UNIVERSITÀ DEGLI STUDI DI PADOVA

DEPARTMENT OF POLITICAL SCIENCE, LAW AND INTERNATIONAL STUDIES

Master's degree in European and Global Studies

Technological Innovations and Policy Making in the European Union: A Focus on Artificial Intelligence

Supervisor: Prof. David BURIGANA

Candidate: Alp ERTAN

2041187

A.Y. 2023 - 2024

ACKNOWLEDGEMENTS

I would like to express my deepest gratitude to my dear family, Zuhal & Kemal Ertan, for always believing in me and supporting me unconditionally throughout this journey. Your encouragement has been my greatest source of strength.

A heartfelt thanks to my doctor, Uzm. Dr. Mehmet Oğuz, for his endless support and guidance, which helped me maintain focus and resilience.

To my friends, thank you for always being by my side. Your companionship and support have been invaluable to me throughout this process.

I am also deeply grateful to ALDA - European Association for Local Democracy, whose work has broadened my perspective on European studies and provided the inspiration for this thesis.

Finally, my sincerest thanks to my supervisor, David Burigana, for his exceptional mentorship. His guidance and insight were crucial in shaping this work.

With love.

ABSTRACT

In the 21st century, rapid technological advancements have significantly influenced policy structures worldwide, particularly in the European Union. Especially with the effect of increasing use of artificial intelligence; states started to come up with their own action plans regarding this situation. This thesis explores the relationship between recent technological developments and policy-making processes in the EU, with a special focus on the field of artificial intelligence. First the thesis provides a comprehensive overview of key technological developments, such as cybersecurity advancements and surveillance technologies, highlighting their transformative impact on global and EU-specific policy frameworks. Then it delves into the global significance of AI, examining why AI is often stated as the next pivotal technological revolution after the internet. This analysis highlights the critical role of AI in shaping future socio-economic and political landscapes, requiring strong regulatory measures. Also it evaluates the European Union's approach toward these technological shifts. It examines the EU's strategic responses to technological advancements, again with a specific emphasis on AI. Finally the thesis compares the EU's regulatory approaches to AI with those of other global regions, investigating whether the EU's policies serve as a benchmark for international standards. It considers the EU's potential pioneering role in AI regulation and its influence on other regions and institutions. By analyzing these dimensions, this thesis aims to provide a detailed understanding of how technological innovations, especially AI, are reshaping policy-making within the EU. The findings emphasize the EU's strategic position in leading global AI governance and the broader implications of its regulatory actions for international policy frameworks.

Key words: Artificial Intelligence, Policy Making, European Union, Technological Developments, AI Regulation

TABLE OF CONTENT

LIST OF PRIMARY ABBREVATIONS

5G	-	Fifth Generation Mobile Network
AI	-	Artificial Intelligence
AI Act	-	Artificial Intelligence Act
AR	-	Augmented Reality
CRISPR	-	Clustered Regularly Interspaced Short Palindromic Repeats
DMA	-	Digital Markets Act
DSA	-	Digital Services Act
ENISA	-	European Union Agency for Cybersecurity
EU	-	European Union
FISA	-	Foreign Intelligence Surveillance Act
GDPR	-	General Data Protection Regulation
IoT	-	Internet of Things
ITU	-	International Telecommunication Union
MFA	-	Multi-Factor Authentication
NATO	-	North Atlantic Treaty Organization
OECD	-	Organisation for Economic Co-operation and Development
UNESCO	-	United Nations Educational, Scientific and Cultural Organization
U4SSC	-	United for Smart Sustainable Cities
VR	-	Virtual Reality

METHODOLOGY

This thesis adopts a comprehensive and interdisciplinary approach to analyze the European Union's role in policy-making related to technological advancements, particularly focusing on Artificial Intelligence (AI) and other emerging technologies. The methodology is designed to integrate both qualitative and comparative research, ensuring a detailed understanding of the EU's regulatory frameworks and their global implications.

1. Research Design

The research is structured around comparative analysis and policy evaluation. It draws on a variety of sources, including legal texts, policy documents, academic articles, and reports from international organizations. By comparing the EU's AI regulation efforts with those of other countries and regions, the thesis aims to highlight the unique aspects of the EU's approach and understand its global influence. This comparative framework allows for the examination of regulatory frameworks across different jurisdictions and the identification of key patterns and differences.

The study also includes case analysis of key EU regulations, such as the General Data Protection Regulation (GDPR), Artificial Intelligence Act (AI Act), Digital Services Act (DSA), and Digital Markets Act (DMA). These case studies provide in-depth analysis of the legal mechanisms, ethical principles and practical challenges involved in implementing these regulations.

2. Data Collection

This research relies on secondary data collected from a wide range of sources. These include:

- Official EU publications: Primary sources of data include EU legal texts, directives, regulations and official communications related to technological regulation. These documents offer the most reliable insights into the EU's legal framework and policy intentions.
- Academic literature: A review of academic articles, journals, and books that discuss AI regulation, technological governance, and the EU's leadership in these fields is conducted. This literature provides theoretical foundations for understanding the broader implications of AI and technology policy.

- Reports from international organizations: Documents from the OECD, UNESCO, NATO and various national governments are used to provide comparative insights into how other global actors approach AI regulation.
- Comparative case studies: AI governance efforts in other regions; including China, the United States, Canada and Japan have been analyzed. This comparative analysis helps to situate the EU's regulatory model within the broader global context.

3. Qualitative Analysis

The thesis employs qualitative content analysis to interpret the regulatory texts and policy documents. This involves a close reading of legal and policy frameworks to understand their underlying principles, objectives and implications. Special attention is given to ethical concerns, human rights protections and data privacy issues embedded in the regulations. By analyzing the language of the legal texts, the study assesses the EU's commitment to fostering a balance between technological innovation and citizen protection.

Additionally, the methodology includes a thematic analysis of key documents, identifying recurrent themes such as transparency, accountability and innovation in AI governance. These themes are critical in understanding how the EU's policies are designed to mitigate the risks associated with emerging technologies while promoting their beneficial use.

4. Comparative Framework

A major aspect of this methodology is the comparative analysis of the EU's regulatory frameworks with those of other leading global players. The thesis examines:

- The U.S. approach to AI regulation, which favors voluntary standards and market-driven innovation over prescriptive legislation.
- China's top-down model, which emphasizes state control and rapid technological development, often at the expense of personal freedoms and data privacy.
- The UK's post-Brexit AI strategy, which reflects an independent approach yet aligns closely with ethical concerns shared by the EU.

By comparing these models, the thesis highlights the global significance of the EU's AI Act, which stands out for its horizontal regulatory framework covering all sectors, as opposed to the more sectoral and application-specific approaches seen in other regions.

5. Ethical Considerations

Given the focus on AI and data privacy, ethical considerations play a central role in the research. The study critically engages with the ethical frameworks outlined in the EU's AI regulations, particularly regarding algorithmic fairness, transparency, and the prevention of bias. The GDPR's emphasis on data protection and the AI Act's focus on ethical AI use are analyzed in light of international ethical standards.

The thesis also reflects on the broader societal implications of AI and other emerging technologies, considering how these policies affect individual freedoms, digital rights and economic opportunities.

6. Limitations

While this methodology offers a comprehensive analysis, it is important to acknowledge certain limitations. The research primarily relies on secondary sources and policy documents, meaning there is a limited scope for empirical investigation. The analysis is also confined to European policy frameworks, with only comparative references to other global approaches. Moreover, the rapidly evolving nature of technology regulation means that the data and policies discussed may change in the near future, which could impact the relevance of some findings.

In conclusion, the methodology used in this thesis provides a careful and detailed approach to analyzing the EU's response to 21st-century technological advancements. By combining comparative policy analysis, qualitative content review and thematic investigation, this research offers valuable insights into the role of AI, IoT, 5G, blockchain and other relevant technologies in reshaping policy-making. The EU's leadership in developing comprehensive regulatory frameworks is explained through this analysis, and it is highlighting its global influence in setting ethical and legal standards for AI and emerging technologies.

INTRODUCTION

In an era where artificial intelligence and technological advancements have started to play a tremendous role in our daily lives, the world has found itself at the edge of an incredible transformation.

As it can be expected, this transformation is not affecting our daily lives only on the individual level but also the higher levels in the world system. This shift in the field of technology has brought many other things together with its development to the other working areas in the world we are living in right now. To adapt to this big change; states, organizations and even individuals have come up with certain ideas and certain policies. Because at the end this is a thing they have to do if those states, organizations and individuals in question would like to maintain their power and their existence in this new world order that has been shaped with the technological investments without the intention of anyone. This is just a structure that has occurred as a result of many things that the world has experienced, and it has become an inevitable fact.[1]

In the 21st century, technological developments have shown an unseen pace that has been never experienced before[2], with artificial intelligence being one of the most transformative effects that is shaping the way societies function.[3] From healthcare to communication, transportation to education, artificial intelligence is doing revolutions in every aspect of our lives. The European Union (EU), as well as other international organizations, have recognized the potential and challenges brought by AI.[4] They have already started to position themselves at the front lines of policy-making in this area. Since artificial intelligence continues to evolve, the implications for governance, policy frameworks, and ethical considerations become increasingly significant, particularly in regions like Europe that aim to set global standards since the establishment of the European Union.

---

[1] Sheng, J., Amankwah-Amoah, J., & Wang, X. (2019). Technology in the 21st century: New challenges and opportunities. Technological Forecasting & Social Change, 143, 321–335. https://doi.org/10.1016/j.techfore.2018.06.009, pp. 321–323.

[2] İstanbul Gedik Üniversitesi. (n.d.). Modern dünyayı şekillendiren 21. yüzyıl icatları. https://uzemigunsem.gedik.edu.tr/modern-dunyayi-sekillendiren-21-yuzyil-icatlari

[3] Fırat, M. (2016). 21. Yüzyılda uzaktan öğretimde paradigma değişimi. Yükseköğretim ve Bilim Dergisi, 6(2), 142–150. https://doi.org/10.5961/jhes.2016.151, p. 1.

[4] Gacar, A. (2019). Yapay Zekâ ve Yapay Zekânın Muhasebe Mesleğine Olan Etkileri: Türkiye'ye Yönelik Fırsat ve Tehditler. Balkan Sosyal Bilimler Dergisi, 8(EUREFE'19), 389–394, pp. 1–3.

Artificial intelligence's integration into the daily life is no longer a distant concept but it is a reality that is present right now. Advanced algorithms that have been used by the artificial intelligence now are ready to use in power search engines, social media platforms, online shopping platforms and even personalized healthcare recommendations. This rapid integration of artificial intelligence has shifted the ways in which individuals, businesses, and governments interact with technology. As machines grow more intelligent and capable of performing complex tasks that were done by the human power earlier; the need for clear, comprehensive, and forward-thinking policies becomes urgent at this point where the people and organizations discover a more functional and easier way. The European Union, in particular, has taken significant steps toward regulating artificial intelligence to ensure that this new technological development benefits society while decreasing potential risks.

One of the key features of artificial intelligence that makes it one of the most used technological investments and helps itself to spread widely in a short amount of time is its ability to learn from large datasets, enabling it to make predictions, improve decision-making, and automate processes. This huge capacity of artificial intelligence that makes it capable to do this work has great implications for industries and sectors across the world. In the area of communication, AI-driven algorithms now play a crucial role in curating content, targeting advertisements, and even moderating online discussions. However, this widespread adoption of AI in the communication sector also raises a lot of concerns about data privacy, misinformation issues and the concentration of power in the hands of a few tech giants in the technology and programming sectors. These challenges are now at the heart of the policy debates that are currently taking place in the European Union and other international organizations in other continents.

The Rise of AI and Its Societal Impact

The rise of the AI technology has started to show certain effects on society and this effect is growing every day. Artificial intelligence has progressed rapidly in recent years and it has grown in a mutual dimension by the advances in concepts such as machine learning, big data, and computational power. The technological development that was once confined to the area of science fiction has now become an integrated part of modern life. The rise of AI is often compared to other revolutionary technological breakthroughs, such as the invention of the internet or the industrial revolution. However, AI differentiate its potential to not only enhance human capabilities but also to autonomously perform tasks traditionally carried out

by normal human beings in daily life without any expertise. This shift is particularly obvious in areas such as autonomous vehicles, facial recognition technologies, and natural language processing systems like chatbots and virtual assistants that have actually been used for many years in different work environments or even social interactions.[5]

In the last decade, the development of AI has focused on making machines to become more expert at learning from experience, recognizing patterns, and making decisions without direct or indirect human intervention to that certain task that has been given by the human at the beginning. Artificial intelligence systems are now capable of performing complex tasks that range from diagnosing diseases and recommending treatments to optimizing supply chains and predicting the consumer's behavior depending on the task, the context or the environment that has been working. These applications made by humans or even maybe from other artificial intelligence capacities have the potential to significantly improve efficiency, reduce costs, and provide new short term or long term solutions to the big or small problems in areas such as healthcare, education, and public safety. Currently, artificial intelligence is capable of providing different kinds of solutions to a certain problem and the users have a chance to implement which solution or solutions fits the most to that issue in question. However, these developments also raise important questions about the future of the working environment in many work sectors, the ethics of AI decision-making, and the potential for unintended consequences that could be done by that artificial intelligence driven programme.[6]

As AI becomes more integrated into the daily life, its influence is greatly started to be felt in areas such as communication, entertainment, and social interactions. AI-driven recommendation algorithms shape what content users see on internet platforms such as YouTube, Netflix and other social media platforms while AI tools are used to generate personalized marketing and advertising strategies for the users. During these innovations offer suitable and tailored experiences, they again also introduce new challenges related to user privacy, the spread of misinformation, and the reinforcement of certain biases. These problems are not special to any specific country or region but they are now becoming global concerns that are requiring international cooperation and regulation. This issue is a small example of how a technological development such as artificial intelligence can be a concern

---

[5] Löhr, G. (2023). Conceptual disruption and 21st century technologies: A framework. Technology in Society, 74, 102327. https://doi.org/10.1016/j.techsoc.2023.102327, p. 1.
[6] McKinsey & Company. (n.d.). The state of AI. https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai

of the bigger picture but not only a daily life problem or just a concern of a specific company in a certain sector.

The EU's Approach to AI Regulation

The European Union has always been a leader in creating policies that address the ethical, legal, and societal implications of emerging technologies since its establishment. In response to the rapid rise of artificial intelligence technologies, they followed the same structure that they have been doing before. The EU has wanted to position itself as a pioneer union in the global effort to regulate artificial intelligence technologies in such a way that promotes innovations while protecting fundamental rights at the same time. Since one of the main purposes of the European Union is to promote human rights from all aspects as possible; the EU's approach to AI regulation is grounded in its commitment to human dignity, fairness, and transparency. This is reflected in key policy documents such as the European Commission's White Paper on Artificial Intelligence and the EU's AI Act, which demonstrates the European Union's vision for "trustworthy AI" idea.[7]

The White Paper on Artificial Intelligence, published in the year 2020, the document highlights the EU's ambition to develop a regular and detailed framework that balances the need for innovation with the protection of fundamental human rights. The White Paper emphasizes the importance of ensuring the artificial intelligence systems that have been using in the European Union borders are transparent, accountable, and free from bias. The White Paper also calls for the establishment of clear standards and certifications for AI applications, particularly those used in high-risk sectors such as healthcare, finance, and transportation. The document recognizes that while AI technologies have a great potential to improve the quality of life for European citizens, this new technology also has a chance to cause significant risks if the artificial intelligence programmes are properly regulated.[8]

Besides the White Paper; the Artificial Intelligence Act was also proposed in 2021. The importance of this act is that it is marking the first attempt by any major economy to comprehensively regulate artificial intelligence technologies in general. The AI Act classifies AI systems into different risk categories, with the most tight regulations applied to high-risk

---

[7] *European Commission. (2021). Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206*

[8] *European Commission. (2020). White Paper on Artificial Intelligence - A European approach to excellence and trust. https://ec.europa.eu/*

AI applications; such as biometric identification and critical infrastructure management. By adopting this risk-based approach, the European Union aims to strike a balance between fostering innovation and protecting citizens from the potentially harmful effects of this new technological development. This Act also promotes the development of ethical guidelines and best practices for AI developers and users. It ensures that AI systems are designed and also deployed in a way that aligns with European values. Even though this could be sound as an utopian idea regarding the capabilities and functionality of artificial intelligence technologies; this at least what the union is aiming to achieve.[9]

Global Impact and the EU's Role in AI Governance

The EU's regulatory framework for AI is significant not only for its member states but also for the global community and other continents in the world system. As a major economic and political power, the EU's policies often set standards that are adopted by other countries and regions. The European Union is well known by its pioneer role in policy making. This phenomenon, known as the "Brussels Effect," has been observed in areas such as data protection, with the EU's General Data Protection Regulation (GDPR) serving as a model for similar laws around the world conducted by different organizations or institutions.[10] It can be said that the EU's proactive role on AI regulation is likely to have a similar impact. It could be stated that the European Union is influencing the development of AI policies in other jurisdictions within the European scope or in other geographical areas around the globe.

Moreover, the EU's efforts to regulate AI are part of a broader global conversation about the need for international cooperation in the governance of emerging technologies. AI is inherently cross-border in nature, and its development and deployment often involve actors from multiple countries, the example of this situation varies in every field. As such, effective AI regulation requires coordination between governments, international organizations and the private sector. From many perspectives, the EU has played a leading role in promoting this kind of collaboration. The Union is working with partners such as the Organisation for Economic Co-operation and Development (OECD) and the United Nations[11] to develop shared principles and guidelines for AI governance.[12]

---

[9] European Commission. (2024). European approach to artificial intelligence. https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence
[10] Center for Governance of AI. (n.d.). The Brussels Effect and artificial intelligence. https://www.governance.ai/research-paper/brussels-effect-ai
[11] United Nations. (n.d.). AI Advisory Body. https://www.un.org/en/ai-advisory-body
[12] OECD. (n.d.). OECD AI principles. https://oecd.ai/en/ai-principles

The EU's approach to AI regulation also reflects its broader vision for digital sovereignty. As global competition in AI becomes more intense every year, particularly between the United States and China, the EU is positioning itself as a third player that prioritizes ethical considerations and the protection of fundamental rights. In that exact matter, it is possible to talk about a pioneer role in policy making regarding prioritizing ethical concerns and human rights. The European Union has a different approach than other bigger competitors such as China and the US, by establishing a strong regulatory framework for AI. The EU seeks to ensure that its values are reflected in the global development and use of AI technologies. This commitment to ethical AI is a key aspect of the EU's strategy to maintain its influence in the global digital economy.

This paper aims to explore how recent technological developments, particularly advancements in artificial intelligence, have influenced policy-making structures within the European Union, focusing on the area of communication. It will examine the EU's responses and regulatory strategies to address these changes, while also evaluating the broader global impact of AI on governance. Also, the research seeks to answer the question of whether the EU is taking on a pioneering role in AI regulation and to what extent these policy shifts are shaping the global landscape.

CHAPTER I

TECHNOLOGICAL DEVELOPMENTS AND POLICY MAKING

The 21st century has become an era of rapid technological advancements and it is marking a pivotal shift in the way societies function, economies operate, and governments do policies in the way of this new technological era that has been growing in a very fast way that has been never experienced before in the history of science and technology. The scale and speed of innovation are unprecedented. With the each new development that is carrying deep implications for industries, governance, and international relations, technological development has turned into a big issue for everyone. From artificial intelligence transforming decision-making processes to blockchain revolutionizing financial systems, these technologies are not only reshaping the world we live in but are also challenging traditional regulatory frameworks. Because of this new system; the humanity tries their best to adapt to all these changes.

