). UNESCO. https://www.unesco.org/en/articles/how-generative-ai-reshaping-education-asia-pacific

Katz v. United States, 389 U.S. 347 (1967). (n.d.). Justia Law. https://supreme.justia.com/cases/federal/us/389/347/

Khan, S. U., Khan, H. U., Ullah, N., & Khan, R. A. (2021, September 3). Challenges and Their Practices in Adoption of Hybrid Cloud Computing: An Analytical Hierarchy Approach. Security and Communication Networks, 2021, 1–20. https://doi.org/10.1155/2021/1024139

Legal Resources | Intelligence Committee. (2005). Retrieved January 8, 2024, from https://www.intelligence.senate.gov/laws/usa-patriot-improvement-and-reauthorization-act-2005

Luan, H., Geczy, P., Lai, H., Gobert, J., Yang, S. J. H., Ogata, H., Baltes, J., Guerra, R., Li, P., & Tsai, C. C. (2020, October 19). Challenges and Future Directions of Big Data and Artificial Intelligence in Education. Frontiers in Psychology, 11. https://doi.org/10.3389/fpsyg.2020.580820

M. Thompson. (2014). The Fourth Amendment Third-Party Doctrine. Retrieved January 8, 2024, from https://sgp.fas.org/crs/misc/R43586.pdf

Mazumdar, S., Seybold, D., Kritikos, K., & Verginadis, Y. (2019, February 11). A survey on data storage and placement methodologies for Cloud-Big Data ecosystem. Journal of Big Data, 6(1). https://doi.org/10.1186/s40537-019-0178-3

Molina, J. L., Tubaro, P., Casilli, A. A., & Ortega, A. S. (2023, April 25). Research Ethics in the Age of Digital Platforms. Science and Engineering Ethics. https://doi.org/10.1007/s11948-023-00437-1

Official Journal of the European Union. (2010). CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION. Retrieved January 6, 2024, from https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:en:PDF

Official Journal of the European Union. (2012). CONSOLIDATED VERSION OF THE TREATY ON THE FUNCTIONING OF THE EUROPEAN UNION. In https://eur-lex.europa.eu/. Retrieved January 6, 2024, from https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:en:PDF

Pedrosa, A. L., Bitencourt, L., Fróes, A. C. F., Cazumbá, M. L. B., Campos, R. G. B., De Brito, S. B. C. S., & Silva, A. C. S. E. (2020, October 2). Emotional, Behavioral, and Psychological Impact of the COVID-19 Pandemic. Frontiers in Psychology. https://doi.org/10.3389/fpsyg.2020.566212

Press corner. (2023). European Commission - European Commission. Retrieved January 8, 2024, from https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752

Rane, N., Choudhary, S., & Rane, J. (2023). Leading-edge Artificial Intelligence (AI)-Powered Financial Forecasting for Shaping the Future of Investment Strategies. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4640828

Ray, P. P. (2023). ChatGPT: A comprehensive review on background, applications, key challenges, bias, ethics, limitations and future scope. Internet of Things and Cyber-Physical Systems, 3, 121–154. https://doi.org/10.1016/j.iotcps.2023.04.003

Scicluna, M., Grenier, J. C., Poujol, R., Lemieux, S., & Hussin, J. G. (2023, January 1). Toward computing attributions for dimensionality reduction techniques. Bioinformatics Advances, 3(1). https://doi.org/10.1093/bioadv/vbad097

Sebastian. (2023). Privacy and Data Protection in ChatGPT and Other AI Chatbots: Strategies for Securing User Information. Retrieved January 31, 2024, from https://www.researchgate.net/profile/GlorinSebastian/publication/370935454_Privacy_and_Data_Protection_in_ChatGPT_and_Other_AI_Chatbots_Strategies_for_Securing_User_Information/links/646a9cd066b4cb4f73c647ef/Privacy-and-Data-Protection-in-ChatGPT-and-Other-AI-Chatbots-Strategies-for-Securing-User-Information.pdf

Secure personal data | European Data Protection Board. (n.d.). https://edpb.europa.eu/sme-data-protection-guide/secure-personal-data_en

