

DOKUZ EYLÜL UNIVERSITY
GRADUATE SCHOOL OF SOCIAL SCIENCES
DEPARTMENT OF INTERNATIONAL RELATIONS
INTERNATIONAL RELATIONS PROGRAM

MASTER’S THESIS

**EUROPEAN UNION’S APPROACH TO ARTIFICIAL
INTELLIGENCE IN THE CONTEXT OF HUMAN RIGHTS**

İŞİL GÖÇEN

Supervisor

Assist. Prof. Dr. Zühal ÜNALP ÇEPEL

İZMİR-2023

DECLARATION

I hereby declare that this master's thesis/non-thesis master's term project titled as "European Union's Approach To Artificial Intelligence In The Context Of Human Rights" has been written by myself in accordance with the academic rules and ethical conduct. I also declare that all materials benefited in this thesis consist of the mentioned resources in the reference list. I verify all these with my honour.

Date

03.07.2023

Işıl GÖÇEN

ABSTRACT

Master's Thesis

**European Union's Approach To Artificial Intelligence In The Context Of
Human Rights**

Işıl GÖÇEN

Dokuz Eylül University

Graduate School of Social Sciences

Department of International Relations

International Relations Program

Artificial intelligence has started to be mentioned in international conferences and literature since the 1950s, but it has become a new trend in the last two decades and has gradually increased its presence in the literature. In the digital age where technology continues to develop without slowing down, Artificial Intelligence has become an important power indicator for states and has even enabled the balance of power in the international system to change. In this context, the European Union's human-centred and regulatory approach to artificial intelligence constitutes an obstacle to the technological progress of the European Union.

Artificial intelligence studies in the literature in the field of social sciences discuss that artificial intelligence may cause undesirable consequences, either intentionally or unintentionally. When data, which is the source of artificial intelligence, is misused or abused, it leads to various human rights violations. The European Union emphasises the importance of an ethical, trustworthy and responsible Artificial Intelligence.

This thesis aims to critically examine the European Union's human-centred approach to artificial intelligence, taking into account the fundamental values on which the European Union is based that are enshrined on the Lisbon Treaty and EU Charter of Fundamental Rights. It aims to fill the gap in the

literature by discussing whether the artificial intelligence regulations (General Data Protection Regulation (2016), Ethics Guidelines For Trustworthy AI (2019), White Paper on Artificial Intelligence: a European approach for excellence and trust (2020), EU Artificial Intelligence Act (2021), Artificial Intelligence Liability Directive (2022)), which the European Union has published constitute a barrier to technological progress and whether the European Union is right in its strict regulatory approach.

Keywords: Artificial Intelligence, European Union, Human Rights, Ethical Artificial Intelligence, Trustworthy Artificial Intelligence, Responsible Artificial Intelligence, Human-Centred Artificial Intelligence, Artificial Intelligence Regulations.

ÖZET

Yüksek Lisans Tezi

Avrupa Birliği'nin İnsan Hakları Bağlamında Yapay Zeka Yaklaşımı

Işıl GÖÇEN

Dokuz Eylül Üniversitesi

Sosyal Bilimler Enstitüsü

Uluslararası İlişkiler Anabilim Dalı

Uluslararası İlişkiler Programı

Yapay zeka 1950'lerden itibaren uluslararası konferanslarda ve literatürde kendinden söz ettirmeye başlamıştır, ancak son yirmi yıl içerisinde yeni bir trend haline gelmiş ve literatürdeki varlığını giderek artırmıştır. Teknolojinin hız kesmeden gelişmeye devam ettiği dijital çağda yapay zekâ devletler için önemli bir güç göstergesi haline gelmiş, hatta uluslararası sistemdeki güç dengelerinin değişmesine olanak sağlamıştır. Bu bağlamda, Avrupa Birliği'nin yapay zekaya insan merkezli ve düzenleyici yaklaşımı Avrupa Birliği'nin teknolojik ilerlemesinin önünde bir engel teşkil etmektedir.

Sosyal bilimler alanında literatürdeki yapay zeka çalışmaları, yapay zekanın kasıtlı ya da kasıtsız olarak istenmeyen sonuçlara sebebiyet verebileceğini tartışmaktadır. Yapay zekanın kaynağı olan veri kötü amaçlarla kullanıldığında ya da suistimal edildiğinde çeşitli insan hakları ihlallerine yol açmaktadır. Avrupa Birliği ise etik, güvenilir ve hesap verebilir bir yapay zekanın önemini vurgulamaktadır. Bu çalışma Avrupa Birliği'nin Lizbon Anlaşması ve AB Temel Haklar Bildirgesi'nde söz edilen dayandığı temel değerleri de göz önüne alarak Avrupa Birliği'nin insan merkezli yapay zeka yaklaşımını eleştirel yönden ele almayı hedeflemektedir. Avrupa Birliği'nin yayınlamış olduğu ve kendisinin de mihenk taşı olarak adlandırdığı yapay zeka regülasyonlarının (Genel Veri Koruma Yönetmeliği (2016), Güvenilir Yapay

Zeka İin Etik Kurallar (2019), Yapay Zeka Üzerine Beyaz Kitap: mükemmellik ve güven iin bir Avrupa yaklařımı (2020), AB Yapay Zeka Yasası (2021), Yapay Zekâ Sorumluluk Direktifi (2022)) teknolojik ilerlemenin önünde bariyer teřkil edip etmediđini, Avrupa Birliđi'nin katı regülatif yaklařımında haklı olup olmadıđını tartıřarak literatürdeki bořluđu doldurmayı hedeflemektedir.

Anahtar Kelimeler: Yapay Zeka, Avrupa Birliđi, İnsan Hakları, Etik Yapay Zeka, Güvenilir Yapay Zeka, Hesap Verebilir Yapay Zeka, İnsan Merkezli Yapay Zeka, Yapay Zeka Regülasyonları.

EUROPEAN UNION’S APPROACH TO ARTIFICIAL INTELLIGENCE IN THE CONTEXT OF HUMAN RIGHTS

CONTENTS

DECLARATION	iii
ABSTRACT	iv
ÖZET	vi
CONTENTS	viii
ABBREVIATIONS	x
LIST OF TABLE	xi
INTRODUCTION	1

CHAPTER ONE

UNDERSTANDING THE EUROPEAN UNION'S ARTIFICIAL INTELLIGENCE POLICIES

1.1. CONCEPTUAL FRAMEWORK: ARTIFICIAL INTELLIGENCE	5
1.2. THEORETICAL FRAMEWORK	7
1.2.1. Humanly Approach	7
1.2.2. Rational Approach	8
1.2.3. European Union Approach	9
1.2.3.1. Copenhagen Criteria (1995)	10
1.2.3.2. EU Charter of Fundamental Rights (2000)	10
1.2.3.3. Lisbon Treaty (2009)	11
1.3. MALICIOUS USES OF THE AI	11
1.3.1. Abuses of Human Rights	12
1.3.2. Data Privacy	13
1.3.3. Unfairness and Discrimination	15
1.3.4. Unethical Uses of AI	16
1.3.5. Cyber Attacks	17
1.4. CONCLUSION	18

CHAPTER TWO

THE GLOBAL RACE FOR AI

2.1. INTRODUCTION	19
2.2. UNITED STATES AS THE LEADER OF THE RACE	20
2.3. CHINA AS THE SECOND LEADER OF THE RACE	23
2.3.1. AI Applications That Threaten Individual Rights In China	25
2.4. EUROPEAN UNION AS THE THIRD LEADER OF THE RACE	26
2.5. CONCLUSION	29

CHAPTER THREE

AI REGULATIONS IN EUROPE

3.1. INTRODUCTION	30
3.2. GENERAL DATA PROTECTION REGULATION (2016)	33
3.3. HIGH LEVEL EXPERT GROUP ON AI	35
3.4. EUROPEAN AI ALLIANCE	37
3.5. WHITE PAPER ON ARTIFICIAL INTELLIGENCE	38
3.6. AI ACT	39
3.7. PROPOSAL FOR AN AI LIABILITY DIRECTIVE	40
3.8. EU DIGITAL STRATEGY	41
3.9. IS THE REGULATORY APPROACH THE REASON WHY THE EU IS LAGGING BEHIND IN AI RACE?	42
CONCLUSION	44
REFERENCES	50

ABBREVIATIONS

AI	Artificial Intelligence
AAAI	Association for the Advancement of Artificial Intelligence
AILD	Artificial Intelligence Liability Directive
DGA	Digital Governance Act
DMA	Digital Markets Act
DSA	Digital Services Act
EDPB	European Data Protection Board
ENISA	The European Union Agency for Cybersecurity
EU	European Union
FP6	6th Framework Programme
FP7	7th Framework Programme
GDPR	General Data Protection Regulation
HLEG	High Level Expert Group
IT	Information Technology
MERICS	Mercator Institute for China Studies
OECD	Organisation for Economic Co-operation and Development
PLD	Product Liability Directive
PRC	Peoples Republic of China
SME	Small And Medium-Sized Enterprises
TTC	Trade and Technology Council
UNESCO	The United Nations Educational, Scientific and Cultural Organization
WTO	World Trade Organization

LIST OF TABLE

Table 1: European States' National AI Strategies

p.31-32

INTRODUCTION

In recent years, artificial intelligence (AI) has received increasing attention in the literature. The unabated continuation of digitalization has integrated AI into all areas of our lives and made AI a subject suitable for research in every field. While researching AI in the field of natural sciences provides concrete contributions to the digitalization process of countries, research in the field of social sciences reveals what awaits countries and societies, how great powers should compete in this field, and most importantly, the humanitarian issues that need to be considered.

Since the 1990s, scholars have begun to pay attention to the approach to AI, and its categorization as rational, and humanly approach (Norvig and Russel, 1995: 5-7). In fact, the foundations of this view were laid in 1950 with Alan Turing's question "Can machines think?" (Turing, 1950: 433). The question of whether machines controlled by AI can replace humans has been frequently discussed in the literature (Ramamoorthy and Yampolskiy, 2018: 77; Yampolskiy, 2016; Isik, 2020), and even singularity¹ (Baum, 2018: 244; Uysal, 2021: 297-309; Braga and Logan, 2019: 73; Vinge, 2003; Wang et al., 2018: 1-15), the idea that the world will be dominated by machines, has been the subject of many research.

AI, a topic that started to become popular in the 1950s, and data, the building block of AI, emerged as a completely different power in the 2010s. (The Economist, 2017) For this reason, many states have developed their own AI policy and have included AI governance in official sources (Galindo et al., 2021: 1-26)². In fact, it would not be wrong to say that technology-related issues are among the priority issues in the national security policies of the states (The National Science and Technology Council, 2022: 1-6). Since 2016, states have started to address the moral and humanitarian dimensions of AI (Fjeld et al., 2020: 2-66), thanks to the leading role of the European Union (EU) (Samsun, 2021: 24-31). As a normative power in the global arena (Manners, 2002: 252), the EU follows a similar approach in the field of AI. Its

¹ "Singularity" in the field of artificial intelligence was first mentioned by Vernor Vinge in 1993. This theory made quite a noise in the literature, and then Ray Kurzweil published his work "The Singularity Is Near" in 2005. Singularity is generally a scenario in which human-created machines and robots will surpass human intelligence and take over the world.

² European Commission's body "AI Watch" is available via this link: https://ai-watch.ec.europa.eu/index_en

normative power depends on the regulative framework of the EU, and it also determines the EU's regulatory and human-centered approaches to AI. Mainly; Treaty of Rome (1957), EU Charter of Fundamental Rights (2000), and Lisbon Treaty (2009) defines the aims and values of the EU to which that adheres.

Although AI facilitates human life in health, finance, education, and tourism, in short, in every field that is thought of; developing technologies have brought up many brand new issues such as the security of our personal data, the trustability, morality, opacity of machines, cybercrime, robot laws (Fjeld et al., 2020: 2-66). AI ethicists have started to worry about the future of AI (Köbis et al., 2021: 1-30; Chin and Robison, 2020: 82-104; Bostrom and Yudkowsky, 2011: 316-334), and for Europe, people should be able to trust the AI machine's so as to Europe will keep supporting its further development (European Commission, 2020a). AI ethicists are not the only ones addressing this issue; scholars that study law, and also lawyers are equally concerned about the state of AI (Palmerini et al., 2016).

The EU, which is at the center of this research, considers the concept of AI from the framework of human rights and determines its policies accordingly. EU with the goal of becoming a global leader in terms of the digital economy and AI (European Commission, 2020a), seeks to create common regulations among the member states (Klasinc, 2022: 1-5). As it is already mentioned, the EU's normative power determines its each policy and shows the strong ties of its commitment to the aims and values that is founded on. This can even be observed on the EU leaders speeches (Noureddine, 2016: 2). This research will analyze the published articles of the EU. The qualitative method will be applied, hence, the methodology of this study is document analysis. In this research the following research questions will be tried to answer; The first one is: how do human rights and ethical issues have affected EU's approach to Artificial Intelligence? And the second one is: Whether the fundamental values of the EU constitute a barrier to technological progress or not? To do so, the official documents of the EU will be analysed. The official documents that were published by the EU authorities on AI will be analysed in this research are as follows; General Data Protection Regulations (2016), Ethics Guidelines For Trustworthy AI (2019), White Paper on Artificial Intelligence: a European approach to excellence and trust (2020), EU Artificial Intelligence Act (2021), AI Liability Directive (AILD)(2022).

With the General Data Protection Regulations (GDPR), the EU has a much broader, more unified regulation that will enable sanctions to be imposed in other countries. The GDPR consists of 11 chapters and 99 articles and in many respects the first attempt at international regulation. Another important concept for the EU, and perhaps the most important one, is ‘trustworthy artificial intelligence’. In 2019, the High-Level Expert Group (HLEG) on AI, which started its work in December 2018, published its study "Ethics guidelines for trustworthy AI", according to which ‘trustworthy AI’ should be achieved if it is lawful, ethical, and robust. (European Commission, 2019a) With the White Paper on Artificial Intelligence on AI, published in 2021, the EU argues that it recognizes AI as a concept that will benefit society at large and that it is linked to fundamental rights, human dignity, and the protection of privacy. The terms “ecosystem of trust” and “ecosystem of excellence” are introduced and policy options to support the development of a trusted AI are discussed in the White Paper on Artificial Intelligence. With the AI ACT, the EU categorizes AI policies according to the level of risk, in line with previous regulations. On the other hand, AILD tries to regulate the market for AI-related sectors.

The literature on the misuse of AI shows that it is indeed one of the greatest threats of our age. The reports that were published in the cyber-security realm show the importance of this issue; Allen and Masollo (2019) mention the current threats that AI may create, Madnick (2022) explains the threats regarding consumer data, Ciancaglini and his friends (2020) study on malicious uses of the AI categorises the unintended consequences of the corrupt AI or its malicious uses like the European Union Agency for Cyber Security (ENISA)³ report (2020). Studies on cybersecurity and cyber-attack cases in our history emphasize the importance of data security and the necessity of a human-centric approach to AI.