Technological breakthroughs such as Artificial Intelligence (AI), the Internet of Things (IoT), and blockchain have created new opportunities and challenges for several institutions, working environments and also of course the policymakers. These innovations have led to increased efficiency, better data analysis, and enhanced connectivity. However they have also introduced us to certain concerns about privacy, security, and ethical issues. Each and every day the humanity finds themselves trusting the growing technology more. This growing reliance on technology in sectors like healthcare, transportation, and finance further highlights the need for strong policy responses that can adapt to these fast-paced changes driven by these technological developments. Governments and states around the world, particularly in the European Union (EU), have been forced to reevaluate existing policies and create new regulations that ensure both the safe use and equal distribution of these technologies.

As the world becomes increasingly more interconnected recently, the effects of these innovations extend beyond borders, influencing global markets, labor forces, and even democratic processes in different countries. Technologies such as 5G networks, autonomous vehicles, and augmented-reality are expected to revolutionize industries since they are seen as big revolutions. But they also raise critical questions about national security, job

displacement, and the balance between innovation and regulation. The complex interplay between technology and policy demands a comprehensive understanding of how these developments shape governance at both national and international levels. So this issue brings new things into the table in the international arena of policy making.

In this chapter, the paper will try to demonstrate some of the most transformative technological developments of the 21st century, delving into their societal impacts, their roles in shaping new industries. Also the challenges they raised for policymakers. The focus will be on the European Union, since the EU navigates the complications of regulating these innovations while also positioning itself as a leader institution in the global technological governance for many perspectives. From AI and IoT to blockchain and 5G, these technologies are reshaping not only markets but also many aspects of policy-making processes. Understanding these developments is critical to understand the broader issues in global governance and the EU's strategic response to them. It is necessary to give certain background information about the recent technological developments before diving into the real subject which is their effect on policy making processes.

1.1 Artificial Intelligence (AI)

It could be said that Artificial Intelligence (AI) stands as one of the most transformative technologies of the 21st century. AI refers to the simulation of human intelligence in machines that are programmed to think, learn, and make decisions autonomously. Over the past two decades, the field of AI has made an important progress, particularly in areas such as machine learning and deep learning. These technologies enable machines to understand, process and analyze vast amounts of data, recognize patterns and improve their performance over time without any human intervention at all.[13]

The implications of AI are varies a lot in the current situation; this technology is influencing sectors such as healthcare, finance, transportation, and education. For example, in healthcare, AI-powered systems are used for diagnosing diseases with higher accuracy than human doctors. Also while in finance, AI algorithms optimize trading strategies and detect the possible frauds. Especially autonomous vehicles, which rely heavily on AI, using AI technology to revolutionize transportation. Lastly; AI-driven customer service systems like

[13] *Russell, S., & Norvig, P. (2020). Artificial Intelligence: A Modern Approach (4th ed.). Pearson, p. 1.*

chatbots are becoming standard in many industries because of their helpful services and making the systems more user friendly from many aspects.

From a policy perspective; the rise of AI occurs several challenges. It can be said that governments and international organizations must address issues such as job displacement, privacy concerns, and the ethical use of AI. Furthermore, the lack of global AI regulations has raised concerns about accountability and governance, making it a priority for policymakers to develop frameworks that ensure AI technologies are used responsibly.[14]

1.2 Internet of Things (IoT)

Another pivotal technological development that has become a debatable subject in the 21st century is the Internet of Things (IoT), which refers to the interconnection of everyday devices through the internet. IoT allows devices to collect and exchange data autonomously, enabling smarter decision-making in real-time. This technology has gained widespread adoption across industries but also from smart homes and cities to healthcare and agriculture. It is now a technology that has been used in daily life.[15]

Some examples on the areas this technology is using; in smart homes, IoT devices like thermostats, security cameras, and other variety of appliances are controlled remotely, they are enhancing convenience and energy efficiency. In cities, IoT technology is used to manage traffic flow, monitor air quality, and optimize waste management systems. In healthcare, IoT devices enable remote monitoring of patients, leading to more personalized care and improved health outcomes in the hospitals.

However, again like other technological developments the rapid spread of IoT devices has raised concerns about data security and privacy. The vast amount of data generated by these devices presents an attractive target for cyberattacks, and this issue is necessitating new cybersecurity policies and regulations. Additionally, the question of who owns and controls this data has become a critical issue for policymakers, especially in the context of the EU's General Data Protection Regulation (GDPR).

---

[14] *Pirim, H. (2006). Yapay Zeka. Yaşar Üniversitesi, p. 92.*
[15] *Wu, M., & Chen, X. (2024). Application of Internet of Things and embedded technology in electronic communication. Measurement: Sensors, 34, 101246. https://doi.org/10.1016/j.measen.2024.101246, pp. 1–4.*

1.3 Blockchain Technology

Blockchain, originally developed as the underlying technology for cryptocurrencies like Bitcoin, has since evolved into a powerful tool for securing and verifying digital transactions across various sectors. Blockchain is essentially a decentralized, distributed “ledger” that records transactions in a secure, transparent and stable manner. This technology has the potential to disrupt industries such as finance, supply chain management and governance.

In finance, blockchain enables peer-to-peer transactions without the need for intermediaries, reducing costs and increasing efficiency. In supply chains, blockchain provides transparency by allowing companies to track products from the point of origin to the consumer, reducing fraud and improving accountability. Governments have also started exploring the use of blockchain for secure voting systems and digital identity verification.[16]

Despite its advantages, blockchain occurs certain regulatory challenges, particularly in terms of financial oversight and consumer protection. As blockchain-based systems become more widespread, policymakers are recently thinking about how to regulate decentralized networks that do not have a single point of control. While mentioning about blockchain IBM uses these words; “Business runs on information. The faster information is received and the more accurate it is, the better.”[17]

1.4 5G Technology

The introduction of 5G, which actually means the fifth generation of mobile network technology, marks a significant jump forward in wireless communication. 5G is defined as "an application-agnostic general-purpose technology (GPT)" that serves as an upstream technology for a wide range of downstream Internet of Things (IoT) applications. It provides a critical input for various network industries and combines different types of QoS-differentiated broadband capacities with complementary big data value chains for data generation, processing, storage, and transmission.[18] With faster speeds, lower latency and the ability to connect more devices simultaneously; 5G is expected to power the next wave of

---

[16] *Yang, T., Ma, C., & Mi, X. (2024). The transformative potential of blockchain technology in developing green supply chain: An evolutionary perspective on complex networks. Computers & Industrial Engineering, 197, 110548. https://doi.org/10.1016/j.cie.2024.110548, p. 2.*

[17] *IBM. (n.d.). What is blockchain?. https://www.ibm.com/topics/blockchain*

[18] Knieps, G. (2024). Internet of Things, critical infrastructures, and the governance of cybersecurity in 5G network slicing. Telecommunications Policy, 48(4), 102867. https://doi.org/10.1016/j.telpol.2024.102867, pp. 2–4.

technological innovation, including autonomous vehicles, smart cities, and industrial automation. Experts say that 5G still has not reached its full potential yet and it is more possible to see more upcoming changes and developments in this technology.

5G will enable more flawless communication between IoT devices, enhance virtual and increased reality experiences and support the development of critical infrastructure like autonomous vehicles. The deployment of 5G networks however has sparked debates over national security, as some countries express concerns about foreign companies' involvement in critical communications infrastructure.

As countries started to spread 5G in their habitats; governments must navigate complex issues related to cybersecurity, privacy, and competition. The European Union for instance has implemented measures to ensure 5G networks are secure, while also fostering innovation and investment in these critical areas.

1.5 Autonomous Vehicles

Autonomous vehicles or with their other names self-driving cars are another significant technological breakthrough in the recent decades. These vehicles rely on a combination of artificial intelligence technology, sensors and real-time data analysis to navigate roads without human intervention. Autonomous vehicles, particularly trucks, are described as a transformative technology in the transportation sector. They have the potential to reduce labor and fuel costs and minimize environmental pollution by lowering emissions. However, for these vehicles to be widely used, careful consideration of control modes, such as road conditions and environmental factors, is required.[19] Companies like Tesla, Waymo, and Uber have invested heavily in developing autonomous driving technologies with the goal of creating safer and more efficient transportation systems for their users.

The potential benefits of autonomous vehicles are substantial. It includes reduced traffic accidents, lower emissions and increased mobility for individuals who are unable to drive because of any reason such as health conditions. However, their widespread adoption raises numerous policy questions, such as liability in the event of accidents, the impact on

[19] *Chen, J., & Chen, F. (2024). Efficient vehicle lateral safety analysis based on Multi-Kriging metamodels: Autonomous trucks under different lateral control modes during being overtaken. Accident Analysis and Prevention, 208, 107787. https://doi.org/10.1016/j.aap.2024.107787, p. 1.*

employment in the transportation sector and the need for new infrastructure to support autonomous driving.

1.6 Augmented Reality (AR) and Virtual Reality (VR)

Augmented reality (AR) and virtual reality (VR) technologies have gained significant development in recent years. This technological investment is offering immersive experiences that blend the physical and digital worlds. AR overlays digital information onto the physical world while VR creates entirely virtual environments that users can interact with. Both technologies are being applied in industries such as entertainment, education, healthcare, and retail. When it comes to the health sector specifically; AR can overlay educational content onto a patient's skin to help them understand treatment plans, while VR immerses patients in a virtual environment to explore their condition and treatment options.[20] These applications empower patients, allowing them to make more informed healthcare decisions.

When we take a look at the areas it has been used; in education, AR and VR provide interactive learning experiences, allowing students to visualize complex concepts and explore virtual environments. In healthcare, VR is used for medical training and therapy, while AR assists surgeons during operations by providing real-time data.

As AR and VR technologies become more sophisticated, they raise new regulatory challenges related to privacy, content moderation, and also a potential for addiction. Policymakers will need to address these issues since AR and VR continue to evolve and in the upcoming years it will be a more trendy topic than current time.

1.7 Big Data

Big data refers to the massive amount of data generated by digital devices, social media, sensors, and other sources. The ability to analyze and extract insights from big data has transformed industries such as marketing, healthcare, and finance. In the risk management sectors it is described as a rapidly advancing research field in operations research, involving large-scale data-driven analyses to solve complex problems. It integrates features such as customer characteristics, prices, and promotions to create models that optimize

[20] *Goldust, M., & Grant-Kels, J. M. (2024). Regulatory considerations for safe and ethical use of augmented reality and virtual reality in dermatology. Clinics in Dermatology, p. 7.*

decision-making processes.[21] In the recent years; companies are using big data analytics to predict consumer behavior, optimize supply chains and personalize customer experiences.

However, the use of big data raises important ethical and legal questions, particularly in relation to data privacy and security. Countries around the world, including the EU, have introduced regulations, especially the GDPR, to protect individuals' data and ensure that it is used responsibly.

1.8 Robotics

The robotics sector has actually existed since nearly the existence of electricity. However it is a matter that evolves symbiotically with the development of new technologies. Robotics has advanced significantly in the 21st century. Robots are now being used in manufacturing, healthcare, agriculture and even domestic settings. Robots can perform repetitive tasks with certainty, they are reducing costs and increasing efficiency in industries such as automotive manufacturing and logistics.

In healthcare, robots assist in surgeries, while in agriculture, they are used for tasks like planting, harvesting, and monitoring crop health. However, as robots take on more tasks traditionally performed by humans, concerns about job displacement and the need for new labor policies have emerged. Robotics adoption has a dual impact on the labor market, displacing certain jobs while simultaneously creating new opportunities, thereby transforming the job landscape rather than simply reducing employment rates.[22]This has become an issue for many governments and they are trying to do certain implications to tackle the problem.

1.9 Genetic and Biotechnological Advances

The field of genetics and biotechnology has seen remarkable progress, particularly with the development of CRISPR technology, which allows for precise gene editing. This technology has the potential to revolutionize healthcare by curing genetic diseases and improving agricultural productivity by creating genetically modified crops.

---

[21] *Clausen, J. B. B., Li, H., & Forget, N. (2024). Empirical risk minimization for big data-driven prescriptive analytics in operations research. Expert Systems with Applications, 232, 120850. https://doi.org/10.1016/j.eswa.2024.120850, p. 1.*

[22] *Sharfaei, S., & Bittner, J. (2024). Technological employment: Evidence from worldwide robot adoption. Technological Forecasting & Social Change, 209, 123742. https://doi.org/10.1016/j.techfore.2024.123742, pp. 1–2.*

However, genetic editing raises significant ethical concerns, particularly regarding its use in human embryos and the potential for "designer babies." Policymakers try to navigate these ethical dilemmas while also fostering innovation in this critical field.

1.10 Cloud Computing

Cloud computing has revolutionized the way data is stored, processed, and accessed. By enabling businesses and individuals to store their data on remote servers, cloud computing offers flexibility, scalability, and cost savings. Currently; companies like Amazon, Google, and Microsoft dominate the cloud services market. They are providing platforms that support a wide range of applications from data analytics to artificial intelligence.

While cloud computing has many advantages, it also presents security and privacy risks, particularly when it comes to sensitive data stored in the cloud. Also cloud computing involves using shared resources over the internet for storing and processing large-scale data. It plays a crucial role in achieving "green" objectives, such as optimizing energy consumption and reducing environmental impact.[23] Governments and businesses are currently working together to establish regulations that ensure the security and privacy of cloud-based data. From many aspects; cloud data has become a daily life thing that has been used for data transferring because of its easy access from many technological devices. It nearly erased the existence of CD and DVDs from the market however when it needs to be compared; the reliability concerning privacy and data protection the risks are now higher.

1.11 Cyber Security Technologies

The rapid digital transformation has increased the need for advanced cyber security measures to protect sensitive data, critical infrastructure and personal privacy. In recent years, technologies such as blockchain, multi-factor authentication (MFA), and encryption techniques have been widely adopted. AI-powered cybersecurity tools are now being used to detect and respond to cyber threats in real-time, identifying potential vulnerabilities and mitigating risks more efficiently. These advancements are crucial for many institutions, governments but also for personalized use in the face of rising cyberattacks and data

[23] *Biswas, D., Jahan, S., Saha, S., & Samsuddoha, M. (2024). A succinct state-of-the-art survey on green cloud computing: Challenges, strategies, and future directions. Sustainable Computing: Informatics and Systems, 44, 101036. https://doi.org/10.1016/j.suscom.2024.101036, p. 1.*

breaches, so these features are making cybersecurity a priority for both governments and private sectors worldwide.[24]

1.12 Surveillance Technologies

If we need to give a certain description to surveillance: In a broad sense, surveillance can be understood as any one-sided systematic, routine monitoring of individuals or groups for a given purpose. Surveillance policies are strategic measures by state authorities to gather information.[25] With the growth of AI and IoT, surveillance technologies have become more sophisticated, enabling real-time monitoring and data collection on a massive scale. Facial recognition systems, drones, and advanced camera networks are now being used in both public and private sectors for security and law enforcement purposes. However, these developments have sparked debates about privacy, data protection, and the ethical implications of constant surveillance. The balance between ensuring public safety and safeguarding individual privacy remains a contentious issue as surveillance technologies continue to evolve and expand.

1.13 Navigating Technological Change: From Innovation to Policy Response

The rapid advancement of these technologies has brought significant changes across various sectors, including communication, healthcare, transportation, finance, and in many others. On one hand, they are offering a plenty of benefits, such as increased efficiency, improved decision-making, personalized user experiences and the automation of complex and intensive tasks. Artificial intelligence for example has enabled more precise data analysis and predictions from enhancing customer service through chatbots to supporting healthcare professionals in diagnosing and treating diseases. Similarly, the Internet of Things (IoT) has paved the way for the creation of smart homes, cities, and even industries, allowing for real-time monitoring and management of resources, which in turn leads to greater efficiency and sustainability.

Blockchain technology, originally known as the backbone of cryptocurrencies, has extended its potential into various fields, including supply chain management, digital identity

---

[24] Knieps, G. (2024). Internet of Things, critical infrastructures, and the governance of cybersecurity in 5G network slicing. Telecommunications Policy, 48(4), 102867. https://doi.org/10.1016/j.telpol.2024.102867, pp. 2–4.

[25] Trüdinger, E.-M., & Steckermeier, L. C. (2017). Trusting and controlling? Political trust, information and acceptance of surveillance policies: The case of Germany. Government Information Quarterly, 34(3), 421–433. https://doi.org/10.1016/j.giq.2017.07.003, pp. 1–2.

verification, and secure voting systems. It promises to bring about more secure, transparent, and tamper-proof transactions, which could revolutionize traditional systems of trust. Autonomous vehicles, driven by sophisticated AI and sensor technologies, are paving the way for safer and more efficient transportation systems, with the potential to significantly reduce accidents and emissions. In parallel to these developments, 5G technology is laying the foundation for faster and more reliable connectivity, enabling the seamless integration of a vast network of devices and applications, from IoT sensors to augmented reality (AR) and virtual reality (VR) platforms.

However, while the benefits of these technologies are vast and transformative, they also present an array of challenges and risks that need to be carefully managed. For instance, the spread of IoT devices raises significant concerns regarding data privacy and security for many individuals and especially for the companies. The vast amount of data collected by these devices can be exploited if the data will not be protected properly as it should be, leading to potential breaches of personal information. Similarly to this situation, AI-driven systems are capable of optimizing processes and providing insights have started debates around ethical issues such as bias in decision-making, job displacement due to automation, and the potential misuse of AI in surveillance and disinformation campaigns. As AI systems become increasingly autonomous, the question of accountability, especially in cases of failure or harm, becomes more complex and pressing.

Cybersecurity has emerged as a critical concern in the digital age, especially as cyberattacks grow comprehensively and frequently, and it has started to become systematic in a certain order. The increased reliance on digital infrastructure has made both individuals and institutions more vulnerable to threats, necessitating stronger regulatory frameworks to protect data and ensure the integrity of critical systems. Blockchain, while offering a decentralized approach to transactions, also poses challenges in terms of regulatory oversight and consumer protection.

Autonomous vehicles, another remarkable technological development, raise questions about safety, liability, and infrastructure. One of the most debated questions regarding this issue is: “Who is responsible if an autonomous car is involved in an accident? The manufacturer, the software developer, or the vehicle owner?” Furthermore, the widespread adoption of these vehicles requires changes in infrastructure, such as smart traffic management systems, that must be carefully planned and regulated. It can be said that these kinds of technologies can be

safe as long as the environment they are working in is suitable for their working behavior and as modern as the technology itself.

5G technology, while promising to revolutionize connectivity, has sparked debates over national security and data privacy as well. The high-speed, low-latency communication offered by 5G enables more advanced IoT applications and real-time data processing, which is crucial for the operation of autonomous vehicles and smart cities. However, the deployment of 5G infrastructure often involving foreign companies has led to concerns about the control and security of critical communication networks.

So; regarding these multilayered challenges, the role of policymakers has become more complex and critical than ever before. Governments and international organizations are now at crossroads about how they must craft regulations that encourage technological innovations while addressing its potential downsides at the same time. This balance is especially crucial in sectors like healthcare, finance, transportation, and public safety, where the implications of technological misuse or failure can have serious consequences. The European Union (EU) has emerged as a leader in this domain, known for its proactive approach to technology regulation. With initiatives such as the General Data Protection Regulation (GDPR), the EU has set global standards for data privacy and protection, emphasizing the rights of individuals in an increasingly digital world where we are currently living in right now.

In the increase of these technological advances, the EU has been taking steps to develop comprehensive regulatory frameworks aimed at guiding the ethical use of AI, protecting the privacy and security of data, and ensuring that technological innovations align with societal values. This effort involves not just the creation of new policies but also the modification of existing ones to address the specific risks and benefits presented by each technological field. Since the technology is a field that renovates and develops every second, the regulations should be as adaptive as possible because of its nature. The EU's approach often emphasizes the need for transparency, accountability, and human-centric development, reflecting its broader commitment to human rights, democracy, and social welfare. This kind of an approach is of course a very predictable style of approach since the European Union has been promoting these norms since nearly its establishment.