Silver, D., Huang, A., Maddison, C. J., Guez, A., Sifre, L., van den Driessche, G., Schrittwieser, J., Antonoglou, I., Panneershelvam, V., Lanctot, M., Dieleman, S., Grewe, D., Nham, J., Kalchbrenner, N., Sutskever, I., Lillicrap, T., Leach, M., Kavukcuoglu, K., Graepel, T., & Hassabis, D. (2016, January 27). Mastering the game of Go with deep neural networks and tree search. Nature, 529(7587), 484–489. https://doi.org/10.1038/nature16961

Silver, D., Huang, A., Maddison, C. J., Guez, A., Sifre, L., van den Driessche, G., Schrittwieser, J., Antonoglou, I., Panneershelvam, V., Lanctot, M., Dieleman, S., Grewe, D., Nham, J., Kalchbrenner, N., Sutskever, I., Lillicrap, T., Leach, M., Kavukcuoglu, K., Graepel, T., & Hassabis, D. (2016, January 27). Mastering the game of Go with deep neural networks and tree search. Nature, 529(7587), 484–489. https://doi.org/10.1038/nature16961

Sivarajah, U., Kamal, M. M., Irani, Z., & Weerakkody, V. (2017, January 1). Critical analysis of Big Data challenges and analytical methods. Journal of Business Research. https://doi.org/10.1016/j.jbusres.2016.08.001

Smith v. Maryland, 442 U.S. 735 (1979). (n.d.). Justia Law. https://supreme.justia.com/cases/federal/us/442/735/

Soori, M., Arezoo, B., & Dastres, R. (2023). Internet of things for smart factories in industry 4.0, a review. Internet of Things and Cyber-Physical Systems, 3, 192–204. https://doi.org/10.1016/j.iotcps.2023.04.006

Tan, T. F., Thirunavukarasu, A. J., Campbell, J. P., Keane, P. A., Pasquale, L. R., Abramoff, M. D., Kalpathy-Cramer, J., Lum, F., Kim, J. E., Baxter, S. L., & Ting, D. S. W. (2023, December). Generative Artificial Intelligence Through ChatGPT and Other Large Language Models in Ophthalmology. Ophthalmology Science, 3(4), 100394. https://doi.org/10.1016/j.xops.2023.100394

Tandon. (n.d.). Challenges of using artificial intelligence. Deloitte United States. Retrieved December 26, 2023, from https://www2.deloitte.com/us/en/pages/consulting/articles/challenges-of-using-artificial-intelligence.html

United States v. Verdugo-Urquidez, 494 U.S. 259 (1990). (n.d.). Justia Law. https://supreme.justia.com/cases/federal/us/494/259/

Unleash the Power of Data Labeling with Label Studio. (2023, November 7). https://www.linkedin.com/pulse/unleash-power-data-labeling-label-studio-machine-learning-reply-de-1tapf/?trk=public_post

USA Congress. (2015). UNITING AND STRENGTHENING AMERICA BY FULFILLING RIGHTS AND ENSURING EFFECTIVE DISCIPLINE OVER MONITORING ACT OF 2015. Retrieved January 8, 2024, from https://www.congress.gov/114/plaws/publ23/PLAW-114publ23.pdf

Viewpoint: Nuclear in the fourth industrial revolution: Perspectives - World Nuclear News. (n.d.). https://world-nuclear-news.org/Articles/Viewpoint-Nuclear-in-the-fourth-industrial-revolut

Xu, Y., Liu, X., Cao, X., Huang, C., Liu, E., Qian, S., Liu, X., Wu, Y., Dong, F., Qiu, C. W., Qiu, J., Hua, K., Su, W., Wu, J., Xu, H., Han, Y., Fu, C., Yin, Z., Liu, M., . . . Zhang, J. (2021, November). Artificial intelligence: A powerful paradigm for scientific research. The Innovation, 2(4), 100179. https://doi.org/10.1016/j.xinn.2021.100179

Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., Zhang, F., & Choo, K. K. R. (2021, March 13). Artificial intelligence in cyber security: research advances, challenges, and opportunities. Artificial Intelligence Review, 55(2), 1029–1053. https://doi.org/10.1007/s10462-021-09976-0

