FACULTY OF LAW
Lund University

Kristina Cornelia Ackermann

The European Artificial Intelligence Act - High-Risk Use Cases for Juridical Purposes and Interplay with the GDPR

JAEM01 Master Thesis

European Business Law
15 higher education credits

Supervisor: Petra Gyöngyi

Term: Spring Semester 2024

Contents

SUMMARY 1

PREFACE 2

ABBREVIATIONS 3

1 INTRODUCTION 4

1.1 Background 4

1.1.1 History of the European Artificial Intelligence Act 4

1.1.2 Reason and Purpose 4

1.1.3 Legal Basis 6

1.1.4 Artificial Intelligence in General 7

1.2 Research Questions 9

1.3 Literature Overview 11

1.4 Methodology 13

2 EUROPEAN AI ACT 15

2.1 Artificial Intelligence 15

2.1.1 Definition of AI 15

2.1.2 Classification of AI 18

2.1.2.1 Low or Minimal Risk and Limited Risk Systems 18

2.1.2.2 General Purpose AI 18

2.1.2.3 High-Risk Systems 20

2.1.2.4 Differentiation between General Risk and High- Risk 21

2.1.2.5 Systems with Unacceptable Risk 22

2.2 Scope of Regulation 23

2.2.1 Territorial Scope 23

2.2.2 Personal Scope 23

2.3 Enforcement 24

2.3.1 AI Management Board 24

2.3.2 AI Office 25

2.3.3 Fines 25

2.4 Resume 26

3 HIGH-RISK SYSTEMS IN DEPTH 27

3.1 Conditions for High-Risk Systems 27

3.2 Requirements for High-Risk Systems 28
3.2.1 Risk Management System 28
3.2.2 Data and Data Governance 28
3.2.3 Technical Documentation, Record-keeping, Transparency and Provisions of Information 29
3.2.4 Human Oversight 30
3.2.5 Accuracy, Robustness and Cybersecurity 31
3.2.6 Obligations 31
3.2.7 Conformity Assessments 32

3.3 Problematic High-Risk Cases 33
3.3.1 AI Systems intended to be used by Judicial Authorities 33
3.3.1.1 SIGA 34
3.3.1.2 Speech-to-Text Machine 35
3.3.1.3 Search Engines 35
3.3.1.4 Natural Language Processing 36
3.3.1.5 AI-Powered Virtual Assistant 37
3.3.2 Assistance of AI 37
3.3.3 Upcoming Problems of Using AI Systems in Judicial Processes 38
3.3.3.1 High Quality Data 38
3.3.3.2 Responsibility 39
3.3.3.3 Human Oversight 40
3.3.3.4 Interfere with EU Principles 41
3.3.3.5 Benefits 42
3.3.4 Replacement of Judges through AI 43
3.3.5 Data Protection 45

4 COMPARISON BETWEEN GDPR AND AI ACT 46

4.1 General Data Protection Regulation 46

4.2 Interplay between GDPR and AI Act 47

4.3 Data Protection in Decision-Making Processes 51

5 CONCLUSION 56

TABLE OF CASES 64

TABLES:

Table 1: Overview of the different AI Definitions 17
Table 2: Comparison of the AI Act and GDPR 49

Summary

This thesis will explore the interplay between high-risk Artificial Intelligence (AI) systems, regulated through the European AI Act (AI Act) in judicial systems and General Data Protection Regulation (GDPR) compliance. In order to do so there will be given a comparative legal analysis, as well as summarisation of principal findings, including challenges like data privacy concerns, transparency and regulatory alignment.

Therefore, leading questions like: *'What are the potential legal conflicts that may arise, when using high-risk AI systems during juridical processes and how does this interfere with Article 22 GDPR?'* as well as: *'What are the specific issues associated with automated decisions made by AI systems, particularly in relation to their impact and functionality?*', will be answered.

It is divided into three main chapters, (1) European AI Act, (2) High-Risk Systems in Depth and (3) Comparison between GDPR and AI Act.
The first chapter examines AI's definition and classification, with the aim of demystify the complexities of AI categorization within legislative contexts. It highlights the AI Act's risk-based approach, emphasizing safety, legality, and trust in high-risk systems, and its potential global impact through the 'Brussels effect'.
The second chapter explores the complex requirements for high-risk AI systems and examines their impact on judicial processes and decisions from a legal and ethical perspective. A thorough assessment of the impact of AI on justice highlights the challenges of aligning AI with core legal standards. The text covers compliance obligations for high-risk AI systems, including risk management, data governance, transparency, human oversight and technical documentation.
During the last chapter there will follow a comparative analysis of the AI Act with the GDPR, while focusing on the regulatory dynamics between both regulations, particularly concerning automated decision-making processes and the safeguarding of individual rights. This analysis aims to highlight potential conflicts and synergies between these regulatory frameworks.