While the EU restricts and regulates the use of data in AI, it also seems to have stifled its development. There have been hundreds of large and small studies on the misuse of malicious use of AI, enough to justify the EU in this fight. While the literature is replete with studies examining the EU’s official AI documents, there is a dearth of studies that vindicate the EU regarding AI policies. In this context, this thesis

³ European Union Agency For Cyber Security which was founded on 2004, with the aim of contributing and enhancing EU’s cyber security policies by cooperating with the Member States and EU bodies.

aims to contribute to filling this gap in the literature by advocating that more regulations in AI and in access to the data also mean more backwardness in the global AI race. This research will analyze the official sources published by the EU so far, try to identify the position of the EU in the global AI race, and argue that one of the reasons for its backwardness is the humanitarian approach to AI.

Despite the EU's goals of becoming a global leader in AI, research shows that it has fallen behind the US and China in various indicators such as investment, number of AI companies, qualified workforce, and government support. In their study published in 2023, Vasse'i and McCrosky showed that it is more difficult to ensure transparency than expected. According to Klasinc (2022), creating a common approach is also much more harder and it presents a problem for the EU. Even if Bradford (2022) and Hacker (2023) have argued the European global soft power and leading role of the regulatory framework by explaining the Brussel Effect, current reports have shown that the European economy is not experiencing its golden age. Strict regulations costs are too much for the business actors, business actors that deals with the technology-related products, and they prioritize the innovation over regulations (Economist Intelligence, 2023). Hence, the EU's economic growth is also losing momentum due to these regulations. For example, the forecast for 2023 suggests that the strongest economic growth will be in Asia, while the weakest will be in Europe. The budget allocated to AI and technology-related areas is significantly higher in the US and China compared to the EU. This study calls for an examination of the EU's AI policies, considering the potential misuse of AI and its impact on fundamental human rights. It also suggests analyzing the reasons behind the EU's lag in the AI race and the importance of a human-centered AI approach.

The first chapter of the study describes the approaches to AI and the terms safe and secure AI and aims to explain the importance of the human-centered AI approach by demonstrating examples of malicious uses of AI applications. The second chapter provides a comparative analysis of the AI policies of the US, China, and the EU on a global scale. The third, namely the last chapter aims to analyse the EU's main AI regulations and analyse impacts on the development of AI.

CHAPTER ONE

INTRODUCTION TO UNDERSTANDING THE EUROPEAN UNION'S ARTIFICIAL INTELLIGENCE POLICIES

1.1. CONCEPTUAL FRAMEWORK: ARTIFICIAL INTELLIGENCE

AI has been started to take place in the literature since the early 1950s. Thanks to the great contributions of Alan Turing, John McCarthy, Allen Newell, and Herbert Simon the idea of AI has been developed and continued to exist since the 1950s, and the evolution has been experienced with the invention of the Internet. AI is one of the most popular research topics, and it will likely remain so for the foreseeable future. Today, no society which is unaware of AI cannot become a community and cannot survive. Although, there is not only one accepted definition of AI, all definitions complement each other. More than a half-century ago, in 1950, Alan Turing who is a mathematician and computer scientist, published an article titled “Computing Machinery and Intelligence” and asked a path-breaking question: “Can machines think?” In 2004, John McCarthy who is a mathematician and computer scientist again, defined AI as the science and ability to make intelligent machines, especially computer programs. In 2018, European Commission HLEG acknowledged a broader definition and defined AI as follows; “Artificial intelligence refers to systems that display intelligent behaviour by analysing their environment and taking actions –with some degree of autonomy- to achieve specific goals.”⁴ Organisation for Economic Co-operation and Development (OECD) accepts the definition of AI as follows: “A machine-based system that can, for a given set of human defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments.”⁵ Like Norvig and Russel (1995) said AI is a universal field and its benefits can be observed in every field; from the health sector to tourism, from finance to education, from law to entertainment.

⁴ The European Commission’s High Level Expert Group On Artificial Intelligence, “A Definition Of AI: Main Capabilities and Scientific Disciplines”, 18.12.2018, https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf, (10.01.2023), p.1

⁵ OECD, “Recommendation of the Council on Artificial Intelligence”, 22.05.2019, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>, (10.01.2023)

AI has been touching, shaping, and controlling our lives. Like all states throughout the world, the EU acknowledges that AI has countless benefits, it has been used in many fields today and this will continue to increase. However, this phenomenon has created concerns about the future of AI and our society. Scientists are worried about the threats of AI and its misuse. Of course, there are many scientists who think that AI cannot be controlled and attempts will not be enough (Yampolskiy, 2016). There are even those who call AI as God and claim that God is an uncontrollable force (Yampolskiy, 2016). According to scholars AI has been used in fighting against cyber security threats too; active firewalls, e-mail scanning, anti-virus applications, automated malware analysis, strong password recommendations, and so on (Ciancaglini et al., 2020: 6-18). But it is important to ask: Who is further?

AI is the machines or software systems that are designed and created by humans. To some extent the systems are biased, but controlling these machines is in the hands of the creators. ENISA was established in 2004, with the aim of contributing to Europe's cyber security policy and enhancing the trustworthiness of AI which is parallel with the White Paper. They have highlighted four crucial points that should be taken into account to secure AI itself and one of them is to create regulations to be sure that AI will be more safe. Today's world accepts the data as the new oil which means is the source of profit. Since the data is the source of the AI (The Economist, 2017) concepts such as the protection of personal data, and safe, secure, and trustworthy AI have come to the fore. European Commission believes that trustworthiness is a precondition for the uptake of the AI, firstly people should be able to trust the AI machines, then they can support it. When the articles and books on AI in the field of social sciences were examined, it can be seen that almost all of them mention the need for safe and secure AI machines.

The term "Safe AI" was first used in the early 1995s (Yampolskiy, 2016) but it gained popularity after the 2010s. Scholars agree that safe and secure AI can only be possible if the AI design is fully transparent and responsible. While AI safety refers to the proper internal functioning of AI and avoidance of unintended harm, AI security refers to the external threats that can be directed to the operating AI systems (Fjedl et al., 2020: 37-40). These threats can be directed at either AI software or hardware. That is why humanity needs regulations to protect fundamental rights. Thanks to the

pioneering role of the EU, it has been understood that AI should be controlled by international regulations, that is the prerequisite of sustainable AI systems.

The EU with the goal of becoming a global leader in terms of the digital economy and AI, seeks to create common regulations among the member states. However, due to legal regulations, restrictions on data access, and human rights being at the forefront, it can be said that the EU has a long way to go to become a global leader. But it is important to note that Europe is the leader in regulating AI; from the works of HLEG to Commission, from the civil societies' efforts to member states themselves. EU has contributed a lot to regulate and control the power, misuse, and threats of AI.

1.2. THEORETICAL FRAMEWORK

In 1995, Stuart J. Russel and Peter Norvig published the most popular AI textbook “A Modern Approach to AI”. This comprehensive book categorises AI approaches into four categories; thinking humanly, acting humanly, thinking rationally, and acting rationally. Their starting point is thought process and behaviour, and they support that AI can be traced back to Aristotle's syllogisms⁶. In this research, the approaches will be examined as rational and humanly approach to make it more clear for the social sciences.

1.2.1. Humanly Approach

The Turing Test; was proposed by Alan Turing in 1950. Turing tried to understand the dynamics of computers, and whether computers can act, and think like humans or not. In the Turing Test, humans are at the center, and it is questioned whether AI machines can imitate humans' behaviour or thinking process perfectly or not. To do so, computers need to have some human skills. Acknowledging the fact that humans are not perfect, are not always rational; instead, humans are emotional and to some extent irrational creatures. Claiming machines can think like humans, requires understanding how human thinks, how the brain works, and how data is processed

⁶ It is a method of deduction by comparing two different data with each other.

which is a field of cognitive science. Once understanding how humans think, a theory about computer thinking can be constructed, and if the program's thinking process is similar to humans, one can talk about programs that can think like humans.

1.2.2. Rational Approach

The founder of rational thinking is Aristotle. His basic logic constructed the very roots of logical thinking. The logicist tradition aims to build a rational AI. The rational agent approach puts correct inferences, and expected or best expected outcomes at the center. Reasoning serves AI to reach good decisions, but at this point, the good decision should be questioned. Which decision is good for whom? Good decisions should be good for all, for the society in which AI operates. Russel and Norvig say that rational AI is more reasonable than the approaches based on human behaviour or human thought, however; this approach is more theoretical and deprived of ethical values. They also acknowledge that being rational -always doing the right thing- is not possible in every environment (Russel and Norvig, 1995).

1.2.3. European Union Approach

EU has a very clear approach to AI. Its aim is to build a resilient Europe in the digital age, to do so EU prefer to follow a regulatory and human-centered AI approach. Although there is no strict nomenclature as EU AI Approach in the literature, it is named as "European Union Approach" by the author due to the sui generis structure of the EU. In fact, the EU's role as a "normative force" in international politics is a concept coined by Ian Manners in 2002 (Nouredine, 2016: 1; Diez, 2021: 2). Manners argued that the EU is a unique actor in the global arena with its emphasis on values such as human rights, democracy and sustainability. The priority of EU's AI approach is making people safe and protected while having a well-developed AI system that can race on a global scale. The Union believes that current approaches to AI will shape the future. It is always emphasized achieving trust and excellence will boost the usage of AI and the general well-being of the people.

In 2018, Union started its efforts to make AI a legal, ethical, and more trustworthy entity. Discussions began in 2018 under the leadership of the European Commission and the EU Approach to AI can be clearly observed by reviewing the published articles of the Commission. According to Commission “trust is a prerequisite to ensure a human-centric approach to AI: AI is not an end in itself, but a tool that has to serve people with the ultimate aim of increasing human well-being.”⁷ To achieve this, the Commission highlighted the role of human participation in design (ethics by design), decision making, monitoring and controlling the operation of machines. Control mechanisms are very important and adaptability, accuracy, and explainability can be achieved through governance mechanisms such as human-in-the-loop, human-on-the-loop, and human-in-command approaches.

In every official document of the Commission, the human-centric AI approach has been emphasized with the aim of using AI for good. EU believes that personal data protection is a must, it is not an alternative. For a trustworthy and excellent AI, the EU published White Paper on Artificial Intelligence in 2020. The document emphasized that the Commission strongly supports a human-centric approach. However; according to the data mentioned in the document, the EU lagged behind North America and Asia in the field of AI, despite a large increase in investments in research and innovation for AI in the previous years.

In this article, it will be discussed that one of the reasons why the EU can only be placed in the third rank in the race for AI is the rule-making role of the EU. Even if European Commission aims to prevent the rules from hindering the creation of a flourishing AI ecosystem in Europe, great efforts are not enough to overtake the global AI race and become the upper hand.

The EU's regulatory approach is centered around its core values that are mentioned in the Copenhagen Criteria (1995), EU Charter of Fundamental Rights (2000), and Lisbon Treaty (2009). The core principles of these documents and relation with the EU's AI Approach will be analysed in the following section.

⁷ European Commission, “Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions Building Trust in Human-Centric Artificial Intelligence, 08.04.2019, <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52019DC0168>

1.2.3.1. Copenhagen Criteria (1995): The Copenhagen criteria checks the admissibility, and eligibility of a country to the EU. These criteria consist of three categories: geographical, political and economic. Geographical criteria requires the accession country to have territory in Europe, which is why Morocco's application was rejected in 1987. Nevertheless, Cyprus was admitted to the EU in 2004, even though it has no territory in Europe (Hillion, 2004). The political criteria are also divided into three categories. These are democracy, rule of law, and human rights and minority rights. Firstly, elections are based on a secret ballot system in which everyone has an equal right to vote. Secondly, states must be governed by documented laws, there is no room for arbitrary rulings in specific conditions. Thirdly, all minorities must be allowed to keep their culture, religion and language as they wish, all forms of slavery are forbidden, it is even forbidden for a person to declare himself a slave. Finally, every country wishing to enter the Union must have a functioning economy and be sufficiently developed to trade with other countries in the EU. The Copenhagen Criteria are important because they establish the fundamental requirements that countries must meet to become EU members, and it also shows the EU's commitment to its core values. Especially; democracy, rule of law, human rights and minority rights are important phenomena in terms of EU's human-centered regulative AI Approach. AI machines can easily have an option to exclude minority groups, make decision in favor of some groups, or violate human rights by infiltrating their personal area. EU wants to ensure that new members are aligned with the EU's core values, principles, and standards, contributing to the stability, coherence, and expansion of the EU. Likewise, EU wants to keep AI safe, trustable, and respectful for human rights as indicated in the White Paper.

1.2.3.2. EU Charter of Fundamental Rights (2000): The EU Charter of Fundamental Rights is a document dealing with the values to which the EU is committed. Accordingly, the EU aims to provide a peaceful and prosperous future for its citizens, and in order to do so, it is committed to a set of common values. As it is said in the preamble of the Charter, the Union places individuals at the centre of its activities, which is also the basis of the EU's AI approach. In the Charter it is dictated that Union's aims are to enhance wellbeing of the its citizens and to create a peaceful

area to live for them. Under Title II of the Charter Article 7 and Article 8 covers the following issues respectively; respect for private and family life, and protection of personal data (Official Journal of The European Union, 2012b). As it has already been discussed and will be discussed that the protection of personal data is very critical for AI. There may be situations such as obtaining, storing, and processing our personal data without consent. There may be situations such as obtaining, maintaining, and storing our personal data without our consent. AI applications like Deepfake, or AI machines that use automated decision-making, and hidden cameras used for mass surveillance contradict the fundamental principles enshrined in the EU Charter, such as the privacy of our personal data and respect for our private life.

1.2.3.3. Lisbon Treaty (2009): Treaty of Lisbon is an important treaty that amended the EU's governing treaties. It came into force on December 1, 2009. Article 2 and Article 6 of the Lisbon Treaty are significant provisions that outline key principles and objectives of the EU (Official Journal of The European Union, 2012a). Article 2 of the Lisbon Treaty sets out the fundamental values and principles of the EU, emphasizing human rights, democracy, and the rule of law. According to Article 2; the Union's basis lies in upholding principles such as honoring human dignity, promoting freedom, supporting democracy, ensuring equality, upholding the rule of law, and respecting human rights, including those of minority groups (Official Journal of The European Union, 2012a). These principles are shared among the Member States in a society where diversity, fairness, tolerance, justice, unity, and gender equality are prominent. On the other hand, Article 6 outlines the EU's goals and approach to its external relations, including promoting its values, maintaining peace, and engaging in international cooperation (Official Journal of The European Union, 2012a). Moreover, Title II of the Lisbon Treaty includes the principles of democratic governance of the Union. These articles are crucial in defining the core principles and international role of the EU.