However, the EU is not alone in its regulatory efforts. Other countries and international organizations are also dealing with similar issues, striving to establish norms and standards

that can guide the responsible development and deployment of these technologies should be must for everyone that is existing in this new era of technology in the 21st century. The global nature of these innovations means that policy responses cannot be confined to national or regional borders so international cooperation is crucial to addressing challenges that transcend boundaries, such as cybersecurity threats and data privacy breaches.

In the upcoming texts; this research will delve into a detailed analysis of how these technological advancements have impacted policy-making processes on a global scale to better understand how these two concepts, technology and policy-making are deeply related. We will explore a couple of regulations, guidelines and measures that governments and international bodies have introduced the benefits of technologies while safeguarding public interest. This analysis will provide insights into the complexities of shaping policy in an era characterized by rapid technological change. These informations will later highlight the EU's unique role in setting global standards and influencing the direction of technological governance in next chapters. In this part, there are going to be examples around the globe except the implications of the European Union. The case of the EU will be deeply analyzed in another chapter where we will also discuss the AI issue which highlights the main study case of this paper.

1.13.1 The United Nations - The ITU Smart Cities Initiative

The initiative is mostly focusing on the IoT and Smart Cities technologies. The ITU Smart Cities Initiative, also known as the "United for Smart Sustainable Cities (U4SSC)" program, was established by the International Telecommunication Union (ITU) which is a UN agency, to support the development of smart cities worldwide. The initiative focuses on leveraging advanced technologies like the Internet of Things (IoT), 5G, and artificial intelligence to create urban environments that are efficient, sustainable and more user-friendly.[26]

The primary goal of the initiative is to make cities more sustainable by promoting the efficient use of resources, reducing carbon emissions, and enhancing the quality of urban life. ITU gives a strong emphasis on standardization, developing global standards for IoT devices and 5G networks to ensure security, privacy and interoperability[27] across different systems.

---

[26] *United for Smart Sustainable Cities (U4SSC). (n.d.). Unlocking Cities of the Future: The Road to Smart Sustainable Cities. ITU. https://u4ssc.itu.int*

[27] *The ability of computer systems or software to exchange and make use of information.: "interoperability between devices made by different manufacturers".*

By adopting these standards in their habitats; cities now can deploy smart technologies without any problems and in a more secure way, they are fostering environments where real-time data analysis[28] informs urban planning[29] and public services. Through IoT sensors and devices, local governments can monitor various aspects such as traffic flow, air quality and energy consumption. By this; they are leading to more proactive and data-driven decision-making[30].

Another key aspect of the ITU Smart Cities Initiative is promoting inclusivity and citizen engagement. ITU advocates for smart cities that improve the lives of all residents, ensuring that technological advancements are accessible and beneficial to diverse populations, including marginalized groups. This approach includes fostering digital inclusion[31] and encouraging citizens' active participation in urban planning processes.[32]

The initiative also highlights the importance of cybersecurity in the context of smart cities. As cities adopt IoT devices and interconnected systems; the potential risks for the data privacy and network security increase importantly. ITU provides guidelines and standards to help cities implement strong cybersecurity measures which are protecting both public infrastructure and citizens' personal information.

Through the United for Smart Sustainable Cities (U4SSC) platform,[33] ITU collaborates with over 16 UN agencies, governments, technology companies, and research institutions to develop policy recommendations and best practices for smart city implementation. ITU also publishes various guidelines and reports, such as its "Toolkit on Environmental Sustainability for the ICT Sector," which offers insights into using ICT[34] solutions to address environmental challenges in urban areas. Additionally, the initiative involves capacity-building activities, including training and workshops, to help city planners and policymakers develop the necessary skills to manage smart city technologies effectively.[35]

---

[28] *The discipline that applies logic and mathematics to data to provide insights for making better decisions quickly*
[29] *The process of guiding and directing the use and development of land, urban environment, urban infrastructure, and related ecosystem and human services*
[30] *The process of collecting data based on your company's key performance indicators (KPIs) and transforming that data into actionable insights*
[31] *Equitable, meaningful, and safe access to use, lead, and design of digital technologies, services, and associated opportunities for everyone, everywhere*
[32] *United for Smart Sustainable Cities (U4SSC). (n.d.). Unlocking Cities of the Future: The Road to Smart Sustainable Cities. ITU. https://u4ssc.itu.int*
[33] https://u4ssc.itu.int/
[34] *Information and Communication Technology*
[35] *ITU. (n.d.). United for Smart Sustainable Cities (U4SSC). https://u4ssc.itu.int/about/*

On a global scale, the ITU Smart Cities Initiative has influenced how cities approach smart technology integration. By developing standardized Key Performance Indicators (KPIs) for smart cities, ITU provides cities with a benchmark to assess their progress in becoming smart and sustainable. This benchmarking process helps cities set targets and measure advancements in areas such as ICT infrastructure, environmental sustainability, and quality of life. In conclusion, the ITU Smart Cities Initiative plays an important role in order to guide cities toward smarter, more sustainable futures. It promotes global standards, offering policy guidance, and fostering collaboration. ITU ensures that smart city solutions are designed with security, inclusivity and sustainability.

1.13.2 Global Cybersecurity Agenda (GCA)

This initiative can be considered one of the most important initiatives that has been taken regarding technological developments; the agenda is very detailed and many experts consider it as the main guideline for cyber security.[36] So it is important to analyze the agenda deeply since it gives us certain important points to better understand how a big international organization like the UN takes action when it comes to providing a healthy environment where humanity benefits the most from important technological developments. The agenda is updating regularly; the biggest update has been conducted during the COVID-19 pandemic.[37]

The Global Cybersecurity Agenda (GCA) is an initiative led by the International Telecommunication Union (ITU), a specialized agency of the United Nations. Briefly; the organization aimed at promoting international cooperation in cybersecurity. It was established in 2007 and it provides a global framework for dialogue, collaboration, and strategic actions to enhance cybersecurity capabilities worldwide. The GCA seeks to address the growing challenges and threats in cyberspace, providing member states and organizations with guidelines, strategies, and tools to strengthen their cybersecurity infrastructure. We can divide the key objectives of the agenda into five main parts:

1. Enhancing International Cooperation: Recognizing that cybersecurity challenges are global in nature, GCA emphasizes the importance of international collaboration. It

[36] *Anderson, A., Ahmad, A., & Chang, S. (2024). Case-based learning for cybersecurity leaders: A systematic review and research agenda. Information & Management, 61(2024), 104015. https://doi.org/10.1016/j.im.2024.104015, p. 7.*
[37] *Akdağ, İ. (2019). Birleşmiş Milletler Tarafından Gerçekleştirilen Siber Güvenlik Çalışmaları. TASAM, p. 525.*

aims to bring together stakeholders from governments, private sector entities, academia, and civil society to collectively address cybersecurity issues.

2. Developing a Global Framework: One of the GCA's main goals is to establish a globally accepted framework for cybersecurity, which includes policy, legal, technical, and organizational measures. This framework is meant to guide countries in developing their own national cybersecurity strategies.
3. Building Capacity: GCA focuses on building the capacity of countries, especially developing nations, to strengthen their cybersecurity infrastructure. This involves providing training, sharing best practices, and facilitating the exchange of knowledge and expertise among countries to ensure a robust global cybersecurity posture.
4. Promoting Cybercrime Legislation: To combat cybercrime effectively, GCA encourages member states to develop and adopt comprehensive cybercrime legislation that aligns with international standards. It promotes harmonization of laws across borders to facilitate the prosecution of cybercriminals and the sharing of information between law enforcement agencies.
5. Establishing Cybersecurity Strategies: GCA offers guidance on developing national cybersecurity strategies. This includes defining roles and responsibilities within government agencies, setting up national cybersecurity response teams (CERT[38]s/CSIRT[39]s), and creating mechanisms for reporting and responding to cyber incidents.[40]

The GCA operates on five key pillars, all pillars are providing a comprehensive approach to addressing cybersecurity challenges:

1. Legal Measures: GCA encourages the development of appropriate legal frameworks to address cybersecurity, including laws related to data protection, privacy, and cybercrime. It works with countries to create legal structures that facilitate international cooperation in prosecuting cybercrimes.
2. Technical and Procedural Measures: This pillar focuses on the development and adoption of technical standards, tools and best practices for cybersecurity in general.

---

[38] A Computer Emergency Response Team (CERT) is a group of information security experts responsible for the protection against, detection of and response to an organization's cybersecurity incidents.

[39] A capability set up for the purpose of assisting in responding to computer security-related incidents; also called a Computer Incident Response Team (CIRT)

[40] International Telecommunication Union. (n.d.). Cybersecurity. https://www.itu.int/en/action/cybersecurity/Pages/default.aspx

It includes initiatives to promote secure software development, enhance network security, and establish CERTs to manage and respond to cyber incidents.

3. Organizational Structures: GCA emphasizes the importance of having clearly defined organizational structures within governments and institutions to oversee cybersecurity efforts. This includes the establishment of national cybersecurity agencies, policy-making bodies, and incident response teams.
4. Capacity Building: Recognizing that human expertise is crucial to cybersecurity, GCA supports training and educational programs. It works to build capacity in areas such as risk assessment, incident response, and cybersecurity policy development, particularly in developing countries.
5. International Cooperation: At the heart of GCA is the promotion of international collaboration. By facilitating the exchange of information, best practices and expertise, GCA helps countries work together to address cross-border cyber threats and challenges.[41]

As it can be understood from their pillars and the key objectives; the agenda has aiming to provide a guideline for cyber security in the whole world. From the beginning of its establishment, the GCA has had a significant impact on enhancing cybersecurity efforts worldwide. Here are some examples of what the GCA achieved and its impact on other initiatives related to cyber security issues.

- Assistance to Member States: GCA provides technical assistance to ITU member states, helping them develop national cybersecurity strategies, establish CERTs, and implement legal frameworks to combat cybercrime.
- Global Cybersecurity Index (GCI): In line with the GCA's objectives, the ITU publishes the Global Cybersecurity Index, which assesses countries' cybersecurity readiness. The GCI serves as a benchmarking tool, highlighting areas for improvement and promoting best practices in cybersecurity.[42]
- Collaboration with International Partners: The GCA collaborates with international organizations, such as the United Nations Office on Drugs and Crime (UNODC), the

[41] *Ntoko, A. (2011, January 17-21). Global Cybersecurity Agenda (GCA): A framework for international cooperation [Conference presentation]. Open-ended Intergovernmental Expert Group on Cybercrime, Vienna, Austria.*

[42] *International Telecommunication Union. (n.d.). Global Cybersecurity Agenda (GCA). https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx*

European Union Agency for Cybersecurity (ENISA), and INTERPOL to coordinate global efforts in combating cyber threats.[43]

As it has been mentioned above; the GCA continues to adapt to the evolving cybersecurity landscape, addressing new threats like ransomware[44], IoT vulnerabilities, and supply chain attacks. Its future direction involves strengthening partnerships, enhancing information sharing among member states and promoting the adoption of advanced cybersecurity technologies to protect critical infrastructure and data. The Global Cybersecurity Agenda is a cornerstone of the ITU's efforts to create a safer digital environment, providing a comprehensive, cooperative framework for global cybersecurity enhancement.[45] They think that providing a safe and cyberly-secured place in the technological environment is a must and it can be on the agenda of all organizations globally.[46] This agenda is a concrete example of how policy making for the organizations and states shift in our century because of recent technological developments. Because for a well functioning political environment; it is now a necessity to learn how to properly use technological investments and think about how to benefit from it with the lowest risk possible.[47]

1.13.3 OECD Blockchain Policies

Because of its characteristic and working area, The Organisation for Economic Co-operation and Development (OECD) is actively involved in the policy making regarding blockchain technology. By recognizing blockchain's transformative potential, the OECD has worked to guide governments and international organizations in understanding the benefits and risks of this technology, and focusing on shaping appropriate regulatory frameworks. In 2018, the OECD established the Blockchain Policy Centre which works as a hub for research and analysis on blockchain and other distributed ledger technologies[48] (DLT). The center provides guidance to OECD member and non-member countries on the regulatory, economic and social implications of blockchain technologies.[49] The center aims to foster international

[43] *Cyber Policy Portal. (n.d.). Cyber Policy Portal. https://cyberpolicyportal.org/*
[44] *A type of malware that permanently blocks access to the victim's personal data unless a "ransom" is paid*
[45] *Schjølberg, S. (2008). ITU Global Cybersecurity Agenda (GCA): Report of the Chairman of the High-Level Experts Group (HLEG). International Telecommunication Union.*
[46] *Anderson, A., Ahmad, A., & Chang, S. (2024). Case-based learning for cybersecurity leaders: A systematic review and research agenda. Information & Management, 61(2024), 104015. https://doi.org/10.1016/j.im.2024.104015, p. 7.*
[47] *Eldem, T. (2021). Birleşmiş Milletler Sistemi ve Küresel Siberalan Güvenliği Regülasyonu. Marmara Üniversitesi Siyasal Bilimler Dergisi, 9(1), 17–45. https://doi.org/10.14782/marmarasbd.876091, pp. 29–32.*
[48] *A decentralized peer-to-peer digital system for recording transactions between parties in multiple places at the same time*
[49] *OECD. (n.d.). Digital finance. https://www.oecd.org/en/topics/sub-issues/digital-finance.html*

cooperation, share best practices and ensure the responsible adoption of blockchain technologies focusing on areas such as finance, supply chains and government services. One of the primary areas where the OECD has focused its blockchain-related work is the financial sector. Blockchain has the potential to disrupt traditional financial systems by enabling decentralized, secure and transparent transactions. The OECD has provided recommendations on regulating cryptocurrencies[50], Initial Coin Offerings[51] (ICOs) and the use of blockchain in digital financial assets. The goal is to promote innovation while addressing risks like fraud, money laundering, and market volatility. The OECD has studied how blockchain can be applied in tax administration and compliance. Blockchain's transparency and immutability can help reduce tax fraud and improve efficiency in tax collection processes. The OECD is particularly interested in how blockchain could streamline cross-border transactions and enhance transparency in tax reporting.[52]

Also since 2018 the OECD has organized the OECD Blockchain Policy Forum, which brings together policymakers, regulators, business leaders and experts from around the world to discuss the future of blockchain technology. The forum addresses the regulatory and policy challenges of blockchain and examines how it can be helpful for economic growth and societal benefits.[53]

1.13.4 G20 Cybersecurity Guidelines

The G20 Cybersecurity Guidelines are a set of principles and recommendations developed by the Group of Twenty (G20) to enhance global cooperation on cybersecurity. These guidelines are aimed at addressing the growing threat of cyberattacks, improving the resilience of financial systems and fostering collaboration among G20 member states to ensure a secure and stable digital environment. As cybersecurity threats have increased in every continent G20 countries have recognized the need for a coordinated international response to protect critical infrastructure, financial systems and individuals from any kinds of cyber risks possible. There certain key objectives they are focusing on currently:

---

[50] *A digital currency, which is an alternative form of payment created using encryption algorithms*
[51] *A relatively new method of raising capital for early-stage ventures. They allow businesses to raise capital for their projects, by issuing digital tokens in exchange for crypto assets or fiat currencies.*
[52] *OECD. (n.d.). Digital strategies in education across OECD countries. https://www.oecd-ilibrary.org/education/digital-strategies-in-education-across-oecd-countries_33dd4c26-en*
[53] *OECD. (2022). OECD Blockchain Policy Forum. https://mneguidelines.oecd.org/oecd-blockchain-policy-forum.htm*

1. Strengthening Cyber Resilience
2. International Cooperation
3. Harmonizing Cybersecurity Standards
4. Fostering Innovation and Security
5. Cybersecurity Awareness and Capacity Building
6. Cyber Incident Response and Recovery

The G20 Cybersecurity Guidelines represent a significant step towards improving global cybersecurity cooperation and resilience. They are promoting international collaboration, harmonizing regulations, and encouraging the adoption of best practices. These guidelines aim to create a safer and more secure digital environment for all nations. As cyber threats continue to evolve, the G20's efforts to coordinate global cybersecurity policies will be essential in safeguarding critical infrastructure, financial systems and the broader digital economy. Since technological developments keep evolving every second and new cyber threats keep emerging; it is important to adapt to every change and new investments.[54]

Recently; during the G20 summit in Brazil, leaders from the G20 countries emphasized the need for international cooperation in digital security, particularly as cyber threats continue to grow with increased global connectivity. They discussed key areas such as artificial intelligence, digital governance, and the protection of vulnerable populations. The leaders agreed that governments must take proactive measures and foster global trust to combat digital threats effectively.[55]

Again at the recent G20 meeting they stated that they understand this feature of the issue and they are adopting more convenient guidelines to be ready for new potential risks. As an example regarding this subject, they are paying attention to ideas of experts on the field such as Professor Danielle Ayres. She emphasizes the importance of cybersecurity for vulnerable groups such as older people and children. She highlights the need for regulatory frameworks to protect users in the digital space and discusses cyber maturity[56] which involves improving states' capabilities to prevent and respond to cyber threats. Ayres also notes the importance of

---

[54] *G20. (2024). Cybersecurity: Strengthening policies to combat threats in the digital world. https://www.g20.org/en/news/cyber-security-strengthening-policies-to-combat-threats-in-the-digital-world*
[55] *Cyber Daily. (2024). G20 leaders call for global cyber regulations. https://www.cyberdaily.au/government/10695-g20-leaders-call-for-global-cyber-regulations*
[56] *A state's or organizations' level of readiness to defend itself and its digital assets against cyberattacks.*

global cooperation, especially through forums like the G20, to create cybersecurity policies that protect all citizens, particularly the most vulnerable ones.[57]

1.13.5 International Telecommunication Union (ITU) - 5G Standards

The International Telecommunication Union (ITU) has been instrumental in defining the technical specifications for 5G networks under the IMT-2020[58] framework. ITU's work ensures that 5G meets high-performance standards such as ultra-reliable, low-latency communication[59], enhanced mobile broadband, and massive machine-type communications, critical for IoT and smart cities. The standards allow global interoperability, ensuring that devices and networks across different regions can function seamlessly together. There are some key Components of ITU's 5G Standards that have been stated.[60]

1. IMT-2020 Specifications: ITU has developed the IMT-2020 requirements that define what constitutes 5G technology. These specifications include higher data transfer speeds, minimal latency (1 millisecond or less), and the ability to support billions of IoT devices.
2. Performance Goals: 5G networks are designed to deliver speeds up to 20 Gbps, support for massive device connectivity (over 1 million devices per square kilometer), and low energy consumption, making it a key enabler for smart cities, autonomous vehicles, and Industry 4.0 applications.
3. Global Interoperability: ITU's standards ensure that 5G technologies are interoperable worldwide, allowing devices and systems to operate seamlessly across different countries and networks. This is crucial for industries like telecommunications, healthcare, and transportation, which rely on consistent, high-quality connectivity across borders.
4. Spectrum Allocation: ITU manages the global allocation of spectrum bands for 5G services, ensuring sufficient bandwidth is available for high-speed data transmission

---

[57] *G20. (2024). According to an expert, cybersecurity should protect more vulnerable groups such as older people and children. https://www.g20.org/en/news/according-to-an-expert-cybersecurity-should-protect-more-vulnerable-groups-such-as-older-people-and-children*

[58] *International Mobile Telecommunications-2020 (IMT-2020 Standard) are the requirements issued by the ITU Radiocommunication Sector (ITU-R) of the International Telecommunication Union (ITU) in 2015 for 5G networks, devices and services.*

[59] *The ability of a computing system or network to provide responses with minimal delay*

[60] *Dahlman, E., Parkvall, S., & Sköld, J. (2024). 5G standardization. In 5G/5G-Advanced (pp. 7–27). Elsevier. https://doi.org/10.1016/B978-0-443-13173-8.00011-6, pp. 7–8.*

while minimizing interference between different services. Spectrum management is vital to support the growing number of connected devices and services.