European approach to artificial intelligence. (2024, May 29). Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence

EU AI Act: first regulation on artificial intelligence | Topics | European Parliament. (2023, August 6). Topics | European Parliament. https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

TURING, A. M. (1950, October 1). I.—COMPUTING MACHINERY AND INTELLIGENCE. Mind, LIX(236), 433–460. https://doi.org/10.1093/mind/lix.236.433

Campbell, M., Hoane, A., & Hsu, F. H. (2002, January). Deep Blue. Artificial Intelligence, 134(1–2), 57–83. https://doi.org/10.1016/s0004-3702(01)00129-1

Campbell, M., Hoane, A., & Hsu, F. H. (2002, January). Deep Blue. Artificial Intelligence, 134(1–2), 57–83. https://doi.org/10.1016/s0004-3702(01)00129-1

Boehm, & D.Cole. (2014, June). Data Retention after the Judgement of the Court of Justice of the European Union. Retrieved January 6, 2024, from https://www.greens-efa.eu/legacy/fileadmin/dam/Documents/Studies/Data_protection/FB_MDC_Study_Data_Retention_Judgment_June_2014_FINAL_EXEC_SUMM.pdf

Klayman v. Obama, No. 14-5004 (D.C. Cir. 2015). (2015, August 28). Justia Law. https://law.justia.com/cases/federal/appellate-courts/cadc/14-5004/14-5004-2015-08-28.html

Van De Ven, I. (2015, November 15). Monumental Novels in a Global and Digital Age. Tilburg university. https://www.academia.edu/18366408/Monumental_Novels_in_a_Global_and_Digital_Age

S., & Rockwell . (2017, August 28). The History of Artificial Intelligence - Science in the News. Science in the News. Retrieved December 26, 2023, from https://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/

Kaplan, A., & Haenlein, M. (2019, January 1). Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. Business Horizons. https://doi.org/10.1016/j.bushor.2018.08.004

Talia, D. (2019, February 11). A view of programming scalable data analysis: from clouds to exascale. Journal of Cloud Computing, 8(1). https://doi.org/10.1186/s13677-019-0127-x

Haenlein, M., & Kaplan, A. (2019, July 17). A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence. California Management Review, 61(4), 5–14. https://doi.org/10.1177/0008125619864925

Haenlein, M., & Kaplan, A. (2019, July 17). A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence. California Management Review, 61(4), 5–14. https://doi.org/10.1177/0008125619864925

Overview of the Privacy Act of 1974. (2021, February 24). https://www.justice.gov/archives/opcl/ten-exemptions

Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021, March 26). AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. SN Computer Science, 2(3). https://doi.org/10.1007/s42979-021-00557-0

Galič, M., & Gellert, R. (2021, April 1). Data protection law beyond identifiability? Atmospheric profiles, nudging and the Stratumseind Living Lab. Computer Law & Security Review. https://doi.org/10.1016/j.clsr.2020.105486

Seo, K., Tang, J., Roll, I., Fels, S., & Yoon, D. (2021, October 26). The impact of artificial intelligence on learner–instructor interaction in online learning. International Journal of Educational Technology in Higher Education, 18(1). https://doi.org/10.1186/s41239-021-00292-9

Chubb, J., Cowling, P., & Reed, D. (2021, October 15). Speeding up to keep up: exploring the use of AI in the research process. AI & SOCIETY, 37(4), 1439–1457. https://doi.org/10.1007/s00146-021-01259-0

Stedman, C. (2022, January 28). data cleansing (data cleaning, data scrubbing). Data Management. https://www.techtarget.com/searchdatamanagement/definition/data-scrubbing

European Court of Human Rights. (2022, March). Guide to the Case-Law of the of the European Court of Human Rights. Retrieved January 8, 2024, from https://www.echr.coe.int/documents/d/echr/Guide_Data_protection_ENG

Data protection under GDPR - Your Europe. (2022, June 7). Your Europe. https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.htm