1.3. MALICIOUS USES OF THE AI

As it was mentioned in the previous section, AI is a rapidly developing field and has brought many innovations to our lives, and perhaps it prepared us for the space age (Leonhard, 2020; 22). In addition to the many innovations, conveniences, and opportunities it has added to our lives, continuously evolving technology has also revealed very serious risks that threaten people's security. There are many publications on how the world's leading companies such as Facebook, Twitter, Netflix, Amazon, Google, Apple, and more have been using technology to analyse their customers, that is, us: humans (Maar, 2020; 11-294). Hence, this has led to the need to protect sensitive data and its collection, and processing. The EU, which set out for exactly this purpose, accepted the GDPR in 2016 and the GDPR entered into force in May 2018. The GDPR emphasizes the need to protect data by design (Ersoy, 2020: 125). Unfortunately, it would not be wrong to say that many of the measures taken to prevent violations of human rights are too late. There are more than enough examples in our history that our personal data has been stolen, processed, and violated. Rowena Rodrigues (2020) has depicted the vulnerable groups regarding the malicious or unethical uses of AI. Rodrigues mentions research where the vulnerability groups have already been addressed. According to her, EquiFrame provides one of the most comprehensive classifications of vulnerable groups, with 12 categories (Mannan et al., 2012). Rodrigues mentions the previous research that was done by Roberto Andorno (2016), Andorno says: "Populations which are particularly prone to being harmed, exploited or discriminated include, among others, children, women, older people, people with disabilities, and members of ethnic or religious minority groups" (Rodrigues, 2020). Rodrigues analyses the sources of vulnerability in 5 groups; physical and technical, social, political, regulatory, and economic. Therefore, Rodrigues suggests three actions to be taken; decreasing the negative effects of AI, building vulnerable group communities, and tackling the root causes of vulnerability. Indeed, researches show that some groups are much more disadvantaged than others, for reasons such as gender, age, race, social status, ethnic origin, etc., and this poses risks to the realisation of human rights.

1.3.1. Abuses Of Human Rights

Algorithms can lead to biased decision-making, social and economic discrimination, and intrusion into our private lives. AI is about making a profit; big companies have been collecting our data without our consent. However, a person's data should not be used without their knowledge and permission. Companies should inform people about the risks, benefits, and alternatives. For example, the first time we visit a website, via a small screen is asked if we accept cookies or not. How aware are we of what authorizations we have given to the other party after clicking the accept option on this screen? The Council of Europe stated in one of its reports that the size of the data collected has reached huge amounts and its unchecked. Moreover, this collected data is concentrated by a small group of leading digital companies (Parliamentary Assembly, 2020: 1-18). These big companies have an opportunity to manipulate people's mind, and decision-making process as in the case of the Cambridge Analytica Scandal⁸ or simply the opposing ideas can be denied by the leading companies which create risks against freedom of expression, and undermine human rights by damaging democracy (Parliamentary Assembly, 2020: 1-18; Wong, 2019). Another example can be given in Myanmar in October 2018, with the fake news that was shared by Myanmar military personnel on Facebook, and the propaganda that led to the ethnic cleansing of the minority groups in Myanmar (Mozur, 2018). Consequently, people have been tracked everywhere by face, voice, and motion recognition technology, which threatens the right to privacy and makes them vulnerable to manipulation. For instance, in 2022 smart robotic vacuum Roomba took photos of a woman in the toilet, and these photographs ended up on Facebook, hence; smart robot vacuum users began to worry about their own safety and security (Guo, 2022).

⁸ Cambridge Analytica is a software and artificial intelligence company that played a major role in Donald Trump's victory in the US presidential election in 2016 by analysing voters' profiles in collaboration with Facebook.

1.3.2. Data Privacy

First and foremost, the regulations should be tightened regarding the usage of personal data, thus algorithms will have less ability to control sensitive data and one more step will be taken for a safer and more trusted AI. EU Charter of Fundamental Rights Article 8 covers the protection of personal data; everyone has the right to access the data collected and to rectify it (Accessnow, 2018). Control over the use of data requires the consent of the owner of the data, people should have the ability to change or remove the collected data. The protection of data is very important the absence of such protection may create unintended consequences such as fake signatures, phishing e-mails (Cheng et al., 2022), manipulation of the voting process, hacked computers, stolen credit card details, and so on (Yampolskiy, 2020). Bruce Schneider who is a well-known security technologist has said “If you think technology can solve your security problems, then you do not understand the problems and you do not understand the technology” (Yampolskiy, 2020). Roman Yampolskiy (2020) contributes to this idea that every security system will eventually fall, if you think your system is 100% safe just wait longer. The institutions of the EU have been dealing with data privacy, data storage, and processing since the 2010s (Rodrigues, 2020). In fact, with the membership of both institutions and the EU to the Global Privacy Assembly⁹, studies have been carried out for data privacy since the 1980s. The ransomware called WannaCry¹⁰, which emerged in 2017, seized 300,000 computers in more than 150 countries, according to Europol's statement, and caused serious problems in countries such as Russia, England, Germany, Italy, and the US¹¹. In addition, facial recognition systems have also been discussed by many researchers and they cause problems in terms of the privacy of personal data. People in China have become hesitant to make financial payments with the face recognition system (Cheng et al., 2022). It should be understood that data security is important not only for individuals but also for social

⁹ In 1979, the first Assembly was held in Bonn, Germany, and has become an international initiative that has been serving for many years with the aim of establishing, implementing and supervising data protection laws in the international arena.

¹⁰ The WannaCry attack is an important cyberattack that demonstrated the global scale and destructive power of ransomware. This incident highlighted the importance of timely security updates and robust cyber security measures to mitigate the risks posed by evolving cyber threats in our history and raised awareness.

¹¹ For details, please see; <https://nabu.com.tr/wannacry-nedir>

security. In 2014, the "One Hundred Years of Study on Artificial Intelligence" examines the effects of AI on societies, and according to this research, one of the areas that will be most affected is public safety (Turkcetin, 2021: 65). As Turkcetin mentioned, in 2018 Nguyen stated that most people are unaware that their data containing sensitive information is being traded (Turkcetin, 2021: 65). In some cases, the data does not even need to be sold or bought, they are available to everyone via open databases. The European Data Portal¹² has discussed the role of data privacy in open databases in a report, while GDPR is another EU publication that has contributed to data privacy¹³.

1.3.3. Unfairness And Discrimination

One of the prerequisites for an AI system that respects human rights is that it is not unfair and discriminatory. There are many researchers who deal with this issue (Rodrigues, 2020; Smith, 2017; Danks and London, 2017; Courtland, 2018; Hacker, 2018; Bostrom and Yudkowsky, 2011; Zeng, 2020; Tükel, 2021: 131-143; Stahl et al., 2021: 374-388). Considering that countries and even different regions within a country do not have equal opportunities to access technology (UNCTAD, 2021), the higher the technology, the greater the injustice, thus unfairness. Unequal access to new critical technologies can exacerbate inequalities. Unfairness and discrimination are often due to bias. Officials stress its importance especially in automated decision-making or machine learning (Klasinc, 2022: 23-27). Josie Young an AI ethicist said when its added new data to the smart bot, it reflects the biases of the teams that were created by (Chin and Robison, 2020). For example, if the data training machines are biased or not balanced, the AI systems that are trained on biased data will not be able to generalise well and will possibly make unfair decisions that can favour some groups over others (Allen and Massolo, 2020). Scholars have argued that sexual bias is widespread around the globe, and girls are particularly more invulnerable in every area of life (Chin and Robison, 2020). According to Chin and Robison (2020), it is seen that the voice of AI

¹² Open database of various data, policy publications, articles, etc. available across the EU.

¹³ For details, please see; https://data.europa.eu/sites/default/files/open_data_and_privacy_v1_final_clean.pdf and <https://citizens-guide-open-data.github.io/guide/4-od-and-privacy>

bots, especially AI intelligent voice assistants such as Alexa, Cortana, Siri, and Google Assistant, belongs to the female stereotype. This is a factor that reinforces gender bias. Previous years ago, Google Translate also has gender-discriminative translation between 2 languages; currently, with the latest updates the roles like maid, firefighter, teacher, and doctor can be translated into both gender (Turkcetin, 2021: 78). Gender discrimination is also common in the field of employment, and today most of the states have eliminated the use of AI in the recruitment process with the proposals of new regulations, because it has been accepted that automated AI decisions are biased and it may be to the benefit of a specific group, or it may be insufficient for decision making fairly (Lankford, 2023). Another discrimination takes place against different races, especially Afro-Americans. Almost all articles mention the disadvantageous position of Afro-Americans in automated credit loan scoring, not only in the financial system but also in the health system (Ledford, 2019; Turkcetin, 2021: 77), education system, and social media platforms (Ghaffary, 2019) also biased against the Afro-Americans (Ledford, 2019; Turkcetin, 2021: 77, Ghaffary, 2019).

1.3.4. Unethical Uses Of AI

HLEG, one of the bodies of the European Commission, started its work for an ethical AI in 2018, and “Ethics Guidelines for Trustworthy AI” was published by HLEG on 8 April 2019 (European Commission, 2019a). The first chapter of the guideline focuses ethical principles of AI in general, and the adoption of fundamental human rights in particular. According to HLEG on AI, the 3 principles that were mentioned in the guideline; lawfulness, ethics, and robustness are indivisible. Some of the key issues that come to mind on AI ethics are as follows; unemployment, inequality, discrimination, and racism. Currently, ethical debates about the use and further promotion of AI have increased. EU policy suggests that ethical AI can be achieved through human control and monitoring mechanisms, however; there are also contrasting ideas that criticize the policies of the EU (Koulu, 2020: 9-46). There are many different opinions regarding AI ethics, while some groups suggest that AI has no morality, some advocate AI as a rational entity that can be moral as well (Chalmers, 2010). To conclude, AI cannot be moral as the creators of AI, human beings, are not

moral in their nature¹⁴ and the world where even robotic insects exist is never the safest place that we can neglect ethical discussions (Chukewad et al., 2020: 1-15).

1.3.5. Cyber Attacks

While technology acts as a catalyst for the development of societies, it makes individuals, societies, and nations much more fragile in many ways, and our adversaries are those who want to exploit our vulnerabilities. As can be understood from the previous sentence, cyber-attacks are not only an issue for individuals but also for societies and nations. Even if there is not an international regime that monitors and controls cyber-crimes in the global level, the EU has been trying to create much more resilient Europe by controlling and applying sanctions to ensure cyber security (Council of the European Union, 2022: 38). The adoption of Convention on Cybercrime (2001), The EU Cyber Security Act (2019), Digital Europe Program (2020), and establishment of Cybersecurity Competence Centre, Cybersecurity Atlas, Horizon Europe, Cyber Security Conference Platform, ENISA and more helps EU to protect its citizens and entities against cyber crimes (Council of the European Union, 2022).

Nevertheless, history has witnessed many devastating cyber attacks, including the Morris Worm, Calce (a.k.a. MafiaBoy), Melissa Virus, WannaCry Ransomware, Mydoom viruses, and more. Some of these viruses have caused massive damage to some of the world's most popular websites (Amazon, E-bay, Google, etc.), but they have also managed to infiltrate government agencies and even took time to be detected. Cyber-attacks are of great importance for the great powers; the US is on high alert for cyber-attacks from Russia (Euronews, 2021). In addition, cyber attacks are increasing every day, for example, at the time of writing this sentence, the number of cyber-attacks is around 2 million 850 thousand, for those who are more curious, can access the live map showing the cyber attacks from the official website of the CheckPoint¹⁵.

¹⁴ Thucydides, Niccolò Machiavelli, Thomas Hobbes, Jean-Jacques Rousseau, and Max Weber, Hans Morgenthau are among the founders of realist theory. One of the main features of realism is that it recognises that human nature is essentially evil and selfish, according to which human beings are primarily self-interested in all circumstances.

¹⁵ One of the leading companies that offers solutions to the cyber security related issues and cyber-attacks.

In conclusion; cyber-attacks are the reality of our age, technology has brought us hundreds of benefits as well as new threats.

1.4. CONCLUSION

To summarise the foregoing briefly, in some cases, the unexpectedly rapid development of AI and the increasing dependence of individuals on technological devices and systems facilitate the violation of human rights. In particular, individuals who are not sufficiently aware of these issues become much more vulnerable to cyber crimes and hacking. There is a high probability that personal data may be misused without consent by malicious actors and groups. In addition, human nature cannot always remain objective and is shaped by biased data, and this means that AI emerges with biased data and a biased creator at the design stage. The EU, on the other hand, stands by its core values and regulates the AI and technology-related fields harshly. However, while the EU's tough regulatory approach has provided individuals with more freedom and a more democratic environment, it has put the EU in a weaker position in the international system.

Data security and privacy are very important for individuals, but also it has become a much more global problem that concerns societies and nations. America's aggressive stance against China and Russia also shows how serious cyber-attacks can be. The EU is closely following these developments and is committed to protecting both the rights and freedoms of individuals and its citizens. Therefore, the next section will try to show the consequences of too many regulations restrictive effects by comparing the EU with the US and China.

CHAPTER TWO

THE GLOBAL RACE FOR AI

2.1. INTRODUCTION

AI is a highly promising sector for the states, and it has created a new area for global leadership; technological leadership will determine who will lead the world, and it has also determined who will take the upper hand in the AI race. According to Suedekum (2019), Europe has faced a set of problems such as demographic change, climate change, rising inequality, and technological change. Perhaps the most important of these problems, and the one most relevant to this research, is "technological change". It is known that Europe is aging and it creates a crucial risk for the sake of the European future. EU with several publications has set its goals of becoming a global leader in the global AI race. However, research shows that the EU has lagged behind in the global AI race, losing priority to the US and China (Suedekum, 2019; Castro and McLaughlin, 2021; Samsun, 2021). Of course, there are those who advocate this view, but there are also those who question whether Europe is losing the race, and there are even studies on the issues where the EU is ahead (Sönmez, 2020: 603-606). Studies generally address similar indicators, such as investment in AI, number of AI companies, qualified workforce in this field, hardware capacities of governments, available data centers, number of research and articles published in this field, government supports, and so on. Moreover, almost every category demonstrates the superiority of the US and China over the EU.

When it is looked at the five biggest companies of the world; Apple, Amazon, Alphabet (Google), Facebook, and Microsoft, none of which belongs to Europe. This data is quite frightening for the EU, given that there is an argument that big corporations ruling the world (Korten, 2015; Fuchs, 2007). In 2018, under the Presidency of Donald Trump, the trade war between the U.S. and China has started and it has still continued. According to Suedekum (2019), the EU will benefit it from that war in the short run, but in the long run, it means that nobody sees the EU as a major threat in the global AI war. The indicators show that China has the capacity to catch up with America by 2030 or sooner; on the other hand, Europe is not seen as a

big player in the game for technological leadership. In 2018, an interview with Emmanuel Macron demonstrates his welcoming position to the AI, he indicates his aim in the following five years would be to catch up with U.S. and China governments in the AI race (Thomson, 2018). 2023 economy forecasts also show that the biggest economic growth will be seen in the Asian economy while the weakest one will be seen in the European region (World Economic Forum, 2023). Another indicator is the budget allocated by regions to AI and technology-related areas. In 2023 single market innovation and digital transformation allocation of the EU budget's commitment are barely above 20 million € (European Commission, 2022a), while the U.S. will make a tremendous amount of investment to preserve its leader position in the global AI war; the U.S. budget allocates 7.8 billion dollars for research and innovation, 880 million \$ to enhance technological capability, 10 million \$ to build and strengthen the national cybersecurity (The White House, 2023). The People's Republic of China allocated a budget of 6.5 billion yuan for scientific and technological development in 2023, an increase of almost 45% over the previous year (The State Council Information Office The People's Republic Of China, 2023).

