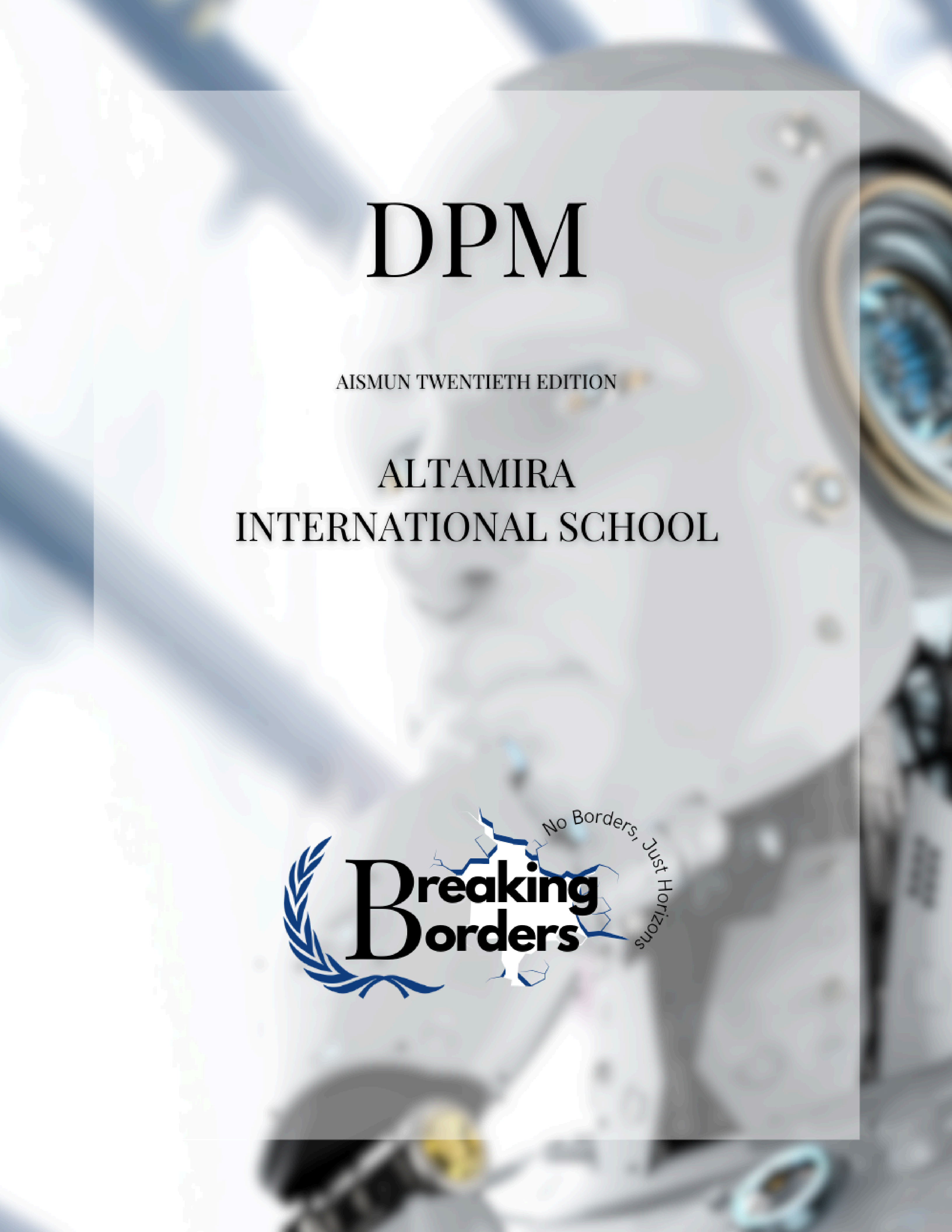
DPM

PRESIDENT SANTIAGO BRAVO

FEBRUARY 29TH –MARCH 3RD

AISMUN XX



DPM

AISMUN TWENTIETH EDITION

ALTAMIRA
INTERNATIONAL SCHOOL

Breaking Borders

No Borders, Just Horizons

Table of Content:

I. Welcoming Letter

Dear Delegates,

Warm greetings and a cordial welcome to AISMUN XX. I am Santiago Bravo, and it is both a privilege and an honor to serve as the Chair of the Data Privacy Management Committee. I'm excited about the journey ahead and the interesting discussions we're about to have. The Data Privacy Management Committee plays a key role in addressing the complex issues of data privacy, especially within the context of Artificial Intelligence. Our main goal is to work together and find responsible solutions to current issues through careful discussions and innovative thinking.

While DPM may not be an official United Nations committee, the principles of diplomacy, respect, and constructive dialogue are fundamental to our proceedings. Let us engage with a spirit of cooperation, always cognizant of the global impact our decisions may wield. Expectations are high for this committee, and your active participation is imperative for our collective success.

This guide is crafted to be a valuable resource, aiding you during your participation in the committee. It offers comprehensive background information and guidance to navigate the intricate terrain of data privacy and Artificial Intelligence. I encourage each delegate to undertake independent research to deepen your understanding of the topics and the character you represent. Please do not hesitate to reach out to me when you need clarification, guidance, or additional information. Your dedication to the committee's mission is crucial, and I am confident that together, we will embark on a remarkable journey, contributing to the responsible development of Artificial Intelligence. Let us approach this challenge with enthusiasm, respect, and commitment to make a meaningful impact.

Warm regards,

Santiago Bravo
Dias, Data Privacy Management Committee

sbravos@altamira.edu.co +57 300 534 8758

II. Introduction to DPM

2.1 History

DPM is a forward-thinking committee focused on a significant global problem—protecting the privacy of user information on major social media platforms like Facebook, Instagram, and TikTok, and understanding how this can affect individuals. It is not officially part of the United Nations, however, it addresses a worldwide issue that impacts the international community. In contrast to traditional committees, DPM does not assign countries to participate in the discussions; instead, it involves leaders such as presidents and CEOs of influential companies. This unique approach allows us to look at the issue from a fresh angle and find creative solutions to safeguard data privacy in our connected world.

2.2 Organization and functions

The delegates are going to be in charge of defending the position of their company, making use of strong arguments, discussing real-life events that impacted users, and seeking solutions to handle these difficulties. Their role is not just to advocate for their company's interests, but also to engage in a rigorous analysis of incidents that have had significant repercussions on user experience and privacy. They are expected to bring forth innovative solutions to complex problems, addressing not only the business implications but also the ethical dimensions of data protection and user rights. The committee's commitment to safeguarding people's privacy is a testament to the evolving understanding of privacy as a fundamental right. Thus, the delegates' responsibilities extend beyond mere representation; they are guardians of trust and integrity in a digital age where information security is paramount. It is important to mention that DPM is not an official committee of the UN, but it is a space for delegates to debate about cybersecurity topics.

2.3 Main goals of the committee

The main goal of this committee is to seek global solutions regarding specific topics such as the dangers of AI. With a multidimensional approach, this committee delves into in-depth research, policy formulation, risk mitigation strategies, international collaboration, public education, and ethical considerations. Its primary focus revolves around understanding, predicting, and addressing the potential risks that arise from the ongoing advancements in AI technology. Establishing global policies and ethical guidelines stands as a cornerstone, ensuring the responsible development and deployment of AI. Mitigating risks like bias, cybersecurity vulnerabilities, and potential societal impacts, the committee fosters collaboration among experts, organizations, and nations to shape policies and enforcement strategies. Furthermore, it plays a vital role in educating the public, and enhancing awareness of both the risks and benefits of AI, while actively engaging in ethical discussions to align AI evolution with fundamental ethical principles and human rights. Through this collective effort involving diverse experts, the committee aims to maximize the benefits of AI while proactively addressing its potential risks on a global scale.

2.4 References

1. Shea, S., & guide, s. (n.d.). What is Cybersecurity? Everything You Need to Know. TechTarget. Retrieved January 23, 2024, from https://www.techtarget.com/searchsecurity/definition/cybersecurity
2. What is Data Privacy? (n.d.). SNIA. Retrieved January 23, 2024, from https://www.snia.org/education/what-is-data-privacy
3. What is Artificial Intelligence (AI) ? (n.d.). IBM. Retrieved January 23, 2024, from https://www.ibm.com/topics/artificial-intelligence
4. Laskowski, N. (n.d.). What is Artificial Intelligence and How Does AI Work? | Definition from TechTarget. TechTarget. Retrieved January 23, 2024, from https://www.techtarget.com/searchenterpriseai/definition/AI-Artificial-Intelligence

III. Topic: Artificial Intelligence

3.1 Introduction

The Data Privacy Management Committee is dedicated to addressing the challenges associated with handling information responsibly in today's digital landscape. In this committee, representatives from various companies and CEOs collaborate to discuss and develop strategies for safeguarding data and respecting individual privacy rights.