Preface

I would like to express my heartfelt gratitude to my supervisor, Petra Gyöngyi, for her invaluable guidance and support throughout the writing of this thesis.

Additionally, I extend my appreciation to Julian Nowag, Lisa Weiland, and Mirea Barrobes for their constructive comments and assistance during the 'work in progress seminar.'

Finally, I am thankful to all other people who gave me advice regarding the content of the thesis.

Lund, 20th of May 2024

Abbreviations

Artificial General Intelligence	*AGI*
Artificial Intelligence	*AI*
Boston Consulting Group	*BCG*
Conformity Assessment	*CA*
Data Protection Impact Assessment	*DIPA*
European Artificial Intelligence Act	*AI Act*
European Court of Justice	*CJEU*
European Union	*EU*
floating point operations	*FLOP*
Functioning of the European Union	*TFEU*
fundamental rights impact assessment	*FRIA*
General Data Protection Regulation	*GDPR*
general-purpose AI	*GPAI*
Natural Language Processing	*NLP*

1 Introduction

1.1 Background

1.1.1 History of the European Artificial Intelligence Act

The European Artificial Intelligence Act (AI Act) will be a legally binding instrument that will enter into force in May or June 2024. It had its origin throughout the White Paper on AI of February 2020.[1] In December 2022, the European Commission proposed a draft standardization request for the AI Act to promote the development of safe and reliable AI technologies. By December 2023, the European Parliament and Council reached a consensus on the Act, which was officially ratified by the European Parliament on February 13, 2024.[2] The application of the provisions of the AI Act is phased over time: regulations concerning prohibited AI will apply after six months, certain regulations for high-risk AI and GPAI after one year, and the remaining regulations will apply two years after enactment, Article 85.[3] For AI systems falling under a regulation listed in Annex II of the AI Act, there is currently even a transition period of 36 months planned.[4]

1.1.2 Reason and Purpose

One fundamental reason is to build governance mechanisms to create safeguards regarding the lawful, safe, and trustworthy use of high-risk systems.[5] High-risk systems briefly are, systems that are intended to be used as a safety component of a product, or the AI system is itself a product,

[1] Sebastian Felix Schwemer, Letizia Tomada and Tommaso Pasini, 'Legal AI Systems in the EU's Proposed Artificial Intelligence Act' (21 June 2021) <https://papers.ssrn.com/abstract=3871099> accessed 12 May 2024

[2] Eva Thelisson and Himanshu Verma, 'Conformity Assessment under the EU AI Act General Approach' (2024) 4 AI and Ethics 113

[3] ibid

[4] Ceyhun Necati Pehlivan, 'The EU Artificial Intelligence (AI) Act: An Introduction [Pre-Publication]' (2024) 5 Global Privacy Law Review 1

[5] Schwemer, Tomada and Pasini (n 1), 3

covered by the Union harmonisation legislation[6], that must conform with European values and human rights (Article 2 Lisbon Treaty).[7]

The AI Act follows a risk-based approach: the higher the risk that an AI system poses to fundamental rights and freedoms, health and safety, the stricter the rules.[8] While AI systems that pose an unacceptable risk are completely banned, and high-risk AI systems are subject to strict technical and organisational requirements, low-risk applications are only subject so certain transparency and information obligation. Risk is therefore defined by Article 3(1a) as the combination of the probability of an occurrence of harm and the severity of harm.[9]

The AI Act is, furthermore, expected to have significant impact on global standards through the "Brussels effect" and influence the development of AI regulations in other countries. This effect describes that other countries take the AI Act as a model for their own national laws.[10] This conformity with fundamental rights, freedoms and democracy may set a precedent for global AI governance.[11]

The main objective of the proposal is to ensure the proper functioning of the internal market by setting harmonised rules in particular on the development, placing on the Union market and the use of products and services making use of AI technologies or provided as stand-alone AI systems.[12] Additionally, it

[6] European Parliament and Council, 'Provisional Agreement resulting from International Negotiations of the European Parliament, Committee on the Internal Market and Consumer Protection Committee on Civil Liberties, Justice and Home Affairs' (2 February 2024).