To understand and make judgments about the EU's AI policies, it is useful to consider the examples of misuse of AI mentioned in chapter one and the extent to which it can be damaging even to democratic regimes. In the next section, the AI policies of the US, China and the EU and their current status regarding the global AI race will be examined comparatively under the relevant sections. The reasons why the EU is lagging behind in this race will also be analysed and the effects of the human-centered AI approach will be shown.

2.2. UNITED STATES AS THE LEADER OF THE RACE

America has been a hegemonic power for many years, especially in the post-Cold War period, when it clearly defeated its Russian adversary. In fact, concepts such as coca-colonization and Mcdonaldization have entered the literature, indicating American hegemony in the international arena. This leading position of the US has also been extended to the fields of technology and information technology (IT), almost three decades ago David Nye referred to American hegemony in technology by coining

the term “technological sublime” (Nye,1996: 17). Under Clinton and the second Bush administrations, it was believed that America's technological leadership would lead others to emulate it. However, the PRC's (Peoples Republic of China) huge success in IT and digital realm has been a game changer. Currently; even though the US technological sovereignty is an unquestionable fact, the American technology industry has been facing serious challenges from the PRC (Atkinson, 2021: 1-14; Glasze et al., 2022: 929; Castro and McLaughlin, 2021; Brattberg et al., 2020; Kennedy, 2022; Larsen, 2022; Salitskii and Salitskaya, 2022: 262-267; Zhang et al., 2022: 1-12). Given that, according to 2022 data, the PRC's population is almost 4 times that of the US, it is quite possible that the PRC will catch up with the US by using its population power. According to Atkinson (2021), the US should implement a grand strategy for maintaining its technological leadership and constraining its adversaries, namely, the authoritarian regimes of China and Russia. At the same time, America's other main objective should be to prevent its enemies from getting stronger through global cooperation, and the most suitable target for global cooperation is the EU. The new initiatives were taken with the proposal and foundation of The Trade and Technology Council (TTC) as a symbol of American and European cooperation in governing technology (Larsen, 2022; American Leadership Initiative, 2021). The analysis of official US documents and reports illustrate that the US always aims to be one step ahead of its adversaries and should pursue aggressive policies if necessary. A report that was published by the American Leadership Initiative (2021) argues the future of the American technological hegemony and it listed the desirable and undesirable scenarios for the American digital future: One undesirable scenario is that EU regulations prevail and the US is left out of the arena (American Leadership Initiative, 2021). However, according to me, this is not quite possible; because the American AI companies are much more than the European ones (Castro and McLaughlin, 2021), and this has been decreasing the global power and influence of the European region in the international system. According to scholars investing in AI, can boost the industry of the nations and contribute to the further development of the economies by increasing productivity, but the EU seems to be willing to miss that opportunity. In particular, the EU's loss of young talents to the US and the relocation of the headquarters of start-ups to the US are two of the strongest indicators of this (Castro and McLaughlin, 2021).

For years, America's aggressive policies and unilateral actions are taken when necessary maybe was key to the success of the global war on AI. The attempts started to be taken place, especially during the World War years, even the deployment of atomic bombs on Japanese cities Hiroshima and Nagasaki were the products of scientific research and innovations. From this point of view, the US has always gave importance to the R&D so as to maintain its national security and enhance its relative power in the international system (Ham & Mowery, 1995: 91). If it is mentioned America's technological leadership today, it is because of the aggressive policies it has pursued over the years to maintain its relative power. Especially, after China joined the World Trade Organization (WTO) in 2001, its rapidly developing and growing economy was perceived as a serious threat by the US. During the Obama period, Huawei along with ZTE, started to be seen as major threats to American national security. In recent years, the Trump administration has imposed several bans on Chinese technology companies and products, and the Biden administration has continued the restrictive policies towards China. The aim of America is to isolate Chinese big tech companies in the global market (Kornbluh and Trehu, 2023: 1-20); restricting Chinese access to semiconductors¹⁶ and high technology products, so yes it is a part of the “Trade War”¹⁷. In 2017, the Association for the Advancement of Artificial Intelligence (AAAI) conference, which has been held annually since 1980, caused disagreements, which can be seen as an example of the US aggressive policies against China (Zhang, 2017: 1-5).

Huawei alone is a threat to the US, and the fact that it is one of the few companies in the world that can produce chips for 5G phones. Indeed, American companies are prohibited from selling any technology to Chinese firms. Comparing America's aggressive policies with those of the EU, it is seen that the EU pursues a

¹⁶ Semiconductors are perhaps one of the most important building blocks for the development of artificial intelligence and advanced technological products. The Semiconductor Industry Association says semiconductors are indispensable in many sectors, from education to health, computing to transport, military to clean energy.

¹⁷ Trade War is the name given to a series of aggressive and deterrent policies against China that emerged in the Trump period. Trump's aim was to cut China's rising power by preventing both American products and European products from entering the Chinese market in the face of China's growing economic power. In addition to these policies, additional import taxes and sanctions are also part of the trade war.

much softer policy and, contrary to the Democratic Peace Theory¹⁸, the European values places human beings at the center of all policy areas for all nations. Recently, the EU cooperates with the US under the TTC, but it should be noted that in 2018 the European Parliament criticized US's "America First" policy (Kornbluh and Trehu, 2023: 1-20). As Kornbluh and Trehu mentioned in their report(2023), many scholars argue that technology is the key to the global competition in our age, and the history has been witnessing the most striking moments of this race in the events between China and America. Especially, the US followed more aggressive policies (applying additional import taxes, banning most Chinese tech companies in the global market, export controls, and so on) than China in the context of global competition and China's accusation of the US for "weaponization and politicization of science and technology by blocking access of China and Russia" supports this idea. In the next section, China's policies to prevail in the global digital race and its attitude toward the United States will be discussed in more detail.

2.3. CHINA AS THE SECOND LEADER OF THE RACE

China has had a communist political system, with the leading role of the Chinese Communist Party, for many years, unlike the Western part of the globe. Especially after the 1980s and early 1990s, China started to open its economy to foreign investment, and to the global market, consequently has experienced unprecedented economic growth (Tseng and Zebregs, 2022: 2). Recently, China has made significant strides in the field of AI and has emerged as a major player in the global AI race. Thus, it has taken its place as America's strongest competitor in the AI race. The Chinese government has recognized the strategic importance of AI and has implemented policies to promote its development, with cooperation with tech giants being the strongest indicator of this. The "Made in China 2025" initiative, launched in 2015, aims to make China a global leader in high-tech industries, "The Internet Plus" initiative also aims to restructure Chinese growing economy from the traditional way to digital, "New Generation Artificial Intelligence Development Plan (2017)" clearly

¹⁸ According to the democratic peace theory, democratic states do not go to war with each other, but they may go to war to bring peace and democracy to non-democratic regions. For more information also see; <https://www.britannica.com/topic/democratic-peace>

sets out its strategies and policies to become a global leader by 2025 (The State Council The People's Republic Of China, 2016).

The government has provided significant funds, incentives, and supportive regulations to promote AI research and development. The fact that the Chinese government works with big techs and that big techs have access to a huge data pool is one of the biggest indicators of the importance the state attaches to AI. In 2017 “national AI team” has been established by the Chinese Ministry of Science and Technology to lead National AI Open Innovation Platform and Baidu, Alibaba, Tencent, and speech recognition company iFlytek have been appointed to lead separate areas of AI, the Ministry developed this practice in the following years, and companies such as Huawei, Jingdong and Xiaomi joined in (Zeng, 2020: 96 ; Tougaard, 2021). Additionally, Zeng (2020) mentions the positive effects of Chinese media on public opinion, rather than emphasizing its malicious use as in the case of the EU. The Chinese government's pursuit of such policies is not only about technological advancement but also about using AI as a tool to strengthen the communist authoritarian party rule (Kania, 2017: 8; Zeng, 2020: 1441-1459). Considering the surveillance system in China, the billions of cameras installed in major cities, and the social scoring system that has become a popular topic, China's approach to AI is in stark contrast to the Western world, especially to the core values of EU. According to Zeng (2020), Chinese society is not as aware of individual and social rights as Europeans, and this provides the Chinese government a comparative advantage (Zeng, 2020). For instance, recent research that was carried out by Deng and his friends has shown that US people have perceived their personal future negatively, while Chinese people have remained neutral (Deng et al., 2022: 87-100). Other researchers point out that China has a comparative advantage over the US and Europe in some areas such as population, language, young talent pool, and generally its unique culture. As Borek and Prill (2021) have emphasized the importance of culture in the digitalization process, Chinese culture also contributes to the developments in the technological field.

2.3.1. AI Applications That Threaten Individual Rights In China

As mentioned in the previous sections, it is known that AI applications can threaten individual and social rights, intentionally or unintentionally; they can even threaten democracies. China's authoritarian approach allows for agile and rapidly developed technological systems, but it raises concerns about data privacy, surveillance, and potential misuse of AI technologies. Especially since 2015, China's technological advances and steps towards becoming a global technology leader have attracted the attention of not only the US but also the Western world (Shi-Kupfer and Ohlberg, 2019: 1-58). China's social scoring system and facial recognition system have been strongly criticized by Europe (Ciancaglini et al., 2020), for instance in the panel of “futureu” citizens of the EU has harshly criticized such policies of China by arguing that the EU should take regulatory steps to prevent this application in the European region (Conference on the Future of Europe, 2022). In 2019, Wright explained that Chinese digital authoritarianism will escalate the conflicts between the regions in which democracy has ruled and China. In the same year, Daniel Araya argued that relentless technological growth would minimize the need for human force in China, enabling the socialism envisioned by Marx and leading to Fukuyama's "End of the History"¹⁹ thesis.

In China, facial recognition is used to fight child trafficking and also to identify individuals who may pose a threat to national security, such as terrorists. In 2018, the number of people per camera was 4.2, while today it is assumed to be as low as 2. To be honest, I felt like I was living in George Orwell's 1984 when I analyzed the AI governance in China from a numerical point of view. Big brother is always watching us, and there is no escape, I thought. For example, in 2019, schools in China started to use electroencephalography (EEG) systems and headbands on students. Although the relevant ministry announced that this practice was intended to measure students' concentration levels and raise more successful generations; parents were very concerned about their children's data privacy and security. Finally, due to the reactions

¹⁹ In 1989 Francis Fukuyama published his world-famous work, which has remained influential for decades. "The End Of History?" has been included in the literature as a theory in itself. This view argues that Western values will dominate the world, that there will no longer be any opinion that will stand against liberalism, and that the world will come to the last point with the triumph of liberalism. For more information also see; <https://www.jstor.org/stable/24027184>

from both the students' families and global social media, this practice was soon abandoned (Liu, 2019). Another drawback of social scoring, surveillance, and headbanding is the problem of biased AI. Consequently, the widespread use of AI in social and public spheres can lead to unfairness, and a culturally flawed approach in China, like the racist approach in the US, may have stuck to the algorithms which cause unintended consequences. Recently, the EU has taken its steps clearly; the US aims to cooperate with other countries to stop China's rise to power, including with the EU. But with the new export bans, the EU needs a much clearer strategy on Chinese digital policies (Gehrke and Ringhof, 2023).

2.4. EUROPEAN UNION AS THE THIRD LEADER OF THE RACE

Studies on the global AI race and technological leadership have shown that the EU is lagging behind the US and China in many sectors (Samsun, 2021: 24-25). In particular, it is argued that the EU's regulatory approach can be a hindrance to development and innovation (Ersoy, 2020: 49-50; MIT Technology Review Insights, 2020). In fact, the purpose of this study is to show that the regulations that the EU has adopted and enacted so far, the approach adopted by the government, and the question marks in citizens regarding their privacy, prevent the development of AI. In a report published by McKinsey, one of the world-renowned consulting firms, in September 2022, the EU's technological gap was mentioned and it is said that this is a benchmark that will affect all sectors from economy, finance, and tourism to healthcare. The indicators of McKinsey's research have shown that Europe is growing more slowly than the US and China, and is gradually moving from an advantageous to a disadvantageous position (McKinsey, 2022). In 2022, Creemers and his friends argued that the EU is heavily dependent on the US and Chinese software industry. Both of the aforementioned studies point out that falling behind in the AI race would entail a loss of international power and a sacrifice of sovereignty, and also there is a common view on this (Brattberg, 2020: 35-40). The EU is also aware of these challenges and is trying to find solutions. However, on the other hand, the EU argues that the EU should stick to a set of rules and values and that investments and support in AI should be in line with the core values of EU (Official Journal of the European Union, 2022a); the core

values that are demarcated in the Convention for the Protection of Human Rights and Fundamental Freedoms (1950), EU Charter of Fundamental Rights (2000) and the Lisbon Treaty (2009) (Europa, 2023). Convention for the Protection of Human Rights is a body to establish for creating binding rules and implementing these set of rules for the individuals that are mentioned in the Universal Declaration of Human Rights “such as the right to life or the prohibition of torture, and certain rights and freedoms which can only be restricted by law when necessary in a democratic society, for example, the right to liberty and security or the right to respect for private and family life” (European Court of Human Rights, 2022). The Charter of Fundamental Rights of the European Union describes the citizens’ rights and freedoms by placing human dignity, freedom, equality, solidarity, and the rule of law at the very center of the EU values. Article 8 of the Charter covers the protection of personal data which is a highly critical issue in terms of AI regulations. Also, Article 21 of the Charter covers the non-discrimination principle, which is also very problematic in processing AI, as discussed earlier biased AI machines can come up with discriminative results based on sex, gender, age, religion, race, or ethnicity. Furthermore, Article 3 of the Lisbon Treaty has laid out the aims of the EU as follows:

“The Union's aim is to promote peace, its values and the well-being of its peoples... In its relations with the wider world, the Union shall uphold and promote its values and interests and contribute to the protection of its citizens. It shall contribute to peace, security, the sustainable development of the Earth, solidarity and mutual respect among peoples, free and fair trade, eradication of poverty and the protection of human rights, in particular the rights of the child, as well as to the strict observance and the development of international law, including respect for the principles of the United Nations Charter²⁰.

According to some scholars European role in the AI age is to lead the regulations, and control the world from the regulatory perspective (Brattberg, 2020). While the EU is trying to cooperate with the other states to monitor and control the

²⁰ Official Journal of the European Union, “Consolidated Versions Of The Treaty On European Union And The Treaty On The Functioning Of The European Union” 07.06.2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12016ME/TXT&from=EN>, (29.06.2023)

compliance of the regulations which promote human rights and privacy, the US is trying to cooperate with the EU and to isolate its adversaries such as Russia and China, and also to prevent the EU winning the AI race and the AI world dominated by the regulations (Kornbluh and Trehu, 2023: 1-20).