5. Cybersecurity and Privacy: Given the increase in connectivity and data flow with 5G, ITU standards also focus on cybersecurity and privacy. They establish guidelines for network security, ensuring that 5G networks are resilient to cyberattacks, protecting both infrastructure and user data.
6. Support for Emerging Technologies: ITU's standards enable 5G to support next-generation technologies, including virtual and augmented reality (VR/AR), autonomous vehicles, and IoT ecosystems. These developments are seen as critical to advancing global digital economies.[61]

ITU's 5G standards are critical for the spread of global 5G networks, because they are expected to have a transformative impact on industries such as telecommunications, manufacturing, healthcare and transportation in the upcoming future.[62] As countries continue to deploy more and more 5G infrastructure, ITU plays the pioneer role of ensuring these technologies to be implemented with a focus on security, efficiency and sustainability.

1.13.6 The United States Foreign Intelligence Surveillance Act (FISA)

The United States Foreign Intelligence Surveillance Act was enacted in 1978. FISA is a United States law that is governing the surveillance of foreign powers, agents and individuals suspected of espionage[63] or terrorism. It allows the U.S. government to conduct electronic surveillance and physical searches without a traditional authority when it involves foreign entities or individuals engaged in intelligence activities.[64] Cases that come to the FISA are conducted in a specific court. FISA Court (FISC) is a special court established to oversee and approve government requests for surveillance and searches. It ensures these requests meet legal standards. This secret court reviews government requests for surveillance under FISA. Although FISC operates largely out of public view, it provides a judicial check on government surveillance efforts. FISA is now considered as the most complicated and inclusive act regarding the protection of communication in general. Because of its inclusivity,

---

[61] *International Telecommunication Union. (2024). ITU-T: Setting the standard. https://www.itu.int/en/mediacentre/backgrounders/Pages/itu-t-setting-the-standard.aspx*
[62] *International Telecommunication Union. (2024). 5G: Fifth generation of mobile technologies. https://www.itu.int/en/mediacentre/backgrounders/Pages/5G-fifth-generation-of-mobile-technologies.aspx*
[63] *The practice of spying or of using spies, typically by governments to obtain political and military information.*
[64] *Bureau of Justice Assistance. (n.d.). Foreign Intelligence Surveillance Act of 1978 (FISA). https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1286*

it plays a pioneer role for most of its equivalents in the other countries or continents. Briefly it aims to provide a healthy environment both in reality and online world for the whole US citizens and every place where the USA is conducting its existence such as military bases. It includes specific provisions that should be highlighted because of its relativity for our subject.

> Section 702: It allows surveillance on foreign nationals outside the U.S. without a warrant for counterterrorism or intelligence purposes. The controversial part of this provision is the incidental collection of U.S. citizens' communications when interacting with foreign surveillance targets.
>
> Title I: Governs the surveillance of foreign agents inside the U.S. The government must show probable cause that the individual is acting as an agent of a foreign power.
>
> Title VII: Focuses on the surveillance of foreign individuals who are not U.S. citizens, without the need for a traditional court order.[65]

Important amendments and Controversies:

> USA PATRIOT Act (2001) expanded FISA's reach post-9/11, allowing greater surveillance powers in the fight against terrorism. The USA Patriot Act significantly altered the collection and analysis of personal information under the Foreign Intelligence Surveillance Act (FISA). The Patriot Act expanded the circumstances under which personal data can be collected, allowing law enforcement to access any 'tangible thing' related to an investigation. The act also enabled wider surveillance capabilities, including roving wiretaps[66] and electronic communication interception[67], with lowered thresholds for obtaining court approval.[68]
>
> Also Section 215 (Sunset in 2020) has allowed the collection of telecommunication metadata, which faced significant controversy after Edward Snowden's disclosures in 2013.

---

[65] *U.S. Office of the Director of National Intelligence. (n.d.). Foreign Intelligence Surveillance Act (FISA). https://www.intelligence.gov/foreign-intelligence-surveillance-act*

[66] *In United States law, a roving wiretap is a special kind of wiretap permit that follows the surveillance target.*

[67] *"Intercept", in relation to a communication, means listening to, monitoring, viewing, reading or recording,*

[68] *Jaeger, P. T., Bertot, J. C., & McClure, C. R. (2003). The impact of the USA Patriot Act on collection and analysis of personal information under the Foreign Intelligence Surveillance Act. Government Information Quarterly, 20(3), 295–314. https://doi.org/10.1016/S0740-624X(03)00057-1, p. 297.*

FISA in general shows some extreme features that are actually designed to protect citizens at all cost from any kinds of risks that could occur from any kinds of communication channel, however at the same time it violates many other human rights from many perspectives. So this issue sparked lots of debates within the US or outside the continent even. FISA has sparked debates about privacy, especially regarding the incidental collection of U.S. citizens' data. The USA Patriot Act broadened FISA's scope, allowing greater access to business records and electronic surveillance, raising concerns about privacy and civil liberties, especially concerning the relaxed standards for surveillance.[69] Critics argue that the FISA process lacks transparency, especially with its secret court proceedings. Many other countries, especially the member states of the European Union, see this act as a huge threat for their data privacy, it is a risk for both higher and individual levels.[70]

Surveillance technologies, especially under frameworks like FISA, have an important impact on policy-making. FISA's minimization procedures aim to balance intelligence gathering with civil liberties protections. These requirements limit the collection, retention, and dissemination of non-public information about U.S. persons unless it pertains to foreign intelligence or evidence of a crime.[71] The development and implementation of laws like FISA illustrate how national security concerns drive legislative changes and it often balances security needs with individual civil liberties. As technology keeps evolving, also the legislative landscapes, with FISA serving as a key example of how policy must continuously adapt to address both emerging threats and privacy concerns. This law is instrumental in shaping the intersection between security and civil rights. FISA is a key law in shaping U.S. intelligence and national security policy and it is balancing the needs of surveillance with civil liberties protections. The law is regularly reviewed and amended by Congress to address emerging concerns about privacy and national security. FISA has been fundamental in shaping the way surveillance is conducted for national security purposes in the U.S. while being a subject of continued debate regarding its impact on civil liberties.

---

[69] Strickland, L. S. (2003). Civil liberties vs. intelligence collection: The secret Foreign Intelligence Surveillance Act court speaks in public. Government Information Quarterly, 20(1), 1–12. https://doi.org/10.1016/S0740-624X(02)00132-6, p. 2.

[70] Geffray, M. (2024). FISA law extension: Impact on European privacy regulations. Oodrive. https://www.oodrive.com/blog/regulation/fisa-law-extension/#:~:text=The%20FISA%20Act%20contradicts%20European,it%20until%20April%2019%2C%202024.

[71] Strickland, L. S. (2003). Civil liberties vs. intelligence collection: The secret Foreign Intelligence Surveillance Act court speaks in public. Government Information Quarterly, 20(1), 1–12. https://doi.org/10.1016/S0740-624X(02)00132-6, p. 2.

In summary, Chapter 1 has provided an in-depth exploration of how the rapid advancement of key technologies such as artificial intelligence (AI), the Internet of Things (IoT), 5G networks, and blockchain has had profound implications on policy-making processes across the world. These technologies have created opportunities that have never been seen before in terms of innovation, efficiency and connectivity. They are fundamentally altering industries ranging from healthcare and transportation to communication and finance. However, these advancements have also raised serious concerns; particularly regarding privacy, data protection, cybersecurity and ethical issues.

AI, with its ability to process large volumes of data and make autonomous decisions, stands out as a transformative force. While AI has enabled more personalized and efficient services across industries, it has also raised questions about accountability, bias and transparency in decision-making processes. This chapter discussed how AI requires particular policy frameworks to ensure that its deployment remains ethical and aligned with human rights values, especially in fields such as law enforcement and healthcare where the consequences of misuse could be more and more.

Similarly to artificial intelligence, the IoT has redefined connectivity by allowing billions of devices to be interconnected within themselves. While this has greatly improved the management of resources in sectors such as smart cities, agriculture and manufacturing; it has also made the need for robust cybersecurity policies more urgent. The chapter emphasized the vulnerabilities created by this massive network of interconnected devices which if left unsecured, could become a target for cyberattacks with devastating consequences for privacy and public safety.

5G technology represents another leap when it comes to technological advancement which is enabling faster and more reliable communication with low latency. This technology has the potential to revolutionize industries like telecommunications, autonomous driving and remote healthcare. However, as highlighted in this chapter, the implementation of 5G also brings forward geopolitical challenges related to data sovereignty, national security and the regulation of infrastructure owned by foreign entities. That is why governments are tasked with ensuring that the deployment of 5G is done securely while balancing the need for international cooperation and technological progress.

Blockchain technology, originally developed to support cryptocurrencies like Bitcoin has found applications in supply chain management, finance and digital identity verification. This chapter also detailed how blockchain offers a secure and transparent method for recording transactions, yet it also presents regulatory challenges due to its decentralized nature. Policymakers face the problem of addressing issues related to fraud, money laundering and illicit transactions[72] while fostering blockchain's potential to improve efficiency in the digital economy.

Throughout this chapter; technological developments that have an important role in the 21st century and the role of governments and international organizations in regulating these technologies has been the main theme. As it will be mentioned in a more detailed way in upcoming chapters; the European Union in particular, has positioned itself as a leader in setting global standards for technology regulation, especially with frameworks like the General Data Protection Regulation (GDPR) and the Artificial Intelligence Act. These policies aim to promote innovation while safeguarding citizens' rights, setting a benchmark for other regions. Other countries and organizations, such as the United States with its Foreign Intelligence Surveillance Act (FISA) and the United Nations with its cybersecurity initiatives, have also been pivotal in addressing the challenges posed by these emerging technologies.

This chapter concludes by emphasizing the need for continuous evolution in policy-making to keep pace with technological advancements. As these technologies continue to reshape industries and society at large, governments must strike a delicate balance between fostering innovation, maintaining national security and upholding individual privacy rights. We analyzed a few of these examples in this chapter from different countries and different institutions. In this rapidly changing technological environment; policy-makers must ensure that regulation is flexible enough to adapt to new developments while also comprehensive enough to mitigate risks and protect citizens. The policy frameworks developed in response to these technologies will shape not only the future of industries but also the broader socio political landscape globally. So once again it can be clearly said that in this century we are living in right now, it is inevitable to not consider technological developments in the policy making processes. However since the subject is changing constantly and it includes many other risks, it is a hard theme to regulate and to find the balance.

[72] *The movement of money across borders that is illegal in its source*

CHAPTER II

GLOBAL IMPACT AND SIGNIFICANCE OF AI

In recent years, artificial intelligence (AI) has emerged as one of the most transformative technological advancements, fundamentally reshaping industries, economies and societies on a global scale. As we transition into a world where data-driven decision-making and automation[73] become integral to both public and private sectors. So it definitely can be said that now artificial intelligence's influence is increasingly widespread. This chapter will mention what this artificial intelligence is and will explore the massive impact that AI has had on various dimensions of global infrastructure, from its role in driving economic growth to its influence on labor markets and the ethical challenges it presents to policymakers but also give examples to its effect on our daily lives to better understand its capabilities overall.

One of the key questions this chapter will address is whether AI represents the new technological revolution comparable to the rise of the internet in the late 20th century. By drawing parallels between these two transformative forces, the chapter will analyze how AI, like the internet before it, has created entirely new business models, disrupted traditional industries and shifted the balance of power in specific sectors.

We will also examine the global implication of the artificial intelligence with particular attention to how different countries and regions are adapting to it and regulating this powerful technology. While the United States and China lead the race in AI development, as we also mentioned a little and also get into that deeply in the upcoming chapters, the European Union's approach to ethical AI governance, exemplified by its AI Act, serves as a model for balancing innovation with human rights and privacy concerns. We will consider AI's impact on the global workforce, particularly in terms of automation and job displacement and how governments are navigating the socio-economic challenges AI introduces.

Additionally, ethical concerns surrounding AI such as biases in algorithms, the potential misuse of surveillance technologies, and the need for transparency in AI decision-makings will be explored. These ethical challenges not only influence public trust in AI but also shape the policy frameworks that governments are developing to manage its integration into society.

---

[73] *The technique of making an apparatus, a process, or a system operate automatically*

Basically this chapter will provide a comprehensive analysis of AI's global significance, not only in terms of technological innovation but also its far-reaching implications on global governance, economy, ethics and social structures. By understanding AI's transformative impact, we can better figure out the challenges and opportunities that lie ahead as this technology continues to evolve.

2.1 What is Artificial Intelligence?

Artificial Intelligence (AI) is the branch of computer science that focuses on building machines capable of performing tasks that typically require human intelligence. These tasks can range from simple problem-solving and decision-making to complex functions like understanding natural language, visual perception and autonomous navigation.

AI operates by mimicking human cognitive processes such as learning from data, which is often through machine learning, reasoning through logic-based systems, and adapting to new information. In practice AI is a technology that covers various technologies, including machine learning algorithms, deep learning[74] models, natural language processing (NLP)[75], and neural networks[76] which enable machines to simulate cognitive abilities like understanding, recognizing patterns and predicting specific outcomes.[77]

AI systems can be classified into two main categories:

- *Narrow AI (Weak AI)*: This refers to systems designed to perform a specific task or set of tasks. Examples include virtual assistants (Siri, Alexa), recommendation algorithms used by platforms like Netflix and AI used in medical diagnostics. Narrow AI focuses on one problem and works within a limited domain, excelling in areas where it's been trained but lacking generalization capabilities beyond those tasks.[78]
- *General AI (Strong AI)*: This is a theoretical form of AI that would have the ability to understand, learn and apply knowledge across a wide range of domains, mirroring the cognitive capabilities of humans. General AI remains a conceptual idea and has not

[74] *A method in artificial intelligence (AI) that teaches computers to process data in a way that is inspired by the human brain.*
[75] *The ability of a computer program to understand human language as it's spoken and written*
[76] *A method in artificial intelligence (AI) that teaches computers to process data in a way that is inspired by the human brain*
[77] *Öztemel, E. (2020). Yapay zekâ ve insanlığın geleceği. In Bilişim teknolojileri ve iletişim: Birey ve toplum güvenliği (pp. 96–112). Türkiye Bilimler Akademisi, p. 101.*
[78] *Labbe, M., & Wigmore, I. (2024). Narrow AI (weak AI). TechTarget. https://www.techtarget.com/searchenterpriseai/definition/narrow-AI-weak-AI*

been realized, as it would require the ability to perform any intellectual task a human can do, including creative thinking and emotional intelligence.

AI is also characterized by its ability to learn and improve over time. Through machine learning, AI systems can analyze large datasets, recognize patterns and improve their decision-making processes without explicit programming for every possible scenario. Deep learning, a subfield of machine learning, uses artificial neural networks to model complex patterns and is particularly effective in tasks like image recognition and language processing.

Another very important key aspect of AI is automation. AI systems are used to automate processes that would otherwise require human intervention, which enhances efficiency and accuracy in areas such as industrial manufacturing, data analysis, and customer service. Automation through AI has allowed businesses and governments to optimize operations, save costs, and scale services.[79]

As AI continues to evolve, its applications extend into nearly every field, from healthcare (AI-driven medical diagnoses, personalized treatment) to finance (automated trading, fraud detection), transportation (autonomous vehicles), and even governance (AI-driven policy analysis). This expansion of AI's role in society raises important questions about ethics, governance, and regulation, as AI technologies are reshaping the way individuals, organizations, and governments operate.[80]

2.2 A Brief History of AI

Although Artificial Intelligence (AI) is often perceived as a recent innovation; its conceptual roots trace back to the early days of computing. We are hearing this new phenomenon constantly in our current time, however this does not mean that it is a new thing; it can be said that this new technology gained popularity in recent years because of the developments on the field. AI, in many ways, is as old as the first computers themselves. The foundational ideas were established during the mid-20th century, with pioneers like Alan Turing theorizing about machines capable of simulating human thought. While the technology behind AI has rapidly evolved in recent years, especially with advancements in machine learning and deep learning, its historical journey started decades ago, making it both an old aspiration and a new

[79] *Labbe, M., & Wigmore, I. (2024). Narrow AI (weak AI). TechTarget. https://www.techtarget.com/searchenterpriseai/definition/narrow-AI-weak-AI*

[80] *Adaş, E. B., & Erbay, B. (2022). Yapay Zekâ Sosyolojisi Üzerine Bir Değerlendirme. Gaziantep University Journal of Social Sciences, 21(1), 326–337. https://doi.org/10.21547/jss.991383, pp. 334–335.*

reality. Despite its long history, the full realization of AI's potential is still unfolding, positioning it at the frontier of modern technological revolutions.

This contrast between AI's long conceptual history and its recent breakthroughs demonstrates how fundamental ideas can take time to mature and integrate into daily life, making AI both a historical and futuristic force. That is why it is important to understand the history of this technology so let us have a look at it briefly;

1. Early Foundations (1940s–1950s):
    - The concept of artificial intelligence can be traced back to Alan Turing, the British mathematician who, in his 1950 paper "Computing Machinery and Intelligence", proposed the idea that machines could simulate any form of reasoning and intelligence through algorithms. He also introduced the Turing Test, which assesses a machine's ability to exhibit intelligent behavior indistinguishable from that of a human.
    - John McCarthy, an American computer scientist, is credited with sparking the term "Artificial Intelligence" in 1956 during the Dartmouth Conference, considered the founding event of AI as a field of study. This conference also marked the beginning of the first wave of AI research.
2. The Birth of AI and Early Development (1950s–1970s):
    - Early AI research focused on creating machines that could solve logical problems, such as puzzles and games. In 1956, Herbert Simon and Allen Newell developed the Logic Theorist, one of the first AI programs capable of proving mathematical theorems.
    - The late 1950s and 1960s saw the rise of symbolic AI, which used rule-based systems[81] to simulate human reasoning[82]. One notable development was the General Problem Solver[83] (GPS), an early AI algorithm capable of solving abstract problems.
    - However, progress was slow and by the 1970s the AI community faced what became known as an "AI winter", a period of reduced funding and interest due

[81] *A basic type of AI model that uses a set of prewritten rules to make decisions and solve problems*
[82] *Human thought that is based on empirical evidence and logic rather than emotion.*
[83] *Uses means-ends-analysis heuristic for solving formalized symbolic problems. A GPS computer program solves simple problems that can be formalized such as the Towers of Hanoi.*

to unmet expectations and technical challenges, particularly with regard to natural language processing and pattern recognition.

