CENTRAL EUROPEAN UNIVERSITY

ARTIFICIAL INTELLIGENCE AND ITS IMPACT ON THE RIGHT TO FREEDOM OF EXPRESSION WITHIN EUROPEAN LEGAL FRAMEWORK

by Salome Shonia

LLM Final Thesis
SUPERVISOR: Marie-Pierre Granger
Central European University - Private University

[17.06.2024]

ABSTRACT

In the digital age, as Artificial Intelligence technologies rapidly integrate into modern life, their influence on fundamental rights, particularly freedom of expression, is increasingly significant. The thesis explores the implications of AI on freedom of expression, addressing issues like misinformation, deepfakes, surveillance, content moderation, bias and discrimination. It evaluates the European AI approach, examining legal frameworks of the Council Of Europe (COE) and the European Union (EU), focusing on recently adopted regulations such as the EU AI Act and the Convention on AI, Human rights, democracy and the rule of law, along with case law analysis. The methodological framework adopted is doctrinal, which allows legal analysis, and examination of legal principles, rules, and doctrines, to gain a holistic understanding of the legal dimensions of AI. The research indicates that current regulations aim to ensure AI development aligns with human rights standards. However, the fast-paced evolution of AI technologies presents ongoing challenges for legal systems. The study underscores the need for continued vigilance and adaptation in AI regulation to protect freedom of expression. It advocates for a collaborative approach of stakeholders to foster ethical AI development that upholds fundamental rights while enabling technological advancement.

Keywords: Artificial Intelligence, Freedom of expression, legal frameworks, recent regulations.

ACKNOWLEDGMENTS

I would like to express my deepest gratitude to those who have supported and guided me through the research and very intensive academic year.

To my supervisor, Professor Marie-Pierre Granger, whose patience, precise feedback and unwavering support have been instrumental in shaping this thesis.

To my professor, Cameran Ashraf, whose classes in AI and technology, not only widened my knowledge of AI but also deepened my analytical approach towards AI. Your dedication, your enthusiasm, the poems you shared before classes and the opportunities you provided were truly inspiring and will be never forgotten.

To my family, whose unconditional love and support, have made me feel capable of achieving anything, no matter where I am in the world.

To my friends, both in Georgia and Austria, especially to Elene, Megi, Sopho, Tatia who's companionship and support kept me sane during the year.

TABLE OF CONTENTS

ABSTRACT ii
ACKNOWLEDGMENTS iii
TABLE OF CONTENTS iv
INTRODUCTION 1
1.AI and its implications on the right to freedom of expression 4
1.1.What is AI? 5
1.2.Types of AI 6
1.3.AI implications on the right of freedom of expression 8
1.3.1 misinformation and deepfakes 9
1.3.2 Content moderation 10
1.3.3 Bias and discrimination 12
1.3.4 surveillance and privacy 14
2.Navigating the European legal landscape: Freedom of expression and AI 17
2.1.Historical overview 17
2.2.Current legal frameworks for Freedom of expression 19
2.2.1.Council of Europe 19
2.2.2The European Union 21
2.3.The current regulation of AI in the context of freedom of expression 22
2.3.1.The European Union 22
2.3.2The Council of Europe 24
2.4.Recent regulatory responses 27
2.4.1.EU AI ACT 27
2.4.2.Convention on Artificial Intelligence, Human Rights, Democracy, and the Rule of Law 30
3. Case law 35
3.1.European Court of Human Rights 35
3.2.Court of Justice of the European Union 39
CONCLUSIONS 46
BIBLIOGRAPHY 48

INTRODUCTION

Artificial Intelligence has rapidly emerged as a transformative technology, influencing every aspect of modern life from healthcare and transportation to communication and education. What we saw twenty years ago in science fiction is now reality. A bioelectronic interface developed by Neuralink was implanted into the human brain for the first time in 2024, aiming to assist individuals with paralysis to regain capabilities, by translating neural signals into commands for external devices. The promise of AI to improve our lives is enormous. AI-based systems are already outperforming humans in every aspect of life. However, AI technology is still in its infant stages, undermining the importance of its regulation and supervision. The potential of AI to both benefit and damage civilization is much greater than any other previous technology.

As Stephen Hawking said, "Success in creating AI would be the biggest event in human history. Unfortunately, it might also be the last, unless we learn how to avoid the risks." As AI is integrated into our daily lives, its impact on our fundamental rights is uncontested, raising concerns about its impact on fundamental rights, particularly the right to freedom of expression. This thesis explores the intricate interplay between AI and freedom of expression in the digital era, focusing on the European context.

Central to this research is the examination of AI's influence on freedom of expression, especially as AI systems increasingly handle content moderation, surveillance, and information dissemination.

To be more precise, I am addressing the following questions:

1) How do AI technologies and their ramifications affect the right to freedom of expression?

2) How do European legal frameworks address the implications of AI on freedom of expression?

3) What are the ethical considerations and regulatory challenges in balancing AI innovation with the protection of freedom of expression?

The topic is of paramount importance in the digitally interconnected world. This research will contribute to the existing knowledge body by providing a comprehensive analysis of the intersection between AI and freedom of expression. It offers a nuanced understanding of how AI technologies can both enhance and challenge the right. Furthermore, the findings of this study have practical implications for policymakers, technologists, civil society organizations and other stakeholders. They can guide the development of ethical, human rights-centric AI, ensuring that the progress of technology does not come at the expense of fundamental rights.

The scope of the thesis is European region, covering both the Council of Europe (COE) and the European Union (EU) legal frameworks. It covers the period of inception of AI technologies to the present day, with a particular emphasis on recent developments in AI regulation.

The study acknowledges several limitations, including the rapidly evolving nature of AI technologies and regulations, which may render some findings outdated. Additionally, the focus on the European context may limit the generalizability of the conclusions to other regions.

The thesis is structured into three main chapters:

The first establishes the theoretical framework by defining AI, exploring its mechanisms, and examining its implications on freedom of expression, including content moderation, bias, surveillance, privacy, misinformation, and deepfakes.

The second chapter evaluates existing European legal frameworks on AI and freedom of expression, encompassing relevant instruments and recent regulatory responses from the COE and EU.

The third chapter delves into case law, analysing the approach of the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU) concerning AI and freedom of expression.

In this research, I will be using the doctrinal method, usually referred to as the "core legal research method." The research design integrates legal analysis, and examination of legal principles, rules, and doctrines, to gain a holistic understanding of the legal dimensions of AI. The study largely covers the recently adopted EU Artificial Intelligence Act and the Convention on Artificial Intelligence, Human Rights, Democracy, and the Rule of Law. Through a systematic doctrinal analysis, the research aims to identify gaps, ambiguities, and inconsistencies in not only drafted proposals but also existing prevailing doctrinal approaches. The research will incorporate a normative should-based approach, concerned with how things ought to be, and how to value them. It will assist me to focus on what are human rights, what is the content and scope of the right of freedom of expression, and how to interpret it with connection to AI.

1. AI and its implications on the right to freedom of expression

Artificial Intelligence is changing the world on a daily basis. The rapid development of AI has transformed various sectors of society, from healthcare and finance to education and justice systems. Automated hiring systems decide whether we are suitable for the job or not, cars on the market can drive themselves, diagnostic systems identify our health issues, and more and more risk assessment algorithms determine whether we are imprisoned or set free after being charged with a crime. The promise of AI to improve our lives is enormous. AI-based systems are already outperforming humans in every aspect of life. However, AI technology is still in its infant stages, undermining the importance of its regulation and supervision. The potential of AI to both benefit and damage civilization is much greater than any other previous technology. As Stephen Hawking said, "success in creating AI would be the biggest event in human history. Unfortunately, it might also be the last, unless we learn how to avoid the risks."

As AI is present daily, its influence on fundamental rights, particularly freedom of expression has garnered significant attention. The internet is currently the fastest and the most comprehensive information source available, serving as a global platform for discussing and expressing ideas. AI has changed the way we seek, receive, impart, and access information, it has changed how we exercise the right of freedom of expression in the digital ecosystem.[1] Those changes have substantial consequences for access to information, individual expression and the overall health of public discourse. This chapter examines AI's impact on the freedom of expression by defining AI, explaining its mechanisms and types, and exploring its implications on specifically content moderation, bias and discrimination, surveillance and privacy, and misinformation and deepfakes.

[1] Barbora Bukovska et al., SPOTLIGHT ON ARTIFICIAL INTELLIGENCE AND FREEDOM OF EXPRESSION, ed. Julia Haas, SPOTLIGHT ON ARTIFICIAL INTELLIGENCE AND FREEDOM OF EXPRESSION (Office of the Representative on Freedom of the Media, 2020). P. 13

1.1.What is AI?

The concept of AI has roots that stretch back to the myths and legends of classical antiquity, which describe mechanical men and artificial entities endowed with intelligence. However, the formal birth of AI as an academic discipline is often traced to a workshop held at Dartmouth College in 1956, where, John McCarthy, one of the founding American scholars of AI, defined it as "the science and engineering of making intelligent machines."[2]

Nowadays, there is no universally accepted definition of AI. According to the Stanford University report, AI is "a science and a set of computational technologies that are inspired by—but typically operate quite differently from-the ways people use their nervous systems and bodies to sense, learn, reason, and take action."[3] In 2018, the European Commission set up a High Level Expert Group on AI. The definition given by AI HLEG reads: "artificial intelligence refers to systems designed by humans that, given a complex goal, act in the physical or digital world by perceiving their environment, interpreting the collected structured or unstructured data, reasoning on the knowledge derived from this data and deciding the best action(s) to take (according to pre-defined parameters) to achieve the given goal. AI systems can also be designed to learn to adapt their behaviour by analysing how the environment is affected by their previous actions."[4]

AI systems operate through a combination of datasets and algorithms, "a series of rules written into computer code."[5] It is a group of instructions, which guide the computer to process the

[2] S. Matthew Liao, "A Short Introduction to the Ethics of Artificial Intelligence," in Oxford University Press eBooks, 2020, 1–42, https://doi.org/10.1093/oso/9780190905033.003.0001. P.3.
[3] "Executive Summary," One Hundred Year Study on Artificial Intelligence (AI100), n.d., https://ai100.stanford.edu/2016-report/executive-summary.
[4] High-Level Expert Group on Artificial Intelligence, "A Definition of AI: Main Capabilities and Scientific Disciplines," European Commission (Directorate-General for Communication, December 18, 2018), https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf. P.7
[5] Cristina Criddle, "What Is Artificial Intelligence and How Does It Work?," Financial Times, July 20, 2023, https://www.ft.com/content/bde93e43-7ad6-4abf-9c00-8955c6a9e343.

input data. Former UN special rapporteur David Kaye defines algorithm as: "code designed and written by humans, carrying instructions to translate data into conclusions, information or outputs."[6] Any AI system consists of sets of algorithms. AI itself can be viewed as a single, complex algorithm that integrates algorithms to perform. So basically, algorithms are used to process data, make decisions and learn from experience.