Our discussions encompass a broad range of crucial topics, including artificial intelligence, cybersecurity, and effective data management. As technology continues to advance, the committee's primary focus is to establish smart and ethical rules that strike a balance between harnessing innovation and ensuring the protection of sensitive information. This involves exploring best practices and developing comprehensive frameworks to guide responsible data governance within the business sector.

The overarching goal of the DPM Committee is to foster an environment of collaboration and knowledge-sharing. Representatives engage in dialogue, share insights, and work collectively to find practical solutions that enhance data security. It serves as a platform for learning and adapting to the evolving digital landscape, promoting responsible practices that not only benefit individual companies but also contribute to a global standard of ethical data management in the business world.

Now, we need to have a deep understanding about one topic: Artificial Intelligence. The field of artificial intelligence has become a transformational force that is changing everyday life and many sectors. The creation of computer systems that are capable of activities that normally require human intelligence is the essence of artificial intelligence. This covers problem-solving techniques, adjusting to new knowledge, and experience-based learning. Artificial Intelligence is now at the forefront of technological innovation thanks to the quick advances in machine learning, neural networks, and natural language processing. These developments have made it possible for intelligent systems to analyze large datasets, make predictions, and automate decision-making processes.

The potential of AI to increase production and efficiency in a variety of industries is one of its main features. AI applications enhance resource usage, minimize errors, and accelerate processes across a variety of industries, including manufacturing, healthcare, and finance. AI-powered diagnostic technologies, for example, can accurately evaluate medical images, helping medical personnel identify problems early on. Artificial intelligence is used in finance to forecast investment opportunities and evaluate market trends. In manufacturing, AI-driven robotics optimizes production lines to increase overall operational efficiency. The widespread application of AI technologies has the power to completely transform our daily lives and work environments, bringing in a period of convenience and innovation never seen before.

But the quick adoption of AI also brings up social and ethical issues. Concerns about accountability, prejudice, and privacy are raised by the advanced technology of AI systems. To avoid discriminatory results, AI algorithms must be open and fair. Ethical frameworks must be put in place to control the use of AI in delicate areas. Furthermore, worries about job displacement are raised by the possible effects of AI on employment, which calls for a careful approach to retraining and upskilling the workforce. Achieving a balance between utilizing AI's advantages and tackling the moral and societal issues that result from its broad use is crucial for managing the technology's future.

3.2 Historical Background

Artificial Intelligence (AI) is a discipline that encompasses a broad range of approaches, techniques, and applications. Its primary goal is to develop systems and machines capable of performing tasks that, until recently, could only be carried out by humans. AI is based on the idea that computers can learn, reason, and make decisions similarly to humans. This field has evolved over the decades, transitioning from symbolic logic in its early days to the current advances in deep learning, where artificial neural networks can model complex data. AI has a profound influence on our daily lives and is transforming entire industries, from healthcare to transportation.

Origins of Artificial Intelligence

The origins of artificial intelligence (AI) date back to the 1950s, though its theoretical foundations were laid earlier through Alan Turing's exploration of the Turing machine. Initially focused on problem-solving and logical reasoning, AI saw pivotal moments with breakthroughs like IBM's Deep Blue, demonstrating machines' capability in complex cognitive tasks. However, the true resurgence of AI emerged in the 21st century due to increased computational power, vast data availability, and advancements in algorithms, propelling the renaissance of neural networks and the ascent of deep learning. This revitalization led to AI applications across numerous fields, including virtual assistants, autonomous vehicles, and robotics. Despite these advancements, the pursuit of artificial general intelligence (AGI) remains a key goal, seeking to create more generalized AI systems capable of human-like adaptability and intelligence.

The history of AI traces its roots to a time when the notion of machines imitating human cognitive functions sparked both fascination and skepticism. In the 1940s, Alan Turing, a British mathematician, laid the groundwork for modern computing and AI with his groundbreaking concept of the Turing machine. Turing's theoretical model demonstrated the idea of computation through a set of rules, offering a basis for the development of algorithms and computing machines that could simulate human reasoning. The term "artificial intelligence" was coined in 1956 during a conference at Dartmouth College, where researchers from various disciplines gathered to explore the possibilities of creating machines capable of intelligent behavior. This event marked the formal birth of AI as a field of study and research.

Early AI endeavors primarily focused on symbolic reasoning and problem-solving techniques. Programs were developed to manipulate symbols based on predefined rules, exemplified by systems like the Logic Theorist, created by Allen Newell and Herbert A. Simon. These efforts aimed to replicate human decision-making processes through logical inference and problem-solving. One of the pivotal moments in the history of AI came in 1997 when IBM's Deep Blue defeated chess world champion Garry Kasparov. This victory showcased the potential of AI in mastering complex games by combining brute computational force with sophisticated algorithms, a significant achievement in demonstrating machine intelligence.

However, the exponential growth and widespread application of AI in the 21st century can be attributed to various factors. Advancements in hardware, particularly the development of faster processors and the parallel processing capabilities of graphical processing units (GPUs), empowered AI systems to handle more extensive and complex computations. Furthermore, the proliferation of big data provided AI systems with an abundance of information, essential for training and improving their algorithms.

The renaissance of neural networks, particularly deep learning, has been a game-changer in the field of AI. Neural networks, which mimic the human brain's structure, had been explored earlier but saw a resurgence due to the availability of vast amounts of data and more sophisticated algorithms. Deep learning techniques, empowered by neural networks with numerous interconnected layers, revolutionized pattern recognition, natural language processing, and image classification, among other tasks.

The applications of AI have diversified across industries, transforming sectors such as healthcare, finance, transportation, and entertainment. AI-powered virtual assistants like Siri and Alexa have become integral parts of daily life while self-driving cars and robotics have showcased the potential for AI in revolutionizing transportation and manufacturing. Despite these significant advancements, the pursuit of artificial general intelligence (AGI) remains an elusive goal. AGI aims to create AI systems that possess human-like adaptability, learning capabilities, and general intelligence across various domains. Achieving AGI would signify a significant leap in the evolution of AI, potentially leading to groundbreaking advancements and innovations.

In conclusion, while the roots of artificial intelligence stretch back to the mid-20th century with foundational concepts from Turing and early explorations in symbolic reasoning, the true resurgence of AI in the 21st century owes much to advancements in computing power, the availability of vast data, and the reinvigoration of neural networks and deep learning. The journey of AI continues, with the quest for artificial general intelligence standing as the ultimate ambition in the field, promising further remarkable advancements in the future.

Current Advances and Future of AI

In recent years, the field of Artificial Intelligence (AI) has witnessed a remarkable resurgence, driven by the emergence of deep learning techniques and unprecedented access to vast troves of data. Deep learning, a subfield of machine learning, has proved to be a game-changer in AI research (IBM, 2023). These sophisticated algorithms are designed to mimic the human brain's neural structure, enabling machines to learn from data and iteratively enhance their performance through experience. This transformative capability has led to a cascade of impressive advancements across various domains.

One of the most striking achievements of deep learning is its profound impact on natural language processing. AI models like OpenAI's GPT-3 and BERT have demonstrated remarkable language understanding and generation capabilities. According to (ZDnet, 2023), they can draft coherent articles, translate languages with exceptional accuracy, and even engage in human-like conversations. These advancements have the potential to revolutionize communication, content creation, and customer service across industries.

Another domain where deep learning has left an indelible mark is computer vision. Convolutional Neural Networks (CNNs), a subset of deep learning, have achieved superhuman performance in image recognition tasks. For instance, in healthcare, AI models can analyze medical images like X-rays and MRIs, aiding doctors in diagnosing diseases with higher accuracy and speed. In the automotive industry, computer vision algorithms enable self-driving cars to navigate complex environments by recognizing and reacting to road signs, pedestrians, and other vehicles.

Additionally, deep learning has catalyzed advancements in autonomous decision-making. Reinforcement learning, a technique within deep learning, has empowered AI agents to excel in games like chess, Go, and Dota 2, surpassing human capabilities. Beyond gaming, these AI models are applied in robotics, where they can control robotic arms with precision, making them invaluable in manufacturing and healthcare.

The future of AI is undeniably promising, with ongoing research poised to expand its frontiers. In medicine, AI is expected to play a pivotal role in personalized healthcare, tailoring treatments to individual patients based on their genetic makeup and medical history. In robotics, AI-driven automation will revolutionize industries by streamlining processes, reducing costs, and enhancing productivity. Education stands to benefit from AI-powered personalized learning experiences, while resource management will leverage AI for the efficient allocation of energy, water, and other critical resources.

As AI continues to evolve, its potential applications are limited only by our imagination and ethical considerations. The collaboration between human ingenuity and AI's computational prowess promises a future where intelligent machines enhance our lives in ways we are only beginning to understand.