In 2019, the Center for Data Innovation published a report comparing the US, China, and the EU in the global AI race (Castro et al., 2019). In 2021, Daniel Castro and Michael McLaughlin revisited this research with updated data and according to the current data, the US is the leader in 4 of the 6 categories (talent, research, development, hardware, adaptation, data) and China is the leader in 2 of them. The EU has not been able to gain any place in these 6 categories (Castro and McLaughlin, 2021). In 2015, the EU ranked first in the world in research on AI, gradually decreasing numbers and in 2018 led Chinese victory for the first time. Although 2018 data is not very up-to-date when it comes to technology, it can help us to make predictions about the ongoing process. For example, in 2021 the report that was published by Mercator Institute for China Studies (MERICS) argued that Europe is highly dependent on the Chinese semiconductor market (Kleinhans and Lee, 2021). Unfortunately, the EU has also lagged behind in the telecommunications sector (Bohlin and Cappelletti, 2022). The ideas of Jens Suedekum (2019), which were not very different from the MERICS report, dictate that Europe is highly dependent on foreign economies in software and hardware technologies. (Suedekum, 2019). For example, in 2020, only 10% of the world's 1 trillion chips were produced in the EU (European Commission, 2022b). After the 2022 global chips crisis, the EU started to take this issue seriously which is clearly seen from the Chips Survey and Chips Report conducted and published in 2022 and in February 2022 with the proposal of the Chips Act (European Commission, 2022c). Another crucial indicator is the number of supercomputers and the ability to invest in cloud systems (Castro and McLaughlin, 2021). However, the GDPR that entered into force on 24 May 2016 is highly constraining the business and researchers (MIT Technology Review Insights, 2020). Perhaps this is why the EU is losing talented researchers and scientists to other regions, especially to the US, because the recording of data has always been a problem in the EU, as stipulated in the GDPR. The EU is not wrong to restrict the storage and usage of data and to emphasize the consent of

citizens. The EU's rightness becomes more apparent when the malicious uses of AI are taken into consideration which were explained in Chapter One.

2.5. CONCLUSION

Currently, the EU has faced a set of crises, and technological change poses a crucial risk to Europe's future, given its aging population. The EU has set goals to become a global leader in the AI race, but research suggests that it has fallen behind the US and China in this regard.

Various studies assess indicators such as AI investment, the number of AI companies, the skilled workforce, government support, and research publications to compare the progress of different regions. In almost every category, the US and China demonstrate superiority over the EU. The fact that none of the world's five biggest companies (Apple, Amazon, Alphabet, Facebook, and Microsoft) are based in Europe is seen as a concerning factor, considering the influence of large corporations in global affairs.

To evaluate EU AI policies, it is important to consider examples of AI misuse and its potential damage to democratic regimes and the fundamental human rights. In this section, examples of misuse of AI are shown and the EU's approach to AI was discussed in comparison with China and the US by considering the core values that are indispensable for the EU.

CHAPTER THREE

AI REGULATIONS IN EUROPE

3.1. INTRODUCTION

The EU was established to strengthen cooperation among European states to ensure global stability and peace in the post-war period. Over time, it has kept pace with the changing trends in the world and has always managed to remain strong. The Brexit process has been challenging for the EU, but it has managed to overcome it. Another challenge was Covid-19, millions of people lost their jobs due to the outbreak of it. Even if some markets have benefited from the disease ,platform workers whose numbers have increased because of the increasing demand for food delivery, most of the economies came to a halt, and eventually, unemployment rose suddenly (Galasso and Foucault, 2020: 4). Spain and Italy were the countries which coronavirus hit harder, and they thought that EU did not respond quickly and accurately to mitigate the effects of Covid-19 in these two states (Ilik and Shapkoski, 2020: 30). After the pandemic, Russia's invasion of Ukraine has become another crisis for the EU, especially the EU's dependence on Russia in energy has put the EU in a much more fragile international environment (Misik and Nosko, 2023: 1-5; Estrada and Koutronas, 2022). In response to continued military aggression in Ukraine by Russia, the EU implemented further sanctions in February 2022. These sanctions specifically focused on the energy, transport, technology, and financial sectors, and also included restrictive measures targeting individuals (Official Journal of the European Union, 2022b).

Today, one of the most important issues to overcome is to have the power and capacity to be a leader in the AI race. The EU places a strong emphasis on ethical considerations and human-centric AI development. Almost all the European states have published their own digital strategy documents based on the core values of the EU which can be seen in a Table 1. From the table, it can be deducted that all the European states have a plan for the development of AI in line with the EU's goal of becoming a global leader in the AI race.

Table 1: European States' National AI Strategies

Country	Strategy Status	Date	Related documents
Austria	Published	August 2021	Annex to the Strategy
Belgium	In progress	TBC	Strategic Report
Bulgaria	Published	December 2020	Digital Transformation Strategy
Croatia	In progress	TBC	
Cyprus	Published	January 2020	Competitiveness Report
Czech Republic	Published	May 2019	
Denmark	Published	March 2019	Digital Growth Strategy
Estonia	Published	July 2019	Taskforce Report
Finland	Published	October 2017	Interim Report
France	Published	March 2018	Strategy Update
Germany	Published	November 2018	Strategy Update & Data Strategy
Greece	In progress	TBC	Preliminary Strategy
Hungary	Published	September 2020	
Ireland	Published	July 2021	Open Data Strategy
Italy	Published	September 2020	Strategy Update & Open Government Action Plan
Latvia	Published	February 2020	
Lithuania	Published	March 2019	
Luxembourg	Published	May 2019	
Malta	Published	October 2019	Roadmap 2025 & Ethical Framework
Netherlands	Published	October 2019	AiNed programme
Norway	Published	January 2020	Our New Digital World
Poland	Published	December 2020	Open Data Guide

Portugal	Published	June 2019	Strategy for Advanced Computing
Romania	In progress	TBC	Draft National Strategy
Slovakia	Published	July 2019	Digital Transformation Action Plan & State R&D Programs
Slovenia	Published	May 2021	
Spain	Published	December 2020	Digital Agenda & Digital Skills Plan
Sweden	Published	May 2018	
Switzerland	Published	December 2019	Artificial Intelligence in Education

Source: European Commission, (2021)

However, because of ethical considerations, the overall position of the EU in the AI race does not look very promising. Rapidly advancing technology and AI have brought with them the unauthorized collection, storage, and even sale of personal data. Recognizing how dangerous this can be, the European states aim to have regulations and to be able to monitor them, not only in their own territory but wherever possible (Council of Europe, 2018). The EU's humanitarian AI approach starts with regulations, but it also hinders the development of new technologies due to the required compliance of data protection (Samsun, 2021: 29; Ersoy, 2020: 49). Kramer and Hoar (2020) argue that organisations and companies have to comply with a set of laws and regulations. The EU is the first region that should come to mind when it comes to regulation. It is also a pioneer in the regulation of AI (Moraes et al., 2020: 159-172).

In 1972, the European Conference of Ministers of Justice stated that national legal arrangements would not be sufficient and that international regulations were essential. In 1981, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, known as Convention 108, was signed by the Council of Europe member states. This convention is the first legally binding document in the realm of data protection (Council of Europe, 2018). After 1981,

Convention 108 was revised in 1999, 2001, and most recently in 2018 according to the changing needs of the world, and is still valid today. This convention, which deals with the fair collection of data, the length of storage, and sensitive data, applies to all persons residing in the territory of the signed parties²¹. According to the studies on law and regulations; robotics law is intertwined; robotics law, which centers on personal rights and fundamental freedoms, also covers regulation in many areas from criminal law, labor law, and patent rights to robot liability (Ersoy, 2020).

In the next section, the AI regulations and initiatives of the EU will be analysed that are considered to be restrictive in terms of the development of AI. This study aims to prove that the EU's human-centered approach to AI and its regulatory power leaves it behind in the global AI race. Namely; the GDPR, HLEG's Ethical Guidelines on AI, and Policy and Investment Recommendations on AI, European AI Alliance works, White Paper on AI, AI Act, and Proposals For An AILD. In light of these documents, the EU's AI policies and future goals will also be analysed and the EU's human-centered AI approach will be critically examined.

3.2. GENERAL DATA PROTECTION REGULATION (2016)

The GDPR²² was adopted by the EU in 2016 and replaced the Data Protection Directive, which came into force in 1995 (European Data Protection Supervisor, 2018). The GDPR consists of 11 Chapters and 99 Articles and is perhaps the first international instrument in the field of data protection to come into force (Moraes et al., 2020: 159-172). According to Kramer and Hoar (2020), the idea behind the GDPR dates back to the OECD, which was established after the Second World War. The Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data published by the OECD gave rise to the idea of GDPR (Moraes et al., 2020: 159-172). Regional regulatory differences were a major problem for the EU and one of the main objectives of the European Commission is to ensure perfect unity and cohesion among member states (Roksandic et al., 2022: 23-27). With the GDPR, the norms used by 27 countries will be unified (Council of Europe, 2018) data transferred

²¹ For more information about Convention 108 and its modernization process, please see; <https://www.coe.int/en/web/data-protection/convention108/background>

²² To access the current version of the GDPR, please see: <https://gdpr-info.eu/>

to other countries will be controlled, and individuals will have a say over their data usage and processing (Moraes et al., 2020: 159-172). While the GDPR is binding for EU countries, it is also binding for parties dealing with data on European territories (Seldağ and Lutz, 2022: 1267-1292). Article 5 of the GDPR covers the processing of personal data, according to it the processing should be lawful, fair, transparent, accurate, and accountable, also it should limit the purpose, the data is used, and storage. Article 7, covers the concept of consent and if the data is processing based on consent, all the necessary requirements should be fulfilled before processing. Article 16, Article 17, and Article 18 of the GDPR covers the rectification and erasure, according to which, the owner of the personal data shall have a right to rectify or right to be forgotten. GDPR also covers the restrictive obligations and responsibilities of the data controller or processor, which can be seen as a burden for those who work in a data-driven sector (Samsun, 2021: 29).

When it is compared the US and the EU in the field of data protection, it is seen that the US is motivated by individual needs and money (Tallberg et al., 2023), but on the contrary, the EU had already taken steps for more unified regulations (Moraes et al., 2020: 159-172). According to Klasinc (2022), creating common approach is also much more harder and it presents a problem for the EU. Clearview AI, a private American software company, stores more than 10 billion photos in its database, including data of European citizens (Roksandic et al., 2022: 23-27). It is therefore very important for the EU that the regulations are internationally adopted, as it is unlikely that there will be sanctions for data transferred to third parties. In addition, while the US Chief Privacy Officer (CPO) does not derive his/her rights from the law, with the GDPR, the Data Protection Officer (DPO) derives his/her official rights and powers from the law (Privacy Europe, 2022). If the use of data is not regulated and monitored, AI applications may produce unfair outcomes because they are man-made. That is why, monitoring the compliance of GDPR rules is crucially important (Seldağ and Lutz, 2022: 1267-1292). The European Data Protection Board (EDPB), and European Data Protection Supervisor (EDPS) were established as independent bodies under the GDPR to maintain the functioning of data protection (Seldağ and Lutz, 2022: 1267-1292). As a result, with the GDPR, the EU has introduced a more comprehensive regulation both in terms of content and territory. Data subject consent, the right to

erasure, and the right to be forgotten; or bodies such as the DPO, EDPB, and EDPS established to monitor the GDPR, or the regulations about the third parties, show that the EU takes this issue seriously.

3.3. HIGH LEVEL EXPERT GROUP ON AI (2018)

In 2016, the European Commission decided to establish expert groups of state or private sector employees, temporary or permanent, in specific areas of expertise in legal documents C(2016)3301 and C(2016)3300 (European Commission, 2016). In Communications of April 25, 2018, and December 7, 2018, the European Commission set out its vision for AI as the following "ethical, safe and cutting-edge artificial intelligence made in Europe" (European Commission, 2019a). In these discussions, the Commission identified three key objectives: to boost AI with public and private investments, to be prepared for socio-economic challenges, and to have ethical and legal regulations that uphold EU values (European Commission, 2019a). Accordingly, HLEG on AI was established to support and realize the Commission's visions in the field of AI, more specifically HLEG on AI was founded to prepare two documents on AI; one is *Ethical Guidelines of AI*, and the second one is *Policy and Investment Recommendations on AI* (European Commission, 2019a). The expert group submitted its first draft in December 2018 (Koulu, 2020: 9-46), followed by more than 500 policy recommendations, and on April 8, 2019, the HLEG on AI published the *Ethics Guidelines for Trustworthy Artificial Intelligence* (European Commission, 2019a). According to HLEG on AI, AI systems need to be human-centered, based on a commitment to their use in the service of humanity and the common good, with the aim of advancing human well-being and freedom (European Commission, 2019). As mentioned in chapter one, while AI systems offer great advantages, they also pose risks to the security and privacy of people and even societies as they work with data. HLEG ,therefore, aims to maximize the benefits of AI systems while at the same time preventing and minimizing their risks. This document refers to trustworthy AI as lawful, ethical, and robust (European Commission, 2019). Firstly, human control is a prerequisite for trustworthy and transparent AI, as Munro and Monarch (2021)

discussed in the book named *Human-in-the-loop-machine learning*²³ (HITL-ML) existence of humans in the process of creating a new AI system is highly critical, otherwise, people can face with a biased intelligent machine, especially against gender or ethnically biased and discriminator against women or ethnic minority groups (Monarch and Munro, 2021). Secondly, AI systems should be technically robust and safe, according to HLEG AI systems should have a fall-back plan which means in case of any failure, there needs to be a plan, a guidance to recover (European Commission, 2019). Thirdly, the document makes emphasis on data privacy and governance; under the conditions of the absence of privacy and data governance, people may see stolen identity details, credit cards, or ransomware personal computers that contain sensitive information (Yampolskiy, 2020; European Commission, 2019). Fourthly, AI systems should be diverse, non-discriminative, and fair (European Commission, 2019). However, in practice, we see that this is not the case and people are not equally fortunate in accessing AI or advanced technologies, that they are discriminated against on the basis of ethnicity, race, gender, age, etc. Justice is not fully achieved, because the creator of AI is human. Fifthly, AI systems should be accountable and transparent in order for people to trust these stranger machines. If people do not know the collected data is used in which chain or for which purpose they may not be able to trust the AI machines and do not share their personal information. Finally, technological advancements should enhance societal and environmental well-being rather than undermining it, as highlighted in The European Green Deal²⁴ (European Commission, 2023).

²³ For more information, please see https://www.google.com.tr/books/edition/Human_in_the_Loop_Machine_Learning/W2U0EAAAQBAJ?hl=en&gbpv=1&dq=human-in-the-loop+machine+learning:+active+learning+and+annotation+for+human-centered+ai+reviews+pdf&printsec=frontcover

²⁴The EU's goal is to achieve climate neutrality and to be the first continent in the world to do so. These proposals aim to ensure that all sectors of the EU economy can meet this challenge. Setting out a trajectory for the EU to achieve its climate goals by 2030, the proposals emphasise fairness, cost-effectiveness and competitiveness.