3. Expert Systems and Revival (1980s):
    - In the 1980s, AI experienced a revival with the development of expert systems. These were rule-based programs designed to emulate the decision-making abilities of a human expert. Industries like medicine and finance saw the potential of AI to assist in diagnostics and decision-making.
    - Systems like MYCIN[84], developed in the 1970s, became foundational for later expert systems. These programs used vast amounts of data and knowledge to provide solutions for specific, narrowly defined problems, which allowed AI to gain renewed interest and funding.
4. Machine Learning and Data-Driven AI (1990s–2000s):
    - The next significant shift in AI came with the rise of machine learning in the 1990s, a subfield of AI focused on systems that can learn from data. Unlike earlier AI approaches that relied on predefined rules, machine learning models used algorithms to find patterns in data and improve their performance over time without explicit programming for every task.
    - Support Vector Machines (SVMs)[85] and neural networks gained popularity as tools for data-driven AI. This era also saw advancements in speech recognition, computer vision and natural language processing.
    - The development of powerful computing hardware and access to vast datasets through the internet further accelerated AI research during the late 2000s.[86]
5. Deep Learning and Modern AI (2010s–Present):
    - The 2010s marked the emergence of deep learning, a subset of machine learning that uses multi-layered neural networks[87] to analyze complex data patterns. Deep learning revolutionized AI applications, particularly in areas like image recognition (e.g., Google's DeepMind), natural language processing and autonomous systems. NLP enables computers and digital devices to recognize, understand and generate text and speech by combining

---

[84] MYCIN was an early backward chaining expert system that used artificial intelligence to identify bacteria causing severe infections, such as bacteremia and meningitis, and to recommend antibiotics.
[85] A type of supervised learning algorithm used in machine learning to solve classification and regression tasks
[86] De Spiegeleire, S., Maas, M., & Sweijs, T. (2017). What is artificial intelligence? In Artificial intelligence and the future of defense: Strategic implications for small- and medium-sized force providers (pp. 25–42). Hague Centre for Strategic Studies. http://www.jstor.org/stable/resrep12564.7, pp. 31–32.
[87] Consists of multiple layers of interconnected nodes or neurons

computational linguistics—the rule-based modeling of human language—together with statistical modeling, machine learning and deep learning.[88]

- One of the most significant milestones was the development of AlphaGo, an AI system by DeepMind that defeated a world champion Go player in 2016, showcasing the power of deep learning in complex, strategic tasks.
- In recent years, Generative Pretrained Transformers (GPT) and other large-scale language models have further pushed the boundaries of AI, allowing machines to generate human-like text, engage in meaningful conversations and even create artistic works.[89]

As it can be seen, Artificial Intelligence is a broad concept with a rich and extensive history. It is far from being a newly emerging phenomenon. The foundations of AI were laid decades ago, dating back to the early developments in computing and theoretical ideas about machine intelligence. While recent advancements in technology have pushed AI to the forefront, its conceptual journey spans over half a century. Thus, AI is a mature, evolving field that has passed continuous developments and it is blending long-standing aspirations with fascinating innovations.[90]

2.3 The Role of Artificial Intelligence in Everyday Life

Artificial intelligence (AI) has become an integral part of our daily routines even without our intention. It has often been included often in ways we may not immediately recognize. From the virtual assistants we interact with such as Siri or Alexa to personalized recommendations on platforms like Netflix and Amazon, AI is arranging our experiences to individual preferences. In healthcare, AI helps to diagnose certain diseases and treatment planning. While in finance; it powers fraud detection and automated trading[91]. Autonomous vehicles, smart home devices and facial recognition systems further demonstrate AI's growing presence, reshaping industries and streamlining daily tasks. AI's huge influence in

---

[88] *IBM. (2024). Natural language processing (NLP). https://www.ibm.com/topics/natural-language-processing*
[89] *Muthukrishnan, N., Maleki, F., Ovens, K., Reinhold, C., Forghani, B., & Forghani, R. (2020). A brief history of artificial intelligence. Neuroimaging Clinics of North America, 30(3), 393–399. https://doi.org/10.1016/j.nic.2020.07.004, pp. 393–396.*
[90] *Türkiye Yapay Zeka İnisiyatifi. (2022). Yapay zeka zaman çizelgesi. https://turkiye.ai/kaynaklar/yapay-zeka-zaman-cizelgesi/*
[91] *A subset of algorithmic trading, uses a computer program to create buy and sell orders and automatically submits the orders to a market center or exchange*

daily life underscores its role as a transformative force, automating processes, improving efficiency and personalizing interactions across various sectors.[92]

Specific AI programs are used as virtual assistants that respond to voice commands, perform tasks such as setting reminders, answering questions or playing music. These systems rely on natural language processing (NLP) to understand user requests and machine learning to improve over time, offering increasingly personalized responses. Siri, Alexa, and Google Assistant are popular and widely used AI-powered virtual assistants designed to perform tasks through voice or written commands. Siri has been developed by Apple and is integrated into iOS devices. It is offering personalized assistance and control over Apple services. Amazon's Alexa, commonly found in Echo devices, is now a superior smart home control that is managing entertainment and online shopping. Google Assistant which is available on Android devices and Google Home products; offers robust search capabilities and interacts with the full range of Google services. All these three AI powers use natural language processing (NLP) to understand and respond to user demands and they are learning from interactions to improve their functionality over time. So that means the more you use these programs the more they get better and they become more useful for you. They are designed to adapt your preferences. Platforms like Netflix and Spotify use AI to analyze user behavior and offer personalized content recommendations. In the automotive industry, AI plays a key role in the development of autonomous vehicles, enabling cars to recognize objects and navigate roads. In smart homes, AI powers devices like thermostats and security cameras that learn user habits to improve energy efficiency and security. Similarly, e-commerce platforms like Amazon leverage AI to recommend products based on past purchases and browsing habits.[93]

In healthcare, AI assists in diagnosing diseases, often using image recognition to analyze medical scans. This technology helps detect conditions like cancer more quickly and accurately than traditional methods. In finance, AI is crucial for fraud detection, monitoring transactions for suspicious activity and alerting users in real-time. AI is also widely used in facial recognition systems for security purposes, such as unlocking smartphones or identifying passengers at airports. AI plays a significant role in online advertising where

[92] *Karakoç Keskin, E. (2023). Yapay Zekâ Sohbet Robotu ChatGPT ve Türkiye internet gündeminde oluşturduğu temalar. Yeni Medya Elektronik Dergisi, 7(2), 114–131. https://doi.org/10.17932/IAU.EJNM.25480200.2023/ejnm_v7i2003, p. 128.*

[93] *Ali, N. (2023, Eylül 30). Yapay zekayı günlük hayatımızda nasıl kullanıyoruz?. Indipendent Türkçe. https://www.indyturk.com/node/664146/bi%CC%87li%CC%87m/yapay-zekay%C4%B1-g%C3%BCnl%C3%BCk-hayat%C4%B1m%C4%B1zda-nas%C4%B1l-kullan%C4%B1yoruz*

platforms like Google and Facebook use algorithms to deliver targeted ads based on user preferences. Moreover, AI-powered chatbots have become essential in customer service, handling queries and providing support with increasing efficiency. Also, tools like Google Translate use AI to provide instant real time language translation, and this things helps breaking down communication barriers across the globe. AI's integration into these everyday technologies continues to transform and enhance user experiences across various sectors.

According to Forbes, many people start their day by unlocking their smartphones using biometrics like Face ID, which relies on artificial intelligence. Apple's FaceID uses AI to project 30,000 infrared dots on a user's face, creating a 3D map. The system then uses machine learning algorithms to compare this scan with stored facial data to ensure the identity of the user. Apple claims that the probability of tricking FaceID is one in a million, showcasing the precision and security of AI in everyday technology.[94]

To better understand the situation about the AI in our daily lives; we will mention about a survey that has been made in the United States:

A research center survey shows that while many Americans are aware of common AI applications like customer service chatbots and product recommendations, only 30% can accurately identify all six uses of AI. The survey, conducted in December 2022 with 11,004 adults, highlights a gap in public understanding of AI's role in daily life. While 27% interact with AI multiple times a day, 44% believe they do not. Public sentiment toward AI remains mixed, with 38% more concerned than excited about its increasing use. Also frequent internet users in the U.S. are more aware of artificial intelligence than less frequent users. Again according to the survey; 38% of those who are online almost constantly answered all six AI awareness questions correctly, compared to 6% of infrequent users. Similarly, people who have heard more about AI tend to score higher on AI knowledge. AI is often encountered online through features like customer service chatbots and personalized product recommendations based on purchasing behavior.[95] So as we can understand from this research; AI is implemented into our lives without our knowledge and we are using this technology constantly. People who are using the internet know more about AI and they are more aware that we are constantly influenced by AI technology.

---

[94] Marr, B. (2019, December 16). The 10 best examples of how AI is already used in our everyday life. Forbes.
[95] Pew Research Center. (2023, February 15). Public awareness of artificial intelligence in everyday activities. https://www.pewresearch.org/science/2023/02/15/public-awareness-of-artificial-intelligence-in-everyday-activities/

So shortly it can be said that the influence of AI in our daily lives is a crystal clear fact and this influence keeps increasing every single day regardless if we are aware of that or not.

2.4 AI Impact on Economy and Employment

Artificial intelligence is having a profound effect on both the global economy and the job market. On one hand, AI enhances productivity, reduces operational costs and fosters innovation across industries, contributing to overall economic growth. It automates repetitive tasks, allowing businesses to improve efficiency and focus on complex problem solving issues. However on the other side AI-driven automation can lead to job displacement, particularly in sectors like manufacturing, retail and logistics where routine jobs are being replaced by machines. In the short term, industries that heavily rely on manual labor, such as transportation and customer service may experience higher levels of job loss. For example, self-driving vehicles could reduce the need for human drivers or AI-powered chatbots may replace customer service agents. This leads to increased concern about unemployment, especially among low-skilled workers who are most vulnerable to automation. Many jobs that once relied on human workers are now being performed faster and more efficiently by AI technologies.

It can be seen as artificial intelligence technologies are harmful for employment and it has only negative effects on job fields however; AI is also creating new job opportunities, particularly in fields like data science, AI development in general and robotics. As industries adopt AI fastly, there is a growing demand for skilled professionals who can develop, maintain and operate AI systems in a healthy way since it is new technology and it is not an easy thing to find skilled engineers in this subject. This opens up new possibilities for employment particularly for those with technical expertise, and leads the way to a new kind of a race field where experts are competing in a way and shows their. So, AI-driven businesses and innovations are contributing to the creation of entirely new markets and services which can generate jobs and economic opportunities that did not exist ever before.[96]

The challenge lies in the need for reskilling and upskilling the workforce. Governments and organizations must invest in education and training programs that equip workers with the necessary skills to thrive in an AI-driven economy. For those displaced by automation,

[96] *Agrawal, A., Gans, J. S., & Goldfarb, A. (2019). Artificial Intelligence: The Ambiguous Labor Market Impact of Automating Prediction. The Journal of Economic Perspectives, 33(2), 31–50. https://www.jstor.org/stable/26621238, pp. 34–43.*

learning new skills and transitioning to AI-supported industries will be crucial for maintaining employment and ensuring economic stability. If we examine it in the long term, the successful integration of AI into the economy depends on finding a balance between leveraging AI for growth and addressing the social challenges it presents. Policymakers will need to implement strategies that support both economic innovation and workers affected by technological change. Social safety nets[97], workforce development programs, and ongoing education will play essential roles in mitigating the negative impacts of AI on unemployment while maximizing its benefits for economic progress. AI enhances decision-making by reducing uncertainty, allowing businesses to automate processes like recruitment, demand forecasting[98] and even brain surgery. This has ambiguous effects on labor, as AI both replaces jobs in prediction tasks while creating new opportunities in decision-based roles. Furthermore, AI is viewed as a general-purpose technology, meaning it impacts a wide range of industries, from healthcare to legal services.[99]

2.5 Ethical Concerns and Social Impact

Artificial intelligence (AI) raises numerous ethical concerns and has a significant social impact as it continues to evolve. One of the primary concerns is bias in AI systems, where algorithms may unintentionally discriminate based on race, gender, or socioeconomic status due to biased data. Additionally, the loss of privacy is another critical issue, as AI can collect and analyze vast amounts of personal data, often without explicit user consent. This leads to concerns about how this data is used and who controls it.

As it has mentioned above before, another ethical concern revolves around job displacement; as automation powered by AI can lead to widespread unemployment, particularly in sectors that rely on manual or repetitive labor. This shift in the labor market exacerbates social inequalities, as low-skilled workers are more vulnerable to job loss while those with advanced technical skills benefit the most from AI's development. The economic divide may be going to widen unless governments and organizations address these challenges through education and reskilling programs. Also the autonomy and accountability of AI systems raise

---

[97] The social safety net consists of non-contributory benefits provided to improve the lives of vulnerable families and individuals experiencing poverty and deprivation.
[98] the prediction of the quantity of goods and services that will be demanded by consumers at a future point in time
[99] Agrawal, A., Gans, J. S., & Goldfarb, A. (2019). Artificial Intelligence: The Ambiguous Labor Market Impact of Automating Prediction. The Journal of Economic Perspectives, 33(2), 31–50. https://www.jstor.org/stable/26621238, pp. 34–43.

ethical questions. When AI systems make decisions whether in healthcare, finance, or autonomous vehicles sectors we have to ask the question: who is responsible when things go wrong? Establishing legal frameworks and accountability structures for AI systems is essential to ensure they operate safely and fairly. Again the development of autonomous weapons and surveillance technologies has sparked debates about the potential misuse of AI, with concerns about how AI might be weaponized or used to infringe on human rights. These issues underscore the need for strong regulatory policies and international cooperation to ensure AI is developed and deployed ethically, with respect for human rights and societal well-being.[100]

In summary it can be said that while AI has transformative potential, it also presents significant ethical challenges that require careful consideration. Addressing these concerns through thoughtful policies and regulations will be crucial in ensuring that AI benefits society as a whole while minimizing the risks it poses to privacy, equality and security in general.

2.6 AI as a Milestone & Comparing AI and the Internet

Artificial intelligence is widely recognized as a technological milestone, much like the internet was during its emergence. Both AI and the internet have revolutionized industries, communication and how people interact with the world. However, AI represents a deeper transformation in how tasks are performed. While the internet connects people and information globally, AI enables machines to make decisions, learn, and automate processes in ways that significantly alter business models, healthcare and everyday tasks. The internet allowed global access to knowledge, commerce and communication, transforming economies and societies. AI, however, goes a step further by automating cognitive tasks, not just connecting people but also acting on their behalf in areas like data analysis, decision-making and problem-solving. For example, AI can predict consumer behavior, drive autonomous vehicles, and improve medical diagnoses.

AI, much like the internet, represents a general-purpose technology, meaning its applications span across multiple industries and sectors. Yet its potential impact is even more profound because it directly influences how decisions are made, how tasks are automated and how insights are generated from vast amounts of data. Actually while the internet is mostly about access to information, AI is about the ability to process, learn and act on that information

[100] *UNESCO. (2023). Recommendation on the ethics of artificial intelligence: Cases. https://www.unesco.org/en/artificial-intelligence/recommendation-ethics/cases*

autonomously. So AI and the internet share a common trajectory in transforming workforces, economies and social structures. As the internet shifted jobs toward more digital, knowledge-based roles, AI is balanced to automate many of those very tasks, pushing the boundaries of innovation while creating new challenges, especially regarding employment and ethics as it has been mentioned.

In short; while both technologies have reshaped the world, AI's ability to simulate human intelligence and decision-making suggests an even more transformative future, fundamentally altering how societies function and interact with technology. So it can be said that AI can be considered as a big milestone as much as the internet was in those times but it is not logical to say that artificial intelligence is going to replace the internet nor will it decrease its importance. (Russell & Norvig, 2020)

2.7 The Future of AI

The future of artificial intelligence (AI) holds incredible potential, as it continues to evolve and integrate into all aspects of life. AI is expected to become even more autonomous with the ability to make more complex decisions in areas such as healthcare, finance and autonomous driving; which are the areas where artificial intelligence is peaking in recent years. In the coming years, AI will likely revolutionize industries by enabling smarter automation, reducing human error and increasing efficiency. However, the future of AI also brings challenges including ethical concerns, privacy issues and job displacement due to automation.

As AI technologies develop, their capabilities will grow exponentially. Superintelligent AI which means the systems surpassing human cognitive abilities may become a reality which are offering advancements that have been never experienced before in fields like medicine and scientific research. However, ensuring ethical AI development will be critical. Safeguards must be implemented to prevent biases, ensure transparency and regulate AI's use in sensitive areas such as surveillance and warfare. Also, there is an increasing focus on AI-human collaboration. Rather than replacing human jobs entirely, AI is expected to extend human work, particularly in areas requiring creativity[101], empathy and complex decision-making. As AI becomes more integrated into everyday life, societies will need to adapt to the changes it brings, addressing potential social and economic impacts through

[101] *Marrone, R., Cropley, D., & Medeiros, K. (2024). How does narrow AI impact human creativity? Creativity Research Journal. https://doi.org/10.1080/10400419.2024.2378264, p. 8.*

education and policy-making. Ultimately, the future of AI is one of both immense opportunity and responsibility.

The future of AI, as outlined by Clocksin, suggests that AI's potential lies in advancing beyond conventional models of problem-solving and symbolic reasoning. He argues that true intelligence in AI will depend on social and emotional interactions, rather than purely logical calculations. This implies a shift towards AI systems that can understand context, engage in [102]meaningful conversations, and demonstrate empathy. As AI technology evolves, the focus will likely move towards systems that can adapt to complex social environments, emphasizing human-like traits such as emotion and social context. Clocksin stated this subject in his writings in 2003. The important thing is that as it can be seen; the expectations from AI are still the same but the AI technology still has not reached its full potential yet. Since all the experts on the area are aware of the insane potential of AI, the developments are likely to continue with a high pace in the future as it was in the recent years.

Today, AI is integrated into numerous fields such as healthcare, finance, transportation, and manufacturing. Autonomous vehicles, smart assistants like Siri and Alexa and AI-driven medical diagnostics are just a few examples of its applications as we have mentioned in our text several times. The future of AI is expected to further explore the development of General AI, although many challenges, particularly ethical ones, still remain. Issues like AI bias, the displacement of human labor due to automation, and concerns about privacy and surveillance have sparked global debates about how to regulate and manage the growth of AI responsibly. Although it is commonly thought that artificial intelligence technology is a recent issue; this technology is as old as the invention of computers. The reason it has gained its importance recently is that now it is a technology that we face nearly everyday and it has become more reachable due to programs like ChatGPT or Siri.

In this chapter, we explored the profound global impact of artificial intelligence (AI), tracing its role across various industries and its comparison to transformative technologies like the internet. AI has reshaped industries such as healthcare, finance, and entertainment by enhancing decision-making and automating complex processes. Moreover, its integration into daily life emphasizes its importance as a pivotal technological milestone.

[102] *Clocksin, W. F. (2003). Artificial Intelligence and the Future. Philosophical Transactions: Mathematical, Physical and Engineering Sciences, 361(1809), 1721–1748. http://www.jstor.org/stable/3559219, p. 11.*

As we've seen, AI's influence is undeniable, and its presence in policy-making processes is inevitable. Just as the internet redefined the modern world, AI now leads a similar revolution. With a deeper understanding of AI's scope, the next chapter will examine the specific policies and regulations governments and institutions have implemented to address the challenges and opportunities posed by AI.

CHAPTER III

EU'S RESPONSE TO TECHNOLOGICAL DEVELOPMENTS

This chapter will explore the European Union's (EU) actions in response to the rapid advancements in technology, with a focus on artificial intelligence (AI). As technological innovation accelerates, the EU has taken proactive steps to address the challenges and opportunities posed by these developments. Key questions will be addressed, such as why the EU feels the need to act on AI and whether these actions are necessary for ensuring ethical and responsible use of technology. We will examine the EU's regulatory approaches, strategic frameworks, and initiatives designed to foster innovation while protecting individual rights and maintaining security. By understanding the motivations and implications behind the EU's policies, we can gain a clearer picture of the critical role that AI plays in shaping modern governance and society.

3.1 Artificial Intelligence Act (AI Act)

It can be clearly said that the Artificial Intelligence Act is one of the most comprehensive regulatory frameworks ever proposed for technological development. Yet it is the first regulation that has been made for Artificial Intelligence and it was adopted on March 13, 2024. It is designed to ensure that AI technologies developed and used within the EU are safe, transparent and aligned with ethical principles. By categorizing AI applications by risk and enforcing clear rules for high-risk technologies, the Act represents a major effort by the EU to lead the world in establishing responsible AI governance. Now, we will explore this crucial development and its potential global impact. As we delve into the Artificial

Intelligence Act, it becomes clear that this regulation marks a pivotal moment in the development of AI technology. The EU is taking bold steps to address the ethical challenges and risks posed by AI, especially in high-stakes sectors like healthcare, law enforcement and critical infrastructure. The Act represents the EU's commitment to ensuring that AI is not only innovative but also aligned with fundamental rights and safety standards, and it is also setting a global example for responsible AI governance to the whole world.[103]

The Artificial Intelligence Act is a proposed regulation by the European Union aimed at establishing a comprehensive legal framework for the development and use of AI technologies across member states. Its main goal is to ensure that AI is developed and deployed in a way that is safe, ethical, and respects fundamental human rights.