Prominent Figures in AI

The history of Artificial Intelligence (AI) is illuminated by the remarkable contributions of individuals who have left an enduring imprint on the discipline. Among these notable figures, Alan Turing stands out as a trailblazer in the realm of computer theory. His pioneering work not only laid the theoretical groundwork for AI but also made significant strides in deciphering the complex realm of machine intelligence (Copeland, 2023). Turing's legacy extends far beyond his era, resonating deeply with modern AI research.

John McCarthy, widely acknowledged as one of the foundational figures in the AI community, not only bestowed the field with its very nomenclature but also embarked on a relentless journey to advance the concept of machines capable of emulating human thought processes. McCarthy's unwavering advocacy for the development of “thinking machines” has had a lasting impact on the philosophical underpinnings of AI.

In the archives of AI history, two luminaries who have left an indelible mark are Marvin Minsky and Geoffrey Hinton. Marvin Minsky's groundbreaking research in cognitive science and neural networks not only paved the way for a paradigm shift in AI but also ignited fresh perspectives in the field. His exploration of neural networks, in particular, laid the groundwork for subsequent innovations in deep learning, reshaping the very fabric of AI research (Fajardo, 2021).

In a parallel trajectory, Geoffrey Hinton's pioneering work in artificial neural networks and deep learning has had a transformative influence on the AI landscape. His unwavering commitment to unlocking the intricacies of neural networks has yielded not only significant advancements in AI but has also reignited interest in the age-old dream of machines that can learn and adapt autonomously.

These distinguished individuals, among others, collectively form the pantheon of AI, molding its trajectory and continually influencing the world today. Their pioneering work, characterized by relentless curiosity and groundbreaking insights, continues to inspire AI researchers and enthusiasts alike.

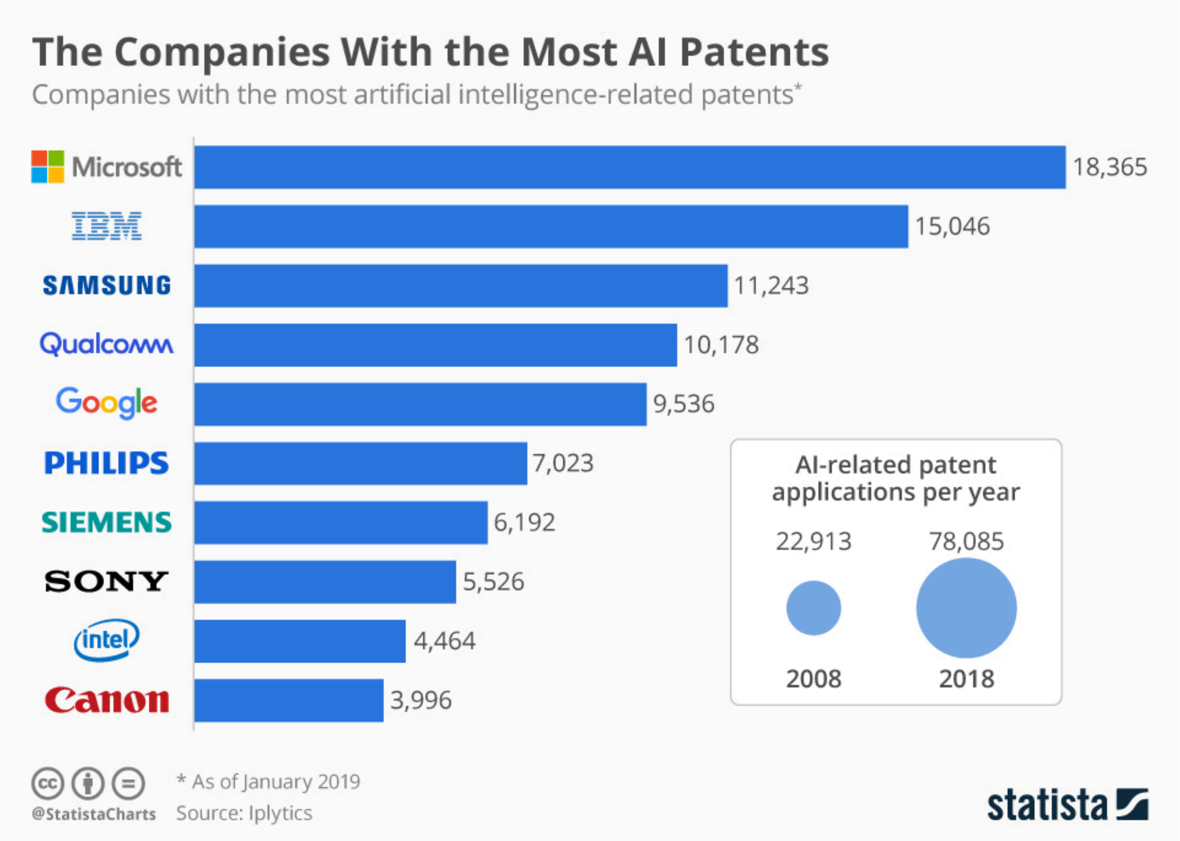
Companies and Investments

Prominent technology companies like Google, Facebook, Microsoft, and Tesla are fiercely competing to lead in the development and implementation of AI technologies. Their strategies encompass strategic acquisitions of AI startups, the formation of specialized teams, substantial investments in research and development, and the integration of AI into their products and services.

These industry leaders strategically identify and acquire promising AI startups, granting them access to cutting-edge technologies and top-tier talent. For example, Google's acquisition of DeepMind in 2014 propelled it to the forefront of AI research. Concurrently, they assemble elite teams of researchers, engineers, and data scientists dedicated to pushing the boundaries of AI technologies.

Significant financial resources are dedicated to AI research and development, with a dual purpose: enhancing existing AI applications and exploring new frontiers. Ethical considerations are central, as these companies actively engage in discussions regarding responsible AI development, algorithmic fairness, and data privacy.

As AI continues to advance, its applications span diverse industries, including healthcare, finance, and transportation. These technologies are reshaping medical diagnoses, making financial predictions more accurate, and even powering autonomous vehicles. The ongoing competition and collaboration among these tech giants are driving the AI landscape forward, promising transformative changes that will shape our digital future in unprecedented ways. With AI at the forefront of technological innovation, the possibilities for its impact on society are continually expanding, and we can expect to witness remarkable advancements in the years to come.



The Companies With the Most AI Patents

Companies with the most artificial intelligence-related patents*

* As of January 2019
Source: Iplytics

Berman, B (2019) *10 Japanese businesses are among the top 16 Artificial Intelligence patent holders, says WIPO report* IP CloseUp

Countries Leading in AI Usage

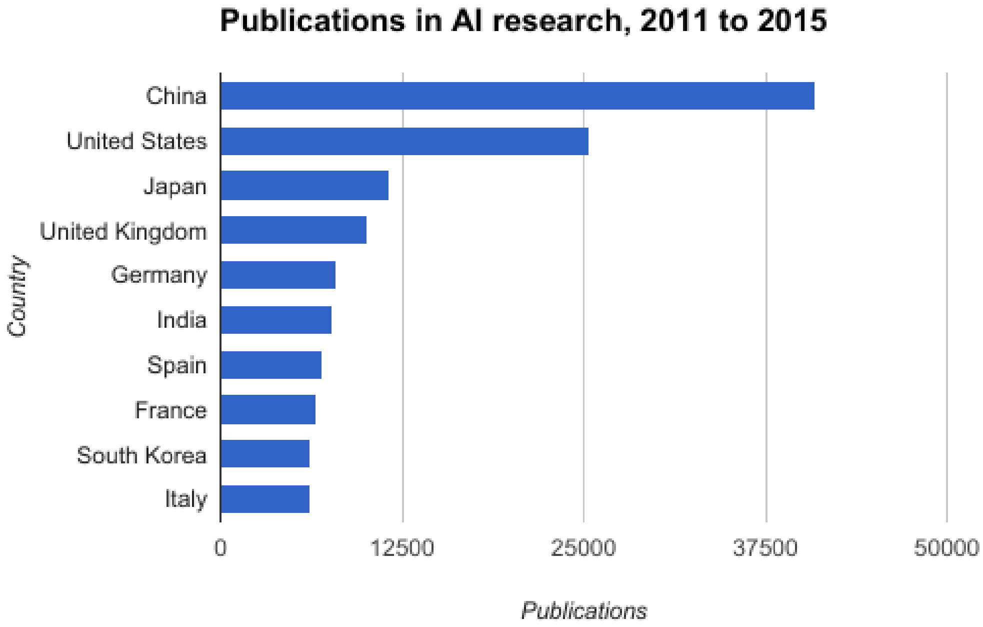
Countries such as China and the United States are undisputed heavyweights in the global AI arena, each contributing uniquely to the field's growth and transformation. China, in particular, has embarked on an audacious mission to establish itself as a dominant force in AI. The country has committed significant resources to research and development, exemplified by initiatives like "Made in China 2025," which prioritizes AI as a key technological focus. This commitment has translated into remarkable advancements, with

AI applications permeating various aspects of daily life, from smart cities to autonomous vehicles. However, China's rapid AI expansion has also sparked concerns about privacy and surveillance, leading to global discussions on ethical AI use. These challenges underscore the importance of responsible AI implementation alongside innovation.