Express Analytics. (2022, July 15). Automated Machine Learning (AutoML): A Guide. Retrieved December 26, 2023, from https://www.expressanalytics.com/blog/what-is-automated-machine-learning-automl/

Overview of the Privacy Act: 2020 Edition. (2022, October 4). https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition/JRA

Privacy Act of 1974. (2022, October 4). https://www.justice.gov/opcl/privacy-act-1974

Overview of the Privacy Act: 2020 Edition. (2022, December 15). https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition/disclosures-third-parties

Singhal, K. (2022, December 26). Large Language Models Encode Clinical Knowledge. arXiv.org. https://arxiv.org/abs/2212.13138

Hillemann, D. (2023, January 30). Does ChatGPT Comply with EU-GDPR Regulations? Investigating the Right to be Forgotten. Fieldfisher. https://www.fieldfisher.com/en/insights/does-chatgpt-comply-with-eu-gdpr-regulations-inves

Calzon, B. (2023, February 14). The Importance of Data Driven Decision Making for Business. BI Blog | Data Visualization & Analytics Blog | Datapine. https://www.datapine.com/blog/data-driven-decision-making-in-businesses/

Suarez, T. V. E. (2023, March 9). ChatGPT: Risks and challenges from a Data Privacy perspective. Datenschutz Notizen | News-Blog Der DSN GROUP. Retrieved January 31, 2024, from https://www.datenschutz-notizen.de/chatgpt-risks-and-challenges-from-a-data-privacy-perspective-0341134/

H. (2023, March 24). United States v. Ganias. Harvard Law Review. https://harvardlawreview.org/print/vol-128/united-states-v-ganias/

Kreitmeir, & Raschky. (2023, April). The Unintended Consequences of Censoring Digital Technology – Evidence from Italy's ChatGPT Ban. Retrieved February 1, 2024, from https://arxiv.org/pdf/2304.09339.pdf

GPDP. (2023, April 12). ChatGPT: Garante privacy, limitazione provvisoria sospesa se OpenAI adotterà le misure richieste. L'Autorità ha dato tempo alla società fino al 30 aprile per mettersi in regola. Retrieved February 1, 2024, from https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9874751#english

Dixon. (2023, May). In the matter of the General Data Protection Regulation. Retrieved January 8, 2024, from https://edpb.europa.eu/system/files/2023-05/final_for_issue_ov_transfers_decision_12-05-23.pdf

catapult creative media. (2023, May 5). ChatGPT-5 Predictions - What Can We Look Forward To. Catapult Creative Media Inc. Retrieved January 23, 2024, from https://catapultcreativemedia.com/chatgpt-5-predictions/

Suarez, T. V. E. (2023, May 12). ChatGPT is back in Italy – What changes have been made and what do users need to know? Datenschutz Notizen | News-Blog Der DSN GROUP. Retrieved February 1, 2024, from https://www.datenschutz-notizen.de/chatgpt-is-back-in-italy-what-changes-have-been-made-and-what-do-users-need-to-know-4642272/

Marr, B. (2023, May 19). A Short History Of ChatGPT: How We Got To Where We Are Today. Forbes. https://www.forbes.com/sites/bernardmarr/2023/05/19/a-short-history-of-chatgpt-how-we-got-to-where-we-are-today/?sh=46bbdb79674f

Younus, H. (2023, June 8). AI and Data Storage: Reducing Costs and Improving Scalability. Astera. https://www.astera.com/type/blog/ai-and-data-storage/

Aldoseri, A., Al-Khalifa, K. N., & Hamouda, A. M. (2023, June 13). Re-Thinking Data Strategy and Integration for Artificial Intelligence: Concepts, Opportunities, and Challenges. Applied Sciences, 13(12), 7082. https://doi.org/10.3390/app13127082

Dhanashree, D. (2023, June 15). Data Automation: A Comprehensive Guide. Nanonets Intelligent Automation, and Business Process AI Blog. Retrieved December 26, 2023, from https://nanonets.com/blog/data-automation/#:~:text=Data%20automation%20uses%20intelligent%20algorithms,data%20quality%2C%20and%20gain%20insights.