Taken as a whole, AI is the capacity of machines to do intelligent tasks, normally done by humans. AI systems are characterized by their ability to learn from data, adapt to new inputs, and perform tasks that typically require human intelligence, such as visual perception, speech recognition, decision-making, and language translation. It involves analysing inputs and generating outputs, taking actions or making predictions based on observed patterns and it seeks to mimic human-like cognitive functions, such as learning or problem-solving. These are systems designed by humans to operate with varying levels of autonomy, which, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments.[7]

1.2. Types of AI

AI can be divided into two broad categories: general and narrow AI. General AI (AGI) is yet unachieved AI system, that can display intelligence in multiple domains, with the ability to learn new skills, and which mimic or even suppress human intelligence.[8] An example would be

[6] United Nations and David Kaye, "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression," report, United Nations, August 29, 2018.
[7] OECD. "Recommendation of the Council on Artificial Intelligence." Report. OECD Legal Instruments, 2024. http://legalinstruments.oecd.org.
[8] _____. "Privacy and Freedom of Expression in the Age of Artificial Intelligence," April 2018. ARTICLE 19 and Privacy International, "Privacy and Freedom of Expression in the Age of Artificial Intelligence," April 2018, https://www.article19.org/wp-content/uploads/2018/04/Privacy-and-Freedom-of-Expression-In-the-Age-of-Artificial-Intelligence-1.pdf. P.6.

HAL 9000 in the 2001 movie A Space Odyssey, who controls the spaceship Discovery One, or Ava in the movie Ex-Machina, representing a humanoid robot with advanced AI, with the ability to understand and simulate human emotions, engage in complex conversations and exhibit self-awareness. The most optimistic scholars believe that the futuristic idea of AI singularity can become a reality by the end of the century. At the same time, experts warn what kind of risks "God-like AI" could pose to humankind.[9]

Narrow AI is what we are familiar with. It resembles human capabilities in narrow domains, with different degrees of autonomy and technical sophistication. [10]It is specialized and limited in scope. An example of narrow AI is voice assistants, social media recommendation systems, image recognition, etc. Narrow AI is implemented through Machine Learning (ML), Deep Learning (DL) and Reinforcement Learning.

- **Machine Learning (ML)** refers to the ability of computer programs to learn from and predictions based on data, without being specifically programmed to do so. ML algorithms can identify patterns in data and improve their performance over time. The vast majority of AI in the world today is powered by ML.[11] Examples of ML include Instagram algorithms, AlphaGo, and Deep Blue.
- **Deep Learning (DL)** is an ML technique that uses "neural networks", modelled on the human brain and is used to solve complex issues, such as speech recognition. The primary distinction between ML and DL is that DL does not require human input to comprehend and learn from data DL is capable of absorbing unstructured data in a raw form and differentiating between distinct data types.[12]

[9] Criddle, "What Is Artificial Intelligence and How Does It Work?"
[10] ARTICLE 19 and Privacy International, "Privacy and Freedom of Expression in the Age of Artificial Intelligence."
[11] Access Now and Lindsey Andersen, "HUMAN RIGHTS IN THE AGE OF ARTIFICIAL INTELLIGENCE," Access Now, 2021, https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf. P.8.
[12] Criddle, "What Is Artificial Intelligence and How Does It Work?"

- **Reinforcement Learning (RL)** is a distinctive approach within Machine Learning (ML) that focuses on learning through interactions with the environment and training based on feedback. AlphaZero, developed by Google DeepMind, exemplifies the power of ML. In 2017, AlphaZero defeated Stockfish, the world's strongest chess program at the time. Remarkably, AlphaZero had no pre-programmed moves or strategies derived from human play. Instead, its creators simply provided it with the rules of chess and instructed it to develop a strategy to maximize its wins. After only four hours of self-play, AlphaZero emerged as the world's most effective chess program. To date, no human has ever beaten it. AlphaZero integrates several advanced AI techniques: DL for learning representations and predicting moves, ML-the broader category encompassing the techniques used, RL-the primary framework for improving through self-play.[13]

1.3. AI implications on the right of freedom of expression

In democratic societies, freedom of expression is the cornerstone of human rights, enabling individuals to receive information, engage in public discourse and hold those in power accountable. This fundamental right is enshrined in numerous international legal frameworks, such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. Within European Legal frameworks, it is enshrined in the European Convention of Human Rights and the Charter of Fundamental Rights of the European Union, highlighting its critical role in fostering an open and democratic society. However, advances in AI have introduced complex challenges and opportunities that profoundly impact freedom of expression. As AI technologies become increasingly integrated into public life, concerns are raised about their effects on the freedom of expression. The dual nature of AI- its capacity to

[13] Henry A Kissinger, Eric Schmidt, and Daniel Huttenlocher, The Age of AI: "THE BOOK WE ALL NEED" (Hachette UK, 2021). P.7-8.

both benefit and undermine freedom of expression- necessitates careful examination of its implications.

1.3.1 misinformation and deepfakes

Access to information can be considered a vital foundation of the freedom of expression. While AI contributes to enhancing access to information on a global scale, it presents several challenges that need to be addressed. Tech companies are designing chatbots, and other technologies like ChatGPT, that can "hallucinate" from time to time and give factually incorrect or made-up information. Much of the data by which those generative AIs are trained comes from the internet. The Internet is full of useful information; however, it is also full of fake information, hate speech and other junk. Chatbots absorb them with implicit and explicit biases.[14] Due to their surprising way of mixing and matching the information, they create convincing language that is untrue. Therefore, algorithms can inadvertently increase the spread of misinformation, disinformation, and fake news, undermining the credibility of information sources and undermining public trust.

Moreover, Inequality in the distribution of access to AI technologies and digital infrastructure worsens the socio-economic imbalances and limits the ability of marginalized communities to benefit from access to information and technological innovation. AI tools also tend to have linguistic inaccuracies and biases, which can lead to foiling cross-cultural communication and restricting access to information in languages other than dominant ones.

The rise of deepfake technology poses a significant threat to freedom of expression. Misuse of generative AI can turn creepy and dangerous. Current deepfakes are so hyper-realistic, that it is

[14] Metz, Cade. "What Makes Chatbots 'Hallucinate' or Say the Wrong Thing?" The New York Times, April 4, 2023. https://www.nytimes.com/2023/03/29/technology/ai-chatbots-hallucinations.html.

almost impossible to distinguish synthetic media from authentic. It can be used as a tool to control the narrative online, political manipulation, harm to individuals' reputations and mental health, increasing societal polarization and division. In 2018, Barack Obama's famous deepfake video was created, where he was giving a speech about the dangers of deepfake technology. In fact, it was filmmaker Jordan Peele, showing the possibilities of Deepfake technologies. Recently, extremist groups started to experiment with AI, in order to create a flood of new propaganda. Previously, a couple of thousand images shared by groups linked to Hezbollah and Hamas were picked up, designed to influence the narrative around Israel -Hamas war.[15] AI-generated images, deepfakes and synthetic media make it increasingly difficult to distinguish between genuine and fabricated content.

Misinformation and deepfakes raise concerns not only for freedom of expression but also for democracy generally. It can be used for election interference, by creating misleading information about candidates and swaying voter opinions it can undermine media integrity and even induce economic disruption or national security.

1.3.2 Content moderation

Content moderation is a crucial challenge for exercising freedom of expression. Nowadays, internet intermediaries are called upon by the state or by law to moderate the content on different platforms.[16] AI tools like spam detection, hash-matching technology, keyword filters, and natural language processing are employed to assess and filter content. Companies argue that AI can efficiently identify and remove inappropriate or illegal content with higher accuracy than human moderation. Both private and public sectors support increasing AI's role in content

[15] David Gilbert, "Here's How Violent Extremists Are Exploiting Generative AI Tools," WIRED, n.d., https://www.wired.com/story/generative-ai-terrorism-content/.
[16] Bukovska et al., SPOTLIGHT ON ARTIFICIAL INTELLIGENCE AND FREEDOM OF EXPRESSION.P.32

moderation to tackle the growing volume of harmful online content.[17] On one hand, it can be beneficial as it detects hate speech, security threats etc and removes it even before sharing it or post factum. However, now we have social media platforms using algorithms that decide whose voices are going to be heard. AI-powered content moderation systems can unintentionally censor legitimate speech by flagging or removing content that is deemed to be controversial or sensitive. AI systems have higher efficiency and accuracy rates compared to human moderation but are limited in understanding context and may lead to errors in content removal, leading to concerns regarding censorship and smothering diverse viewpoints. AI-enabled censorship results in the restriction of freedom of religion when it is used to identify and take down religious content. It also threatens the freedom of association when it results in the removal of online groups, pages, and content that facilitate the gathering of individuals.[18] This applies both to private sector representatives and the government. Authoritarian powers can use content moderation to maintain power, oppress opposition and control the narrative.

Moreover, the lack of transparency in AI-driven moderation decisions can erode public trust in these systems. In the context of content removal of security threats, hate speech, media diversity, and surveillance implications concerns are raised regarding the transparency and accountability of social media platforms.

[17] United Nations and David Kaye, "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression," report, United Nations, August 29, 2018. P.8.
[18] Artificial Intelligence and the Law (Intersentia, 2021). P.128.