Key Elements of the AI Act:

1. Risk-Based Approach: The regulation classifies AI systems based on the risks they pose to safety, privacy, and fundamental rights. It divides AI applications into four categories:
    - Unacceptable Risk: Systems deemed harmful or dangerous, such as AI used for social scoring[104] by governments, which are prohibited.
    - High Risk: These include AI used in critical infrastructure, healthcare and law enforcement, requiring tough regulations and oversight.
    - Limited Risk: AI systems with minimal risk are subject to transparency requirements where users should be aware they are interacting with AI (e.g., chatbots).
    - Minimal or No Risk: This includes applications like AI in video games which are largely unregulated.
2. Regulation of High-Risk AI Systems: High-risk AI systems must bear assessments before their deployment, ensuring they meet high standards of accuracy, reliability and transparency. Systems used in sensitive areas like healthcare or judicial decisions must be designed and operated with strict oversight to avoid bias or misuse.
3. Transparency and Accountability: The AI Act requires that users are informed when they are interacting with an AI system and companies developing AI must maintain

[103] *Kosinski, M., & Scapicchio, M. (2024). EU AI Act. IBM. https://www.ibm.com/topics/eu-ai-act*
[104] *Such AI systems evaluate or classify the trustworthiness of natural persons based on multiple data points and time occurrences related to their social behavior in multiple contexts or known or predicted personal or personality characteristics.*

thorough documentation and records of how the system was built and tested. This ensures that AI systems can be audited and that accountability is clear when issues arise.

4. Governance and Compliance: The Act proposes the creation of national supervisory bodies to oversee AI deployments, ensuring that AI systems comply with the standards set by the regulation. The EU also plans to set up a centralized European Artificial Intelligence Board to coordinate the enforcement of the rules across member states.
5. Ethics and Human Rights: A core aspect of the AI Act is its emphasis on protecting fundamental rights. AI systems used for biometric identification, facial recognition and decision-making must align with human rights laws, avoiding bias, discrimination, or surveillance that infringes on privacy.[105]

There are some certain purposes of this act because of critical necessities. The AI Act is a response to the growing use of AI in both public and private sectors where the potential benefits must be balanced against the risks of misuse. By regulating high-risk applications and encouraging transparency, the Act aims to prevent unethical AI practices while fostering innovation. The EU's approach is meant to promote trust in AI technologies and ensure that they serve society in a responsible and inclusive way.[106]

This regulatory framework is one of the first of its kind globally and highlights the EU's commitment to leading the charge in ethical AI development. By establishing a clear set of rules, the EU aims to set global standards for AI, promoting both innovation and protection in the digital age. (European Parliament and Council, 2024)

Now that we have explored the Artificial Intelligence Act and its overall structure, we will delve into some of its most critical components. In the following section, we will examine specific articles that address key aspects such as the scope of the Act, prohibited AI practices, data governance and the conformity assessment required for high-risk AI systems. These articles will highlight the comprehensive nature of the Act and its role in shaping the responsible use and regulation of AI across the European Union. Here let us now look at these essential provisions in more detail.

---

[105] *Future of Life Institute. (2024, May 30). High-level summary of the AI Act. https://artificialintelligenceact.eu/high-level-summary/*
[106] *Kosinski, M., & Scapicchio, M. (2024). EU AI Act. IBM. https://www.ibm.com/topics/eu-ai-act*

- **Article 2: Scope** – This article outlines the AI Act's applicability to all AI systems used within the EU, regardless of whether they are developed within or outside the EU. It specifies that the Act applies to providers, users and any actors involved in placing AI systems on the market. This article is crucial because it ensures the Act applies to all AI systems operating within the EU, even if it has been developed abroad. It guarantees that all actors, from developers to users, are held accountable for compliance and they are making the regulation globally significant.
- **Article 5: Prohibited AI Practices** – This article lists AI applications that are banned within the EU, such as systems that manipulate behavior in ways that could harm people or exploit vulnerable groups (e.g., minors) or those used for social scoring. This is important as it bans harmful AI practices, such as systems that exploit vulnerable populations or use biometric data for surveillance. It sets clear boundaries on unethical AI usage, protecting citizens' rights and privacy.
- **Article 10: Data Governance for High-Risk AI** – This focuses on the quality of data sets used in high-risk AI systems, ensuring they are accurate, representative, and free from bias. It mandates specific data documentation and accountability procedures. Data quality is key to AI's fairness and reliability. This article mandates that data used in high-risk AI systems must be accurate and unbiased, ensuring that AI decisions are based on trustworthy and representative data and this is reducing discrimination risks.
- **Article 15: Human Oversight** – AI systems, especially those classified as high-risk, must have human supervision to ensure that critical decisions are monitored, and corrective actions can be taken if necessary. Human oversight is crucial to prevent harmful automated decisions. This article emphasizes the need for human control over AI systems, particularly in high-risk applications like healthcare or law enforcement, safeguarding accountability and intervention when necessary.
- **Article 20: Conformity Assessment** – This article mandates that high-risk AI systems attract thorough testing and assessment to ensure they comply with all regulatory requirements before being deployed in the EU market. This ensures that high-risk AI systems attract strict evaluation before deployment. By making sure these systems are safe, transparent, and compliant with the law, it helps maintain public trust in AI technologies.[107]

[107] *European Parliament and Council. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 on harmonised rules on artificial intelligence and amending certain Union legislative acts. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2024/1689/oj*

3.2 General Data Protection Regulation (GDPR)

Now that we have covered the Artificial Intelligence Act, we move on to one of the most significant regulations concerning data protection in the EU; the General Data Protection Regulation (GDPR).[108] This important regulation, which came into effect in 2018, is designed to protect personal data and ensure privacy for individuals and institutions within the European Union. In this section, we will explore the key principles of GDPR, its importance in safeguarding personal information in this digital age we are living in right now and its global impact on businesses and technology companies across the world. Let's now dive into the details of this critical regulation.[109]

The General Data Protection Regulation (GDPR) is one of the most significant data protection regulations in the world, enacted by the European Union in 2018. It was designed to safeguard individuals' personal data and give them more control over how their information is collected, used and stored by companies and organizations. GDPR applies not only to businesses within the EU but also to any company processing the data of EU citizens, regardless of where the company is based. This makes it one of the most far-reaching regulations concerning data privacy. Again like any other regulations. General Data Protection Regulation has also its own key principles;

1. Lawfulness, Fairness, and Transparency: Personal data must be processed legally, transparently and fairly. Companies must clearly inform users about why and how their data will be processed and collected.
2. Purpose Limitation: Data can only be collected for specified, explicit and legitimate purposes. It cannot be further processed in ways that are incompatible with the original reason for collection.
3. Data Minimization: Organizations should collect only the data that is necessary for the intended purpose. This principle prevents unnecessary or excessive data collection, reducing the risk of misuse.
4. Accuracy: Data must be accurate and kept up to date. If data is incorrect or outdated it must be corrected or deleted.

---

[108] *European Parliament and Council. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union.*

[109] *Council of the European Union. (n.d.). Data protection regulation (GDPR). https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/*

5. Storage Limitation: Personal data should only be stored for as long as necessary. After this period, the data should be erased or anonymized unless legally required to be kept longer.
6. Integrity and Confidentiality: Data must be processed in a way that ensures its security, protecting it from unauthorized access, breaches, or accidental loss. Organizations must take appropriate technical and organizational measures to secure data.
7. Accountability: Data controllers and processors are responsible for complying with GDPR standards and must be able to demonstrate compliance through proper documentation and internal policies.[110]

Also GDPR gives individuals extensive rights over their personal data. Some of the important ones are including:

- Right to Access: Individuals can request access to the personal data an organization holds about them, including information on how it is processed and for what purposes.
- Right to Rectification: Individuals have the right to request the correction of inaccurate data.
- Right to Erasure ("Right to be Forgotten"): Under certain circumstances, individuals can request that their personal data be deleted, especially if the data is no longer needed for its original purpose.
- Right to Data Portability: Individuals can request their data be transferred to another service provider in a commonly used format.
- Right to Object: Individuals can object to their data being used for certain purposes, such as direct marketing or profiling.[111]

GDPR has had a profound impact on how businesses and also specific institutions operate, particularly those that rely heavily on personal data for marketing, analytics or service personalization. Non-compliance can result in significant fines, reaching up to 20 million euros or 4% of a company's global annual turnover, whichever is higher.[112] This has prompted

[110] *Council of the European Union. (n.d.). Data protection regulation (GDPR). https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/*
[111] *European Data Protection Supervisor. (n.d.). Rights of the individual under the GDPR. https://www.edps.europa.eu/data-protection/our-work/subjects/rights-individual_en*
[112] *IT Governance. (2023). DPA and GDPR penalties. https://www.itgovernance.co.uk/dpa-and-gdpr-penalties*

organizations to revise their data collection practices, ensure user consent for data processing and adopt more strict security measures.[113]

GDPR has also influenced data protection laws beyond the EU, with many countries introducing similar regulations to protect individuals' data. As a result, GDPR is seen as setting a global standard for data privacy and security in the digital age. It is just another example of how the European Union is playing a pioneer role in such regulations and influencing other organizations and other states. Especially when it comes to laws and regulations regarding technological developments; the EU has always become the first one who thinks about the individuals in the first place and prioritizes them.

In conclusion, the GDPR is a critical development in the digital era, where the collection and use of personal data have become central to business operations. It ensures that individuals have greater control over their personal information, holds organizations accountable for how they handle data and sets a strong foundation for privacy protection worldwide.[114]

3.3 Digital Services Act (DSA)

The Digital Services Act (DSA) represents a major regulatory revision by the European Union to address the growing influence and responsibilities of online platforms in today's digital world. It is designed to protect users from illegal content, misinformation and harmful practices while promoting transparency and accountability among digital services. The DSA primarily targets online platforms such as social media sites, search engines and marketplaces; with very strict obligations for larger platforms that have significant market influence.

One of the DSA's central goals is to create a safer digital environment by imposing stricter rules on content moderation. It requires online platforms to take proactive measures in identifying, removing, and preventing the spread of illegal content, including hate speech, child exploitation, counterfeit goods and so on. By enforcing these standards, the EU aims to

---

[113] *Hoofnagle, C. J., van der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: What it is and what it means. Information & Communications Technology Law, 28(1), 65–98. https://doi.org/10.1080/13600834.2019.1573501, pp. 9–10.*

[114] *European Parliament, & Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L119, 1–88.*

make the internet a safer place, ensuring that users are not exposed to harmful material while maintaining freedom of expression. Platforms are now obligated to report on how they moderate content, which brings greater transparency to their algorithms and decision-making processes.

Moreover, the DSA introduces specific rules for very large online platforms (VLOPs)[115] which are actually the platforms with a significant number of users, like Facebook, Google and Amazon.[116] These companies must assess and mitigate potential risks related to their services, such as the spread of disinformation or the manipulation of user data for political or commercial purposes. They must also open their algorithms to critical examination, allowing regulatory bodies and third-party auditors[117] to examine how content is prioritized and delivered to users. This is crucial in addressing concerns about algorithmic biases and how these platforms influence public discourse.

The DSA also addresses targeted advertising which is requiring platforms to provide users with clearer information on how their data is being used for ads. Users must be given the choice to opt-out of targeted advertising[118] if they wish. This move towards greater transparency is expected to shift the power balance between platforms and users. It is also allowing individuals to have more control over their personal data and how it's utilized in the digital ecosystem. This way of using is now very widespread and most of the big companies like Apple or Samsung are forced to integrate this technology in their personal mobile phones.[119] It can be considered as one of the biggest achievements of DSA to spread these critical applications to the global market and big technology companies. It is also a very important example of how the European Union has influenced the global arena in the issue of policy making on technological developments.

Another critical point of the DSA is its emphasis on cross-border cooperation. Since many digital platforms operate across multiple countries, the regulation enhances coordination between national authorities in EU member states to ensure uniform enforcement. The

---

[115] The DSA classifies platforms or search engines that have more than 45 million users per month in the EU as very large online platforms (VLOPs) or very large online search engines (VLOSEs).
[116] European Commission. (n.d.). Digital Services Act (DSA) and very large online platforms (VLOPs). https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops
[117] independent evaluations conducted by external organizations or certification bodies
[118] A form of advertising, including online advertising, that is directed towards an audience with certain traits, based on the product or person the advertiser is promoting
[119] *Hollister, S. (2021, September 2). Apple will prompt you to enable personalized ads in iOS 15 even if you previously opted out. The Verge. https://www.theverge.com/2021/9/2/22654121/apple-personalized-ads-ios-15-prompt-app-tracking*

European Commission will have oversight authority, particularly for the largest platforms, ensuring that the rules are applied consistently across the EU.

In its essence; the DSA aims to modernize the digital regulatory landscape to reflect the realities of the current internet ecosystem. By imposing responsibilities on online platforms and creating safeguards for users, the Act sets a global example for regulating the digital space. It strikes a balance between fostering innovation and competition while ensuring user safety and protecting fundamental rights, such as freedom of speech and data privacy. As digital platforms continue to play a central role in shaping communication and commerce, the DSA ensures that they operate under rules that benefit society as a whole.[120]

This Act also reflects the EU's ambition to lead globally in digital regulation, establishing standards that are likely to influence policy in other regions as countries seek to regulate the growing power and influence of large tech companies.

In short; The Digital Services Act (DSA) positions the European Union as a global leader in digital regulation, setting standards that will likely influence policy frameworks around the world. By addressing issues like content moderation, data privacy and platform accountability, the DSA is not only shaping the future of the digital landscape within the EU but also establishing a model for regulating large online platforms globally. Its focus on transparency, safety and user rights makes it a pioneering step toward global digital governance.

3.4 Digital Markets Act (DMA)

The Digital Markets Act (DMA) is a significant regulation introduced by the European Union to ensure fair competition in the digital economy, particularly targeting large tech companies that serve as "gatekeepers" in online markets. The primary objective of the DMA is to prevent these dominant platforms, such as Google, Amazon, and Facebook, from engaging in practices that could harm competitors or limit consumer choice.

Gatekeepers, under the DMA, are defined as companies that hold a dominant position in multiple key digital markets, controlling access to large user bases and services essential to the functioning of the online economy. The DMA places stringent rules on these companies

[120] *European Commission. (n.d.). Digital Services Act package. https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package*

to ensure they do not abuse their market power. Some of the important key prohibitions can be listed like that:

- Self-preferencing: Gatekeepers are banned from favoring their own services or products over those of competitors, ensuring smaller businesses can compete in an equal way.
- Data hoarding: The DMA prohibits gatekeepers from restricting access to data or forcing business users to provide their data without sufficient justification. It ensures that other companies can access necessary data for innovation.
- Interoperability: The Act requires gatekeepers to ensure interoperability with other services, meaning that smaller businesses can interact with gatekeeper platforms more easily, avoiding lock-in effects[121]. (European Commission, n.d.)

The DMA also includes a series of obligations, such as allowing users to uninstall pre-installed apps on smartphones and preventing companies from combining data from different services without user consent. It seeks to give users more control over their data and experience on digital platforms.

One of the most impactful aspects of the DMA is its enforcement. The European Commission has been given broad powers to investigate and enforce this Act, including conducting market investigations and imposing severe penalties for non-compliance. Companies that break the rules could face fines of up to 10% of their global turnover, with repeat offenders potentially facing even more stringent penalties, including the possibility of breaking up parts of the company.[122]

The Digital Markets Act represents a significant shift in how the EU approaches regulating large tech companies. It reflects the EU's determination to create a fairer and more open digital market where innovation is encouraged and market dominance is not abused. By ensuring that dominant platforms do not suppress competition, the DMA aims to protect consumers, foster innovation and create a more competitive digital economy across the EU.[123]

---

[121] *A Lock-in effect exists when a customer is so strongly tied to a company that switching is only possible with considerable effort and expense.*

[122] *Sánchez Nicolás, E. (2020). Online giants could face 10% fines under new EU law. EUobserver. https://euobserver.com/science/150396*

[123] *European Commission. (n.d.). Digital Markets Act (DMA). https://digital-markets-act.ec.europa.eu/index_en*

Like the Digital Services Act (DSA), the DMA positions the European Union as a global leader in digital regulation. The DMA is expected to set international standards for competition in the digital age, influencing regulatory approaches not only in Europe but around the world. This move by the EU signals a stronger stance against monopolistic practices and represents a broader strategy to regulate digital markets and ensure that power is not concentrated in the hands of a few dominant players.[124]

3.5 Cybersecurity Act

Now, as we move on to the Cybersecurity Act as our last act we will analyze, we'll explore its significance as a key regulation introduced by the European Union to address the growing risks and challenges of cybersecurity. The EU Cybersecurity Act is aimed at strengthening Europe's digital resilience by creating a unified framework for the cybersecurity of digital products, services and processes. It establishes the EU-wide cybersecurity certification framework which helps improve the security standards of digital infrastructure across member states. This Act is a crucial step towards ensuring a secure and robust digital ecosystem in the EU.

The EU Cybersecurity Act, which was enacted in 2019, is a major regulation aimed at improving Europe's digital resilience by establishing a unified approach to cybersecurity. One of its key provisions is the creation of the EU Cybersecurity Certification Framework, which sets standardized security certifications for digital products, services and infrastructure. This ensures a consistent level of protection across member states and enhances trust in the digital economy.[125]

The Act also strengthens the role of ENISA (the European Union Agency for Cybersecurity), giving it a permanent mandate and more resources to support member states in addressing cybersecurity threats. ENISA now plays a central role in coordinating EU-wide cybersecurity efforts, providing expertise and helping governments and industries prepare for and respond to cyber incidents.[126] Its role includes not only prevention but also developing strategies for more strong incident reporting and maintenance.

---

[124] VanMeter, R., Toffaletti, S., LePape, A., Bertola, V., & Miseviciute, J. (2022, March 14). Open letter regarding the EU Digital Markets Act (DMA). Coalition for App Fairness, European Digital SME Alliance, Coalition for Competitive Digital Markets, pp. 2–3.
[125] European Commission. (2023). Cybersecurity Act. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act
[126] European Union Agency for Cybersecurity. (n.d.). ENISA. https://www.enisa.europa.eu/

The certification framework under the Cybersecurity Act helps create clear security benchmarks for industries such as cloud services, IoT devices and critical infrastructure like energy grids and transportation networks. By offering certifications for various levels of risk, the framework helps ensure that even high-risk technologies meet strong security standards before being deployed within the EU. This framework is also meant to facilitate cross-border cybersecurity measures and reduce fragmentation among member states, creating a more cohesive defense against cyberattacks. The Cybersecurity Act addresses the need for international cooperation in tackling cyber threats. It recognizes that cybersecurity is a global challenge and that coordinated efforts are necessary to combat the rising frequency and sophistication of attacks. The Act encourages partnerships between the EU and other global players to ensure that cybersecurity strategies are aligned and that best practices are shared across borders.[127]

The Act's forward-looking approach is particularly important in the context of the EU's digital transformation, as new technologies like artificial intelligence, 5G and the Internet of Things (IoT) require secure infrastructure. The Act lays the groundwork for securing these technologies, ensuring that innovation can continue without compromising user safety or privacy.[128]

In short, the Cybersecurity Act is a crucial part of the EU's strategy to enhance the security of its digital landscape. By establishing clear certification standards, empowering ENISA and fostering international cooperation, the Act provides the tools necessary to protect the EU's critical infrastructure, digital services and citizens from the increasing threat of cyberattacks. It is a proactive response to the growing risks in the digital era and ensures that the EU remains a global leader in cybersecurity.

In this chapter, we have explored the key regulations that the European Union (EU) has introduced in response to the rapid technological advancements of the 21st century. From the General Data Protection Regulation (GDPR), which set a global standard for data privacy, to the Artificial Intelligence Act, which aims to ensure that AI technologies are developed responsibly, the EU has taken proactive measures to address the risks and challenges of emerging technologies. The Digital Services Act (DSA) focuses on creating a safer digital

[127] *European Commission. (2024). Cybersecurity policies. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies*
[128] *European Commission. (2023). Cybersecurity Act. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act*

space by regulating online platforms and content, while the Digital Markets Act (DMA) ensures fair competition by limiting the power of dominant tech companies. Finally, the Cybersecurity Act strengthens Europe's digital defenses through a unified framework for securing digital infrastructure.