[7] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007; Thelisson and Verma (n 2), 2

[8] David Bromhard and Marieke Merkle, 'Regulation pf Artificial Intelligence – The EU Commissions proposal of an AI Act' (08 April 2021) 6 EuCML, 258

[9] European Parliament and Council Article 3 (n 6)

[10] Pehlivan (n 4)

[11] Court of Justice of the European Union, 'Artificial Intelligence Strategy' (11 July 2023) Directorate-General for Information 6 <cjeu_ai_strategy.pdf (europa.eu)> accessed 18 April 2024

[12] European Commission, 'Accompanying the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts; and Annexes' (21 April 2021), 2, 5

contains rules on the protection of individuals with regard to the processing of personal data.[13]

Therefore, the Commission regulated the framework on AI with the following specific objectives:

- 'Ensure that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values;
- Ensure legal certainty to facilitate investment and innovation in AI;
- Enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems;
- Facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation.'[14]

The regulations set forth in the AI Act are closely integrated with other EU legislative initiatives, such as the Data Governance Act and the Open Data Directive, forming part of the comprehensive EU strategy on data.[15]

1.1.3 Legal Basis

The legal basis for the AI Act is Article 16 (data protection) and Article 114 of the Treaty on the Functioning of the European Union (TFEU), which provides measures to ensure the establishment and functioning of the internal market.[16] This operates by establishing harmonised regulations, in particular with regard to the development, marketing, and use of products and services that apply AI techniques or are stand-alone AI systems.[17] The AI Act is directly applicable throughout the European Union and aims to prevent fragmentation of the internal market caused by divergent national AI laws, that could impede the free movement of AI-embedded goods and services.[18]

[13] ibid, 5; CJEU (n 11), 16

[14] ibid, 4; CJEU (n 11), 5

[15] European Commission (n 12), 4; European Parliament and Council, 'Data Governance Act' (n 13); Commission Communication, A European strategy for data COM/2020/66 final

[16] European Commission Article 16 and 114 TFEU (n 12), 6

[17] Reason 2.1 AI Act, 7.

[18] Bromhard and Merkle (n 8), 257

AI represents a ground-breaking technological advancement. In legal practice, AI has significantly influenced the analysis and outcomes of judicial processes, offering enhanced accuracy, comprehensive insight, and speed of execution.[19] Therefore, the European Commission introduced a proposal draft of the AI Act. The current need to regulate AI applications and their implementation is driven by the need to protect individual privacy and data, ensure accountability and ethical standards in AI operations, and protect against security vulnerabilities.[20] Regulation is also essential to mitigate economic disruption and promote equitable benefits from AI advances. The establishment of comprehensive legal frameworks is thus crucial to address these multifaceted challenges and ensure that AI technologies are developed and deployed responsibly and transparently.[21]

1.1.4 Artificial Intelligence in General

Addressing one of the foremost challenges, liability, invariably raises the question, 'Who is responsible for the damages caused by AI?'. Is it the developer of the AI system, or the user, possibly due to their oversight or preventive responsibilities? These questions are becoming increasingly prevalent, yet often remain unresolved due to the absence of uniform regulatory frameworks. In the context of civil liability in the use of AI, two principal attribution challenges arise, decision-making and free will. As AI operates more autonomously, detached from human actions, the human element of intent diminishes, reducing responsibility. Furthermore, the predictability of AI actions, essential for assigning liability, also becomes less certain.[22]

[19] Mahmoud Khalifa and Mahmoud Sabry, 'The Challenges of The Artificial Intelligence of Law in The Context of Technological Development' [2024] 2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS), Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS), 2024 ASU International Conference in 1, 105

[20] European Commission (n 12), 2

[21] EU Legislation in Progress, 'Artificial intelligence act' (March 2024) EPRS, 2

[22] BGH St NStZ-RR 2006, 372, BGH St. 10, 17; Dieter Krimphove, 'Artificial AI in Law, an overview', (2021)7 Juristische Ausbildung 764

To address this inquiry, it is essential to first identify the various types of AI technologies, categorise them according to their associated risks, and then provide precise regulatory guidelines tailored for both users and deployers of these systems.[23] This allows for a better categorization and estimation of liability issues. AI is the simulation of human intelligence processes by machines, especially computer systems. These processes include learning (acquiring information and rules for using the information), reasoning (using rules to reach approximate or definite conclusions) and self-correction.[24]