3.4. EUROPEAN AI ALLIANCE (2018)

The European AI Alliance is an initiative set up by the European Commission in 2018 to create an open policy dialogue on AI, gathering diverse views through online events and meetings (European Commission, 2022d). The European AI Alliance was initially established to oversee the two documents that HLEG was responsible to publish. However, after the HLEG mandate ended, it became an open forum for sharing work and policy recommendations to support the Commission's concept of trustworthy AI (European Commission, 2022d). With more than 6000 participants, the Alliance also engages with European bodies as well as international organizations (European Commission, 2018b). The Alliance held the first AI Alliance Assembly on 26 June 2019, the second on 09 October 2020, and the third on 14 and 15 September 2021 (European Commission, 2022d). The main objectives of the Alliance is about the developments and investments on AI, as parallel with the aim of the Commission to become a global leader on AI. However, the current situation of the EU is far more away from being a global leader in the field of AI, these discussions have also started to take place among EU AI Alliance members. According to Roberto Reale (2023), one of the members of the AI Alliance, experts in this field suggest that the EU should rethink the AI Act, especially the high-risk category. He also adds that “Holding the world’s most advanced regulatory framework for AI bears scant worth if we are mere consumers of the technology we seek to regulate” (European Commission, 2023). To conclude, the AI Alliance established by the European Commission in 2018, serves as an open platform for policy dialogue on AI, initially overseeing the key publications of the High Level Expert Group (HLEG) and later evolving into a forum for sharing work and policy recommendations. Despite aiming to become a global leader in AI, the EU is currently facing challenges in this field and should rethink the AI Act and the high risk category to ensure meaningful regulation and avoid becoming just a consumer of technology.

3.5. WHITE PAPER ON ARTIFICIAL INTELLIGENCE (2020)

The foundation of the White Paper on AI has been laid in 2018. In 2018, with the establishment of HLEG on AI and the Guideline they published, the importance of the concept of ethical and reliable AI was emphasized. The White Paper clearly sets out the EU's AI strategy to become a global leader, while emphasizing the risks of AI and the importance of regulations. For AI to thrive, people should be able to trust it, which is possible with AI applications that support human rights and dignity. The paper discusses the EU's position in the global AI race in terms of investments in innovation and research, and concludes that the EU lags behind North America and Asia. According to the paper, a multiple approach is needed to achieve the goals which were mentioned; policy recommendations for member states, research communities, small and medium enterprises (SMEs), the public and private sectors, and even the international arena (UNESCO, OECD, WTO, ITU, global players, and third countries) are discussed. The EU not only lacks investment in AI, it also lacks skills in this area. Policymakers always emphasize regulations and restricted access to data. However, recent reports have shown that business actors in the EU prefer innovation over regulation and consider regulations too strict for AI adoption (Tallberg et al., 2023). However, in the White Paper, it was promoted that the European regulatory approach would build trust, and enhance the development of technology, and the regulatory framework should not hinder the development of AI. Another report has shown that the so-called transparency cannot be achieved at the beginning of the year 2023, as it was indicated in the White Paper (Vasse'i and McCrosky, 2023). It is more difficult to ensure transparency than expected. The White Paper also stated that AI could undermine fundamental principles of the EU, and said that rights such as freedom of expression, freedom of assembly, human dignity, non-discrimination based on gender, racial or ethnic origin, religion or belief, disability, age or sexual orientation, protection of personal data and privacy, or the right to an effective remedy and fair trial, and consumer protection could be affected. The examples of malicious uses of AI mentioned in Chapter One also show that the EU is right in this argument. While White Paper acknowledges that the EU has a strict regulatory framework, it proposes a risk-based approach so as to prevent too much burden on the manufacturers of AI systems.

3.6. AI ACT (2021)

The AI Act (AIA) proposed by the European Commission on 21 April 2021 seeks to establish a legal framework for AI systems, focusing on ensuring their safety, transparency, accountability, and ethical use. It covers both AI systems developed within the EU and those used from outside the EU. It has an impact on EU citizens or people residing within the EU market. The act aims to strike a balance between fostering innovation and protecting the rights and well-being of individuals and society; it contributes to GDPR, Coordinated Plan on AI, Digital Services Act (DSA), Digital Markets Act (DMA), and the Digital Governance Act (DGA) (Edwards, 2022: 4-5). Scholars agree that it is a comprehensive proposal that covers too many realms. It includes provisions regarding high-risk AI systems, transparency requirements, conformity assessments, and enforcement mechanisms. The proposal introduces risk-based approach for AI systems and identifies four categories: unacceptable risk, high risk, limited risk, and minimal risk (Kop, 2021: 1-11). AI systems are designed to exploit vulnerabilities, and social scoring, AI systems that use remote biometric identification displays unacceptable risks and they are banned under the Act. High-risk AI systems include those used in critical sectors such as healthcare, transportation, infrastructure, and law enforcement. Specific requirements are imposed on these systems to ensure their safety, accuracy, and transparency. These requirements may involve data governance, technical documentation, and compliance with standards. Additionally, the limited or minimal risks categories are subject to lighter regulation.

EU wants member states to comply, modify, notify, and monitor compliance. However, there is a load of skepticism in the literature regarding the implication of AIA, even if it was declared that the regulations should not hinder AI development in the legal documents of the Commission AIA raises questions about the strict regulations. As Mauritz Kop (2021), dictated that American people tend to support the free market and laissez faire economy regarding the development of AI, EU's humanitarian approach is a way different. The research that was carried out by Jonas Tallberg and his friends (2023), has demonstrated that the AIA for business actors has important implications regarding innovation and it may affect the competitive positions of the companies. While Ebers et al. (2021) believed that AIA is an

appropriate step for regulating AI they also argued that AIA needs to be revised. According to them, there is a gap between theory and practice. The transparency report of Mozilla (2023) has concluded that the implication of transparency is in an uncertain position. Although the AIA has received several criticisms, one of which is that the EU Green Deal is not among the privileged subjects and not gaining enough attention from the policymakers (Pagallo et al. 2022: 359-376). Bradford has in fact published a study that explains the Brussel Effect and argues that the EU is a global regulatory power in the world, in order to demolish the notion of the EU as a declining power in recent years (Sönmez, 2022: 603-606). Also, Hacker (2023), states that the EU has the potential to shape the global regulatory framework, especially US. He adds that the US is following the regulations of the EU on AI closely, and has been affected especially by the AIA. (Hacker, 2023: 3)

3.7. PROPOSAL FOR AN AI LIABILITY DIRECTIVE

The Product Liability Directive (PLD) is one of the policy proposals contained in the White Paper and was published as a proposal by the EU Commission in September 2022. The PLD addresses producer liability for defective products and aims to create trust among consumers. The proposal for an AILD stresses the Commission's goal of introducing AI on a larger scale. However, before that can happen, there is a need to address civil liability issues caused by AI (European Commission, 2022e). It covers several aspects of AI technologies: including liability, legal uncertainty, and economic effects, making it a valuable resource for individuals seeking a deeper understanding of AI-enabled products and services (European Commission, 2022e).

EU intervention is highly requested by EU citizens, consumer organizations, and academic institutions to alleviate the burden of proof challenges faced by victims. However, businesses, even though they acknowledge the drawbacks of uncertain liability rules, still call for targeted measures to avoid stifling innovation (European Commission, 2022f). The suggested policy would promote the competitiveness of companies, including SMEs, by ensuring the protection of victims and reducing legal uncertainty. This, in turn, would increase the market value of AI and allow for more efficient cost allocation through insurance. Moreover, the policy aims to balance

certain aspects of liability without undermining national laws and includes a review mechanism. The review mechanism will assess further harmonization of strict liability (European Commission, 2022e). Silva (2023) examines the limitations of a proposed tool aimed at disclosing evidence related to high-risk AI systems. He argues that the definition of high risk should not be restricted to the AI Act alone, as these systems may cause harm that does not meet the criteria for classification as high risk. Additionally, it is challenging for customers to determine whether the damages are caused by high-risk AI or not. He also expresses the concerns regarding the disclosure of evidence. The documentation and evidence provided by AI operators can be highly complex and technical, making it difficult for consumers to assess on their own. It may require the assistance of experts such as computer scientists; however, this external help poses a financial burden for consumers and is not preferred. Hacker (2023) argues that both AILD and PLD lack clarity on AI liability and address the challenge of technical opacity in AI models and the need for explainability. While the AILD and PLD proposal attempt to address institutional opacity through evidence disclosure mechanisms, they do not adequately address technical opacity (Hacker, 2023).

3.8. EU DIGITAL STRATEGY

In its digital policies, the EU has always pursued policies that defend the EU's values, overlap with and support the EU Charter of Fundamental Rights. Since 2006, the EU has celebrated EU Data Protection Day on January 28, outside Europe it is known as Privacy Day (Council of Europe, 2023). Data Protection is at the very core of European values, and it has been shaping, and also shaped by Europe's Digital Policy. Even if, the EU-US Privacy Policy adopted in 2016 was subsequently repealed following President Biden's Executive Order signed on October 7, showing that EU citizens' data is subject to protection even in the territories of the US (European Commission, 2022). The need for privacy and protection of data is one of the most important issues for governments, especially in the age of technology where data is the most important catalyst for AI.

The EU has also published several programs in the field of research and innovation, these can be listed as the 7th Framework Programme (FP7) and the 6th

Framework Programme (FP6) (2002 - 2013), Horizon 2020 (2014 - 2020), and Horizon Europe (2021 - 2027) in chronological order (European Commission, 2022). While FP7 has offered a 55 billion euro budget, the budget allocation for Horizon 2020 was 80 billion euro. For Horizon Europe the budget allocation will be 95.5 billion euro for the years 2021-2027 (European Commission, 2018; European Commission, 2020; European Commission, 2021). Horizon Europe has set its goals and expectations based on lessons learned from the Horizon 2020 program. The Horizon 2020 program appears to be successful overall, but key findings have identified some barriers to innovation. More policies to support innovation should be adopted and regulations and standards should not be barriers in front of the development (European Commission, 2017). Indeed, the European regulatory framework is too wide that aims to control, monitor, and regulate almost all realms of technology. GDPR, HLEG, White Paper, and then the AI Act, which was last held on June 14, 2023, are all restrictive documents in their own way. Over time, the EU has also recognized that it is lagging behind in the AI race and it has taken the necessary steps (Ragonnaud, 2022). Recently, close cooperation with the US, Chips Act (2023), Digital Europe Program, inventing innovation hubs, and implementing the EU digital identity wallet were discussed at the Digital Assembly in Stockholm and ideas were exchanged for the EU to achieve the 2030 targets (Swedish Presidency of the Council of the European Union, 2023; Ragonnaud, 2022).

3.9. IS THE REGULATORY APPROACH THE REASON WHY THE EU IS LAGGING BEHIND IN AI RACE?

The EU has prioritized data protection and privacy through regulations like the GDPR. While these regulations aim to safeguard personal data, they can present compliance challenges for AI development. Some argue that the strict regulations hinder EU companies from innovating and competing globally. The EU also emphasizes ethical AI development, exemplified by initiatives like the Ethics Guidelines for Trustworthy AI. These principles of transparency, fairness, and accountability, while commendable, can potentially slow down AI progress compared to countries with fewer ethical considerations. The US and China have made

substantial investments in AI research, creating thriving innovation ecosystems, their larger markets, financial resources, and talent pools provide advantages. The EU is working to increase AI investment but may take time to catch up. The EU's regulatory landscape is fragmented across member states, leading to variations in AI regulations. Harmonizing regulations and fostering a unified approach can be challenging, potentially contributing to slower progress compared to more centralized systems. While the EU faces challenges in the AI race, its regulatory approach prioritizes responsible and human-centric AI development. The EU's emphasis on privacy, ethics, and accountability aligns with a vision of AI that respects fundamental rights and societal values. Striking a balance between innovation and ethics is a complex task crucial for the sustainable long-term development of AI.

Examples of malicious uses of AI can certainly justify the EU's regulatory approach to AI. While AI offers numerous benefits and opportunities, it also presents potential risks and challenges. The EU's regulatory focus on AI is driven by the recognition of these risks and the need to establish safeguards. Malicious uses of AI can include the development of AI-powered tools for cyberattacks, deepfake technology for spreading misinformation or disinformation, algorithmic biases leading to discriminatory outcomes, and AI-powered surveillance systems infringing on privacy rights, among others. These instances highlight the potential harm that can arise from unregulated or unethical AI deployments. The EU's regulatory framework aims to address these concerns by prioritizing principles such as transparency, fairness, accountability, and human rights in AI development and deployment. By implementing regulations and guidelines, the EU seeks to minimize the risks associated with malicious uses of AI and ensure that AI technologies are developed and used in a responsible and ethical manner. The EU's approach also reflects a broader societal perspective, taking into account the concerns of citizens, consumer protection, and the potential impact on democratic values. The regulatory framework seeks to strike a balance between fostering innovation and ensuring the well-being and rights of individuals. Overall, the EU's regulatory approach to AI is shaped by the understanding that AI technologies should be developed, deployed, and used in a manner that is aligned with societal values, protects individual rights, and mitigates potential risks, including the malicious use of AI.

For example, China has been criticized for its extensive use of surveillance technologies, including facial recognition and AI-powered systems, to monitor its citizens. These surveillance measures have been associated with violations of privacy rights and the potential for suppressing dissent and limiting freedom of expression. China has been implementing a social credit system that utilizes AI and data collection to monitor and score individuals based on their behavior and adherence to government policies. Critics argue that this system can lead to social control, discrimination, and violations of personal freedoms. Another reports suggest that AI and surveillance technologies are used in the surveillance and repression of Uyghur Muslims in the Xinjiang region. Facial recognition, biometric data collection, and predictive policing systems have been deployed in a way that violates human rights, including arbitrary detentions, forced labor, and cultural suppression. Also, China has stringent internet censorship and control mechanisms, known as the Great Firewall, which restrict access to information and curtail freedom of expression online. AI technologies are employed to monitor online activities, detect and censor sensitive content, and identify and punish dissenting voices. All applications that are mentioned above is completely contrasting with the EU's core values and that is why EU criticize Chinese way of AI development.

CONCLUSION

AI, which has been frequently mentioned since the 1950s, has become one of the most popular research topics in the 2000s and has started to shape our lives. Almost every researcher who has worked in the field of AI emphasises that while AI makes our lives easier in many ways, it can also pose new threats. AI has started to control our lives day by day, and the risks it brings with it are undeniable, especially in terms of human rights. When AI is considered from the EU perspective, it is seen that AI may be in contradiction with the EU's fundamental values. Therefore, this research aims to examine the EU's unique AI approach and argues that one of the reasons why the EU has lagged behind in the AI race is that the EU has adopted a regulatory approach because the risks brought by AI are in conflict with the EU's core values.

This research has demonstrated the EU's regulatory and human-centered AI approach by conducting a literature review and analysing the EU's legal documents. The EU has stated in all its documents that it recognises regulations as a prerequisite for respectful of human rights, trustworthy and responsible AI. The EU has also stated its goal of becoming a global power in the field of AI by keeping regulations balanced, and also goal of creating common regulations among the member states. However, the various studies on EU's AI policies found out that EU is far away from the being a global leader in terms of technology-related sectors and even it is dependent on Asian economy especially on semiconductor industry. This fact has also been recognised by the EU in impact assessment reports and policy recommendations have been made. When it is examined the literature, numerous studies have been conducted and the results have shown almost the same findings. It is almost the fact that the EU is lagging behind in the AI race, exaggerating regulations, and has been struggling to follow the trends in AI race. Of course, there are many examples of the misuse of AI, and the fact that it threatens the most fundamental rights of individuals, even threatening democracy, has been addressed by many authors.

The misuse of AI, historical events such as the WannaCry virus and the Cambridge Analytica scandal may explain and justify the EU's strict regulatory approach. Additionally, the Communist Party's restrictive policies can be seen as an

another justification for the EU's AI policies; mass surveillance systems, social scoring, and strict controls all over the big cities seems like a dystopia.