In the United States, the heart of technological innovation lies in Silicon Valley, where industry leaders like Google, Facebook, and Tesla drive AI research and development. Top-tier universities and research labs across the nation further solidify the United States' status as an AI powerhouse. Yet, the country faces its own set of challenges, including ethical considerations in areas such as surveillance, data privacy, and cybersecurity.

Beyond these two powerful nations, countries like Canada, the United Kingdom, and various European nations have made significant strides in AI. Canada, known for its deep pool of AI talent, has produced influential researchers like Geoffrey Hinton. The United Kingdom's AI sector is thriving, marked by investments in AI startups and research endeavors. European countries, as a collective force, have demonstrated their commitment to AI through initiatives like the European Commission's "Digital Europe Program."

However, in the global AI landscape, international collaboration and ethical concerns are increasingly crucial. Responsible AI development and equitable access to AI innovations are shared responsibilities among nations. This ensures that AI technologies continue to benefit humanity while addressing challenges related to privacy, security, and fairness.



Baker, S (2017) Which countries and universities are leading on AI research? | THE News

Risks and Ethics of AI

AI poses ethical and societal challenges. AI systems can make biased decisions if trained on partial data, potentially amplifying existing inequalities. There is also concern that AI could displace jobs in certain industries, necessitating careful attention to retraining and job transition. Additionally, AI security is a critical issue, as its misuse could have severe consequences.

AI presents complex ethical and societal challenges that demand careful consideration. One major concern is the potential for AI systems to perpetuate biases found in their training data, which can lead to discriminatory outcomes. For instance, facial recognition technology has demonstrated higher error rates for individuals with darker skin tones due to underrepresentation in the training data, thereby reinforcing racial inequalities.

Additionally, the automation capabilities of AI raise worries about job displacement in various industries. As AI and robotics are increasingly integrated into workplaces, there is a risk of job loss in sectors such as manufacturing and customer service. This necessitates a proactive approach, including job transition programs and workforce retraining initiatives, to ensure that the workforce can adapt to these changes and thrive in an AI-driven world. These ethical and societal challenges underscore the importance of responsible AI development and the need for regulations and safeguards to ensure that AI technologies benefit society as a whole.

Where We Encounter AI

AI has become an integral part of our daily lives, permeating a multitude of sectors and applications. Beyond the realm of conversational AI, exemplified by ChatGPT, its presence is felt in various domains. In the world of e-commerce, AI-driven recommendation systems, as seen on platforms like Amazon, analyze user preferences to suggest products, significantly influencing purchasing decisions. In finance, AI algorithms play a crucial role in fraud detection, credit scoring, and algorithmic trading, bolstering security and efficiency in the financial sector.

In healthcare, AI assists in medical image analysis, leading to more accurate diagnoses in radiology and pathology. Chatbots and virtual health assistants provide patient support and healthcare information. The entertainment industry leverages AI in streaming services like Netflix, which uses AI to personalize content recommendations based on viewers' history, enhancing user experiences. From gaming and education to energy optimization, agriculture, and language translation, AI's transformative power continues to reshape industries and improve our daily interactions with technology. It has established itself as an indispensable tool across various sectors, enhancing productivity, accuracy, and convenience in our everyday lives.

3.3 Current Situation

As of 2024, artificial intelligence continues to advance in many aspects. Research efforts are driving improvements in machine learning, natural language processing, and computer vision. Industries are increasingly integrating AI technologies to enhance efficiency, productivity, and decision-making. Ethical considerations in AI development are gaining prominence, leading to discussions on bias, fairness, and accountability. In healthcare, AI plays a pivotal role in diagnostics, personalized medicine, and drug discovery. Governments are actively developing regulations to govern AI use, addressing ethical and privacy concerns. Natural language processing is evolving, enabling more natural and context-aware interactions. Automation, driven by AI, is transforming industries, while challenges such as interpretability and robustness persist, prompting ongoing research for solutions. The deployment of AI on edge devices is also becoming more prevalent, contributing to real-time processing and reduced latency.

Additionally, AI in 2024 sees an increased emphasis on collaboration between academia, industry, and policymakers to foster responsible AI innovation. Robust ecosystems are emerging, nurturing startups and fostering interdisciplinary research initiatives.

Explainability and interpretability of AI models are becoming focal points of development, ensuring transparency and trust in AI applications. Continuous efforts in upskilling the workforce in AI-related competencies are underway to address the growing demand for skilled professionals. AI's role in addressing global challenges, such as climate change and public health crises, is gaining recognition, with researchers exploring innovative solutions. The dynamic nature of the AI field, marked by continuous breakthroughs, challenges, and societal impact, underscores its integral role in shaping the future across diverse sectors.

3.4 Focus 1: Ethics in the Creation of Advanced Artificial Intelligence

This topic could explore ethical challenges related to the creation of AI systems that have the ability to make autonomous and complex decisions. What should be the role of ethics in AI programming? How can we ensure that AI systems act in a morally responsible manner? These pressing questions become even more significant as we venture into an era where AI's decision-making prowess encroaches upon domains traditionally governed by human discretion. The role of ethics in AI programming is not just to serve as a passive framework but to actively guide the development and deployment of AI systems. It is a multi-layered process that requires embedding ethical considerations into every phase of AI development, from the initial design to the final output.

Ensuring that AI systems act in a morally responsible manner requires a proactive approach. This involves not only the incorporation of ethical codes but also the establishment of robust mechanisms for monitoring and enforcing these principles. Developers and stakeholders must work hand in hand to define what constitutes ethical behavior for AI, translating abstract moral concepts into programmable criteria that can guide AI behavior in a consistent and predictable manner. It also necessitates an interdisciplinary dialogue to define and operationalize ethical guidelines that are informed by a diverse array of cultural and philosophical perspectives.

Furthermore, the establishment of oversight bodies to govern the ethical deployment of AI could provide a layer of accountability. These bodies would not only set standards but also evaluate AI systems for ethical compliance, similar to ethical review boards that oversee research involving human subjects. Additionally, engaging the public in conversations about the ethical implications of AI can help to ensure that the development of these systems aligns with societal values and expectations. The ethical programming of AI also extends to its data sources. The data used to train AI systems must be scrutinized for bias and representativeness to prevent the perpetuation of inequalities. There is a need for transparent methodologies and data governance models that prioritize the ethical use of information, respecting privacy and consent, and recognizing the rights of individuals whose data is utilized.

As AI systems grow more complex, the strategies to ensure their moral responsibility must also evolve, integrating advanced ethical reasoning capabilities within AI. This could involve simulating human ethical decision-making processes or creating novel frameworks that enable AI to navigate moral dilemmas autonomously. In essence, the quest to instill moral responsibility in AI is not just a technical challenge but a societal imperative, calling for a collective commitment to steer the course of artificial intelligence toward a future that reflects our shared ethical ideals.

3.5 Focus 2: Impact of Artificial Intelligence on Employment and the Economy

AI-driven automation is changing labor and economic dynamics. Delegates could explore how to mitigate potential negative impacts on employment and how to encourage workforce adaptation as AI expands. This pivot point in the evolution of work calls for a nuanced understanding of the transformation AI brings. Policymakers, businesses, and educational institutions must collaborate to identify strategies that not only cushion the disruption but also harness the potential of AI to create new opportunities.

Addressing the displacement of jobs due to automation requires a proactive re-skilling agenda. As routine tasks are automated, the workforce must be prepared with skills that AI cannot replicate easily, such as critical thinking, emotional intelligence, and creative problem-solving. Investment in continuous learning and vocational training programs becomes imperative, ensuring that workers can transition to roles that complement the capabilities of AI. Furthermore, there is an urgent need to reassess economic policies and consider the introduction of safety nets such as universal basic income, especially for sectors most vulnerable to automation. The goal is to create an economy that accommodates the shifts in labor demand, promotes entrepreneurial ventures, and facilitates the creation of new industries that AI and automation may spawn.