1.3.3 Bias and discrimination

Discrimination is a crucial topic when it comes to the use of AI because the very purpose of machine learning algorithms is to categorise, classify and separate.[19] Bias in AI arises from various sources, including the data used to train algorithms, the design of the algorithms themselves, and the societal context in which they are deployed. As mentioned above, AI can absorb biases in training data, it can be as fair as the data itself. Furthermore, algorithms are developed by humans and therefore reflect geography, social and cultural practices, social class, race, gender, and conscious and unconscious bias. These biases in AI can materialize in ways that disproportionally affect certain groups, leading to discriminatory outcomes and undermining the principle of equality in expression. Artificial intelligence-driven newsfeeds may perpetuate and reinforce discriminatory attitudes, while artificial intelligence profiling and advertising systems have demonstrably facilitated discrimination along racial, religious and gender lines.[20]

In 2016, Microsoft released an artificial intelligence chatbot, named Tay, via Twitter, designed to train and pick up lexicons and syntax from interactions with real people posting on Twitter. They had to shut it down, as after a couple of hours of training Tay became racist, misogynist, sexist, and nazi, that started spewing a series of lewd and racist tweets. [21] This hard lesson showed the world that Large Language Models (LLMs) and humans are both mirroring each other. In healthcare, biased algorithms can worsen already existing inequalities in diagnosis and treatment. One such case was revealed in a study published in Science Translational Medicine, which revealed racial bias in an algorithm that assessed patient's need for additional care. It

[19] European Union Agency for Fundamental Rights, "GETTING THE FUTURE RIGHT: ARTIFICIAL INTELLIGENCE AND FUNDAMENTAL RIGHTS," report (Publications Office of the European Union, 2020), https://doi.org/10.2811/58563.
[20] United Nations and David Kaye, "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression," report, United Nations, August 29, 2018 P.8.
[21] James Vincent, "Twitter Taught Microsoft's AI Chatbot to Be a Racist Asshole in Less Than a Day," The Verge, March 24, 2016, https://www.theverge.com/2016/3/24/11297050/tay-microsoft-chatbot-racist.

showed that the algorithm, predicting which patient would benefit from additional care for complex medical needs, systematically underestimated Black patients' needs compared to White patients.[22] This emphasises one more time the crucial need for thoughtful evaluation of AI algorithms for fairness and equity, especially in healthcare when its outcomes can have consequences on human life.

Another, prominent example of AI bias is language and cultural bias. AI systems are often trained primarily on data from dominant languages and cultures, leading to poorer performance for non-dominant languages and dialects. This can marginalize speakers of these languages, limiting their ability to participate fully in online discourse.

Predictive policing algorithms are criticized for being racist because they reinforce systemic racism by disproportionately targeting Black communities as well. These algorithms are influenced by arrest rates, which show that Black individuals are more likely to be arrested than white individuals. As a result, the data these algorithms rely on, like arrest records, can lead to biased assessments and unfairly focus on young Black people.[23]

Furthermore, AI hiring algorithms are used broadly by companies to streamline the recruitment process. However, these systems can inadvertently perpetuate existing biases present in historical hiring data. Amazon's AI recruitment tool, developed to review job applications and identify top candidates, was found to be biased against women. The system was trained on resumes submitted to the company over a ten-year period, which predominantly came from

[22] Ziad Obermeyer et al., "Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations," Science 366, no. 6464 (October 25, 2019): 447–53, https://doi.org/10.1126/science.aax2342.
[23] Will Douglas Heaven, "Predictive Policing Algorithms Are Racist. They Need to Be Dismantled.," MIT Technology Review, June 21, 2023, https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/.

men. Consequently, the AI system learned to prefer male candidates and penalized resumes that included the word "women's," such as "women's chess club captain." [24]

1.3.4 surveillance and privacy

AI-powered surveillance tools pose profound implications for the freedom of expression. Artificial intelligence-driven decision-making systems depend on the collection and exploitation of data, ranging from ambient, non-personal data to personally identifiable information, with the vast majority of data used to feed artificial intelligence systems being somewhere in the middle — data that are inferred or extracted from personal data, or personal data that have been anonymized (David Kaye, 2018). Artificial intelligence (AI)-driven surveillance tools are able to watch your online actions, gather data, and identify which applications you use. They can also determine what kind of information you like and dislike, as well as how long you spend staring at a particular piece of content when scrolling. AI tools use techniques like video surveillance, facial recognition, and behaviour analysis. These technologies enable extensive monitoring and data collection, raising concerns about the potential for abuse and the erosion of civil liberties.

In addition to the private sector, governments have the ability to utilize mass surveillance techniques against their citizens. State mass surveillance can have a “chilling effect”, which describes the perception of being constantly surveyed or monitored by AI surveillance systems. It can lead to self-censorship, discouraging people from freely expressing themselves online or engaging in controversial viewpoints. Surveillance affects anonymity and the ability to seek and receive information without being identified. The lack of free communication impedes journalists’ ability to research or overall limits the media’s role in holding the government

[24] Erin Winick, “Amazon Ditched AI Recruitment Software Because It Was Biased Against Women,” MIT Technology Review, June 17, 2022, https://www.technologyreview.com/2018/10/10/139858/amazon-ditched-ai-recruitment-software-because-it-was-biased-against-women.

accountable. For example, a 2016 study showed a significant drop in Wikipedia traffic to articles about terrorism following Snowden's 2013 disclosures, indicating a chilling effect. Another study found that awareness of NSA surveillance reduced willingness to express minority opinions on social media.[25]

AI-powered facial recognition can identify journalists or activists at protests or trace their digital activities, risking their confidentiality and safety. In Russia, the government actively monitors social media accounts and uses surveillance cameras against activists. Especially, after Russia invaded Ukraine in February 2022, online censorship and prosecutions for social media posts and comments spiked so much that it broke all existing records. A major factor was a law, adopted one week after the invasion, which criminalized antiwar sentiment and outlawed spreading false information about or "discrediting" the army. As rights advocates say, Russia tracks, censors, and spies on its citizens, building what some call "cyber gulag."[26]

Ultimately, AI's profound effect on how we exercise freedom of expression in the digital era is undeniable. The dual nature of AI- the capacity to both enhance and erode the foundation of democracy at so far unimaginable levels, is both exciting and terrifying. On the one hand, it can broaden access to information, enhance its quality, make it more affordable, efficiently moderate content, and cease unlawful information. On the other hand, it can deliberately cause censorship, erode public trust and reinforce preexisting social biases. Issues such as misinformation and deepfakes, biased algorithms, privacy violations and mass surveillance call for the urgent need for ethical guidelines in the development of AI and a robust legal framework

[25] Bukovska et al., SPOTLIGHT ON ARTIFICIAL INTELLIGENCE AND FREEDOM OF EXPRESSION. P.61-64.
[26] Dasha Litvinova, "The Cyber Gulag: How Russia Tracks, Censors and Controls Its Citizens | AP News," AP News, May 23, 2023, https://apnews.com/article/russia-crackdown-surveillance-censorship-war-ukraine-internet-dab3663774feb666d6d0025bcd082fba.

to ensure that AI technologies uphold fundamental human rights and freedoms, including freedom of expression.

2. Navigating the European legal landscape: Freedom of expression and AI

Freedom of expression is the cornerstone of all democracies, fostering an environment where people can engage in open discourse, access information, express themselves and even hold those in power accountable. It is not only a fundamental right, but also a key enabler of other rights and freedoms. It encompasses the interrelated principles of freedom of speech, freedom of the press, freedom of assembly and association, and Freedom of thought and conscience. In the digital age, the interplay between freedom of expression and AI has emerged as a critical area of concern. The transformative potential of AI presents both unprecedented opportunities and complex challenges. Central to this concern is the need to balance the protection of fundamental rights, particularly freedom of expression with the regulatory measures necessary to address risks associated with AI. This chapter delves into the current European legal framework governing freedom of expression in the context of AI, foundational principles, national jurisdictions and proposed regulatory responses. Ultimately, this chapter seeks to analyse, the ongoing efforts within the European legal system to ensure that the promise of AI is leveraged in a manner that upholds the fundamental principles of liberty, democracy and human dignity.

2.1.Historical overview

The history of freedom of expression in Europe long predates the international human rights instruments. Its origins can be seen in the ancient civilization of Athens in the 6th and 5th centuries BC, with emerging free speech and participatory governance. However, it was during the Enlightenment period when freedom of expression began to solidify as a fundamental human right.

Enlightenment thinkers, such as John Locke and Voltaire upheld the concept of free speech and exchange of opinions. In his work, “Two Treatises of Government", Locke emphasizes the importance of the right to express one’s ideas freely, without fear of censorship, as a tool of progress and a pillar of individual autonomy. The invaluable invention of the Printing Press by Johannes Gutenberg in the 1450s made information accessible and played a crucial role in intellectual exchange, catalysing the spread of ideas.

Later, the Declaration of the Rights of the Man and Citizen, adopted during the French Revolution in 1789, specifically declared that the freedom of speech is inherent and indisputable. Article 11 of the Declaration states: “The free communication of ideas and opinions is one of the most precious of the rights of man. Every citizen may, accordingly, speak, write, and print with freedom, but shall be responsible for such abuses of this freedom as shall be defined by law.” [27]

In the aftermath of World War II, the fight for the right of freedom of expression reached the turning point, by adopting the Universal Declaration of Human Rights in 1948. UDHR reflected the global commitment to safeguarding fundamental freedoms and rights. Article 19 unequivocally declares that: “Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." [28]

Nowadays, the right to freedom of expression is recognised and protected in international and national human rights law. The right is enshrined in Article 19 of the International Covenant on Civil and Political Rights, Article 13 of the American Convention on Human Rights and Article

[27] “Declaration of the Rights of Man and of the Citizen.” n.d. https://web.archive.org/web/20130606053037/http://www.hrcr.org/docs/frenchdec.html.
[28] United Nations. n.d. “Universal Declaration of Human Rights | United Nations.” https://www.un.org/en/about-us/universal-declaration-of-human-rights.

9 of the African Charter on Human and Peoples' Rights.[29] Within the European region, freedom of expression is grounded in the European Convention on Human Rights (ECHR)[30] and the Charter of Fundamental Rights of the European Union (CFR). [31]

Fast forward to the digital age, first the internet and then AI revolutionized the way we seek, receive and share information. It changed the scope and speed of communication, empowering individuals in every corner of the world to engage in global discourse. However, alongside its promise, AI brings new complex challenges: issues of censorship, surveillance, dangers of misinformation and deep fakes and the ability to exaggerate existing social biases in digital reality. European regulatory bodies and courts are navigating these challenges to ensure that AI does not threaten the democratic society, by adapting legal frameworks.

2.2. Current legal frameworks for Freedom of expression

2.2.1.Council of Europe

Aiming to preserve democracy, human rights and the rule of law, the Council of Europe (COE) was founded in 1948, by the Treaty of London. Initially formed by 10 European states, it now includes 46 members. One of its most famous and main entities is the European Court of Human Rights (ECtHR), which rules on individual and state application, is the main source of interpretation of the ECHR. The Convention itself ratified by the COE state parties, provides robust protection for freedom of expression and remains the cornerstone of human rights protection in Europe.