Another point to be discussed is that, given the EU's core values and aims set out in the EU Charter of the Fundamental Rights and the Lisbon Treaty, the automatic decision-making mechanism poses a great risk. For example, automated vehicles have been the subject of much ethical and legal debate; indeed, there is no internationally recognised law on who is responsible when an automated vehicle has an accident. Or, the fact that it is not known to what extent the AI systems used in the employment process make accurate and transparent decisions paves the way for discriminative decisions. Moreover, researchs show that racist attitudes, especially in the US, may also be attached to AI systems in the creation process.

The EU, which focuses on a soft-power approach in order to minimise the negative effects of AI and to ensure the security and peace of mind of citizens, has had a groundbreaking regulation with the GDPR adopted in 2016. With the GDPR, the EU has a much more unified regulation. In addition, with this regulation, which deals with the consent of the individual, EU citizens have much wider rights and powers regarding the collection, storage, processing, and even erasure of their personal data. Four years later, the AI White Paper was published in 2020 clearly stated the EU's ambition to become a global leader and referred to the ecosystem of trust and excellence based on trustworthy AI. The White Paper on AI is actually a document that laid the foundation for the AI Act, where the idea of risk-based approach was discussed for the first time. In 2021, the EU took its strict regulatory approach a step further by adopting the AI Act. Biometric recognition, social scoring, and AI applications that violate human dignity and pride are strictly banned with the Act, namely the AI operations which are in a complete contradiction with the EU's fundamental rights. Although there are many sceptical citizens who are satisfied with this Act, the AI Act in general has caused a lot of controversy in the literature. The fact that AI is a constantly developing area makes it a difficult field to regulate. While GDPR and AIA are well-equipped against the threats posed by AI, regulations for ever-evolving technology and AI are still evolving and should continue to do so. It is worth noting that the EU's regulations in its own territory may also harm its bilateral trade relations. EU trade, which already has to deal with many crises, could be harshly

impacted by such regulations, notably the AILD. While the EU aims to protect the consumers' rights, it also damages the ongoing trade relations, because the burden on the business owners' shoulders is incredibly huge to cope with it.

One of the costs of the EU's human-centred approach to AI is its lagging behind in the AI race. Regulations restrict access to, use of, and even storage of data, which is the source of AI. This poses a problem for many researchers, inventors, software developers, etc. working with data within the EU territories and adds burden to their shoulders. For this reason, the EU is mostly losing its qualified staff in the field of AI to America. While the human-centred AI approach adopted by the EU can be seen as an advantage for the civilian population residing in the EU, it is a disadvantage for companies, software developers, data analysts, in short, for every sector that collects, stores and processes data. AI that works with less data almost under the all conditions means less advanced AI technology.

In practice, the EU has neither achieved the desired results from the applied regulations nor become a global AI power. When it is considered the normative power of the EU, it is obvious that the EU has not been and will not be very successful in convincing other regions to follow a regulatory AI approach. Even if international regulations were to be adopted, the EU cannot be sure how far signatory parties would adhere to these sanctions and would find itself in a much worse situation.

Another important point to be mentioned is how far the criteria set by the EU for a reliable AI are achievable in practice. Various studies have shown that it is more difficult to ensure transparency than expected; it is mostly due to the lack of skills or technical knowledge of the end users of the AI products. AI products are very complicated that anyone cannot be capable of understanding all the functions and operability of the machine. It is therefore very difficult to understand to what extent the AI product used is transparent, reliable and opaque.

Also according to the 2023 WEF forecasts, Asia region is the region with the highest economic growth, while Europe is the weakest region. This has a negative impact not only on the EU's strength in the global arena but also on business actors in the EU, who, according to Tallberg et al. (2023), favour innovation over regulation. As the researchers point out, it is very important to maintain the balance between

regulations and innovation, otherwise regulations create a barrier to development. According to this thesis it can be advocated that the EU seems to have gone a bit overboard with restrictive norms, especially with the AI Act.

At this point, a constructive approach to the TTC co-operation initiated by the EU with the US is suggested. Even if the EU has a much longer way to go than its competitors, it has the strengths and capabilities to do so and should focus on them. Gradually, a shift from strict regulation to a more lenient approach should be adopted by the EU, and a balance between regulation and innovation should be ensured. Although AI raises many questions about the breach of our data and contradicts the EU's core values to some extent, in the information age the state with the most advanced technology will have the most say and the right to rule the world. Therefore, the steps that the EU should follow in this regard are to sacrifice some of its core values and adopt more liberal policies in the field of AI. It should allocate more resources to researchers, engineers and universities working in the field of technology and increase incentives. In doing so, the EU should strike a great balance between regulations and technological developments, as mentioned in the White Paper, and ensure that strict regulations do not constitute an obstacle to technological development.

To finalise, the EU seems to have recently realised the negative outcomes of its restrictive policies. Especially as stated in the evaluation paper of Horizon 2020, regulations have unfortunately hampered the EU's innovation. The extent to which the EU will improve its position in the global AI race in the coming period may be the subject of new researches. As a result, this study has revealed that the EU's human-centred and regulatory approach to AI is an obstacle to its technological development. This is mostly due to the reason that, AI is a data-driven industry, and today machines that can even learn and infer on their own have been created. Always, there is a potential that the data on which AI works may be biased, or distorted. Examples of the misuse of AI also show that AI can indeed create contradictions to the principles of democracy, freedom, equality, and rule of law enshrined in the EU's Lisbon Treaty and the EU Charter of Fundamental Rights. To elaborate further, the Cambridge Analytica scandal shows that the Trump administration in the United States did not come to power as a result of a democratic election, but that voters were manipulated through AI and social media. In addition, gender-based AI applications such as Amazon,

Google, Siri are in contradiction with the EU's core values mentioned in Article 2 of the Lisbon Treaty.

REFERENCES

Accessnow. (01.11.2018). Mapping Artificial Intelligence Strategies In Europe. https://www.accessnow.org/?s=artificial&_paged=6, (11.03.2023).

Allen, G. (06.02.2019). Understanding China's AI Strategy: Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security. <https://www.cnas.org/publications/reports/understanding-chinas-ai-strategy>, (20.05.2023).

Allen, J., Massolo, G. (18.10.2020). "AI in the Age of Cyber-Disorder" <https://www.ispionline.it/en/publication/ai-age-cyber-disorder-28309>, (27.02.2023).

American Leadership Initiative. (13.07.2021). Next Steps for U.S. Digital Leadership. https://static1.squarespace.com/static/5c9904eaeafc7f03f980b72a/t/611420656e0f5e13222dc6f0/1628708965770/ALI-White_Paper-081121-Final2.pdf, (21.05.2023).

Atkinson, R. (19.01.2021). A U.S. Grand Strategy for the Global Digital Economy. <https://itif.org/publications/2021/01/19/us-grand-strategy-global-digital-economy/>, (21.05.2023).

Baum, S. (2018). Countering Superintelligence Misinformation. AI And The Singularity A Fallacy Or A Great Opportunity? (45-60). Switzerland: MDPI.

Berk, R. (2017). An Impact Assessment Of Machine Learning Risk Forecasts On Parole Board Decisions And Recidivism. *Journal of Experimental Criminology*. 13(2): 193-216.

Besteman, C., Gusterson, H. (2020) *Algoritmalarla Yaşamak*. Çev. Birol Akmeriç. İstanbul: Doğa Basım.

Bohlin, E., Cappelletti, F. (2022). Europe's Future Connected Policies and Challenges For 5G And 6G Networks. https://liberalforum.eu/wp-content/uploads/2022/06/Europes-Future-Connected_ELF-Study_Techno-Politics_vol.2-2.pdf, (03.04.2023).

Bonnefon, J., Köbis, N., Rahwan, I. (2021). Bad Machines Corrupt Good Morals. *Toulouse School of Economics*. 1-31.

Borek, A., Prill, N. (2021). *Veri Ve Yapay Zekayla Dijital Dönüşüm İşletmelerde Dijital Dönüşüm, Makine Öğrenimi ve Yapay Zeka*. Çev. Derman Gülmez Aydın, Murat Demirekin, Özge Nur Küskün. İstanbul: Optimum Basım Yayın.

Bostrom, N. (2014). *Super Intelligence Paths, Dangers, Strategies*. United Kingdom: Oxford University Press.

Bostrom, N., Yudkowsky, E. (2014). *The Ethics Of Artificial Intelligence*. Cambridge University Press: 1-20.

Braga, A., Logan, K. (2019) *AI and the Singularity: A Fallacy or a Great Opportunity?* Switzerland: MDPI.

Brattberg, E., Csernaton, R., Rugova, V. (09.07.2020). Europe and AI: Leading, Lagging Behind, or Carving Its Own Way? <https://carnegieendowment.org/2020/07/09/europe-and-ai-leading-lagging-behind-or-carving-its-own-way-pub-82236>, (06.06.2023).

Castro, D., McLaughlin, M. (January, 2021). Who Is Winning The AI Race: China, the EU, or the United States? – 2021 Update. <https://datainnovation.org/2019/08/who-is-winning-the-ai-race-china-the-eu-or-the-united-states/>, (13.05.2023).

Chalmers, D. (2010). The Singularity: A Philosophical Analysis. *Journal of Consciousness Studies*. 2010(17): 7-65.

Cheng, X., Lin, X., Shen, X., Zarifis, A., Mou, J. (22.02.2022). The Dark Sides of AI. <https://link.springer.com/article/10.1007/s12525-022-00531-5>, (23.02.2023).

Chin, C., Robison, M. (2020). How AI Bots and Voice Assistants Reinforce Gender Bias. *AI in the Age of Cyber-Disorder Actors, Trends, and Prospects*. (p. 82-104). Italy: ISPI.

Chukewad, Y. (2020). Robofly: An Insect-Sized Robot With Simplified Fabrication That Is Capable Of Flight, Ground, And Water Surface Locomotion. *IEEE Transactions On Robotics*. 20(10): 1-15.

Ciancaglini, V., Gibson, C., Sancho, D. (2020). Malicious Uses and Abuses of Artificial Intelligence. *Trend Micro Research*. 4-79.

Council Of The European Union, (27.01.2022). Limite En – European Council. <https://data.consilium.europa.eu/doc/document/ST-10572-2022-INIT/en/pdf>, (15.01.2023).

Council Of The European Union, (31.08.2022). Selection Of The Seat Of The EU Cybersecurity Competence Centre. <https://www.consilium.europa.eu/en/policies/cybersecurity/seat-selection-cybersecurity-centre/>, (15.01.2023).

Courtland, R. (2018). The Bias Detectives. *Springer Nature*. Vol.558: 358-360.

Crawford, K., Calo, R. (2016). There Is A Blind Spot In AI Research. *Nature*. Vol.538: 311-313.

Cyber Security Conference Platform. (2023). The 10th Annual European Cyber Security Conference 2023. <https://eucybersecurity.com/>, (15.01.2023).

Dalli, H. (2021). Artificial Intelligence Act. *European Parliamentary Research Service*. 1-9.

Deng, W., Rosenblatt, A., Talhelm, T., Putnam, A. (2022). People From The U.S. And China Think About Their Personal And Collective Future Differently. *Memory & Cognition* 2023(51): 87–100.

Diez, T. (2021). The EU In A Changing World Order: In Defence Of Normative Power 2.0. *Marmara Journal Of European Studies*. 29(1): 1-20.

Economist Intelligence. (20.09.2023). Why AI Matters? <https://services.eiu.com/campaigns/why-ai-matters-sep-2023/>, (21.09.2023).

Ersoy, Ç. (2020). *Robotlar, Yapay Zeka ve Hukuk*. İstanbul: Onikilevha.

Euronews. (28.07.2021). Biden: ABD Gerçek Bir Savaşa Girerse Bu Siber Saldırıları Nedeniyle Olur. <https://tr.euronews.com/2021/07/28/biden-abd-gercek-bir-savasa-girerse-bu-siber-sald-r-lar-nedeniyle-olur>, (12.04.2023).

European Commission, (2017). “Key Findings From The Horizon 2020 Interim Evaluation” <https://op.europa.eu/en/publication-detail/-/publication/46cfbdd3-5c78-11e7-954d-01aa75ed71a1/language-en/format-PDF/source-77918402> (04.06.2023).

European Commission. (2018a). “Annex To The Communication From The Commission To The European Parliament, The European Council, The Council, The European Economic And Social Committee And The Committee Of The Regions

Coordinated Plan On Artificial Intelligence”, (07.12.2018) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0795>, (03.04.2022).

European Commission, (2018b). “Communication From The Commission To The European Parliament, The European Council, The Council, The European Economic And Social Committee And The Committee Of The Regions Artificial Intelligence For Europe”. (25.04.2018). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN>, (15.01.2023).

European Commission. (2019a). “Ethics guidelines for trustworthy AI” 08.04.2019, <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>, (05.08.2022).

European Commission. (2019b). “Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions, Building Trust in Human-Centric Artificial Intelligence, 08.04.2019, <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52019DC0168>, (03.04.2022).

European Commission. (2019c). “The First European AI Alliance Assembly”. (26.06.2019). <https://digital-strategy.ec.europa.eu/en/events/first-european-ai-alliance-assembly#:~:text=The%20European%20AI%20Alliance%20is,future%20of%20AI%20in%20Europe>. (10.06.2023).

European Commission. (2021a). “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” 21.04.2021, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206>, (03.04.2022).

European Commission. (2020a). “White Paper On Artificial Intelligence - A European Approach To Excellence And Trust” 19.02.2020, https://commission.europa.eu/document/download/d2ec4039-c5be-423a-81ef-b9e44e79825b_en?filename=commission-white-paper-artificial-intelligence-feb2020_en.pdf, (25.02.2020).

European Commission, (2022a). “Financial Year 2022: Implementation On 30/11/2022 - By Policy Area”. (07.12.2022). <https://commission.europa.eu/system/files/2022-12/Expenditure%20COM%20PA.pdf>, (04.06.2023).

European Commission, (2022b). “European Chips Act”. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_en, (07.04.2023).

European Commusion, (2022c). “European Chips Survey”. (04.08.2022). <https://digital-strategy.ec.europa.eu/en/library/european-chips-survey>, (07.04.2023).

European Commission, (2022d). “The European AI Alliance”. (05.08.2022). <https://digital-strategy.ec.europa.eu/en/policies/european-ai-alliance>, (07.04.2023).

European Commission, (2022e). “Commission Staff Working Document Executive Summary Of The Impact Assessment Report” (28.09.2022). https://commission.europa.eu/system/files/2022-09/1_5_197611_summary_impact_asse_dir_ai_en.pdf, (04.06.2023).

European Commission, (2022f). “Directive Of The European Parliament And Of The Council On Adapting Non-Contractual Civil Liability Rules To Artificial Intelligence (AI Liability Directive)” (28.09.2022), https://commission.europa.eu/system/files/2022-09/1_1_197605_prop_dir_ai_en.pdf, (04.06.2023).