The EU's motivation for implementing these regulations is rooted in the need to protect citizens, maintain ethical standards and promote fairness in an increasingly digital world. These regulations ensure that technological advancements do not compromise user safety, privacy or competition. The internet, AI and other technologies are transforming economies and societies, but with that transformation comes a host of ethical and security concerns that must be addressed. Without these regulatory frameworks there would be a greater risk of exploitation, monopolization and vulnerability to cyber threats.

As we analyzed throughout this chapter, the EU's actions were not only necessary but essential for shaping a safe, transparent and fair digital environment. The regulations act as safeguards, ensuring that technology serves the public good and remains aligned with democratic values. As technological progress continues, the EU's proactive stance on regulation demonstrates its commitment to leading the way in responsible governance of the digital era.

CHAPTER IV

EU'S ROLE AND INFLUENCE IN AI REGULATION

In the previous chapter, we explored the key regulatory frameworks the European Union has implemented in response to the technological advancements of the 21st century, such as the GDPR, AI Act, DSA, DMA, and the Cybersecurity Act. Now, we arrive at the final and a crucial chapter which will define the EU's role as a global leader in AI regulation. This chapter serves as the summit of our analysis, highlighting how the EU's approach influences not only Europe but also the global stage in shaping the future of AI. In this chapter also we will explore how the European Union has positioned itself as a global leader in shaping the rules and guidelines for the development and use of artificial intelligence. The EU's regulatory efforts, such as the Artificial Intelligence Act, demonstrate its commitment to setting ethical standards for AI that promote transparency, accountability and safety. This chapter will analyze the EU's role not only inside its member states but also on the global stage by comparing its approach to AI regulation with other countries and organizations.

This chapter will examine how the EU's comprehensive AI framework influences policies outside Europe, encouraging other regions to follow its lead in establishing ethical and legal safeguards. The EU's pioneering role in AI regulation not only impacts the technology industry but also addresses pressing issues such as bias in AI systems, privacy concerns, and the potential misuse of AI for harmful purposes.

As we delve deeper into this chapter, we will consider the broader global implications of the EU's actions, looking at how its policies influence innovation, trade and cross-border cooperation. Also, it will explore more again why the EU feels the need to take such a proactive stance in AI regulation, particularly in the context of maintaining human rights, ethical standards, and economic competitiveness in an increasingly digital and AI-driven world. In short; this chapter will compare other responses in the world regarding the issue and the EU's responses. And will try to answer such questions like; "Are the EU's actions about AI affecting other regions or institutions?" or "Is the EU playing a pioneer role in this issue?"

4.1 Global Responses to AI: International Organizations and Key National Initiatives

The United States has taken a somewhat decentralized approach to AI regulation, focusing on promoting innovation while ensuring safety. The National Institute of Standards and Technology (NIST) has developed guidelines to ensure that AI systems are reliable, transparent and secure.[129] Furthermore, the Algorithmic Accountability Act has been proposed to promote transparency in AI algorithms, requiring companies to conduct impact assessments of their AI systems, ensuring they do not discriminate or harm consumers. The U.S. strategy is largely driven by promoting economic competitiveness, technological innovation and protecting national security interests.[130]

China has emerged as a global leader in AI development through its New Generation AI Development Plan, announced in 2017, which outlines its ambition to become the world's leader in AI by 2030. China heavily invests in AI for sectors like surveillance, healthcare, and education, and it is known for integrating AI into its social credit system and public surveillance infrastructure. However, China's approach is closely aligned with state control, where the government regulates and directs AI development with a focus on both economic growth and political stability.[131] China's rapid advancements in AI have also sparked concerns about privacy, human rights, and security on a global scale.[132]

Canada has positioned itself as a leader in the ethical development of AI through its Pan-Canadian Artificial Intelligence Strategy, launched in 2017. The country focuses on fostering innovation, ethical AI research, and international cooperation. Canadian policymakers have made significant investments in AI research and education, with an emphasis on addressing the ethical challenges posed by AI, including bias, transparency, and accountability. Canada's AI strategy is notable for its emphasis on human rights and inclusivity, aiming to ensure that AI benefits all citizens.[133]

---

[129] *National Institute of Standards and Technology. (n.d.). Fundamental AI. https://www.nist.gov/fundamental-ai*
[130] *Szczepański, M. (2024). US approach to artificial intelligence [EPRS At a Glance Report]. European Parliamentary Research Service. https://www.europarl.europa.eu/thinktank, p. 1.*
[131] *Zhou, X., Cai, Z., Tan, K. H., Zhang, L., Du, J., & Song, M. (2021). Technological innovation and structural change for economic development in China as an emerging market. Technological Forecasting & Social Change, 167, 120671. https://doi.org/10.1016/j.techfore.2021.120671, p. 2.*
[132] *Khanal, S., Zhang, H., & Taeihagh, A. (2024). Development of New Generation of Artificial Intelligence in China: When Beijing's Global Ambitions Meet Local Realities. Journal of Contemporary China, 1–24. https://doi.org/10.1080/10670564.2024.2333492, pp. 4–5.*
[133] *Innovation, Science and Economic Development Canada. (2022). Canada's AI strategy. https://ised-isde.canada.ca/site/ai-strategy/en*

Japan has taken a more human-centered approach to AI with its Social Principles of Human-Centric AI. Japan's vision for AI is focused on harnessing technology to improve social well-being while ensuring ethical considerations such as fairness, safety, and privacy are prioritized.[134] Japan is heavily investing in AI for sectors such as healthcare, robotics and eldercare, because of its aging population. The country's policy highlights the integration of AI in society in a way that enhances human capabilities rather than replacing them.

The Organization for Economic Cooperation and Development (OECD) has developed the AI Principles, which have been adopted by over 40 countries, including the U.S., Canada and Japan. These principles are designed to ensure that AI is developed in a way that is trustworthy, respects human rights and promotes inclusive growth. The OECD's AI guidelines emphasize transparency, accountability and the responsible management of data. They encourage member countries to adopt AI frameworks that protect privacy, prevent discrimination and ensure the safety and fairness of AI systems.[135]

In 2021, **NATO** launched its Artificial Intelligence Strategy, focusing on the use of AI in defense and security applications. NATO's strategy aims to promote the responsible and ethical use of AI in military contexts, ensuring that AI systems comply with international law and NATO's core values. Key areas of focus include AI in cybersecurity, decision-making, and autonomous weapons systems. [136]NATO's efforts are centered around safeguarding security while maintaining ethical standards in the deployment of AI technologies.

The United Nations has also taken steps toward regulating AI, primarily through UNESCO's Recommendation on the Ethics of Artificial Intelligence. This framework provides guidelines for the ethical development and use of AI, emphasizing the importance of protecting human rights, ensuring privacy and promoting transparency.[137]The UN calls for global cooperation to ensure that AI does not promote inequality or violate fundamental freedoms. UNESCO's recommendations are designed to help countries adopt ethical AI practices that promote inclusive and sustainable development.

---

[134] *Cabinet Office, Government of Japan. (2019). Social principles of human-centric AI. https://www8.cao.go.jp/cstp/english/humancentricai.pdf, pp. 7–11.*
[135] *OECD. (2024). OECD AI principles. https://www.oecd.org/en/topics/ai-principles.html*
[136] *NATO. (2024). Summary of NATO's revised Artificial Intelligence (AI) strategy. https://www.nato.int/cps/en/natohq/official_texts_227237.htm*
[137] *UNESCO. (2024). Recommendation on the ethics of artificial intelligence. https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence, p. 26.*

Collectively, these global efforts reflect the growing recognition that AI is a transformative technology with important implications for society, economy and governance. As the race to develop AI is getting more important; countries and international organizations are working to balance innovation with regulation, ensuring that AI systems are transparent, ethical, and aligned with democratic values. The EU, with its Artificial Intelligence Act, is among the global leaders setting precedents for how AI should be regulated, influencing other countries and international bodies to follow itself.

In conclusion, various countries and international organizations have recognized the importance of AI and are shaping their policies to ensure that AI is deployed responsibly. From the United States' sectoral approach to China's state-driven AI plan, and from Canada's ethical AI strategy to NATO's defense-oriented focus, the global response to AI is diverse yet united by a common need to harness AI's potential while mitigating its risks. The EU's role in this global dialogue is crucial, as its comprehensive regulatory frameworks are likely to influence the direction of AI governance worldwide.

4.2 Comparative Analysis: The EU's Leadership in AI Regulation Versus Global Approaches

When comparing the EU's approach to AI regulation with other global players; several distinctions stand out. The EU has positioned itself as a global leader in AI regulation by establishing comprehensive frameworks, such as the Artificial Intelligence Act and GDPR, that are aiming to balance innovation with strong ethical and safety standards. In contrast to countries like the United States, which have taken a more sectoral, innovation-driven approach, the EU's regulations are much broader and emphasize privacy, transparency and fundamental rights. The regulatory approaches to AI differ significantly between the United States and Europe. In the U.S., regulators typically rely on existing frameworks and voluntary standards, aiming to foster innovation by providing flexibility to AI developers. This approach allows for market-driven innovation without stringent oversight. In contrast, European regulation adopts a more detailed and prescriptive model, as seen in the AI Act, which establishes specific rules and requirements for various AI applications to ensure ethical use, safety, and transparency. This difference underscores Europe's focus on strong regulatory

frameworks to address potential risks posed by AI technologies while maintaining user protections.[138]

So if we need to continue our comparative analysis, we should mention China first; since they can be considered as the second biggest policy makers when it comes to AI technology. While China focuses on leveraging AI for economic and political power, prioritizing rapid development with state control; the EU's approach is more careful, prioritizing the protection of citizens' rights. China's New Generation AI Development Plan emphasizes government control and surveillance, which contrasts with the EU's ethical principles of limiting the use of AI in areas such as mass surveillance. China regulates AI primarily to uphold national security and social stability, explicitly prohibiting AI outputs that "endanger national security" or "promote ethnic hatred or violence." These regulations are comprehensive, but their enforcement relies heavily on government discretion, making them less transparent compared to the EU's detailed risk-based model. (Benizri, Evers, Mercer, & Jessani, 2023) China's AI regulations place significant emphasis on algorithm transparency and accountability. Companies are required to register detailed information about their algorithms, ensuring regulatory oversight and clarity in how AI systems function. Unlike the EU's broad AI Act, which takes a comprehensive approach to regulating all AI applications, China's regulatory system is vertical and iterative, meaning it adjusts AI regulations for specific applications over time to address evolving challenges. This makes China's approach more application-specific, while the EU focuses on a wide-ranging regulatory framework.[139]

If we need to compare other countries with the EU; countries like Canada and Japan are also working on ethical AI frameworks, but they do not have the same extensive, legally binding regulations as the EU. The EU's approach is notable for being binding across all member states, creating a unified legal framework that fosters trust in AI technologies. The Digital Services Act and Digital Markets Act further complement the AI regulation by addressing competition and transparency issues in the digital market, ensuring that tech giants follow ethical guidelines.

---

[138] *Broadbent, M. (2021). What's Ahead for a Cooperative Regulatory Agenda on Artificial Intelligence? Center for Strategic and International Studies (CSIS). http://www.jstor.org/stable/resrep30085, pp. 2–4.*

[139] *Sheehan, M. (2023). The Underlying Structure of China's AI Regulations. In China's AI Regulations and How They Get Made (pp. 15–16). Carnegie Endowment for International Peace. http://www.jstor.org/stable/resrep52039.7*

France, Germany, and the UK each offer distinct approaches to AI regulation and development within Europe, reflecting the broader diversity of strategies across the continent. France focuses on creating a European data ecosystem that emphasizes ethical AI development and inclusivity. Its top-down, government-led approach prioritizes the retention of AI talent and investment in interdisciplinary research, positioning France as a leader in the European AI landscape. The French government's heavy focus on developing infrastructure and supporting innovation highlights its commitment to ethical AI. Germany, on the other hand, places a strong emphasis on technology transfer and establishing AI standards at both the national and international levels. However, Germany faces challenges in attracting top AI talent due to salary constraints within its academic institutions. Despite these challenges, Germany remains committed to playing a central role in shaping AI standards and policy frameworks within Europe. The UK's approach differs slightly, as it has focused on significant investments in AI and has established institutions such as the Centre for Data Ethics and Innovation. However, while the UK has made strides in AI governance, it lacks a definitive timeline for implementing its broader AI strategy. This creates uncertainty in how the UK will align its efforts with other European nations. These varying approaches illustrate the unique contributions of each country to Europe's overall AI development, while also highlighting the need for continued cooperation and alignment under broader EU frameworks like the AI Act.[140]

When it comes to the international bodies like NATO and the UN are taking important steps in AI regulation, focusing on defense and ethical use, but they lack the enforceable regulatory power that the EU holds over its members. The UNESCO AI ethics framework provides valuable guidelines, but it is not legally binding, unlike the EU's far-reaching laws.[141]

Since the year 2018, the European Union is taking important actions regarding artificial intelligence technology. Here is the list of important milestones;

---

[140] *Brattberg, E., Csernatoni, R., & Rugova, V. (2020). National European Efforts on AI. In Europe and AI: Leading, Lagging Behind, or Carving Its Own Way? (pp. 11–21). Carnegie Endowment for International Peace. http://www.jstor.org/stable/resrep25784.6, pp. 14–16.*

[141] *Benizri, I., Evers, A., Mercer, S. T., & Jessani, A. A. (2023, July 17). A comparative perspective on AI regulation. Lawfare. https://www.lawfaremedia.org/article/a-comparative-perspective-on-ai-regulation*

- March 2018: AI expert group and European AI Alliance formed, initiating wide engagement with stakeholders.
- April 2018: European Commission communication: "Artificial Intelligence for Europe"; declaration of cooperation on AI; press release on AI for Europe; staff working document on liability for emerging digital technologies.
- June 2018: Launch of the European AI Alliance and setup of the High-Level Expert Group on AI.
- December 2018: European Commission adopts the coordinated plan on AI; press release: AI made in Europe; stakeholder consultation on draft ethics guidelines for trustworthy AI.
- April 2019: High-Level Expert Group on AI publishes ethics guidelines for trustworthy AI.
- June 2019: First European AI Alliance Assembly; High-Level Expert Group provides policy and investment recommendations for AI.
- December 2019: High-Level Expert Group pilots an assessment list for trustworthy AI.
- February 2020: European Commission publishes white paper on AI, focusing on excellence and trust.
- July 2020: High-Level Expert Group on AI releases the final assessment list on trustworthy AI (ALTAI).
- October 2020: 2nd European AI Alliance Assembly.
- April 2021: European Commission proposal for harmonized rules on AI and updated coordinated plan on AI.
- June 2021: Public consultation on civil liability for AI and adapting liability rules to the digital age.
- November 2021: Council of the EU releases SI Presidency compromise text on the AI Act.
- December 2021: Committee of the Regions and European Central Bank issue opinions on the AI Act.
- June 2022: Launch of the first AI regulatory sandbox in Spain.
- September 2022: Proposal for an AI liability directive.
- December 2022: Council of the EU adopts a general approach on the AI Act.
- June 2023: European Parliament adopts its negotiating position on the AI Act.

- December 2023: Political agreement on the AI Act reached by co-legislators.
- January 2024: AI innovation package launched to support startups and SMEs.
- February 2024: European AI Office established.
- August 2024: AI Act enters into force.

As we can see; the Union has started to take important steps way before other institutions have done. That kind of an early approach can be considered as another evidence to their policy-driven role in the issue of artificial intelligence technologies. With their words; “The EU’s approach to artificial intelligence centers on excellence and trust, aiming to boost research and industrial capacity while ensuring safety and fundamental rights. The European AI Strategy aims at making the EU a world-class hub for AI and ensuring that AI is human-centric and trustworthy. Such an objective translates into the European approach to excellence and trust through concrete rules and actions.” (European Commission, 2024)

In summary; the EU’s emphasis on protecting human rights, accountability and transparency makes it a pioneer in global AI regulation. Its focus on ethical AI development, combined with strong enforcement mechanisms, distinguishes it from other approaches and makes the EU’s efforts a model that other countries and organizations are likely to follow as we already discussed. And it is more likely to be like that in the future developments in the policy making process.

CONCLUSION

The 21st century has been defined by rapid technological advancements that have profoundly impacted societies, economies and governance in the whole world. This paper has explored these developments, focusing on key technologies such as Artificial Intelligence (AI), Internet of Things (IoT), 5G networks or blockchain.; and how they have influenced policy-making processes. Throughout the research, we have examined the role of the European Union (EU) in responding to these changes and its pioneering efforts in establishing regulatory frameworks that set global standards.

Chapter 1 provided a detailed analysis of the most transformative technologies of our time. AI, with its unparalleled ability to process data and make autonomous decisions, has emerged as a central technological force, reshaping industries such as healthcare, finance and transportation. Other than that, IoT has connected billions of devices, revolutionizing resource management and creating new vulnerabilities in cybersecurity. 5G technology, offering a brilliant speed and reliability, has enabled advancements in telecommunications and autonomous systems; but also raised concerns regarding national security and infrastructure control. Blockchain, initially known for its role in cryptocurrencies, has expanded its applications to sectors like supply chain management and digital identity verification, and encountered unique regulatory challenges. These technologies are not only transforming industries but are also pushing governments and organizations to adapt their policies to address the associated risks and ethical dilemmas. This is a challenge that policymakers are dealing with right now.

In Chapter 2, the paper shifted its focus to the global significance of AI, positioning it as a transformative technology in parallel with the internet revolution. AI's impact has affected multiple sectors, from automating complex tasks to reshaping labor markets. However, its rise has also triggered ethical concerns, particularly regarding algorithmic bias, surveillance and privacy. The chapter emphasized the necessity of a global governance structure to ensure that AI development remains aligned with human rights and ethical standards. The comparison to the internet revolution highlighted how AI, much like the internet, is creating new business models and disrupting traditional industries.

Chapter 3 delved into the European Union's proactive approach to addressing these technological advancements, especially AI. The EU has positioned itself as a global leader in technological governance by implementing comprehensive regulatory frameworks such as the General Data Protection Regulation (GDPR), Artificial Intelligence Act (AI Act), Digital Services Act (DSA), Digital Markets Act (DMA), and the Cybersecurity Act. Each of these regulations addresses specific aspects of the digital economy, from ensuring data privacy and user safety to promoting fair competition and securing digital infrastructure. The EU's actions are motivated by the need to protect its citizens while fostering innovation, maintaining ethical standards, and safeguarding the democratic values of transparency and fairness. Through these frameworks, the EU not only addresses current technological challenges but also anticipates future developments, ensuring that Europe remains at the forefront of responsible governance.

Last but not least; chapter 4 highlighted the EU's role and influence in AI regulation on the global stage. As a pioneer in setting ethical standards for AI, the EU's regulatory efforts have become a benchmark for other regions. The AI Act, in particular, sets clear guidelines for the development and deployment of AI technologies, ensuring that they are safe, transparent, and aligned with human rights principles. This chapter also examined how the EU's policies have influenced other nations and organizations, and encouraged them to adopt similar approaches. The "Brussels Effect", a phenomenon in which EU regulations become de facto global standards, was particularly evident in the spread of the GDPR model to other jurisdictions. The EU's leadership in AI regulation has cemented its position as a key player in shaping the global digital landscape.

As this thesis has demonstrated; the European Union plays a crucial role in policy-making related to technological advancements, particularly in the regulation of AI and other emerging technologies. Its comprehensive regulatory frameworks are designed to ensure that technological progress does not compromise ethical standards, privacy or safety. The EU's proactive approach in addressing the challenges posed by these innovations positions it as a global leader in technological governance, and it is also setting an example for other nations and regions to follow it.