AI can be classified into different types, such as narrow AI, strong AI and Artificial General Intelligence (AGI). Narrow AI refers to AI systems that are designed to handle a specific task or a set of related tasks. These systems operate under a limited set of constraints and capabilities. As their intelligence and performance is focused on a single task and do not possess general or wide-ranging capabilities, it is called 'narrow AI'.[25]Strong AI or full AI refers to an artificial intelligence system that can understand and reason about the world as well as a human can. This type of AI can perform any intellectual task that a human being can, but it goes beyond specialised expertise to demonstrate broad general intelligence across domains. Strong AI has not yet been achieved, and it remains largely theoretical at this point.[26] Last, AGI is a type of AI that matches or surpasses human intelligence, the ability to perform any intellectual task that a human can. AGI combines the capabilities of various Narrow AIs, enabling it to operate across a broad range of domains. It is a step beyond Strong AI, providing not only the skills that match human expertise and decision-making abilities but also the capacity for self-awareness, emotional understanding, and creative problem solving.[27]

[23] Pehlivan (n 4), 13

[24] CJEU (n 11), 2

[25] Luciano Floridi and others, 'capAI - A Procedure for Conducting Conformity Assessment of AI Systems in Line with the EU Artificial Intelligence Act' (23 March 2022) <https://papers.ssrn.com/abstract=4064091> accessed 12 May 2024, 9

[26] Konstantinos Kouroupis, 'The AI Act in Light of the EU Digital Agenda: A Critical Approach'

[27] Floridi and others (n 7), 6; CJEU (n 11), 6

AI systems can be classified based on their implementation risks, ranging from low or minimal to high risk. The categorization dictates the compliance requirements that must be met. This discussion will primarily focus on high-risk AI systems. High-risk systems are for example, such used in healthcare systems, AI- powered diagnostic tools that analyse medical images to detect diseases such as cancer.[28] Furthermore, self-driving cars that utilise AI to navigate and make real-time decisions on the road.[29]

As the scope of the thesis otherwise will be extended, it focuses particularly on those engaged in administrative and decision-making processes, analysing both general aspects and specific applications.

The AI act is primarily a preventive prohibition act that bans the use of AI in certain application scenarios or makes the use of AI subject to technical and organisational preconditions and security requirements. Its intended to create an ‘ecosystem of trust’ and strengthen human confidence in the use of AI.[30]

Furthermore, the use and implementation of AI systems raise significant (personal) data protection concerns. Consequently, it is essential to examine the specific regulations established by the GDPR and their interaction with the AI Act, particularly in terms of data protection during automated processes involving AI systems.

1.2 Research Questions

This thesis will focus on the regulations of the AI Act itself, specifically on high-risk systems used in juridical administration and the interplay with the GDPR. Specific problems such as incompatibilities of the usage of AI systems during in juridical authorities within the current EU Law, as well as a possible overlap between the AI Act and GDPR will be explained. There will be answered the main research question during chapter 3 and 4:

‘What are the specific challenges and implications of implementing high-risk AI systems within judicial processes, and how do these systems impact

[28] Thelisson and Verma (n 2), 3

[29] Fabian Rack, ‘Rechtsfragen zur generativen KI’ (2024) 44 ABI Technik 39.

[30] Bromhard and Merkle (n 8), 257

judicial decision-making and procedural fairness?' and '***How do the regulatory requirements of the AI Act intersect with those of the GDPR, particularly in terms of data governance, transparency, and human oversight, and what conflicts or synergies arise from this interplay?'.***

Initially, in chapter 2 the thesis will provide an overview of the intricate definitions of AI, and explore its scope of application. To address the sub-question,

'What can be seen as AI and how can AI be classified under the AI Act?',

the thesis will categorise AI based on its functionalities and implications within the legal framework, thereby clarifying the varying degrees of AI integration in legal contexts.

Furthermore, there will be explained, the differences between high-risk AI systems and GPAI systems, more specific the connection of GPAI to high-risk cases, for example regarding ChatGPT will be explained. GPAI will not be discussed to full extend, because this will fall outside of the scope of this thesis.

The main focus in chapter 3 will be on specific high-risk AI systems and problems which can occur while using them in official institutions and during decision-making processes in court.

There will be answered the sub-question:

'What are the specific challenges and implications of implementing high-risk AI systems within judicial processes, and how do these systems impact judicial decision-making and procedural fairness?'