Encouraging workforce adaptation also means fostering a culture of lifelong learning, where adapting to technological changes is an integral part of career development. Partnerships between industry and academia can yield specialized curriculums that are in sync with the evolving requirements of the job market. Moreover, by leveraging AI itself, personalized learning platforms can be developed to facilitate more efficient and accessible education. In the wake of AI's ascendancy, it is also vital to deliberate on ethical labor practices and ensure that AI-driven tools are designed to support workers rather than replace them. This entails establishing frameworks for ethical AI use in the workplace, protecting workers' rights, and promoting an inclusive approach that considers the diverse impacts of automation across different demographics.

Ultimately, as AI continues to advance, the collective challenge will be to steer these developments towards augmenting human potential and securing economic resilience. By anticipating the changes and preparing accordingly, society can aim to not only mitigate the risks associated with AI and automation but also unlock a future of greater innovation and prosperity.

3.6 Focus 3: Cybersecurity and Artificial Intelligence Threats

AI can be used both to protect and attack information systems. Delegates could discuss emerging AI-driven cybersecurity threats and how governments and businesses can defend against them.

To address these threats, countries, industries, and experts in cybersecurity need to collaborate. Delegates can explore creating global rules and standards for sharing information about threats and the best ways to handle them. Working together helps us better handle AI-related cyber threats, making the digital world safer for everyone.

Additionally, it's crucial to consider the ethics of using AI for cybersecurity. When governments and businesses use AI to defend against attacks, there should be clear rules to ensure responsible use. This involves being transparent about how AI works, taking responsibility for decisions it makes, and implementing safeguards to avoid unintended consequences. By considering ethics, delegates contribute to building a secure digital world that balances innovation with responsible use.

3.7 Focus 4: AI and Sustainable Development

Explore how artificial intelligence can help make the economy better and solve big problems around the world. Talk about how AI can be used to use resources smarter, make industries work better, and help take care of the environment. Look into how AI can come up with new ideas to tackle problems like climate change, poverty, and inequality. Think about how AI can affect the economy by improving things like renewable energy, smart buildings, and sustainable farming. Delegates in the discussion can figure out ways to use AI to reach goals for sustainable development, making sure that economic growth helps protect the environment and treat everyone fairly. The main idea is to find ways that AI can be a positive force for the economy and make sure it helps with long-term sustainability.

3.8 Guiding Questions

1. How can governments balance the need for data privacy regulations with the promotion of innovation in AI technologies?

2. What measures can be taken to ensure that AI algorithms do not perpetuate biases and discrimination in decision-making processes?

3. In the era of IoT, how can individuals maintain control over their personal data generated by interconnected devices?

4. How can AI-driven surveillance technologies be regulated to protect individual privacy rights while addressing security concerns?

5. What ethical considerations should be taken into account when deploying AI in healthcare, especially in cases involving patient data and diagnoses?

6. How can organizations ensure transparency and accountability in AI systems, particularly in contexts where autonomous decision-making is involved?

7. What role can international cooperation play in addressing global data privacy challenges associated with cross-border data flows and AI applications?

8. What strategies should be employed to protect data privacy in the age of AI-powered virtual assistants and chatbots that handle personal information?

9. How can data anonymization techniques be improved to balance the need for data analysis with the protection of individual privacy?

10. What are the potential risks and benefits of using AI in the legal sector, particularly concerning document review and contract analysis?

3.9 Recommendations

The dais recommends delegates to investigate thoroughly what the company that is being represented has done with regard to the management of data and AI, and how they have handled the matter of privacy and security. As well as for the world leaders that are part of the committee, it is recommended that they investigate the country's position regarding the topic so that representatives get a broader understanding of the different positions in the committee. Finally, keep in mind the formality of this system.

3.10 Useful Links

- What is Artificial Intelligence (AI) ? (n.d.). IBM. Retrieved September 13, 2023, from https://www.ibm.com/topics/artificial-intelligence

- What are the risks of artificial intelligence (AI)? (n.d.). Tableau. Retrieved September 13, 2023, from https://www.tableau.com/data-insights/ai/risks

- Haan, K. (2023, April 24). How Businesses Are Using Artificial Intelligence In 2023. Forbes. Retrieved September 13, 2023, from https://www.forbes.com/advisor/business/software/ai-in-business/

- Artificial Intelligence (AI) vs. Machine Learning | Columbia AI. (n.d.). Columbia University. Retrieved September 13, 2023, from https://ai.engineering.columbia.edu/ai-vs-machine-learning/

- Zenonos, A. (n.d.). Artificial Intelligence and Data Protection | by Alexandros Zenonos, PhD. Towards Data Science. Retrieved September 13, 2023, from https://towardsdatascience.com/artificial-intelligence-and-data-protection-62b333180a27

- AI Ethics. (n.d.). IBM. Retrieved September 13, 2023, from https://www.ibm.com/topics/ai-ethics

3.11 Glossary

1. ***Data Privacy:*** Data privacy refers to the protection of personal information from unauthorized access or disclosure. It encompasses practices, regulations, and technologies aimed at safeguarding sensitive data.

2. ***Artificial Intelligence (AI):*** AI is a branch of computer science that focuses on creating intelligent machines capable of learning from data, reasoning, and making decisions.

3. ***Machine Learning:*** Machine learning is a subset of AI that involves the development of algorithms that enable computers to learn and make predictions or decisions without explicit programming.

4. ***Deep Learning:*** Deep learning is a subfield of machine learning that uses neural networks with multiple layers to process and analyze complex data, such as images and text.

5. ***Privacy by Design:*** Privacy by design is an approach to system development that prioritizes data privacy and protection from the outset, rather than as an afterthought.

6. ***Biometric Data:*** Biometric data refers to unique physical or behavioral characteristics, such as fingerprints or facial recognition, used for authentication and identification.

7. ***Consent Management:*** Consent management involves obtaining and managing user consent for the collection and processing of their personal data, in compliance with privacy regulations.

8. ***GDPR (General Data Protection Regulation):*** GDPR is a European Union regulation that governs data protection and privacy, setting strict standards for the handling of personal data.

9. ***Data Breach:*** A data breach is an unauthorized access, disclosure, or acquisition of sensitive data, often resulting in the exposure of personal information.

10. ***Algorithm Bias:*** Algorithm bias occurs when AI systems make unfair or discriminatory decisions due to biases present in the training data.

11. ***Encryption:*** Encryption is the process of converting data into a coded form to prevent unauthorized access, ensuring data privacy and security.

12. ***IoT (Internet of Things):*** IoT refers to interconnected devices and objects that collect and exchange data, raising privacy concerns regarding data generated by these devices.

13. ***Anonymization:*** Anonymization is the process of removing personally identifiable information from data to protect individuals' privacy while allowing for analysis and research.

14. ***Data Protection Impact Assessment (DPIA):*** DPIA is a systematic evaluation of data processing activities to assess and mitigate potential risks to data privacy.

15. ***Ethical AI:*** Ethical AI refers to the development and use of AI technologies responsibly and ethically, considering fairness, transparency, and societal impact.

3.12 References

- Cloudian. (2022, 20 junio). Data Protection and Privacy: 12 Ways to Protect User Data. **https://cloudian.com/guides/data-protection/data-protection-and-privacy-7-ways-to-protect-user-data/**

- *Cyber / online crime | The Crown Prosecution Service*. (2022, 3 noviembre). https://www.cps.gov.uk/crime-info/cyber-online-crime

- *Personal Data Protection and Privacy | United Nations - CEB*. (s. f.). https://unsceb.org/privacy-principles

- *OHCHR | Special Rapporteur on the right to privacy*. (s. f.). OHCHR. https://www.ohchr.org/en/special-procedures/sr-privacy
- Klosowski, T. (2021, 8 septiembre). *The State of Consumer Data Privacy Laws in the US (And Why It Matters)*. Wirecutter: Reviews for the Real World. https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/

- Data Protection and Privacy Legislation Worldwide. UNCTAD. (n.d.). Retrieved November 7, 2022, from https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

- Electronic transactions act. Electronic Transactions Act - Uniform Law Commission. (n.d.). Retrieved November 7, 2022, from https://www.uniformlaws.org/committees/community-home?CommunityKey=2c04b76c-2b7d-4399-977e-d5876ba7e034#:~:text=The%20Uniform%20Electronic%20Transactions%20Act,removing%20barriers%20to%20electronic%20commerce.