Article 10 of ECHR guarantees the right to freedom of expression, including freedom to hold opinions and to receive and impart information and ideas without interference by public

[29] Andrew Puddephatt, Freedom of Expression, The essentials of Human Rights, Hodder Arnold, 2005. p. 128
[30] European Convention on Human Rights, 1950.
[31] Charter of Fundamental Rights of the European Union, 2000.

authority and regardless of frontiers. Over the years, ECtHR has handed down several landmark rulings that have shaped the understanding and application of freedom of expression within the Council of Europe's member states.

One such ruling is the case of Handyside v. United Kingdom (1976),[32] where the Court emphasized the importance of freedom of expression as one of the essential foundations of a democratic society and stressed that it is applicable not only to information or ideas that are favourably received but also to those that "offend, shock, or disturb the state or any sector of the population."[33]

While freedom of expression is a fundamental human right, it is not an absolute right. Article 10(2) of the Convention, allows restrictions on freedom of expression that are "necessary in a democratic society" and prescribed by law for legitimate aims, such as national security, public safety, prevention of disorder or crime, protection of health or morals, protection of the reputation or rights of others, ECtHR assesses the necessity and proportionality of restrictions on freedom of expression, emphasizing the importance of balancing individual rights with the broader interests of society. [34]

In its landmark ruling in the case of Lingens v. Austria (1986),[35] the Court stressed the vital role of freedom of expression in democratic societies and emphasized that restrictions on this right must be narrowly interpreted and subject to strict scrutiny. The case reaffirmed how crucial is to protect even controversial or upsetting speech, as long as it is lawful.

[32] Handyside v. the United Kingdom (Application no. 5493/72), 1976. EctHR https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57499%22]}.
[33] Ibid, Par. 49

[35] Lingens v. Austria (Application no. 9815/82),1986, EctHR https://hudoc.echr.coe.int/fre#{%22fulltext%22:[%22Lingens%20v.%20Austria%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-57523%22]}.

As affirmed by EctHR rulings, ECHR continues to be a fundamental pillar in protecting the right to freedom of expression across Europe. ECtHR plays a crucial role in shaping the understanding, application and limits of it, emphasising the balancing of individual rights with the broader interest of society.

2.2.2The European Union

After the initial stages of European integration began after World War II, the EU was established in 1993, by the Maastricht treaty, in 1993, with the goal of promoting economic integration, social progress and political cooperation within member states. The central instrument of the EU is the Charter of Fundamental Rights of the European Union. As the Charter has the same legal value as EU treaties,[36] all EU institutions and bodies are bound by the Charter, as are member states when they act within the scope of EU law.[37]

The Charter enshrines the right to freedom of expression in Article 11, guaranteeing the freedom to hold opinions, and to receive and impart information and ideas without interference by public authority and regardless of borders. Similarly, according to ECHR freedom of expression is not an absolute right and can be limited under EU law, while limitations are prescribed by law, pursuing legitimate aims and being proportionate and necessary in a democratic society.

EU law is implemented through a multi-layered approach involving EU institutions, national authorities and the judiciary. Mechanisms include regulations, directives and decisions. The European Commission oversees the implementation and enforcement of EU law, ensuring compliance by member states. The national courts also play a crucial role in applying EU law,

[36] Treaty on European Union, 2007. Article 6.
[37] Åklagaren v. Hans Åkerberg Fransson [GC], 26 February 2013, CJEU, Par. 17, 20. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62010CJ0617

often referring questions concerning interpretation or validity to the CJEU through the preliminary ruling procedure under Article 27 of the Treaty on the Functioning of the European Union (TFEU).[38]

CJEU has addressed numerous cases involving freedom of expression, often clarifying how EU law should be applied consistently across member states. In its ruling the court reinforced the EU's commitment to protecting freedom of expression, highlighting that any restriction of the right must be proportionate and respectful to fundamental rights. In case Case C-70/10, Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs (SABAM),[39] the court balanced the intellectual property right with freedom of expression, stressing that internet access is a vital right in the digital era and any limitation on it should be carefully considered.

While the EU ensures a robust framework for freedom of expression through its charter and legal instruments, CJEU's role is indispensable in interpreting and enforcing these rights, therefore contributing to a unified and right are respecting European Legal landscape.

2.3. The current regulation of AI in the context of freedom of expression

2.3.1.The European Union

Besides the foundational documents, there are other regulations of AI in the context of freedom of expression within Europe. A central piece, in this context, is the General Data Protection Regulation (GDPR-Regulation (EU) 2016/679), [40]enacted by the EU in 2018. While it is not AI-specific, its principles of data protection are highly relevant to AI applications, as most of them are highly dependent on data. GDPR aims to protect data privacy and personal information

[38] Treaty on the Functioning of the European Union, 1958. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:4301854.
[39] Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM). 2011, ECLI:EU:C:2011:771 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62010CJ0070
[40] General Data Protection Regulation (GDPR-Regulation (EU) 2016/679) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

and give individuals greater control over their data. Furthermore, it imposes strict rules on the automated processing of data in the European Economic Area (EEA) and obliges organizations that collect, store and process personal data to follow requirements, including obtaining consent, notifying data breaches and carrying out data protection impact assessment. Article 22 of GDPR gives individuals the right not to be subject to decisions based solely on automated processing, including profiling, which significantly affects them. AI systems making automated decisions must include human oversight and safeguards to protect individual's rights and freedoms.[41]

GDPR is coupled with another EU directive- the Law Enforcement Directive (LED) 2016/680.[42] While GDPR covers general data processing activities, the LED specialises in law enforcement data processing. Its primary goal is to ensure that personal data processed by competent authorities such as the police or judicial authorities for law enforcement purposes are adequately protected. This includes data processed for the prevention, investigation, detection, or prosecution of criminal offences and the execution of criminal penalties. LED emphasises data protection principles like Lawfulness and fairness, purpose limitation, Data minimalization, accuracy, storage limitation, confidentiality, and integrity and gives individuals the right to access their data, request correction of inaccurate data or deletion in certain instances and restrict processing of their data. Both GDPR and LED complement each other, establishing a robust framework within the EU for protecting personal data. Non-compliance with them can lead to legal consequences, including fines, penalties or even loss of business opportunities.

[41] "Art. 22 GDPR – Automated Individual Decision-making, Including Profiling - General Data Protection Regulation (GDPR)," General Data Protection Regulation (GDPR), July 26, 2018, https://gdpr-info.eu/art-22-gdpr/.
[42] Law Enforcement Directive (2016/680) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ENG&toc=OJ%3AL%3A2016%3A119%3ATOC
.

In regard to discrimination in AI algorithms (especially in automating hiring decisions), EU non-discrimination law is key for safeguarding human rights, including freedom of expression. Furthermore, directives on Employment Equality (2000/78/EC)[43], the Racial Equality (2000/43/EC)[44] and the recast Gender Equality Directive (2006/54/EC)[45] with different scope provide more specific protection.

European commission established High Level Expert Group (HLEG) on AI, also developed guidelines for trustworthy AI[46] in 2019, with the goal of ensuring that AI serves the common good and complies with ethical and societal values. The guideline focuses on the principles of human-centric AI, including human oversight, general safety, accuracy, diversity, non-discrimination, fairness, accountability and transparency, and sustainable and environmentally friendly AI.

2.3.2The Council of Europe

In addition, the COE Convention for the Protection of Individuals about Automatic Processing of Personal Data[47] is a pioneer, the first legally binding treaty dealing with privacy and data protection, adopted in 1981, is another source of European data protection obligation. It has served as a model for data protection legislation, including the GDPR. In 2018, the COE approved the modernization of the convention, acknowledging AI technology developments and following risks. As the Committee of the convention reported, "personal data have

[43] Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32000L0078.
[44] Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32000L0043.
[45] Directive 2006/54/EC of the European Parliament and of the Council of 5 July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (recast) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32006L0054.
[46] "Ethics Guidelines for Trustworthy AI," Shaping Europe's Digital Future, April 8, 2019, https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai
[47] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981. https://rm.coe.int/1680078b37

increasingly become both the source and the target of AI applications."[48]Changes in the convention included obligation to declare data breaches, greater transparency of data processing and new rights for the persons in an algorithmic decision-making context.[49]

Another COE convention relevant to risks related to AI is the Convention on Cybercrime, known as Budapest Convention.[50] It was adopted in 2001 and is the first international treaty seeking to address the internet and cybercrimes. The convention covers a wide range of cybercrimes including hacking, fraud, child pornography and copyright infringement. It also sets out guidelines for the investigation and prosecution of cybercrimes, as well as measures to enhance international cooperation in fighting cybercrime. It is not only a legal document, but also a framework, that permits hundreds of practitioners from Parties to share experiences and create relationships that facilitate cooperation in specific cases, including in emergencies, beyond the specific provisions foreseen in this Convention.[51]

Besides regulations, the Committee of Ministers of the COE has issued several recommendations, and soft law instruments to guide member states in addressing human rights risks associated with the development and application of AI. Among those, two important recommendations are Recommendation CM/Rec (2020)1 on the Human Rights Impacts of Algorithmic Systems[52] and Recommendation CM/Rec (2020)2 on the Development and Application of Bioethics in the Field of AI. Recommendation CM/Rec (2020)1 addresses broad

[48] Council of Europe, "New Guidelines on Artificial Intelligence and Data Protection," Data Protection, February 4, 2019.https://www.coe.int/en/web/data-protection/-/new-guidelines-on-artificial-intelligence-and-personal-data-protection.
[49]"Modernisation of the Data Protection 'Convention 108' - Portal - www.coe.int," Portal, n.d., https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet.
[50] Convention on Cybercrime, 2001 https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185.
[51] "Budapest Convention - Cybercrime - www.coe.int," Cybercrime, n.d., https://www.coe.int/en/web/cybercrime/the-budapest-convention.
[52] "Recommendation CM/Rec(2020)1 of the Committee of Ministers to Member States on the Human Rights Impacts of Algorithmic Systems - Freedom of Expression - www.coe.int," Freedom of Expression, April 8, 2020, https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/aDXmrol0vvsU/content/recommendation-cm-rec-2020-1-of-the-committee-of-ministers-to-member-states-on-the-human-rights-impacts-of-algorithmic-systems.

human rights implications of algorithmic systems, underscoring transparency, accountability, redress and human oversight and impact assessments, meaning before deploying AI systems, comprehensive human rights impact assessments should be conducted to identify and mitigate potential negative impacts. While sharing the general principles of the above recommendation, Recommendation CM/Rec (2020)2 focuses on integrating bioethical principles into the development and application of AI systems that are used in healthcare and biomedicine. Its emphasis on human dignity informed consent and ethical considerations should guide AI research and innovation in biomedicine.