Thus, this analysis will explore systems such as SIGA, natural language processing (NLP), and speech-to-text technologies concerning their roles in enhancing administrative efficiency and their scope of support within judicial processes. The study also addresses the highly debated question of whether a fully autonomous AI judge is feasible and if such an implementation aligns with the fundamental rights established by EU Law.[31]

[31] CJEU (n 11), 6

Lastly, in chapter 4, there follows a comparison between the GDPR and the European AI Act. Therefore, the main focus will be on differences, resemblances and data protection regarding automatized decision processes, especially made through AI. This is where Article 22 GDPR will be discussed.

The sub-question: '*What are the ethical and legal considerations associated with the use of AI in judicial contexts, and how can effective human oversight and accountability be ensured to uphold fundamental rights and maintain public trust?'* will be answered during this part.

As the AI Act is not implemented right now, questions about interferences just started to arise. Because of the complexity and expected extended scope, there will be no focus on blockchains, which can provide assurances that the data has not been tampered with, but it does not address the issue of data bias, incompleteness, or representativeness.[32]

1.3 Literature Overview

The following literature overview provides an examination of existing research and highlights the unique contributions of this thesis.

First, there is existing European AI Regulation Framework analysis, from for example Flordi et. Al (2022) which provides a comprehensive analysis of the AI Act, discussing its foundational principles and regulatory mechanisms. Their work underscores the Act's risk-based approach and its potential global influence through the 'Brussels effect'.[33] Furthermore the thesis used the legal analysis of De Graaf ad Veldt (2022) to explore the legal implications of the AI Act, regarding the requirements for high-risk AI systems.[34]

Within chapter 4, the thesis made use of Bygrave (2019) analysis, which offers an in-depth examination of the GDPR, with particular attention to its

[32] Simona Ramos and Joshua Ellul, 'Blockchain for Artificial Intelligence (AI): Enhancing Compliance with the EU AI Act through Distributed Ledger Technology. A Cybersecurity Perspective' (2024) 5 International Cybersecurity Law Review 10

[33] Floridi and others (n 25)

[34] Tycho De Graaf and Gitta Veldt, 'The AI Act and Its Impact on Product Safety, Contracts and Liability' (2022) 30 European Review of Private Law 803

provisions on automated decision-making and profiling. Furthermore, Kuner et al. (2020) provide a detailed commentary on the GDPR, including Article 22's stipulations on automated decision-making. Their analysis clarifies the legal boundaries for processing personal data and the necessity of human oversight.[35]

When discussing the intersection of AI and data protection, papers of Gentile (2022) and Forgo (2023) helped to introduce the challenges of integrating AI within the existing data protection framework, as well as, examines the implications of using AI in legal contexts, particularly in judicial processes.[36]

While the existing literature provides substantial insights into the AI Act and the GDPR, there are several areas where this thesis makes unique contributions.

First, a comparative legal analysis of the AI Act and GDPR, focusing on their regulatory dynamics and potential conflicts. Unlike previous studies, it provides a side-by-side comparison of key provisions, highlighting both complementary and conflicting aspects.

Second, building on Forgó's exploration of AI in legal contexts, this thesis delves deeper into the specific challenges of implementing high-risk AI systems within judicial processes. It examines the feasibility, ethical implications, and legal compliance issues associated with using AI for decision-making in courts.[37]

Third, this thesis expands on the concept of human oversight, as mandated by both the AI Act and Article 22 GDPR. It provides a nuanced discussion on how effective human oversight can be ensured in practice, addressing the technical, legal, and ethical dimensions.

[35] Lee A Bygrave, 'Article 22 Automated Individual Decision-Making, Including Profiling' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) <https://doi.org/10.1093/oso/9780198826491.003.0055> accessed 12 May 2024; Lee A Bygrave, 'Minding the Machine v2.0: The EU General Data Protection Regulation and Automated Decision Making' (6 February 2019) <https://papers.ssrn.com/abstract=3329868> accessed 12 May 2024

[36] Giulia Gentile, 'AI in the Courtroom and Judicial Independence: An EU Perspective' (22 August 2022) <https://papers.ssrn.com/abstract=4198145> accessed 12 May 2024; Nikolaus Forgó, 'Zur Regulierung Künstlicher Intelligenz, Auch in Der Strafverfolgung' (2023) 106 Monatsschrift für Kriminologie und Strafrechtsreform 44