- Protecting your identity - YouTube Help. (s. f.). https://support.google.com/youtube/answer/2801895?hl=en

- Global Legal Group. (s. f.). Data Protection Laws and Regulations Report 2022 Norway. International Comparative Legal Guides International Business Reports. https://iclg.com/practice-areas/data-protection-laws-and-regulations/norway

- Regulations. (s. f.). Datatilsynet. https://www.datatilsynet.no/en/regulations-and-tools/regulations/

- Copeland, B. (2023, November 1). Alan Turing | Biography, Facts, Computer, Machine, Education, & Death. Britannica. Retrieved November 8, 2023, from https://www.britannica.com/biography/Alan-Turing

IV. Topic B: Cyberattacks

4.1 Introduction

According to IBM “A cyberattack is any intentional effort to steal, expose, alter, disable, or destroy data, applications or other assets through unauthorized access to a network, computer system or digital device”. This behavior can take many forms, such as attempting to steal sensitive data, exposing it to unauthorized parties, altering digital assets for deception or disruption, disabling systems causing downtime, or destroying digital information or infrastructure. Unauthorized access is the common thread that allows cyberattackers to carry out operations such as data theft, manipulation, or computer system harm. Cyberattacks range from malware and phishing to ransomware and distributed denial-of-service attacks, with reasons ranging from financial gain to political motivations, activism, or espionage. As technology improves, so do cyberattacker techniques, stressing the crucial need of cybersecurity in protecting digital assets and maintaining the integrity of information systems.

4.2 Historical Background

In 1834, there was the first-ever cyberattack in France. Two criminals broke into the French Telegraph System and took financial market data. Over time, more "hackers" appeared to interfere with wireless telegraphy and phone service, but things didn't get very interesting until 1940.

Rene Carmille appeared as the pioneer of ethical hacking in 1940. In France during the Nazi occupation, he was an expert on punch-card computers and a member of the Resistance. He was the owner of the information processing devices used by the Vichy government in France. After learning that the Nazis were locating Jews with the use of the machines, he offered to let them use his. After they fell for the bait, he exploited their access to hack them and sabotage their plans.

The first computer passwords were created at MIT in 1962 with the goal of limiting student computer use and protecting their privacy. A punch card invented by MIT student Allan Scherr caused the computer to print every password stored in the system. He then gave them to his friends and utilized them to gain more computer time. Additionally, they broke into their teacher's account and sent them harsh texts as a form of harassment.

The University of Washington Computer Center is thought to have used the first computer virus in 1969. On one of the machines, an unidentified individual installed malicious software that became known as the "RABBITS Virus." The software started copying itself until the computer was overloaded and shut down.

It's common to refer to Kevin Mitnick as the original cybercriminal. Mitnick gained access to some of the world's safest and most guarded networks, such as Motorola and Nokia, between 1970 and 1995. He used complex methods of social engineering to trick important employees of the businesses into giving him codes and passwords, which he then used to access the internal computer networks. The FBI put him under detention and charged him with multiple federal offenses. Mitnick became an author and cybersecurity consultant after leaving prison.

4.3 Current Situation

Cyberattacks continue to present a complex threat environment. Supply chain vulnerabilities put enterprises at risk of extensive compromises, and ransomware assaults, which target essential infrastructure and businesses, are still on the rise. People are still being tricked by phishing and social engineering techniques, which highlights the human factor in cybersecurity. Advanced and enduring threats are a result of nation-state cyber activities, which are characterized by geopolitical tensions. A growing number of IoT devices are becoming connected, and this raises concerns about possible weaknesses in vital infrastructure. Organizational migration presents cloud security problems, with misconfigurations and insufficient access restrictions providing potential hazards. The sophistication of attacks is increased by the harmful usage of AI and machine learning techniques. An extra degree of difficulty is introduced by zero-day attacks that target unreported software and hardware problems. Navigating this environment requires being aware, putting best practices into effect, and giving cybersecurity measures the highest level of importance.

4.4 ***Focus 1: Norms and Rules in Cyberspace***

The fast growth of cyberspace in today's globalized world has made it necessary to comply with the international conventions and regulations that restrict state activity. Given the interdependence of digital systems and the possibility of cyber dangers extending across national borders, it is essential that a comprehensive framework is created for regulating responsible behavior in the world of technology. The growing dependence of governments on digital infrastructure for important functions has raised serious concerns about the possibility of malicious cyber actions disrupting vital services, compromising confidential data, and jeopardizing national security.

Guidelines for responsible state behavior in cyberspace are essential to the creation of a sustainable international framework. These rules operate as the basis for encouraging responsible behavior, developing a common understanding of appropriate behavior, and reducing the possibility of miscommunication or error in the digital world. At the same time, it's crucial to draw boundaries around activities that are generally considered inappropriate in cyberspace, such cyber-espionage, attacks on vital infrastructure, and meddling in other countries' political processes. The international community may provide a single platform for denunciation and deter governments from participating in careless cyber operations by establishing these red lines.

Moreover, the determination of appropriate consequences for malicious cyber activities is a crucial aspect of ensuring accountability and discouraging states from crossing the boundaries of acceptable behavior. A well-defined consequence framework, ranging from diplomatic measures to economic sanctions and collective defensive actions, serves as a deterrent and reinforces the commitment to upholding the integrity and security of cyberspace. Encouraging member states to actively participate in international efforts aimed at crafting a code of conduct for cyberspace is imperative. Through diplomatic channels, multilateral forums, and collaboration with various stakeholders, nations can contribute to the development of a robust and universally accepted framework, fostering stability and minimizing the risk of escalating cyber conflicts.

4.5 ***Focus 2: Capacity Building and Cybersecurity Education***

Recognize the importance of building the capacity of member states, particularly those with limited resources, to strengthen their cybersecurity defenses. Propose initiatives that promote cybersecurity education, training programs, and technical assistance to enhance the capabilities of national cybersecurity agencies. Discuss the creation of international partnerships to provide support in developing robust cybersecurity strategies, promoting awareness, and improving incident response capabilities globally.

To address the pressing need for bolstering cybersecurity defenses, it is crucial to recognize the unique challenges faced by member states with limited resources. Initiatives aimed at building the capacity of these nations should prioritize comprehensive cybersecurity education and training programs. By investing in educational initiatives that reach a broad spectrum of stakeholders, from government officials to private-sector entities and the general public, member states can cultivate a cyber-aware culture. This not only helps in mitigating potential threats but also empowers individuals and organizations to proactively contribute to the overall cybersecurity posture of the nation. Furthermore, technical assistance programs should be tailored to the specific needs and capabilities of each state, ensuring that they have the expertise and tools necessary to protect their critical digital infrastructure.

The creation of international partnerships plays a pivotal role in providing sustained support for developing robust cybersecurity strategies. Collaborative efforts can include knowledge-sharing initiatives, joint research and development projects, and the exchange of best practices. These partnerships should extend beyond the governmental level, involving industry leaders, academic institutions, and international organizations. By fostering a collaborative approach, member states can leverage the collective expertise and resources of the global community to strengthen their cybersecurity capabilities. Additionally, international partnerships can facilitate the establishment of mechanisms for coordinated incident response, ensuring a swift and effective global response to cyber threats that may transcend national borders. This not only enhances the resilience of individual nations but also contributes to the overall stability of the interconnected digital ecosystem.

4.6 *Focus 3: Protection of Individual Privacy and Data Security*

In the context of escalating cyber threats, prioritizing the discussion on safeguarding individual privacy and enhancing data security is paramount. Member states must recognize the imperative of establishing and enforcing robust data protection laws to shield citizens from unauthorized access and data breaches. These laws should encompass clear guidelines on data collection, processing, and storage, with stringent penalties for entities that fail to adhere to these standards. By placing a strong emphasis on legal frameworks, member states can create a protective shield around individuals, instilling confidence in the digital landscape and fostering a sense of security in the online environment.

Moreover, there is a critical need to encourage the development of international standards for data security and privacy. Collaboration among member states can lead to the establishment of universally accepted principles that govern responsible data handling practices. These standards should encompass not only legal requirements but also best practices for encryption, secure data storage, and incident response. By creating a cohesive global framework, member states can collectively address the challenges posed by cross-border data flows and strengthen the overall resilience of the digital ecosystem.

As technology companies play a pivotal role in the digital landscape, their responsibility in protecting user data cannot be overstated. Member states should engage in a dialogue with these entities to ensure that privacy is prioritized in the design and implementation of digital technologies. Striking a balance between national security interests and the right to privacy is essential in the digital age. Member states should explore mechanisms that enable lawful access for security purposes while safeguarding individual privacy rights. Additionally, legal frameworks must be established to hold entities accountable for mishandling or inadequately securing personal information, thereby promoting a culture of responsibility and accountability in the digital realm.

4.7 Guiding Questions

1. What are zero-day vulnerabilities, and how do they contribute to the success of advanced persistent threats (APTs)?

2. What challenges exist in accurately attributing cyber incidents, and how does it impact international relations?

3. How do supply chain attacks work, and why are they considered a significant threat?

4. In what ways can blockchain technology enhance cybersecurity, and where are its limitations?

5. How does the integration of IoT (Internet of Things) and OT (Operational Technology) impact cybersecurity risks?

6. What strategies should be considered for building resilient, adaptive, and sustainable cybersecurity frameworks?

7. How do large-scale cyber attacks, such as ransomware incidents or data breaches, impact the economy on both a micro and macroeconomic level?