Even though OECD (Organisation for Economic Co-operation and Development), is not limited to Europe, its principles on AI issued in 2019 are still relevant, as most European countries are member states. The principles, represent intergovernmental standards on AI, sharing a common perspective on trustworthy and human-centric AI development.[53]

The regulation of AI within the context of freedom of expression in Europe is complex but quite comprehensive. It is primarily anchored by the GDPR (General Data Protection Regulation), the LED (Law Enforcement Directive), and various conventions and recommendations from the Council of Europe (COE). While these frameworks address specific applications and risks of AI and collectively safeguard data protection, uphold human rights and promote the ethical development of AI, the legal landscape is still missing a foundational, main, legally binding document, addressing all risks and concerns regarding AI, covering both private and public sector. EU AI Act and Convention on AI together promise to take that role. Furthermore, there is a significant disparity in the rate of advancement of AI systems compared to the legal system. Therefore, continuous vigilance and adaptation are essential to meet the evolving challenges posed by AI technologies.

[53] "OECD AI Policy Observatory Portal," n.d., https://oecd.ai/en/ai-principles.

2.4.Recent regulatory responses

2.4.1.EU AI ACT

As many foreseeable safety risks through the AI implementation process exist, the European Union worked on regulating the development, deployment, and use of artificial intelligence (AI) technologies. One of the main objectives of this regulation is to ensure that AI is developed and used responsibly and ethically respecting fundamental rights and avoiding safety risks.

The European Commission launched a white paper in 2020, "A European Approach to Excellence and Trust Public Consultation on a European Approach to Excellence and Trust in AI". The commission focused on the concept of "European AI" and highlighted that "European AI must be grounded in our values and fundamental rights such as human dignity and privacy protection".[54] The white paper marked the beginning of a comprehensive public consultation phase, that gathered input from different stakeholders, such as AI developers and deployers, companies and business organizations, public administrations, civil society organizations, academics and citizens.[55] Through the consultation, the commission gathered diverse perspectives and concerns from stakeholders and helped shape the draft regulation.

In April 2021 the European Commission introduced a proposal outlining an EU regulatory framework for AI. The draft AI act was the first-ever attempt to enact a horizontal regulation of AI and on 21 May 2024, the Council of European Union approved the Act. This is the final

[54] "White Paper on Artificial Intelligence: A European Approach to Excellence and Trust." n.d. European Commission. https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en. P.2.
[55] "White Paper on Artificial Intelligence: Public Consultation Towards a European Approach for Excellence and Trust." 2020. Shaping Europe's Digital Future. July 17, 2020. https://digital-strategy.ec.europa.eu/en/library/white-paper-artificial-intelligence-public-consultation-towards-european-approach-excellence-and.

stage in the legislative process, leading to the formal signing of the legislation and its publication in the EU Journal.

EU AI Act is an ambitious framework, the world's first law governing AI. It is part of a wider package of policy measures to support the development of trustworthy AI, which also includes the AI Innovation Package and the Coordinated Plan on AI, aiming to foster trustworthy AI within Europe and beyond. [56] According to Article 2 of the regulation, it applies to AI providers, deployers, importers and distributors, product manufacturers, affected persons that are located in the Union. It also applies to AI systems used in the EU, even if they are made elsewhere.[57]

The Act established a tiered risk-based approach, classifying AI systems into high-risk, low-risk, and minimal-risk categories, each with corresponding regulatory obligations, ensuring proportionate regulation based on potential harm. "High-risk," AI systems are those used in critical infrastructure, law enforcement, educational or vocational training, employment, essential private and public services, and certain remote biometric identification systems. “AI systems are always considered high-risk if they profile individuals, i.e. automated processing of personal data to assess various aspects of a person’s life, such as work performance, economic situation, health, preferences, interests, reliability, behaviour, location or movement.”[58] Developers and deployers of high-risk AI systems must adhere to several obligations, such as: Conducting risk assessments and implementing risk management systems, ensuring high-quality data sets to minimize biases and ensure accuracy, providing transparency to users about the AI system's capabilities and limitations, detailed documentation and record-keeping. Furthermore, it introduces an EU database for high-risk AI systems for transparency.

[56] “AI Act,” Shaping Europe’s Digital Future, May 29, 2024, https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.
[57] EU AI Act, 2024. Article 2. https://artificialintelligenceact.eu/article/2/
[58] “High-level Summary of the AI Act | EU Artificial Intelligence Act,” n.d., https://artificialintelligenceact.eu/high-level-summary/.

Limited-risk AI systems are subject to lighter transparency obligations, such as developers and deployers must ensure that end-users are aware that they are interacting with AI. Minimal Risk is unregulated. Furthermore, the Act establishes unacceptable risks, that are prohibited, including social scoring systems, subliminal, manipulative, or deceptive techniques, and systems exploiting vulnerabilities related to age, disability, or socio-economic circumstances to distort behaviour.

In February 2024, the European Commission established the European AI Office, which will oversee the AI Act's enforcement and implementation with member states. It aims to foster international collaboration with institutions, stakeholders and experts, strengthen the development and use of trustworthy AI and position Europe as a leader in the ethical development of AI.[59]

While the AI Act provides a comprehensive regulatory framework aiming to balance individual protection, legal certainty, and innovation promotion, encompasses support for innovation, and introduces transparency and flexibility, there are some concerns and critiques for potentially excessive regulation that might deter investment in European AI startups and slow digital economy growth. Furthermore, its overlap with GDPR and ambiguity in territorial scope for AI systems used in the EU but developed outside of it need clearer definitions. Error-free training data requirements can be considered overly stringent as well, potentially hindering smaller organizations and innovation. The readiness of national authorities to comply with the regulation is heavily questionable as well.[60] Moreover, critiques emphasize that while the AI Act includes initial provisions on environmental impact, it lacks a comprehensive framework

[59] "European AI Office," Shaping Europe's Digital Future, n.d., https://digital-strategy.ec.europa.eu/en/policies/ai-office.
[60] Sandy Tsakiridi, " The draft AI Act: the good, the bad and the ugly," Privacy and Data Protection, 2022. https://advance.lexis.com/api/document?collection=analytical-materials&id=urn:contentItem:64HR-4J61-F27X-60DT-00000-00&context=1516831. P. 3-7

to manage the significant energy and resource consumption associated with large-scale AI models. It also lacks substantial public investment compared to global competitors like the US and China, which hampers Europe's ability to innovate and compete in AI development and deployment.[61]

In addition, the EU recently adopted two significant acts: Digital Services Act (DSA)[62] and the Digital Markets Act (DMA)[63], aiming to modernize the EU legal framework governing the digital market and services. DSA applies online platforms, social media networks, and e-commerce platforms and addresses online disinformation, illegal content, and the responsibilities of digital service providers. It obliges platforms to implement measures to mitigate harmful online activity risks, enhance users' rights protection and increase transparency requirements. On the other hand, DMA promotes fair competition between online platforms in the digital market by setting out dos and don'ts, to ensure the dominant platforms do not abuse their market power. It requests gatekeepers to provide fair access to their services for competitors and users and prohibit unfair practices.

2.4.2.Convention on Artificial Intelligence, Human Rights, Democracy, and the Rule of Law

A similar approach is integrated into the proposed convention on AI by the Council of Europe. The Committee of Ministers has tasked the Committee on Artificial Intelligence (CAI) in 2019

[61] Philipp Hacker, What's Missing From the EU AI Act, n.d., https://doi.org/10.59704/3f4921d4a3fbeeee.https://verfassungsblog.de/whats-missing-from-the-eu-ai-act/.
[62] "The EU's Digital Services Act," European Commission, n.d., https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en.
[63] "The Digital Markets Act: Ensuring Fair and Open Digital Markets," European Commission, n.d., https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en.

with elaborating a legally binding instrument on the development, design and application of AI systems based on the Council of Europe's standards on human rights, democracy and the rule of law, based on such basic principles.

On May 17, 2024, the COE adopted the first international, legally binding treaty on AI. It is designed to create a balanced framework that harnesses the benefits of AI while mitigating its risks to human rights, democracy and the rule of law while being conducive to technological innovation. To endure time, the convention does not regulate technology and is completely technology-free, aiming to fill in any legal gap that may result from the rapid development of technology. The convention covers the use of AI systems by both Public authorities and the private sector.[64] Fundamental rights are a key priority for the COE in AI regulation. It aims to ensure that AI is developed, deployed, and used in a way that respects people's dignity, privacy, non-discrimination, and other fundamental rights. The [framework] Convention focuses on ensuring the continuous application of human rights and the principle of the rule of law in situations where AI systems are helping or replacing human decision-making or performing other relevant tasks in these situations. Furthermore, AI systems are used only in a way that does not directly or indirectly harm or undermine the democratic processes.

Furthermore, the convention requires party states to establish procedures allowing affected persons to lodge complaints with competent authorities. the Committee on Artificial Intelligence (CAI) will oversee the implementation and compliance process by state parties. The framework establishes a follow-up mechanism, the conference of the Parties, composed of

[64] Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, 2024 https://rm.coe.int/1680afae3c

official representatives of the Parties to the Convention to determine the extent to which its provisions are being implemented.[65]

While the Council of Europe's (Coe) initiative to create the first legally binding international instrument on AI has garnered strong support from various stakeholders, it has also faced constructive criticism. The European Data Protection Supervisor (EDPS), the independent data protection authority of the European Union (EU), has provided a critical assessment of the Convention. The EDPS suggests that the Convention might miss the opportunity to establish a robust and effective legal framework essential for the development and adoption of trustworthy AI. The assessment emphasizes that the high level of generality and the declarative nature of the draft provisions could lead to inconsistent application across different states, thereby undermining legal certainty. There is significant concern over the absence of explicit prohibitions ('red lines') in the draft Convention against AI applications that pose unacceptable risks. The EDPS stresses the need for clear criteria and examples of prohibited AI uses to guide member states in implementation, ensuring legal certainty and foreseeability for developers, providers, and users of AI applications. Consequently, the EDPS calls for the Framework Convention to incorporate stronger and clearer safeguards.[66]

Moreover, civil society organizations have expressed their concerns as well in an open letter to convention negotiators, emphasising the need for equal coverage for public and private sectors, as some negotiating states are attempting to exclude private companies The letter urges the

[65] "The Framework Convention on Artificial Intelligence - Artificial Intelligence - www.coe.int," Artificial Intelligence, n.d., https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence.