European Union Agency For Cyber Security. (2020). “AI Cyber Security Challenges Threat Landscape for Artificial Intelligence”, (14.11.2020) https://www.enisa.europa.eu/enisa-search/#/?SearchableText=cyber%20security%20challenges%20threat%20landscape&date_end=2021-01-04&sort_on_date=false&sort_on_relevancy=true, (13.01.2023).

Finn, E. (2020). *Algoritmalar Ne İster?* Çev. Songül Köse, İstanbul: Tellekt Can Sanat Yayınları.

Fjeld, J., Achten, N., Hilligoss, H., Nagy, A., Srikumar, M. (2020). Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI. *Berkman Klein Center For The Internet & Society At Harvard University*. 2020(1): 1-70.

Galasso, V., Foucalt, M. (24.07.2020). Working during COVID-19: Cross-Country Evidence from Real-Time Survey Data OECD Social, Employment And Migration Working Papers No. 246. https://www.oecd-ilibrary.org/social-issues-migration-health/working-during-covid-19_34a2c306-en, (10.05.2022).

Galindo, L., K. Perset and F. Sheeka (2021). An Overview Of National AI Strategies And Policies, Going Digital Toolkit Note, No. 14, https://goingdigital.oecd.org/data/notes/No14_ToolkitNote_AIStrategies.pdf. (20.06.2023).

Gehrke, T., Ringhof, J. (17.05.2023). The power of control: How The EU Can Shape The New Era Of Strategic Export Restrictions. <https://ecfr.eu/publication/the-power-of-control-how-the-eu-can-shape-the-new-era-of-strategic-export-restrictions/>, (22.05.2023).

Ghaffary, S. (15.08.2019). The Algorithms That Detect Hate Speech Online Are Biased Against Black People.

<https://www.vox.com/recode/2019/8/15/20806384/social-media-hate-speech-bias-black-african-american-facebook-twitter>, (12.04.2023).

Hacker, P. (20.01.2023). The European AI Liability Directives. <https://arxiv.org/abs/2211.13960>, (20.06.2023).

Ham, R., Mowery, D. (1995). Enduring Dilemmas In U.S. Technology Policy. *California Management Review*. 37(4): 89-107.

Hillion, C. (2004). The Copenhagen Criteria And Their Progeny. *EU Enlargement*. 1-20.

Ilik, G., Shapkoski, V. (2020). Coherence on Trial: The Coronavirus Outbreak as a Critical Test for the European Union. *Studia Europejskie - Studies in European Affairs* 4:25-43.

Isik, B. (2020). *Yapay Zekaya Sahip Robotların Avrupa Birliğinde Serbest Dolaşımı Önünde Ortaya Çıkacak Sorunların Hukuki Sorumluluk Müessesesi Çerçevesinde Değerlendirilmesi*. Kuzey Kıbrıs: Doğu Akdeniz Üniversitesi Hukuk Fakültesi.

Joint Research Centre. (23.05.2022). AI Watch: Estimating AI Investments in the European Union. https://ai-watch.ec.europa.eu/publications/ai-watch-estimating-ai-investments-european-union_en, (20.09.2023).

Klasinc, J. (27.03.2022). IEEE Xplore. <https://ieeexplore.ieee.org/document/9803769>, (03.11.2022).

Kleinhas, J., Lee, J. (08.12.2021). China's Rise In Semiconductors And Europe. <https://merics.org/en/report/chinas-rise-semiconductors-and-europe-recommendations-policy-makers>, (07.06.2023).

Kop, M. (18.11.2021). EU Artificial Intelligence Act: The European Approach to AI. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3930959, (21.09.2022).

Kornbluh, K., Trehu, J. (01.03.2023). The New American Foreign Policy of Technology. https://www.gmfus.org/sites/default/files/2023-03/Report%20-%20The%20New%20American%20Foreign%20Policy%20of%20Technology_1.pdf, (25.05.2023).

Koulu, R. (2020). Human Control Over Automation: EU Policy and AI Ethics. *European Journal of Legal Studies*, 12(1): 9-46.

Köbis N.C., Doležalová, B., Soraperra, I. (2021). Fooled Twice: People Cannot Detect Deepfakes But Think They Can. *iScience*. 24(11): 24-29.

Lankford, A. (20.01.2023). States And Cities Limit AI Use In Employment Decisions. <https://www.mcafeetaft.com/states-and-cities-limit-ai-use-in-employment-decisions/>, (12.04.2023).

Leonhard, G. (2020). *Teknolojiye Karşı İnsanlık*. Çev. Cihan Akkartal. İstanbul: Siyah Kitap.

Liu, L. (11.05.2019). Orwellian Nonsense Or Innovation In The Classroom? <https://www.eetasia.com/orwellian-nonsense-or-innovation-in-the-classroom/>, (02.05.2023).

Maar, B. (2020). *Büyük Veri İş Başında*. Çev. Başak Gündüz. İstanbul: MediaCat.

Madnick, S. (March 2022). The Rising Threat To Consumer Data In The Cloud. <https://www.apple.com/newsroom/pdfs/The-Rising-Threat-to-Consumer-Data-in-the-Cloud.pdf>, (27.02.2023).

Major, L., Julie, S. (2022). *Robotları Beklerken Neler Olacak? İnsan – Robot İş Birliğinin Geleceği*. Çev. Melis Zeren. İstanbul: Kültür Bakanlığı Yayıncılık.

Manners, Ian (2002). “Normative power Europe: a contradiction in terms?”. *Journal of common market studies*. 40(2): 235-258.

Marktler, T. (2006). The Power of The Copenhagen Criteria. *CYELP* 2: 343-363.

McKinsey Global Survey. (08.11.2021). *The state of AI in 2021*. <https://www.mckinsey.com/capabilities/quantumblack/our-insights/global-survey-the-state-of-ai-in-2021>, (14.01.2023).

MIT Technology Review Insights. (26.03.2020). “*The Global AI Agenda: Promise, Reality, And A Future Of Data Sharing*” <https://www.technologyreview.com/2020/03/26/950287/the-global-ai-agenda-promise-reality-and-a-future-of-data-sharing/>, (06.06.2023).

Moor, J. (2006). The Dartmouth College Artificial Intelligence Conference: The Next Fifty Years. *AI Magazine*. 27(4): 87-91.

Moore, G. (2022). Huawei, Cyber-Sovereignty And Liberal Norms: China’s Challenge to the West/Democracies. *Journal of Chinese Political Science*. 2023(28):151-167.

Mozur, P. (15.10.2018). A Genocide Incited on Facebook, With Posts From Myanmar’s Military. <https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html>, (10.05.2022).

Moraes, G., Almeida, E., Pereira, J. (2021). Smile, You Are Being Identified! Risks And Measures For The Use Of Facial Recognition In (Semi-)Public Spaces. *AI and Ethics* (2021) 1:159–172.

National Science And Technology Council, “Critical And Emerging Technologies List Update” (February, 2022), <https://www.whitehouse.gov/wp-content/uploads/2022/02/02-2022-Critical-and-Emerging-Technologies-List-Update.pdf>, (05.02.2023).

National Science and Technology Council. (12.11.2020). “The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update.” <https://www.whitehouse.gov/wp-content/uploads/2023/05/National-Artificial-Intelligence-Research-and-Development-Strategic-Plan-2023-Update.pdf>, (20.05.2023).

Norvig, P., Russell, S. (1995). *Artificial Intelligence A Modern Approach*. Upper Saddle River, New Jersey: Pearson.

Nouredine, R. (02.06.2021). Normative Power Europe and in Field of Human Rights: is the EU a Force for Good in the World? <https://openjournals.library.sydney.edu.au/ANZJES/article/view/15169>, (08.09.2023).

Nye, D. (1996). *American Technological Sublime*. Newyork: The MIT Press.

Official Journal of The European Union. (2016). “General Data Protection Regulation” 27.04.2016, <https://eur-lex.europa.eu/eli/reg/2016/679/oj>, (10.06.2023).

Official Journal of The European Union. (2012a). “Consolidated Version of The Treaty On European Union” 26.10.2012, (08.09.2023).

Official Journal of the European Union. (2012b). “Charter of Fundamental Rights of The European Union” 26.10.2012, (08.09.2023).

Pagallo, U., Sciolla, J., Durante, M. (2022). The Environmental Challenges Of AI In EU Law: Lessons Learned From The Artificial Intelligence Act (AIA) With Its Drawbacks. *Transforming Government: People, Process and Policy*. 16(3): 359-376.

Palmerini, E., Bertolini, A., Battaglia, F., Koops, B., Carnevale, A., Salvini, P. (2016). RoboLaw: Towards A European Framework For Robotics Regulation. *Robotics and Autonomous Systems*. Vol.86: 78-85.

Parliamentary Assembly. (24.09.2020). Need For Democratic Governance Of Artificial Intelligence. <https://pace.coe.int/en/files/28742>, (25.10.2021)

Peschke, S., Peschke, L., (2022). Artificial Intelligence And The New Challenges For EU Legislation. *YBHD*.2022(2): 1267-1292.

Ragonnaud, G. (2022). The EU Chips Act Securing Europe's Supply Of Semiconductors. *European Parliamentary Research Service*. 1-12.

Ramamoorthy, A., Yampolskiy, R. (2018). Beyond Mad?: The Race For Artificial General Intelligence. *ITU Journal*: 1(2): 1-8.

Rodrigues, R. (2020). Legal and Human Rights Issues Of AI: Gaps, Challenges And Vulnerabilities. *Journal of Responsible Technology*.4(10005).

Roksandic, S., Protrka, N., Engelhart, M. (2022). Trustworthy Artificial Intelligence And Its Use By Law Enforcement Authorities: Where Do We Stand? *MIPRO*. 23-27.

Ryan, R., Al-Rubaye, S., Braithwaite, G. (31.10.2022). IEEE Xplore. <https://ieeexplore.ieee.org/document/9925869>, (03.11.2022).

Salgado-Criado, J., Fernández-Aller, C. (03.06.2021). A Wide Human-Rights Approach to Artificial Intelligence Regulation in Europe. IEEE Xplore. <https://ieeexplore.ieee.org/document/9445794>, (03.11.2022).

Salitskii, A., Salitskaya, E., (2022). China on the Way to Global Technology Leadership. *Herald of the Russian Academy of Sciences*. 92(3): 262-267.

Samsun, A. (2021). Yapay Zeka Yarışında Avrupa Birliği'nin Konumu. *Europolitika*. 5(8): 24-31.

Saygın, A., Cicekli, I., Akman, V. (2000). Turing Test: 50 Years Later. *Minds and Machines* 10: 463–518.

Shi-Kupfer, K., Ohlberg, M. (07.04.2019). China's Digital Rise Challenges For Europe. https://merics.org/sites/default/files/2020-05/MPOC_No.7_ChinasDigitalRise_web_final_1.pdf. (04.06.2023).

Silva, J. (2022). Cyber security and the Leviathan. *Computers & Security*. 116(2022): 1-17.

Sönmez, P. (2022). The Brussels Effect: How the European Union Rules The World, Anu Bradford. , 17(2): 603-606.

Suedekum, J. (04.02.2019). Europe In The Global Race For Technological Leadership. <https://www.hoover.org/research/europe-global-race-technological-leadership>, (10.05.2023).

Tallberg, J., Lundgren, M., Geith, J. (19.05.2023). AI Regulation In The European Union: Examining Non-State Actor Preferences. <https://arxiv.org/ftp/arxiv/papers/2305/2305.11523.pdf>, (05.06.2023).

The Economist. (06.05.2017). The world's most valuable resource is no longer oil, but data. <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>, (26.10.2022).

The White House Washington. (2023). Budget Of The U.S. Government. https://www.whitehouse.gov/wp-content/uploads/2022/03/budget_fy2023.pdf, (04.06.2023).

Thomson, N. (31.03.2018). Emmanuel Macron Talks To WIRED About France's AI Strategy. <https://www.wired.com/story/emmanuel-macron-talks-to-wired-about-frances-ai-strategy/>, (12.04.2023).

Tougaard, E. (23.02.2021). China's AI Champions. <https://www.china-experience.com/china-experience-insights/chinas-ai-champions>, (10.05.2023).

Tseng, W., Zebreg, H. (2022). Foreign Direct Investment In China: Some Lessons For Other Countries. <https://www.imf.org/external/pubs/ft/pdp/2002/pdp03.pdf>, (04.06.2023).

Turing, A. (1950). Computing Machinery And Intelligence. *Mind*. 49: 433-460.

Turkcetin, A. (2021). Etik Yapay Zeka Tasarımı. Yapay Zeka Etiği (p.63-81). Ankara: Nobel Yayınevi.

Ufert, F. (2020). AI Regulation Through The Lens Of Fundamental Rights: How Well Does The GDPR Address The Challenges Posed By AI? *Insight*. Vol.5: 1087-1097.

Uysal, İ. (2021). Teknolojik Tekillik ve Etik. Yapay Zeka Etiği (p.297-310). Ankara: Nobel Yayınevi.

Villani, C. (2018). For A Meaningful Artificial Intelligence Towards A French And European Strategy.

Vinge, V. (1993). Technological Singularity. *VISION-21 Symposium* (p.30-31)

Yampolskiy, R. (October 2016). Artificial Intelligence Safety And Cybersecurity: A Timeline Of AI Failures, https://www.researchgate.net/publication/309424933_Artificial_Intelligence_Safety_and_Cybersecurity_a_Timeline_of_AI_Failures (20.10.2022).

Zeng, J. (2020). Artificial Intelligence And China's Authoritarian Governance. *International Affairs*. 96(6): 1441–1459.

Zhang, L., Zhao, S., Kern, P., Edwards, T., Zhang, Z. (26.11.2022). The Pursuit Of Indigenous Innovation Amid The Tech Cold War: The Case Of A Chinese High-Tech Firm. www.sciencedirect.com/science/article/pii/S096959312200107X?via%3Dihub, (25.04.2023).

Zhang, S. (16.02.2017). China's Artificial-Intelligence Boom. www.theatlantic.com/technology/archive/2017/02/china-artificial-intelligence/516615/, (02.06.2023).

Wang, P., Liu, K., Dougherty, Q. (2018) Conceptions of Artificial Intelligence and Singularity. AI And The Singularity A Fallacy Or A Great Opportunity? (p.251-266). Switzerland: MDPI.

Wang, L. (2022). China's Huawei in the Us-China Trade War in the Communications Sector Game. *Advances in Economics, Business and Management Research*. Vol.656: 485-497.

Wong, J. (18.03.2019). The Cambridge Analytica scandal changed the world – but it didn't change Facebook. *The Guardian*.

<https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook>, (10.05.2022).

World Economic Forum. (May 2023). Chief Economists Outlook. https://www3.weforum.org/docs/WEF_Chief_Economists_Outlook_May2023.pdf, (04.06.2023)

Wright, G. (25.08.2014). Historical Foundations of American Technology. https://www.researchgate.net/publication/46464596_Historical_Foundations_of_American_Technology?enrichId=rgreq-aebc67135544bdca584d7f411eb9e39d-XXX&enrichSource=Y292ZXJQYWdlOzQ2NDY0NTk2O0FTOjEzNDE3NjE4NzYyMTM3N0AxNDA5MDAxNTA0MDk5&el=1_x_2&_esc=publicationCoverPdf, (21.05.2023).