The 21st century's technological developments are reshaping the world at an unprecedented pace. These technologies are no longer optional; they have become integral to the functioning of societies and economies, demanding a shift in policy-making focus. The EU's foresight in

creating regulations that balance innovation with ethical concerns is evidence to its leadership in the global technological landscape. As these technologies continue to evolve, so too must the policies that govern them. The EU's continued influence and leadership will be essential in ensuring that the digital revolution benefits all while reducing its risks.

In conclusion, the European Union's role in shaping AI regulation and its broader approach to governing emerging technologies has set a global standard. As AI and other technologies continue to integrate into every aspect of daily life, the EU's regulatory frameworks will play a critical role in ensuring that these advancements are aligned with democratic values, human rights, and the broader public good.

Future Research Directions and Emerging Questions

This thesis has provided a detailed analysis of the European Union's approach to AI and technological regulation, yet the rapid evolution of these technologies suggests many opportunities for further research. One key area worth exploring is the long-term impact of the EU's AI regulations on innovation and competitiveness, especially in comparison to regions like the United States or China, which have fewer restrictions. Future studies could investigate whether the EU's regulatory framework fosters or suppresses innovation within European tech industries. Additionally, as AI becomes increasingly transnational, research on cross-border governance and international cooperation will be crucial. Understanding how international organizations like the UN or OECD might help foster global AI standards and how the EU can take a leadership role in these discussions, could provide valuable insights into the future of AI governance.

Another potential research direction involves the ethical integration of AI in high-risk sectors like healthcare, law enforcement and autonomous vehicles. These areas present significant ethical dilemmas that will need careful regulation to avoid compromising public trust. Similarly, the divergence between the EU and the UK's AI regulatory frameworks post-Brexit presents a new research opportunity. Future studies could explore how this divergence affects AI development, competition and collaboration between the two regions.

As data becomes increasingly central to AI, future research could also delve into the challenges that data-driven societies face, particularly regarding privacy. While the GDPR has set a high standard, the rise of AI introduces new questions about data sovereignty and user consent. Research could focus on how privacy regulations must evolve to meet these

new challenges. Additionally, understanding the public's perception of AI regulation is crucial. Studying how public trust in AI technologies and government regulation is built or got old over time, and what kind of role transparency plays in this, would offer valuable insights for policymakers aiming to foster greater societal acceptance of AI.

Lastly, the global debate on AI regulation often focuses on developed regions like the EU, U.S., and China, but there is a need to consider how AI adoption and regulation will unfold in emerging economies. Investigating the unique challenges that these countries face and how global governance frameworks can assist in developing fair and effective AI policies for these regions, represents an important area for future research. By pursuing these questions, scholars can contribute to both the academic understanding of AI and inform the real world policy decisions as these technologies continue to shape society.

REFERENCE LIST

- Adaş, E. B., & Erbay, B. (2022). Yapay Zekâ Sosyolojisi Üzerine Bir Değerlendirme. Gaziantep University Journal of Social Sciences, 21(1), 326–337. https://doi.org/10.21547/jss.991383, pp. 334–335.
- Agrawal, A., Gans, J. S., & Goldfarb, A. (2019). Artificial Intelligence: The Ambiguous Labor Market Impact of Automating Prediction. The Journal of Economic Perspectives, 33(2), 31–50. https://www.jstor.org/stable/26621238, pp. 34–43.
- Akdağ, İ. (2019). Birleşmiş Milletler Tarafından Gerçekleştirilen Siber Güvenlik Çalışmaları. TASAM, p. 525.
- Ali, N. (2023, Eylül 30). Yapay zekayı günlük hayatımızda nasıl kullanıyoruz?. Indipendent Türkçe. https://www.indyturk.com/node/664146/bi%CC%87li%CC%87m/yapay-zekay%C4%B1-g%C3%BCnl%C3%BCk-hayat%C4%B1m%C4%B1zda-nas%C4%B1l-kullan%C4%B1yoruz
- Anderson, A., Ahmad, A., & Chang, S. (2024). Case-based learning for cybersecurity leaders: A systematic review and research agenda. Information & Management, 61(2024), 104015. https://doi.org/10.1016/j.im.2024.104015, p. 7.
- Benizri, I., Evers, A., Mercer, S. T., & Jessani, A. A. (2023, July 17). A comparative perspective on AI regulation. Lawfare. https://www.lawfaremedia.org/article/a-comparative-perspective-on-ai-regulation
- Biswas, D., Jahan, S., Saha, S., & Samsuddoha, M. (2024). A succinct state-of-the-art survey on green cloud computing: Challenges, strategies, and future directions. Sustainable Computing: Informatics and Systems, 44, 101036. https://doi.org/10.1016/j.suscom.2024.101036, p. 1.
- Brattberg, E., Csernatoni, R., & Rugova, V. (2020). National European Efforts on AI. In Europe and AI: Leading, Lagging Behind, or Carving Its Own Way? (pp. 11–21). Carnegie Endowment for International Peace. http://www.jstor.org/stable/resrep25784.6, pp. 14–16
- Broadbent, M. (2021). What's Ahead for a Cooperative Regulatory Agenda on Artificial Intelligence? Center for Strategic and International Studies (CSIS). http://www.jstor.org/stable/resrep30085, pp. 2–4
- Bureau of Justice Assistance. (n.d.). Foreign Intelligence Surveillance Act of 1978 (FISA). https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1286

- Cabinet Office, Government of Japan. (2019). Social principles of human-centric AI. https://www8.cao.go.jp/cstp/english/humancentricai.pdf, pp. 7–11.
- Center for Governance of AI. (n.d.). The Brussels Effect and artificial intelligence. https://www.governance.ai/research-paper/brussels-effect-ai
- Chen, J., & Chen, F. (2024). Efficient vehicle lateral safety analysis based on Multi-Kriging metamodels: Autonomous trucks under different lateral control modes during being overtaken. Accident Analysis and Prevention, 208, 107787. https://doi.org/10.1016/j.aap.2024.107787, p. 1.
- Clausen, J. B. B., Li, H., & Forget, N. (2024). Empirical risk minimization for big data-driven prescriptive analytics in operations research. Expert Systems with Applications, 232, 120850. https://doi.org/10.1016/j.eswa.2024.120850, p. 1.
- Clocksin, W. F. (2003). Artificial Intelligence and the Future. Philosophical Transactions: Mathematical, Physical and Engineering Sciences, 361(1809), 1721–1748. http://www.jstor.org/stable/3559219, p. 11.
- Council of the European Union. (n.d.). Data protection regulation (GDPR). https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/
- Cyber Daily. (2024). G20 leaders call for global cyber regulations. https://www.cyberdaily.au/government/10695-g20-leaders-call-for-global-cyber-regulations
- Cyber Policy Portal. (n.d.). Cyber Policy Portal. https://cyberpolicyportal.org/
- Dahlman, E., Parkvall, S., & Sköld, J. (2024). 5G standardization. In 5G/5G-Advanced (pp. 7–27). Elsevier. https://doi.org/10.1016/B978-0-443-13173-8.00011-6, pp. 7–8.
- De Spiegeleire, S., Maas, M., & Sweijs, T. (2017). What is artificial intelligence? In Artificial intelligence and the future of defense: Strategic implications for small- and medium-sized force providers (pp. 25–42). Hague Centre for Strategic Studies. http://www.jstor.org/stable/resrep12564.7, pp. 31–32.
- Eldem, T. (2021). Birleşmiş Milletler Sistemi ve Küresel Siberalan Güvenliği Regülasyonu. Marmara Üniversitesi Siyasal Bilimler Dergisi, 9(1), 17–45. https://doi.org/10.14782/marmarasbd.876091, pp. 29–32.
- European Commission. (2020). White Paper on Artificial Intelligence - A European approach to excellence and trust. https://ec.europa.eu/

- European Commission. (2021). Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206
- European Commission. (2023). Cybersecurity Act. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act
- European Commission. (2024). Cybersecurity policies. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies
- European Commission. (2024). European approach to artificial intelligence. https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence
- European Commission. (n.d.). Digital Markets Act (DMA). https://digital-markets-act.ec.europa.eu/index_en
- European Commission. (n.d.). Digital Services Act (DSA) and very large online platforms (VLOPs). https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops
- European Commission. (n.d.). Digital Services Act package. https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package
- European Data Protection Supervisor. (n.d.). Rights of the individual under the GDPR. https://www.edps.europa.eu/data-protection/our-work/subjects/rights-individual_en
- European Parliament and Council. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union.
- European Parliament and Council. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 on harmonised rules on artificial intelligence and amending certain Union legislative acts. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2024/1689/oj
- European Parliament, & Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L119, 1–88.

- European Union Agency for Cybersecurity. (n.d.). ENISA. https://www.enisa.europa.eu/
- Fırat, M. (2016). 21. Yüzyılda uzaktan öğretimde paradigma değişimi. Yükseköğretim ve Bilim Dergisi, 6(2), 142–150. https://doi.org/10.5961/jhes.2016.151, p. 1.
- Future of Life Institute. (2024, May 30). High-level summary of the AI Act. https://artificialintelligenceact.eu/high-level-summary/
- G20. (2024). According to an expert, cybersecurity should protect more vulnerable groups such as older people and children. https://www.g20.org/en/news/according-to-an-expert-cybersecurity-should-protect-more-vulnerable-groups-such-as-older-people-and-children
- G20. (2024). Cybersecurity: Strengthening policies to combat threats in the digital world. https://www.g20.org/en/news/cyber-security-strengthening-policies-to-combat-threats-in-the-digital-world
- Gacar, A. (2019). Yapay Zekâ ve Yapay Zekânın Muhasebe Mesleğine Olan Etkileri: Türkiye'ye Yönelik Fırsat ve Tehditler. Balkan Sosyal Bilimler Dergisi, 8(EUREFE'19), 389–394, pp. 1–3.
- Geffray, M. (2024). FISA law extension: Impact on European privacy regulations. Oodrive. https://www.oodrive.com/blog/regulation/fisa-law-extension/#:~:text=The%20FISA%20Act%20contradicts%20European,it%20until%20April%2019%2C%202024.
- Goldust, M., & Grant-Kels, J. M. (2024). Regulatory considerations for safe and ethical use of augmented reality and virtual reality in dermatology. Clinics in Dermatology, p. 7.
- Hollister, S. (2021, September 2). Apple will prompt you to enable personalized ads in iOS 15 even if you previously opted out. The Verge. https://www.theverge.com/2021/9/2/22654121/apple-personalized-ads-ios-15-prompt-app-tracking
- Hoofnagle, C. J., van der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: What it is and what it means. Information & Communications Technology Law, 28(1), 65–98. https://doi.org/10.1080/13600834.2019.1573501, pp. 9–10.
- IBM. (2024). Natural language processing (NLP). https://www.ibm.com/topics/natural-language-processing

- IBM. (n.d.). What is blockchain?. https://www.ibm.com/topics/blockchain
- Innovation, Science and Economic Development Canada. (2022). Canada's AI strategy. https://ised-isde.canada.ca/site/ai-strategy/en
- International Telecommunication Union. (2024). 5G: Fifth generation of mobile technologies. https://www.itu.int/en/mediacentre/backgrounders/Pages/5G-fifth-generation-of-mobile-technologies.aspx
- International Telecommunication Union. (2024). ITU-T: Setting the standard. https://www.itu.int/en/mediacentre/backgrounders/Pages/itu-t-setting-the-standard.aspx
- International Telecommunication Union. (n.d.). Cybersecurity. https://www.itu.int/en/action/cybersecurity/Pages/default.aspx
- International Telecommunication Union. (n.d.). Global Cybersecurity Agenda (GCA). https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx
- IT Governance. (2023). DPA and GDPR penalties. https://www.itgovernance.co.uk/dpa-and-gdpr-penalties
- ITU. (n.d.). United for Smart Sustainable Cities (U4SSC). https://u4ssc.itu.int/about/
- İstanbul Gedik Üniversitesi. (n.d.). Modern dünyayı şekillendiren 21. yüzyıl icatları. https://uzemigunsem.gedik.edu.tr/modern-dunyayi-sekillendiren-21-yuzyil-icatlari
- Jaeger, P. T., Bertot, J. C., & McClure, C. R. (2003). The impact of the USA Patriot Act on collection and analysis of personal information under the Foreign Intelligence Surveillance Act. Government Information Quarterly, 20(3), 295–314. https://doi.org/10.1016/S0740-624X(03)00057-1, p. 297.
- Karakoç Keskin, E. (2023). Yapay Zekâ Sohbet Robotu ChatGPT ve Türkiye internet gündeminde oluşturduğu temalar. Yeni Medya Elektronik Dergisi, 7(2), 114–131. https://doi.org/10.17932/IAU.EJNM.25480200.2023/ejnm_v7i2003, p. 128.
- Khanal, S., Zhang, H., & Taeihagh, A. (2024). Development of New Generation of Artificial Intelligence in China: When Beijing’s Global Ambitions Meet Local Realities. Journal of Contemporary China, 1–24. https://doi.org/10.1080/10670564.2024.2333492, pp. 4–5.
- Knieps, G. (2024). Internet of Things, critical infrastructures, and the governance of cybersecurity in 5G network slicing. Telecommunications Policy, 48(4), 102867. https://doi.org/10.1016/j.telpol.2024.102867, pp. 2–4.

- Kosinski, M., & Scapicchio, M. (2024). EU AI Act. IBM. https://www.ibm.com/topics/eu-ai-act
- Labbe, M., & Wigmore, I. (2024). Narrow AI (weak AI). TechTarget. https://www.techtarget.com/searchenterpriseai/definition/narrow-AI-weak-AI
- Löhr, G. (2023). Conceptual disruption and 21st century technologies: A framework. Technology in Society, 74, 102327. https://doi.org/10.1016/j.techsoc.2023.102327, p. 1.
- Marr, B. (2019, December 16). The 10 best examples of how AI is already used in our everyday life. Forbes. https://www.forbes.com/sites/bernardmarr/2019/12/16/the-10-best-examples-of-how-ai-is-already-used-in-our-everyday-life/
- Marrone, R., Cropley, D., & Medeiros, K. (2024). How does narrow AI impact human creativity? Creativity Research Journal. https://doi.org/10.1080/10400419.2024.2378264, p. 8.
- McKinsey & Company. (n.d.). The state of AI. https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai
- Muthukrishnan, N., Maleki, F., Ovens, K., Reinhold, C., Forghani, B., & Forghani, R. (2020). A brief history of artificial intelligence. Neuroimaging Clinics of North America, 30(3), 393–399. https://doi.org/10.1016/j.nic.2020.07.004, pp. 393–396.
- National Institute of Standards and Technology. (n.d.). Fundamental AI. https://www.nist.gov/fundamental-ai
- NATO. (2024). Summary of NATO's revised Artificial Intelligence (AI) strategy. https://www.nato.int/cps/en/natohq/official_texts_227237.htm
- Ntoko, A. (2011, January 17-21). Global Cybersecurity Agenda (GCA): A framework for international cooperation [Conference presentation]. Open-ended Intergovernmental Expert Group on Cybercrime, Vienna, Austria.
- OECD. (2022). OECD Blockchain Policy Forum. https://mneguidelines.oecd.org/oecd-blockchain-policy-forum.htm
- OECD. (2024). OECD AI principles. https://www.oecd.org/en/topics/ai-principles.html
- OECD. (n.d.). Digital finance. https://www.oecd.org/en/topics/sub-issues/digital-finance.html

- OECD. (n.d.). Digital strategies in education across OECD countries. https://www.oecd-ilibrary.org/education/digital-strategies-in-education-across-oecd-countries_33dd4c26-en
- OECD. (n.d.). OECD AI principles. https://oecd.ai/en/ai-principles
- Öztemel, E. (2020). Yapay zekâ ve insanlığın geleceği. In Bilişim teknolojileri ve iletişim: Birey ve toplum güvenliği (pp. 96–112). Türkiye Bilimler Akademisi, p. 101.
- Pew Research Center. (2023, February 15). Public awareness of artificial intelligence in everyday activities. https://www.pewresearch.org/science/2023/02/15/public-awareness-of-artificial-intelligence-in-everyday-activities/
- Pirim, H. (2006). Yapay Zeka. Yaşar Üniversitesi, p. 92.
- Russell, S., & Norvig, P. (2020). Artificial Intelligence: A Modern Approach (4th ed.). Pearson, p. 1.
- Sánchez Nicolás, E. (2020). Online giants could face 10% fines under new EU law. EUobserver. https://euobserver.com/science/150396
- Schjølberg, S. (2008). ITU Global Cybersecurity Agenda (GCA): Report of the Chairman of the High-Level Experts Group (HLEG). International Telecommunication Union.
- Sharfaei, S., & Bittner, J. (2024). Technological employment: Evidence from worldwide robot adoption. Technological Forecasting & Social Change, 209, 123742. https://doi.org/10.1016/j.techfore.2024.123742, pp. 1–2.
- Sheehan, M. (2023). The Underlying Structure of China's AI Regulations. In China's AI Regulations and How They Get Made (pp. 15–16). Carnegie Endowment for International Peace. http://www.jstor.org/stable/resrep52039.7
- Sheng, J., Amankwah-Amoah, J., & Wang, X. (2019). Technology in the 21st century: New challenges and opportunities. Technological Forecasting & Social Change, 143, 321–335. https://doi.org/10.1016/j.techfore.2018.06.009, pp. 321–323.
- Strickland, L. S. (2003). Civil liberties vs. intelligence collection: The secret Foreign Intelligence Surveillance Act court speaks in public. Government Information Quarterly, 20(1), 1–12. https://doi.org/10.1016/S0740-624X(02)00132-6, p. 2.
- Szczepański, M. (2024). US approach to artificial intelligence [EPRS At a Glance Report]. European Parliamentary Research Service. https://www.europarl.europa.eu/thinktank, p. 1.

- Trüdinger, E.-M., & Steckermeier, L. C. (2017). Trusting and controlling? Political trust, information and acceptance of surveillance policies: The case of Germany. Government Information Quarterly, 34(3), 421–433. https://doi.org/10.1016/j.giq.2017.07.003, pp. 1–2.
- Türkiye Yapay Zeka İnisiyatifi. (2022). Yapay zeka zaman çizelgesi. https://turkiye.ai/kaynaklar/yapay-zeka-zaman-cizelgesi/
- U.S. Office of the Director of National Intelligence. (n.d.). Foreign Intelligence Surveillance Act (FISA). https://www.intelligence.gov/foreign-intelligence-surveillance-act
- UNESCO. (2023). Recommendation on the ethics of artificial intelligence: Cases. https://www.unesco.org/en/artificial-intelligence/recommendation-ethics/cases
- UNESCO. (2024). Recommendation on the ethics of artificial intelligence. https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence, p. 26.
- United for Smart Sustainable Cities (U4SSC). (n.d.). Unlocking Cities of the Future: The Road to Smart Sustainable Cities. ITU. https://u4ssc.itu.int
- United Nations. (n.d.). AI Advisory Body. https://www.un.org/en/ai-advisory-body
- VanMeter, R., Toffaletti, S., LePape, A., Bertola, V., & Miseviciute, J. (2022, March 14). Open letter regarding the EU Digital Markets Act (DMA). Coalition for App Fairness, European Digital SME Alliance, Coalition for Competitive Digital Markets, pp. 2–3.
- Wu, M., & Chen, X. (2024). Application of Internet of Things and embedded technology in electronic communication. Measurement: Sensors, 34, 101246. https://doi.org/10.1016/j.measen.2024.101246, pp. 1–4.
- Yang, T., Ma, C., & Mi, X. (2024). The transformative potential of blockchain technology in developing green supply chain: An evolutionary perspective on complex networks. Computers & Industrial Engineering, 197, 110548. https://doi.org/10.1016/j.cie.2024.110548, p. 2.
- Zhou, X., Cai, Z., Tan, K. H., Zhang, L., Du, J., & Song, M. (2021). Technological innovation and structural change for economic development in China as an emerging market. Technological Forecasting & Social Change, 167, 120671. https://doi.org/10.1016/j.techfore.2021.120671, p. 2.