[66] European Data Protection Supervisor. "EDPS Statement in View of the 10th and Last Plenary Meeting of the Committee on Artificial Intelligence (CAI) of the Council of Europe Drafting the Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law," September 3, 2024. https://www.edps.europa.eu/press-publications/press-news/press-releases/2024/edps-statement-view-10th-and-last-plenary-meeting-committee-artificial-intelligence-cai-council-europe-drafting-framework-convention-artificial_en#:~:text=Notwithstanding%20this%2C%20the%20EDPS%20is,and%20more%20generally%20its%20added.

negotiators to reject blanket exemptions for national security and defence activities. The CSOs argue that such exemptions would erode safeguards that are typically applied under international, European, and national laws.[67]

Both the recent regulatory responses by the EU and the COE face complex challenges. While both aim to regulate AI, their approaches differ. The EU AI Act is more detailed and methodical, focusing on establishing clear technical and legal standards. Its tiered approach categorizes AI systems based on risk, imposing proportionate regulatory measures to address potential harms. By establishing a database for high-risk AI systems, it promotes transparency and accountability. However, there are concerns that the detailed regulatory burdens and requirements may stifle technological innovation and economic growth, hindering the aim of the EU to position Europe as a leader in ethical AI development. Meanwhile, in contrast, the Framework Convention emphasizes broader ethical principles and human rights considerations. This distinction underscores the Council of Europe's wider mandate, which extends beyond market regulation and aims to strengthen fundamental rights protections to supplement the AI Act.

In conclusion, the current legal framework for freedom of expression in Europe, portrayed by the COE and the EU, with their respective judicial bodies, constitutes strong protections intending to balance individual liberties with societal interests. The regulatory landscape governing AI and its intersection with freedom of expression is characterized by a diverse array of legal frameworks and instruments, such as GDPR, and LED, that set strict standards for data protection and privacy, complemented by COE's conventions and recommendations, ensuring ethical considerations in AI development. Most importantly, the EU AI Act and the Convention

[67] "Open Letter to COE AI Convention Negotiators: Do Not Water Down Our Rights," ECNL, n.d., https://ecnl.org/news/open-letter-coe-ai-convention-negotiators-do-not-water-down-our-rights.

on AI, Human Rights, Democracy and the Rule of Law form a comprehensive regulatory framework aiming to mitigate the potential harms of AI and at the same time balance innovation and protection of fundamental rights. Moreover, the EU and COE frameworks underscore Europe's commitment to global leadership in ethical AI governance, positioning the region as a model for responsible innovation in the digital era. However, as the advancement of AI technologies continues, these regulatory frameworks will require ongoing adaptation and reinforcement to address emerging challenges effectively.

3. Case law

This chapter will delve into the key cases focusing on the intersection of AI and freedom of expression from the European Court of Human Rights (ECtHR), the Court of Justice of the European Union (CJEU) and various national courts. Through the case analysis, this chapter seeks to uncover emerging trends, highlight existing gaps and identify how different legal frameworks across Europe address challenges posed by AI technologies. Understanding these dynamics helps navigate the evolving legal landscape that seeks to balance technological development and fundamental rights protection in the digital era.

3.1.European Court of Human Rights

Despite the absence of specific laws on AI, the ECtHR still issued significant rulings that address risks associated with AI. These landmark cases illustrate the court's approach to AI's impact on freedom of expression. They highlight how the court navigates the delicate balance between advancing technology and safeguarding individual rights, particularly in the context of content moderation and state surveillance.

Delfi AS v. Estonia [GC] - 64569/09[68] is the landmark decision of ECtHR that involved a question of liability for user-generated content on online platforms. The case was brought by one of the largest Estonian news portals Delfi. In 2006, Delfi published an article about a ferry company, that caused heated discussion in the comment section. Some of the users posted comments that were found defamatory towards the ferry company's majority shareholder. The majority shareholder sued Delfi, arguing that the portal should be held liable for the defamatory comments made by its users. All instances of Estonian domestic court found Delfi liable for

[68]Delfi AS v. Estonia [GC] - 64569/09 https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-155105&filename=001-155105.pdf

defamatory comments. However, Delfi brought the case before ECthR arguing that the Estonian court's decisions violated its right to freedom of expression under Article 10 of ECHR.

In the judgement, the court acknowledged the transformative role of user-generated content on the Internet in facilitating unprecedented freedom of expression. However, alongside these benefits, the court recognised significant risks of the rapid spread of hate speech, unlawful speech and even incitements to violence, which sometimes can remain online permanently. Balancing these realities while upholding freedom of expression and the right to privacy, requires preserving the essence of both rights. Thus, the court undermined the importance of maintaining the possibility of imposing liability for unlawful speech online as a necessary remedy to protect individuals' personality rights. [69]

ECtHR acknowledged that the comments in question, representing hate speech and incitement to violence were clearly unlawful and were promptly removed by Delfi upon notification. Despite the removal, the court highlighted the limitations of Delfi's filtering system, which failed to detect and remove hate speech effectively, allowing unlawful comments to remain online for weeks. Even though the court held that the Estonian Court's decision was an infringement of Delfi's freedom of expression, it did not constitute a disproportionate restriction. ECtHR ruled that there had been no violation of Article 10 in this case and held Delfi liable for the defamatory comments, rejecting Delfi's argument that it should be protected under the E-Commerce Directive, which provides immunity to internet service providers for third-party content.

This significant judgement set a precedent regarding the accountability of online platforms for user-generated content and emphasised the need for regulation of online platforms and the balance between freedom of expression and the protection of reputation. It highlighted the

[69] Ibid, Par.110

importance of effective content moderation and prompt removal of unlawful content. The ruling underscores the responsibility in content moderation processes, even when AI technology is used. However, at that time Delfi's content moderation was not based on AI technology, as it was not advanced. While AI can enhance moderation efforts by effectively identifying and removing unlawful content, it is not a panacea, and platforms must ensure that freedom of expression is protected while harmful content is effectively moderated.

Big Brother Watch and Others v. The United Kingdom 2018 (Applications nos. 58170/13, 62322/14 and 24960/15)[70] is another landmark decision by ECtHR concerning mass surveillance practices conducted by the UK government. The case centred around the UK's intelligence agency, GCHQ and its use of Bulk interception of communications (collection of vast amounts of internet traffic, including emails and browsing histories), bulk acquisition of communications data (collection of metadata (who contacted whom and when), bulk personal datasets and sharing of intelligence with foreign governments. Several NGOs including Big Brother Watch challenged the surveillance practices, arguing they violated the right to privacy under Article 8 of ECHR.

The court underscored that technological advancement has amplified both the volume of communications and the complexity of threats faced by states, such as terrorism, cyberattacks, and drug trafficking. These threats highlight the necessity for states to employ advanced surveillance technologies to detect and respond to digital threats effectively. [71] Despite that the court recognized the necessity of bulk interception, the court identified significant deficiencies in the UK's surveillance regime, such as insufficient clarity on the categories of selectors targets, lack of independent authorization for interception and inadequate internal authorization

[70] Ebig Brothers Watch and others v. the United Kingdom, 2021, EctHR https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-210077%22]}.
[71] Ibid, 323-323

for selectors linked to individuals. The court found the violation of both Articles 8 and 10 under ECHR. It emphasized that even though the bulk interception did not target journalists specifically, without clear legal arrangements and safeguards protecting journalistic confidentiality, it found the interference in the right of freedom of expression. The UK enjoyed a wide margin of appreciation for national security reasons.

This judgement is a landmark decision governing the balance between national security and individual rights. It also underscored the interconnected nature of the right to privacy and the right to freedom of expression, highlighting the necessity to safeguard both rights in the digital age. The court highlighted the need for strong safeguards and oversight mechanisms to ensure that the surveillance activities do not unduly infringe on fundamental rights. The principles laid out in the judgement are relevant for the use of AI technologies in surveillance, as it is getting more and more sophisticated and governments are incorporating AI and advanced data analytics capabilities. The judgement principles suggest that surveillance techniques, including the ones based on AI systems, must be used in a way that upholds fundamental rights.

The ruling of ECtHR in the cases of Delfi v. Estonia and Big Brothers Watch v. the UK indicate how the court is taking a proactive approach to consider how new technology can impact fundamental rights. Despite the absence of a specific law on AI, these landmark rulings reveal Ecthr's intention to strike a balance between technological development and the protection of individual rights. IN Delfi v. Estonia, the court dealt with the liability issue of online platforms for user-generated content, which remains a pressing issue, as AI technologies become increasingly integral to content moderation. The court's ruling emphasised the necessity of imposing liability for unlawful speech to protect individual personality rights. This stresses a pivotal principle: while AI can enhance content moderation by swiftly detecting and removing unlawful speech, platforms must ensure that this technical efficiency does not come at the

expense of freedom of expression. It suggests a balanced approach to guarantee free speech and ensure proportionality in restrictions.

On the other hand, the Big Brother Watch case illustrates EctHR's careful consideration of the interplay between national security imperatives and individual rights. In this case, the court examined the UK's mass surveillance practices, stressing that technological advancements in surveillance must be tempered with stringent legal safeguards to protect privacy and freedom of expression. Though the court acknowledged, the legitimate need for states to employ sophisticated surveillance technologies to address contemporary threats, is also identified deficiencies in the UK's legal framework, specifically a lack of clarity and independent oversight. This case shows the fundamental principle for AI-driven surveillance: the necessity for transparency, accountability and robust oversight mechanisms to prevent undue infringements of fundamental rights.

In conclusion, both judgements suggest a judicial framework that could guide future cases involving AI, emphasising the principles of Accountability and oversight, proportionality and necessity and a human-centric approach. The principles established by the court will play a crucial role in harmonizing innovation with the protection of the rights that are the cornerstone of democratic societies.

3.2.Court of Justice of the European Union

The Court of Justice of the European Union (CJEU) also addressed significant cases involving AI and its implications on the right to freedom of expression, particularly in relation to online platforms, data protection and the right to be forgotten.