8. What systemic risks are associated with cyber threats in the financial sector, and how can they be mitigated?

4.8 Recommendations

As we approach the Cyber Attacks Committee, I strongly recommend investigating the latest developments in cybersecurity, conducting research on key terms, and utilizing useful links to enhance your understanding. Actively participate in discussions, promote collaboration, and maintain a proactive yet diplomatic negotiation approach. Be flexible and open to adjusting your positions as the committee's dynamics evolve. Take advantage of opportunities to showcase your unique perspectives and innovative solutions, contributing not only to your personal experience but also to the overall success of the MUN conference. Wishing you the best in navigating the complexities of cyber threats. May your efforts be both impactful and memorable.

4.9 Useful links

1. Kondruss, B. (n.d.). The terrifying list of cyber attacks worldwide 2024 / 2023 today. KonBriefing.com. Retrieved January 15, 2024, from https://konbriefing.com/en-topics/cyber-attacks.html
2. What is Ransomware? (n.d.). IBM. Retrieved January 15, 2024, from https://www.ibm.com/topics/ransomware
3. What is a cyberattack? (n.d.). IBM. Retrieved January 15, 2024, from https://www.ibm.com/topics/cyber-attack
4. What is a phishing attack? (n.d.). IBM. Retrieved January 15, 2024, from https://www.ibm.com/topics/phishing
5. Baker, K. (2023, November 9). 10 Most Common Types of Cyber Attacks Today. CrowdStrike. Retrieved January 15, 2024, from https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/
6. Baker, K. (2023, November 9). 10 Most Common Types of Cyber Attacks Today. CrowdStrike. Retrieved January 15, 2024, from https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/

4.10 Glossary

1. **Malware:** Malicious software designed to harm or exploit computer systems.
2. **Phishing:** Deceptive attempts to acquire sensitive data by pretending to be trustworthy.
3. **Ransomware:** Software that encrypts data, demanding payment for its release.
4. **DDoS:** Distributed Denial of Service, overwhelming a system with traffic.
5. **Firewall:** Security barrier that monitors and controls incoming/outgoing network traffic
6. **Encryption:** Converting data into a code to secure it from unauthorized access.
7. **Incident Response:** Organized approach to managing and mitigating the aftermath of cyberattacks.
8. **Cybersecurity:** Protocols and practices to safeguard digital systems from cyber threats.
9. **Penetration Testing:** Simulating cyberattacks to identify and address system vulnerabilities.
10. **Incident Response:** Organized approach to managing and mitigating the aftermath of cyberattacks.

4. 11 References

1. What is a phishing attack? (n.d.). IBM. Retrieved January 15, 2024, from https://www.ibm.com/topics/phishing

2. Baker, K. (2023, November 9). 10 Most Common Types of Cyber Attacks Today. CrowdStrike. Retrieved January 15, 2024, from https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/
3. Baker, K. (2023, November 9). 10 Most Common Types of Cyber Attacks Today. CrowdStrike. Retrieved January 15, 2024, from https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/
4. How cyber attacks work - NCSC.GOV.UK. (n.d.). National Cyber Security Centre. Retrieved January 22, 2024, from https://www.ncsc.gov.uk/information/how-cyber-attacks-work
5. What is a phishing attack? (n.d.). Cloudflare. Retrieved January 22, 2024, from https://www.cloudflare.com/learning/access-management/phishing-attack/

V. Expectations

As we approach the Cyber Attacks Committee, we would like to offer some valuable tips to our esteemed delegates. Start by researching the latest developments in cybersecurity to gain a solid foundation. A clear understanding will strengthen the discussion. Second, actively engage with other participants during the discussion and take a proactive approach. Encourage collaborative discussion, exchange ideas, look for common ground and create a constructive atmosphere. Additionally, remember to balance proactiveness and diplomacy, as effective negotiation is key to navigating the complexity of the cyber threat landscape. Be adaptable and be willing to change your position as the discussion within the committee develops. Finally, take advantage of every opportunity to showcase your unique perspective and innovative solutions. Your commitment to these principles will not only enhance your personal experience, but will also greatly contribute to the overall success of the MUN conference. We wish you good luck. May your efforts in dealing with cyber-attacks be effective and memorable.

VI. Annexes and Guidelines

6.1 Opening Speech

6.1.1 Clarifications

The opening speech effectively follows a structured format commonly employed in formal settings. It begins with a polite and respectful greeting to the members of the dais, distinguished delegates, and observers, setting a tone of professionalism. The introduction presents IBM, the speaker, and thanks everyone for the chance to participate in the UN committee on data privacy discussions. The speaker effectively demonstrates the topic of artificial intelligence's relevance in modern society by highlighting how widely used it is in both everyday tasks and political decision-making. A foundation for future discussion is established by drawing a direct line between the cognitive processes of AI and its possible impact on society. The speech then explores the company's history, mission, and dedication to accessibility and safety in technology advancement.

It is notable that IBM recognized the concerns related to artificial intelligence, especially those connected to privacy, and has taken proactive steps to reduce those risks (like stopping the use of face recognition software to improve security) are noteworthy. A statement from the CEO is included to further emphasize the company's commitment to improving the world. In an acknowledging and formal manner, the speech ends by thanking the dais, emphasizing the committee's enthusiasm for collaboration and debate.

6.1.2 Opening Speech Model

Good morning honorable members of the Dais, distinguished delegates, and observers.

We, at the International Business Machines Corporation, are deeply honored to be present in the, though not official, Data Privacy UN committee to discuss detrimental matters for the adequate development and employment of artificial intelligence.

As we all know, artificial intelligence has become a social tendency, being utilized for simple human tasks and complex matters in governmental decisions. In these two situations, there is one thing in common, that is, AI simulates the cognitive processes of a human. IBM is a company based in the United States of America with the purpose of developing technology that can ensure safety for its users and accessibility, always looking forward to progress. The corporation is aware of the risks AI development poses for modern society, as leaks in governmental databases or thievery of identity could potentially wreak havoc. Nonetheless, at our company, privacy and trust are prioritized, which is why for example we have stopped using facial recognition systems in order to have stronger security.

As our C.E.O. stated, “Our clients’ systems support modern society. In making them faster, more productive, and more secure, we don’t just make business work better. We make the world work better. ”

IBM looks forward to collaborating with all those present on this committee to reach a consensus regarding AI regulations for data privacy.

Thank you honorable dais.

6.2 Position Paper

6.2.1 Clarifications

A well-structured position paper, such as the one provided, typically consists of key elements that guide the reader through a clear and organized argument. The work starts with a brief opening that provides an overview of the chosen subject, in this case, artificial intelligence. The introduction gives the reader a concise description of the issue, including the variety of people involved, and possible outcomes. The organization's position on the subject is then articulated in a concise and powerful thesis, often known as a position statement.

The elaboration part, which follows the thesis, offers three convincing arguments in support of the viewpoint, including relevant quotations, agreements, or statements from trustworthy sources. The reasons given need to make sense and provide a convincing argument for the point of view that has been taken. The position paper then addresses counterarguments, recognizing and successfully disputing opposing viewpoints. This well-rounded strategy strengthens the position as a whole.

Recommendations for actions to be taken by the committee follow, offering practical and feasible solutions to address the identified issues. These recommendations are often linked back to the organization's stance, reinforcing the commitment to responsible AI development. The conclusion then summarizes the main points, reiterates the organization's position, and leaves a lasting impression.

To put it simply, a concise position paper has the following logical and structured structure: introduction, problem description, thesis, development of viewpoint, recommendation section, defense against counterarguments, and conclusion. A coherent and convincing argument is produced by building on the ideas presented in each part before it. Evidence, quotations, and rational arguments are used to support the position and create a strong case for a certain viewpoint on the subject at question.

6.2.2 Position Paper Model

POSITION PAPER Objective: **Plan the course of action of a delegation before the meeting** by taking into consideration each country's position on the topics to be discussed at the conference.
Topic: Artificial Intelligence
General Sentence:

At IBM, we firmly believe artificial intelligence innovations should be available to everyone without discrimination, centered towards the SDG's and with the guarantee of total privacy.

Complete name	**International Business Machines Corporation**
Current President	**Arvind Krishna**
Type of government	**N.A.**
Capital	N.A.
Language	English
Population	About 27.3 million people monthly
Religion	N.A.