[37] Forgó (n 36)

In summary, this thesis builds upon the foundational work of scholars like Floridi, Bygrave, and Forgó, while offering new perspectives on the intersection of AI regulation and data protection.[38] Its comparative analysis, focus on judicial applications, and practical recommendations provide valuable contributions to the ongoing discourse on AI governance and data privacy.[39]

1.4 Methodology

This thesis primarily adopts a juridical perspective, doctrinal research method, and focuses on the legislative developments occurring from February 2024 to April 2024. It begins with an examination of articles concerning the proposed AI Act of the European Union, specifically focusing on its key components and regulatory scope.[40] These foundational documents, which include the preliminary proposal and the final draft of the AI Act, provide a detailed understanding of the regulatory landscape.[41] The thesis is structured to initially explore the rationale, legal foundation, historical development, and organizational structure of the AI Act. It then delves into defining and categorizing AI, comparing the initial and revised drafts issued by the Commission to trace the evolution of the Act's provisions.[42]

The thesis also utilises information from the Commission's AI website to provide insights into the explanations and timelines for implementation. Given the lack of case law pertaining to the AI Act, academic articles are employed to elucidate differences among high-risk systems. The analysis is particularly focused on high-risk AI systems designated for legal applications, examining documents from the Commission that discuss plans for future

[38] Bygrave, 'Minding the Machine v2.0' (n 35); Forgó (n 36); Floridi and others (n 25)
[39] ibid
[40] Thelisson and Verma (n 2), 113; Bromhard and Merkle (n 8), 257
[41] European Commission (n 12); European Parliament and Council (n 6).
[42] CJEU (n 11).

use.[43] This scrutiny aims to identify potential challenges associated with the trustworthiness of AI and data protection issues. Therefore, the thesis examines both the benefits and drawbacks of artificial intelligence within the legal sector, revealing key insights. A notable finding emphasises the necessity to balance the integration of AI and human roles to prevent AI from supplanting human cognitive functions. It advocates for the legal community to harness AI as an auxiliary tool, supported by a robust legal framework that governs its use and clarifies legal accountability for this innovative technology. This approach aims to optimise AI's contribution to judicial administration and enhance the overall justice system.[44]

To critically assess problems associated with the implementation of the AI Act, the thesis draws on insights from prominent law firms such as Bird & Bird and Clifford Chance, providing a practical perspective.[45]

The complex interplay between the AI Act and the GDPR is thoroughly analysed, especially in terms of scope and its influence on decision-making processes. Discussions focus on Article 22 GDPR and its relevance to data protection under the AI Act, integrating scholarly critiques to contrast with the new regulatory measures proposed in the Act.[46] This methodological approach facilitates a comprehensive understanding of potential challenges and implications within the evolving regulatory framework. Because of the extended legal analysis, this thesis will not focus on existing judgements of the CJEU or other important case law regarding the GDPR and its practical implementation.

[43] CJEU (n 11); EU Legislation in Progress, 'Artificial Intelligence Act' (March 2024) EPRS 1

[44] Andrew C Michaels, 'Artificial Intelligence, Legal Change, and Separation of Powers' (2020) 88 University of Cincinnati Law Review

[45] 'Analysing the Impact of the EU AI Act Vote on Businesses' <https://www.twobirds.com/en/insights/2024/global/analysing-the-impact-of-the-eu-ai-act-vote-on-businesses> accessed 12 May 2024

[46] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) Article 22; Bygrave, 'Article 22 Automated Individual Decision-Making, Including Profiling' (n 35) 22

2 European AI Act

This chapter provides an in-depth analysis of the regulations outlined in the AI Act. The primary focus is to elucidate the concept of AI, exploring both its definition and the criteria for its classification within regulatory frameworks. This approach aims to clarify the complexities and categorizations of AI as legislated, offering a comprehensive understanding of its governance.

2.1 Artificial Intelligence

To address the sub-question, *'What can be seen as AI and how can AI be classified?'*, this study will first outline the evolution of the definition of AI. Subsequently, it will explore the various classification systems used to categorise AI, elucidating the criteria that distinguish different types of AI systems within these frameworks. This approach aims to clarify the conceptual underpinnings and categorization strategies that define the field of AI.