One of the relevant and significant cases of CJEU is the case of Google Spain SL, Google Inc. v. Agencia Española de Protection de Datos (2014),[72] where the court established the "right to be forgotten. According to the case facts, Mario Costeja González filed a complaint with the Spanish Data Protection Agency (AEPD) against a Spanish newspaper, Google Spain SL and Google Inc. The Applicant wanted his name removed from a newspaper's online archives and from Google search results, which linked to newspaper pages announcing a foreclosure auction on his home, a matter that has been resolved long ago. The AEPD denied the request to remove, as the publication was lawful, however ordered Google to remove the links to applicants' data upon his request, considering Google as a data controller subject to Directive 95/46/EC, regulating data protection within the EU. Google Spain and Google Inc. appealed AEPD's decision to the Spanish High Court. The court to CJEU concerning the interpretation of the directive.

The court emphasised the need to balance the right to privacy and protection of data against the legitimate interest of search engine operators and the public's right to access information. It noted that the data which was accurate at the time of the publication might become irrelevant over time. The need to keep data up-to-date and relevant is crucial. This is particularly true if the data becomes "inadequate, irrelevant or no longer relevant, or excessive about the purposes for which they were processed."[73] If the data subject requests the removal of the links revealing personal data and it is found that the information is outdated or irrelevant, those links must be erased from the search results, even if the information in the original publication was lawful. the court acknowledged an exception when there is a "preponderant interest" of the public in

[72] Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, ECLI:EU:C:2014:317, 2014, CJEU. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131
[73] Ibid, Par.92.

accessing the information, such as in cases of public figures or matters of significant interest. [74]

In this case, CJEU recognized the importance of freedom of expression and the right to receive information, however, these rights should be balanced against the right to privacy and protection of personal data. It also mentioned that the privacy and data protection rights enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the EU will override the economic interests of search engine operators and public interest in accessing the data unless the data or its subject plays a significant role in public life. [75] Furthermore, the right to request the removal of information does not require the data subject to be negatively impacted by its presence. The request is justified enough by the passage of time and the data's irrelevance. Thus, the court recognized the "right to be forgotten", allowing individuals to request the removal of links revealing personal information from search engine results.

The judgement had faced criticism, arguing that CJEU overly prioritized privacy rights at the expense of freedom of expression and access to information, neglecting public interest. It gives individuals excessive rights to censor public materials by submitting a request. Critiques note that while the Directive acknowledges the importance of the free flow of data for economic reasons, the court's interpretation subordinates it to the right to privacy, without considering the economic impact on businesses like Google.[76]

In conclusion, the Google Spain case is a critical reference point for AI systems on how to balance privacy rights and freedom of expression, that privacy is protected without undull restrictions on access to information. It also highlights the responsibilities of AI systems as data

[74] Par. 97-98
[75] Par.97
[76] Review, Harvard Law. 2023. "Google Spain SL V. Agencia Española De Protección De Datos." Harvard Law Review. March 24, 2023. https://harvardlawreview.org/print/vol-128/google-spain-sl-v-agencia-espanola-de-proteccion-de-datos/. P. 738 from PDF.

collectors, focusing on how to handle personal data and provide up-to-date, relevant information. The “right to be forgotten" has significant implications for AI, as it needs to incorporate mechanisms to comply with removal requests. The ruling’s emphasis on the exception of public interest stresses the ethical considerations for AI. Determining what constitutes public interest and discerning between private data and information that serves public good necessitates nuances and context-aware AI.

The case of Facebook Ireland Ltd. V. Schrems II (2020)[77] is one of the most important international cases ruled by CJEU addressing the legality of data transfers between the EU and the USA. Austrian PhD student and private advocate Max Schrems brought a complaint against Facebook incorporated in Ireland to the Irish Data Protection Commissioner, challenging the transfer of his data to the US Facebook. The case led to CJEU to invalidate the Privacy Shield Framework, a replacement for the Safe Harbour Framework (that was invalidated by CJEU in 2015 in the case Facebook Ireland Ltd. v. Schrems I. Privacy Shield Framework was a mechanism, governing EU-US data transfers by providing a mechanism for US companies to certify their compliance with EU standards of privacy principles.

In its judgement, the court invalidated the EU-US Privacy Shield, as it found US surveillance laws were not in line with EU standards set by GDPR, especially regarding the lack of redress for EU citizens. Furthermore, the court upheld the validity of Standard Contractual Closes (SCC),[78] issued by the European Commission, as a mechanism for transferring personal data outside the EU. However, highlighted that SCCs alone are not sufficient to guarantee adequate protection of data transferred outside of the EU due to concerns about the level of personal data

[77] Facebook Ireland Ltd, v. Maximillian Schrems C-311/18, 2018. CJEU ,https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=113537.

[78] “Standard Contractual Clauses (SCC).” 2021. European Commission. June 4, 2021. https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

protection provided by US law and surveillance programs. Thus, additional safeguards may be required, such as the assessment of the data recipient's legal system. Data exporters and importers must conduct case-by-case assessments of data protection in third countries. If the protection is not adequate, they must suspend the transfer. The judgement reinforced the protection of the personal data of EU citizens and emphasised the importance of maintaining high data protection standards in international data transfers. [79]

As AI becomes increasingly global, data flows are essential for the development and deployment of it. CJEU's ruling stresses the importance of international agreements and standards of data protection to foster Global trust in AI. It raises concerns regarding state surveillance, how social media platforms are handling, and processing user-data, and addresses the potential impact of cross-border transfers of data. It underscores the need for responsible data handling practices and ethical considerations in the development and deployment of AI to uphold fundamental rights.

The analysis of these landmark rulings represents the commitment of CJEU to protect individual rights in the era of digitally interconnected era. While the stringent decisions focused primarily on the protection of privacy rights and the protection of data, CJEU acknowledged the importance of upholding public interest and access to information. With the pivotal establishment of the "right to be forgotten" and CJEU's vigilance against the global data flow standards, positions it is a stringent mechanism for upholding individual rights in the digital era. While the approach may stifle the innovation and digital economic growth process, the

[79] "Judgment in Case C-311/18 Data Protection Commissioner V Facebook Ireland and Maximillian Schrems." Press-release. Press Release. July 16, 2020. https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf.

decisions set precedents on responsible data handling, emphasising the role of the legal framework in balancing innovation with the protection of individual rights.

In conclusion, this chapter explored the significant intersection of AI and freedom of expression through the lens of key judicial decisions. The analysis of the landmark rulings by EctHR and CJEU, reveals a judiciary keenly aware of the impacts technological advancements can have on fundamental rights. Both courts consistently strive to balance the benefits of technology with the individual's rights protection. In the judgements, the principles of accountability, transparency, proportionality, and oversight are consistently emphasised, indicating a trend towards a more regulated and rights-centric approach to AI.

The lack of specific legislation on AI remained a critical gap. The courts were forced to adapt the existing legal frameworks to address the ramifications of AI-related issues. For instance, in the case of Delfi v. Estonia, the court had to apply general principles of liability and freedom of expression to a scenario involving clear content moderation. The lack of AI-specific laws can lead to inferior rulings, missing out on the essential risks, and undermining democracy and the rule of law generally. Furthermore, the inconsistency of international approaches complicates the legal landscape. The issue of international data transfers and flows, involving mass surveillance practices from both government and private actors (Facebook Ireland, in the Schrems II case) represents the lack of international agreement and cooperation, common standards that can adequately address the complexities of AI and data protection.

Overall, the judiciary of the European courts underscores the nuanced approach that respects both innovation and safeguards fundamental rights. The role of the judiciary in shaping the legal landscape is pivotal. The principles established in these landmark cases with recent regulatory responses, such EU AI Act and the Convention on AI, will guide future cases and be instrumental in ensuring that the development and deployment of AI are aligned with the core

values of democratic societies. In conclusion, this chapter delved into the significant intersection of AI and freedom of expression through key judicial decisions. The analysis of landmark rulings by ECtHR and CJEU reveals a judiciary keenly aware of the impacts of technological advancements on fundamental rights. Both courts consistently strive to balance the benefits of technology with the protection of individual rights. In the judgments, the principles of accountability, transparency, proportionality, and oversight are consistently emphasized, indicating a trend towards a more regulated and rights-centric approach to AI.

The lack of specific legislation on AI remains a critical gap. The courts have had to adapt existing legal frameworks to address the ramifications of AI-related issues. For instance, in the case of Delfi v. Estonia, the court had to apply general principles of liability and freedom of expression to a scenario involving content moderation. The absence of AI-specific laws can lead to subpar rulings, overlooking essential risks, and undermining democracy and the rule of law in general. Furthermore, the inconsistency of international approaches complicates the legal landscape. The issue of international data transfers and flows, involving mass surveillance practices from both government and private actors (Facebook Ireland, in the Schrems II case) reflects the lack of international agreement and cooperation, as well as common standards that could adequately address the complexities of AI and data protection.

Overall, the European courts' judiciary underscores a nuanced approach that respects both innovation and safeguards fundamental rights. The role of the judiciary in shaping the legal landscape is pivotal. The principles established in these landmark cases, along with recent regulatory responses such as the EU AI Act and the Convention on AI, will guide future cases and be instrumental in ensuring that the development and deployment of AI align with the core values of democratic societies.

CONCLUSIONS

AI technologies, while offering exceptional advancements, also pose substantial threats to freedom of expression. In the digital era, those threats define the way exercise the right. Critical areas impacting freedom of expression include content moderation, misinformation, surveillance and discrimination. While AI algorithms can efficiently filter harmful information, they often lack nuanced, contextualised understanding, leading to over-censorship and suppression of legitimate speech. The development of realistic fake content through AI enables spread of misinformation and manipulation of public opinion, eroding media integrity and public trust. AI's capacity for extensive surveillance, utilized by governments and private sector, can cause "chilling effect", deterring individuals from openly expressing themselves online or exploring controversial perspectives crucial for a vibrant democracy. Furtehrmore, as AI absorbs implicit and explicit biases in the training data, it can perpetuate social prejudices and hinder marginalized communities to expressing themselves freely.