Bandi, A., Adapa, P. V. S. R., & Kuchi, Y. E. V. P. K. (2023, July 31). The Power of Generative AI: A Review of Requirements, Models, Input–Output Formats, Evaluation Metrics, and Challenges. Future Internet, 15(8), 260. https://doi.org/10.3390/fi15080260

Analytics, D. (2023, July 26). The Power of Data-Driven Decision Making. https://www.linkedin.com/pulse/power-data-driven-decision-making-data-and-analytics-magazin/

THE EUROPEAN DATA PROTECTION SUPERVISOR. (2023, August 22). THE EUROPEAN DATA PROTECTION SUPERVISOR. www.edps.europa.eu. Retrieved June 3, 2024, from https://www.edps.europa.eu/system/files/2023-08/2023-0730_d2425_opinion_en.pdf

Balch, D. E. (2023, August 25). Artificial Intelligence: The Rise of ChatGPT and Its Implications. Faculty Focus | Higher Ed Teaching & Learning. https://www.facultyfocus.com/articles/teaching-with-technology-articles/artificial-intelligence-the-rise-of-chatgpt-and-its-implications/

AppleTech. (2023, September 1). Data Processing Services: Unlocking Insights for Informed Decision-Making. Retrieved December 26, 2023, from https://www.linkedin.com/pulse/data-processing-services-unlocking-insights-informed-decision-making/

Lukács, A., & Váradi, S. (2023, September). GDPR-compliant AI-based automated decision-making in the world of work. Computer Law & Security Review, 50, 105848. https://doi.org/10.1016/j.clsr.2023.105848

Lawton, G. (2023, September 18). Generative AI vs. predictive AI: Understanding the differences. Enterprise AI. https://www.techtarget.com/searchenterpriseai/tip/Generative-AI-vs-predictive-AI-Understanding-the-differences

Javaid, S. (2023, September 27). Ultimate Guide to Data Collection with 15+ Use Cases in 2023. AIMultiple. https://research.aimultiple.com/data-collection/

Team, I. (2023, September 27). A Brief History of The 4 Industrial Revolutions that Shaped the World. Institute of Entrepreneurship Development. https://ied.eu/project-updates/the-4-industrial-revolutions/

Nayak, A. (2023, October 5). Artificial Intelligence: The Next Industrial Revolution. https://www.linkedin.com/pulse/artificial-intelligence-next-industrial-revolution-alok-nayak/

Torabi, N. (2023, December 5). Unlocking the Power of AI in Product Management: A Comprehensive Guide for Product Professionals. Medium. https://medium.com/beyond-the-build/unlocking-the-power-of-ai-in-product-management-a-comprehensive-guide-for-product-professionals-53198782153e

Lawton, G. (2023, December 15). What is generative AI? Everything you need to know. Enterprise AI. https://www.techtarget.com/searchenterpriseai/definition/generative-AI#:~:text=Generative%20AI%20was%20introduced%20in,and%20audio%20of%20real%20people.

Sinha, S. (2023, December 15). From GPT-1 to GPT-4: A Look at the Evolution of Generative AI. HGS. https://hgs.cx/blog/from-gpt-1-to-gpt-4-a-look-at-the-evolution-of-generative-ai/

Industrial Revolution. (2023, December 16). Wikipedia. https://en.wikipedia.org/wiki/Industrial_Revolution

chatgpt4admin. (2024, January 11). Talking ChatGPT in Europe: Unification at its Roots 2023 - ChatGPT4. ChatGPT4. Retrieved January 31, 2024, from https://chatgpt-4.fyi/chatgpt-in-europe/#ChatGPT_Takes_Off_Across_Europe

Data Protection. (2024, January 25). European Data Protection Supervisor. https://edps.europa.eu/data-protection/data-protection_en

GPDP. (2024, January 29). ChatGPT: Garante privacy, notificato a OpenAI l'atto di contestazione per le violazioni alla normativa privacy. Retrieved February 5, 2024, from https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9978020

IBM. (n.d.). What is explainable AI? | IBM. Retrieved December 26, 2023, from https://www.ibm.com/topics/explainable-ai