Introduction Brief and concise description of a State's international organisation's or NGO's position and priorities for a given for a given committee. **ANSWER:** What is the problem? Who does it affect? How does it affect them?	Artificial intelligence has become a trend, entering every aspect of day-to-day life. Ranging from algorithms that perform simple activities, like face recognition systems, to governmental programs that analyze estatal data, AI has one great although worrying capability, which is the capability to store private data. A leak in these databases could potentially cause the use of personal information with malicious intent.
Sentence stating country's position. (**Thesis**)	At IBM, we firmly believe that artificial intelligence innovations should be available to everyone without discrimination, centered towards the SDG, and with the guarantee of total privacy.
Elaboration of the position (**3 arguments in favor** of the position)	- Here at IBM, we recognize consumer privacy as one of the most valuable elements we can be trusted with, which is why we have a set of data

Options: quotes from the UN charter, agreements/ resolutions your member state has ratified; quotes from statements made by your head of state, head of government, ministers, delegates to the UN, and any other relevant international documents including but not limited to Reports from the UN Secretary -General on the topic.	privacy and ethical regulations. These include compliance with each country/region's set of regulations. Most of all, consent is prioritized, and recently, IBM has stopped producing facial recognition software to ensure accurate data privacy. - AI is a helpful tool when it comes to achieving the Sustainable Development Goals. Artificial intelligence is able to analyze weather patterns and maximize crops while reducing environmental impact. In addition, it is able to optimize traffic and, in consequence, optimize the use of fuel. - In the health industry, AI has already impacted in a great scale medical diagnosis due to its ability to recognize illnesses and conditions at their early stages for better treatment. An example is cancer diagnosis, in which the AI can identify early symptoms based on the patient's medical and family history.
Defense of the position (**3 counterarguments** of the position)	- Demis Hassabis, CEO of DeepMind Technologies stated whilst talking to Elon Musk that " Machines could become superintelligent and surpass us mere mortals, -perhaps even decide to dispose of us." meaning he sees AI as a threat to humanity. - Several artificial intelligence programs such as ChatGPT, MidJourney, etc, create a sort of replicas of already existing art. Why so? These algorithms work based on an input (the person's request) and an output (from a database with already-made art) which exposes creativity to thievery and plagiarism. - Although AI seems to be objective, it may have underlying biases. An article by Harvard states, "A growing body of research exposes divergent error rates across demographic groups, with the

	poorest accuracy consistently found in subjects who are female, Black, and 18-30 years old." This research just shows how artificial intelligence really is biased depending on the programmer and how it is written.
Recommendations for actions to be taken by the committee	- Technology companies must agree upon a specific AI governance, which refers to respecting regulations and organizing data, and fact sheets, in order to have clarity on what is and what is not allowed for AI development. The governance information would be managed by the UN Data Privacy Management or a new committee to make annual revisions about the accorded governance. - The International Business Machines Corporation calls other big companies such as Google, Facebook, Twitter, and Amazon, among others, to comply with regional data privacy regulations such as the GDPR in the EU and others. This is to have a starting point from which new restrictions can be implemented, such as the IBM initiative of AIDMDR (Artificial Intelligence Data Management and Development Restrictions).
Conclusion (**Restatement of the country's position**)	In the present day, in which artificial intelligence has become such a fundamental tool in everyday life, IBM encourages other global technological powers to make artificial intelligence accessible to everyone, with safe data privacy and focused towards a sustainable Earth.

References:

- Shvartsman, D. (2023). IBM: The Most Innovative and Prizewinning Tech Company. Retrieved from https://www.investing.com/academy/statistics/ibm-facts/#:~:text=Over%2027.3%20million%20people%20use,global%20revenue%20diminished%20by%2022%25

- Rossi, F. (2022). AI ethics. IBM. https://www.ibm.com/impact/ai-ethics#:~:text=At%20IBM%2C%20we%20believe%20AI,not%20just%20the%20elite%20few.&amp;text=IBM%20clients’%20data%20is%20their,and%20equitable%20and%20prioritize%20openness.
- IBM. (2023). *Government Regulatory Overview*. IBM Policy. https://www.ibm.com/policy/government-regulatory-new/
- Department of Economic and Social Affairs. (2023). *The 17 goals | Sustainable Development*. United Nations. https://sdgs.un.org/goals
- Isarsoft. (2023, August 2). *AI In Traffic Management*. https://www.isarsoft.com/article/ai-in-traffic-management#:~:text=Role%20of%20AI%20in%20improving%20Traffic%20Efficiency,-The%20use%20of&text=AI%20technologies%20offer%20traffic%20planners,where%20everything%20functions%20like%20clockwork.
- Yoon, S., & Amadiegwu, A. (2023, June 21). *AI can make healthcare more accurate, accessible, and sustainable*. World Economic Forum. https://www.weforum.org/agenda/2023/06/emerging-tech-like-ai-are-poised-to-make-healthcare-more-accurate-accessible-and-sustainable/#:~:text=AI%20algorithms%20can%20catalyse%20the,privacy%20and%20security%20are%20essential.
- Isaacson, W. (2023, September 6). *Inside elon musk’s struggle for the future of ai*. Time. https://time.com/6310076/elon-musk-ai-walter-isaacson-biography/
- Vincent, J. (2022, November 15). *The scary truth about AI copyright is nobody knows what will happen next*. The Verge. https://www.theverge.com/23444685/generative-ai-copyright-infringement-legal-fair-use-training-data
- Dr Mark van Rijmenam, C. (2023, April 7). *Privacy in the age of AI: Risks, challenges and solutions*. Dr Mark van Rijmenam, CSP | Strategic Futurist Speaker. https://www.thedigitalspeaker.com/privacy-age-ai-risks-challenges-solutions/#:~:text=One%20of%20the%20primary%20challenges,as%20identity%20theft%20or%20cyberbullying
- Nijabi, A. (2020, October 26). *Racial discrimination in face recognition technology*. Science in the News. https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/#:~:text=Face%20recognition%20algorithms%20boast%20high,and%2018%2D30%20years%20old.

- Martineau, K. (2023, November 16). *How AI governance wouldn't exist without our maritime past*. IBM Research Blog. https://research.ibm.com/blog/AI-governance-explained

6.3 Press Release

6.3.1 Clarifications

It's important to communicate the main ideas of a press release in an efficient way while keeping a formal, serious tone. Start with a list of the primary actors and highlight the importance of the collaboration between CEOs and companies like Amazon, Apple, IBM, Microsoft, Tesla etc. Clearly state the partnership's goal, in this case, it was to create and put into effect strong rules under the frameworks for artificial intelligence data management and development restrictions, users data management program, and artificial users data protection. Also, explain the shared commitment to user privacy protection, here the heads of block Jeff Bezos and OpenAI remark on the moral necessity of ethical AI research. End with a formal acceptance from the CEOs and companies, stating that they support the new implementations like the UDMP, AIDMDR, and AUDP programs' global applicability. The press release ought to be signed by chosen representatives and include the support of other participating companies and CEOs.

6.3.2 Press Release Model

Press release,

Amazon , Apple, Bill gates, Donald Trump, Elon musk , Fei Fei Li , IBM, Jeff Bezos , Mark Zuckerberg , Microsoft , OpenAI , Satya nadella , Sam Altman , Tesla, and X.

To the DPM committee,

12:00 pm

The delegation of Open AI and Jeff Bezos have agreed to

Leading artificial intelligence company OpenAI and well-known businessman Jeff Bezos, along with other companies and CEOs, are collaborating to raise the bar for user privacy in AI systems. This partnership represents a turning point in the industry's dedication to protecting user data and guaranteeing moral AI procedures with the purpose of providing security to the users. This will be achieved through several guidelines and solutions that will be implemented in order through the Users Data Management Program (UDMP). The Artificial intelligence Data Management and Development Restrictions (AIDMDR), and Artificial Users Data Protection (AUDP) to ensure proper use of artificial intelligence regarding data privacy.

Concerns about user privacy have grown more critical in a time when technology breakthroughs have expedited AI's capabilities. The pioneers of AI research OpenAI and IT industry visionary Jeff Bezos have realized how urgent it is to address these issues and protect people's fundamental rights. According to OpenAI, "protecting user privacy is not just an ethical imperative; it's the cornerstone of responsible AI development," In collaboration with Jeff Bezos.

Finally, the corporations and CEOs have acknowledged the new implementations of the delegation's of Open AI Regarding the UDMP, AIDMDR and AUDP for its usage worldwide and of Jeff Bezos.

This press release was signed by the delegation of Jeff Bezos And Open AI, other companies and CEOs.

VIII. Country List

1. Google
2. Elon Musk
3. Bill Gates
4. Apple
5. Microsoft
6. Amazon
7. OpenAI
8. IBM
9. Donald Trump
10. Youtube
11. X
12. Tesla
13. Jeff Bezos

14. Nvidia
15. Sam Altman
16. JP Morgan
17. Jeff Dean
18. Mark Zuckerberg
19. Goldman Sachs
20. Intel
21. Tiktok
22. Alibaba
23. Huawei
24. Satya Nadella