Analysing the European legal framework, focusing on both COE and EU and their approach to AI, reveals robust protection of individual rights amidst the recognition of technology impacts. Regulatory frameworks include array-specific instruments, such as for the protection of data, oil of AI, GDPR and LED, complemented with the COE's conventions. Newly adopted, but not yet enforced EU AI Act and the Convention on AI, Human Rights, Democracy and the Rule of Law represent ambitious, however comprehensive AI AI-specific regulations. While The EU AI Act is more detailed and methodical, focusing on establishing clear technical and legal standards, pushing "Brussels effect", the Convention emphasizes broader ethical principles and human rights considerations, together underscoring Europe's commitment to global leadership in ethical AI governance.

The landmark rulings by the ECtHR and the CJEU have underscored the need for a balanced approach that safeguards individual rights while fostering innovation. Principles such as accountability, transparency, proportionality, and oversight have been consistently emphasized, reflecting a trend towards a more regulated and rights-centric approach to AI.

In conclusion, there is a crucial need to balance the benefits of AI with the protection of fundamental rights. Policymakers must ensure that AI is developed and deployed in a way that respects and enhances freedom of expression and, however, regulates it in a way that does not kill its greatness. Existing regulatory frameworks must be strengthened to address unique challenges provided by AI but stay flexible enough to adapt to new technological advancements. Increasing awareness among the public and policymakers to understand AI and its implications is crucial. Educating individuals about the potential risks and benefits of AI can empower them to make informed decisions and advocate for their rights. Finally, I believe that by adopting forward-looking regulatory measures and fostering a society both technologically advanced and right-conscious, we can harness the potential of AI to benefit society while protecting fundamental human rights.

BIBLIOGRAPHY

Access Now, and Lindsey Andersen. “HUMAN RIGHTS IN THE AGE OF ARTIFICIAL INTELLIGENCE.” Access Now, 2021. https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf.

Aizenberg, Evgeni, Jeroen Van Den Hoven, Department of Intelligent Systems, Delft University of Technology, Delft, The Netherlands, AiTech multidisciplinary program on Meaningful Human Control over Autonomous Intelligent Systems, Delft University of Technology, Delft, The Netherlands, and Department of Values, Technology, and Innovation, Delft University of Technology, Delft, The Netherlands. “Designing for Human Rights in AI.” Big Data & Society, July 1, 2020, 1–14. https://doi.org/10.1177/2053951720949566.

ARTICLE 19 and Privacy International. “Privacy and Freedom of Expression in the Age of Artificial Intelligence,” April 2018. https://www.article19.org/wp-content/uploads/2018/04/Privacy-and-Freedom-of-Expression-In-the-Age-of-Artificial-Intelligence-1.pdf.

Artificial Intelligence and the Law. Intersentia, 2021.

Artificial Intelligence. “The Framework Convention on Artificial Intelligence - Artificial Intelligence - www.coe.int,” n.d. https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence.

Bukovska, Barbora, Amy Brouillette, Barbora Bukovska, Julia Haas, Fanny Hidvégi, Nani Jansen Reventlow, Lorena Jaume-Palasi, et al. SPOTLIGHT ON ARTIFICIAL INTELLIGENCE AND FREEDOM OF EXPRESSION. Edited by Julia Haas. SPOTLIGHT ON ARTIFICIAL INTELLIGENCE AND FREEDOM OF EXPRESSION. Office of the Representative on Freedom of the Media, 2020.

Charter of Fundamental Rights of the European Union, 2000.

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981.

Convention on Cybercrime, 2001

Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin

Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation

Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, 2024

Council of Europe. “New Guidelines on Artificial Intelligence and Data Protection.” Data Protection, February 4, 2019. https://www.coe.int/en/web/data-protection/-/new-guidelines-on-artificial-intelligence-and-personal-data-protection.

Criddle, Cristina. “What Is Artificial Intelligence and How Does It Work?” Financial Times, July 20, 2023. https://www.ft.com/content/bde93e43-7ad6-4abf-9c00-8955c6a9e343.

DATA & SOCIETY, and Mark Latonero. Governing Artificial Intelligence: Upholding Human Rights & Dignity. DATA & SOCIETY, n.d. https://datasociety.net/wp-content/uploads/2018/10/DataSociety_Governing_Artificial_Intelligence_Upholding_Human_Rights.pdf.

David Gilbert, “Here’s How Violent Extremists Are Exploiting Generative AI Tools,” WIRED, n.d., https://www.wired.com/story/generative-ai-terrorism-content/.

Directive 2006/54/EC of the European Parliament and of the Council of 5 July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (recast)

Donahoe, Eileen, and Megan MacDuffee Metzger. “Artificial Intelligence and Human Rights.” Journal of Democracy 30, no. 2 (January 1, 2019): 115–26. https://doi.org/10.1353/jod.2019.0029.

European Commission. “Standard Contractual Clauses (SCC),” June 4, 2021. https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

European Commission. “The Digital Markets Act: Ensuring Fair and Open Digital Markets,” n.d. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en.

European Commission. “The EU’s Digital Services Act,” n.d. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en.

European Commission. “White Paper on Artificial Intelligence: A European Approach to Excellence and Trust,” n.d. https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en.

European Convention on Human Rights, 1950.

European Data Protection Supervisor. “EDPS Statement in View of the 10th and Last Plenary Meeting of the Committee on Artificial Intelligence (CAI) of the Council of Europe Drafting the Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law,” September 3, 2024

European Union Agency for Fundamental Rights. “GETTING THE FUTURE RIGHT: ARTIFICIAL INTELLIGENCE AND FUNDAMENTAL RIGHTS.” Report. Publications Office of the European Union, 2020. https://doi.org/10.2811/58563.

Feldstein, Steven and Boise State University. “How Artificial Intelligence Is Reshaping Repression.” Journal of Democracy 30–1 (2019): 40–52.

Freedom of Expression. “Recommendation CM/Rec(2020)1 of the Committee of Ministers to Member States on the Human Rights Impacts of Algorithmic Systems - Freedom of Expression - www.coe.int,” April 8, 2020.

General Data Protection Regulation (2016/679)

Hacker, Philipp. What’s Missing From the EU AI Act, n.d. https://doi.org/10.59704/3f4921d4a3fbeeee.

Heaven, Will Douglas . “Predictive Policing Algorithms Are Racist. They Need to Be Dismantled.,” MIT Technology Review, June 21, 2023, https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/.

High-Level Expert Group on Artificial Intelligence. “A Definition of AI: Main Capabilities and Scientific Disciplines.” European Commission. Directorate-General for Communication, December 18, 2018. https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf.

High-level Summary of the AI Act | EU Artificial Intelligence Act, n.d. https://artificialintelligenceact.eu/high-level-summary/.

Kissinger, Henry A, Eric Schmidt, and Daniel Huttenlocher. The Age of AI: “THE BOOK WE ALL NEED.” Hachette UK, 2021.

Law Enforcement Directive (2016/680)

Liao, S. Matthew. “A Short Introduction to the Ethics of Artificial Intelligence.” In Oxford University Press eBooks, 1–42, 2020. https://doi.org/10.1093/oso/9780190905033.003.0001

Litvinova, Dasha. “The Cyber Gulag: How Russia Tracks, Censors and Controls Its Citizens | AP News.” AP News, May 23, 2023. https://apnews.com/article/russia-crackdown-surveillance-censorship-war-ukraine-internet-dab3663774feb666d6d0025bcd082fba.

McCarthy-Jones, Simon. “The Autonomous Mind: The Right to Freedom of Thought in the Twenty-First Century.” Journal-article. Edited by Frontiers in Artificial Intelligence, Nicola Lettieri, and Istituto nazionale per l’analisi delle politiche pubbliche (INAPP). Frontiers in Artificial Intelligence. Vol. 2, September 26, 2019. https://doi.org/10.3389/frai.2019.00019.

Metz, Cade. “What Makes Chatbots ‘Hallucinate’ or Say the Wrong Thing?” The New York Times, April 4, 2023. https://www.nytimes.com/2023/03/29/technology/ai-chatbots-hallucinations.html.

Obermeyer et al., “Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations,” October 25, 2019.

OECD AI Policy Observatory Portal, n.d. https://oecd.ai/en/ai-principles.

OECD Legal Instruments, n.d. https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449.

One Hundred Year Study on Artificial Intelligence (AI100). “Executive Summary,” n.d. https://ai100.stanford.edu/2016-report/executive-summary.

Portal. “Modernisation of the Data Protection ‘Convention 108’ - Portal - www.coe.int,” n.d. https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet.

Raso, Filippo A., Hannah Hilligoss, Vivek Krishnamurthy, Christopher Bavitz, Levin Kim, and Berkman Klein Center for Internet & Society. “Artificial Intelligence & Human Rights: Opportunities & Risks,” September 25, 2018. https://ssrn.com/abstract=3259344.

Review, Harvard Law. 2023. “Google Spain SL V. Agencia Española De Protección De Datos.” Harvard Law Review. March 24, 2023. https://harvardlawreview.org/print/vol-128/google-spain-sl-v-agencia-espanola-de-proteccion-de-datos/.

Shaping Europe’s Digital Future. “AI Act,” May 29, 2024. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.

Shaping Europe’s Digital Future. “Ethics Guidelines for Trustworthy AI,” April 8, 2019. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

Shaping Europe’s Digital Future. “European AI Office,” n.d. https://digital-strategy.ec.europa.eu/en/policies/ai-office.

Shaping Europe’s Digital Future. “White Paper on Artificial Intelligence: Public Consultation Towards a European Approach for Excellence and Trust,” July 17, 2020. https://digital-strategy.ec.europa.eu/en/library/white-paper-artificial-intelligence-public-consultation-towards-european-approach-excellence-and

Treaty on European Union, 2007.

Treaty on the Functioning of the European Union, 1958

Tsakiridi, Sandy " The draft AI Act: the good, the bad and the ugly," Privacy and Data Protection, 2022.

United Nations, and David Kaye. “Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression.” Report. United Nations, August 29, 2018.

United Nations. “Universal Declaration of Human Rights | United Nations,” n.d. https://www.un.org/en/about-us/universal-declaration-of-human-rights

Vincent, James. “Twitter Taught Microsoft’s AI Chatbot to Be a Racist Asshole in Less Than a Day.” The Verge, March 24, 2016. https://www.theverge.com/2016/3/24/11297050/tay-microsoft-chatbot-racist.

Winick, Erin. “Amazon Ditched AI Recruitment Software Because It Was Biased Against Women,” MIT Technology Review, June 17, 2022, https://www.technologyreview.com/2018/10/10/139858/amazon-ditched-ai-recruitment-software-because-it-was-biased-against-women.