2.1.1 Definition of AI

Article 3 of the European Union's proposed regulation introduces an initial broad definition of AI systems.[47] This definition emphasises a wide range of techniques and approaches, including machine learning methods (such as supervised, unsupervised, and reinforcement learning with deep learning techniques), logic and knowledge-based approaches (including knowledge representation, inductive programming, inference engines, and expert systems), statistical methods, and search and optimisation techniques.[48]

[47] AI system means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with.

[48] Pehlivan (n 27), 4

As nearly every program fits into the definition, including handcrafted rules, heuristics-based methods, and legal expert systems,[49] there was the need for a narrower definition, although the regulation refers to the evolving nature of AI technologies.[50] The proposed definition aligns with the OECD's definition, emphasizing the ability of AI systems to make predictions, recommendations, or decisions. [51]

In the final draft, Article 3(1) defines AI systems as: ‘a machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments’.[52]

After more than two years of deliberation, the Commission reached a decision on AI that encompasses all types of AI systems. Ultimately, they focused on two fundamental aspects common to all AI systems: autonomy and learning capacity.[53]

[49] Schwemer, Tomada and Pasini (n 1), 2; Bromhard and Merkle (n 8), 258

[50] Pehlivan (n 4), 4

[51] Schwemer, Tomada and Pasini (n 1), 2

[52] European Parliament and Council Artcile 3 (n 6)

[53] Rack (n 29); Floridi and others (n 25)

Table 1: Overview of the different AI Definitions[54]

Commission 2021 Proposal[55]	**Parliament Mandate**[56]	**Council Mandate**[57]	**OECD AI Principles**[58]
Software that is developed with one or more of the techniques and approaches listed in Annex I and	A machine-based system that is designed to operate with varying levels of autonomy and that can,	A system that is designed to operate with elements of autonomy and that, based on machine and/or human-provided data and inputs,	A machine-based system that,
can, for a given set of human-defined objectives	for explicit or implicit objectives	infers how to achieve a given set of objectives using machine learning and/or logic knowledge -based approaches	for explicit or implicit objectives, infers, from the input it receives
generate outputs	generate outputs	and produces system-generated outputs	how to generate outputs
such as content, predictions, recommendations, or decisions influencing the environments they interact with.	as predictions, recommendations, or decisions, that influence physical or virtual environments.	such as content (generative AI systems), predictions, recommendations or decisions, influencing the environments with which the AI system interacts.	such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.
Recital 6: AI systems can function with different levels of autonomy, either integrated into a product (embedded) or separately (non-embedded) (non-embedded).	Recital 6: AI systems are designed to operate with varying levels of autonomy, meaning that they have at least some degree of independence.	Recital 6: AI systems can vary in autonomy and can either be standalone or integrated into products, whether physically embedded or serving their function externally (non-embedded).	Different AI systems vary in their levels of autonomy and adaptiveness after deployment.[59]

[54] The original source oft he table is from Pehlivan (n 4), 5. The table was shortened and created more specifically fort he purpose of this chapter to give a short overview on the different definitions.

[55] Commission, supra n. 49

[56] Parliament, AI Act, 2021/0106(COD) Draft Version 2 of draft after TM of 20 July 2023) (22 Jul. 2023).

[57] ibid

[58] OECD, supra n. 49

[59] Pehlivan (n 4), 5

2.1.2 Classification of AI

2.1.2.1 Low or Minimal Risk and Limited Risk Systems

AI systems classified as low or minimal risk are not subject to specific regulatory obligations. Instead, they are governed by general legal standards, particularly those established in the GDPR. Article 69 AI Act encourages providers of such low-risk AI systems to develop and adopt ’codes of conduct’.[60] For example, a basic data sorting algorithm that does not involve personal data would fall under this category and would be guided by general GDPR compliance.[61]

In contrast, limited risk systems, which involve interactions with humans, detection of human presence, determination of a person's categorization based on biometric data, or the production of manipulative content, are subject to more stringent requirements.[62] For instance, chatbots like ChatGPT, which interact with users and potentially gather biometric data, must comply with specific transparency obligations as outlined in Article 52 AI Act.[63] These obligations ensure that users are informed about the AI's functions and the data it processes.[64]

2.1.2.2 General Purpose AI

Throughout Article 52a AI Act the EU defines a general purpose AI model with systemic risk as one that either demonstrates high-impact capabilities based on technical evaluations or is designated by the Commission after expert alerts.[65] The European Parliament proposed to define the GPAI as ‘an AI system that can be used in and adapted to a wide range of applications for which it was not intentionally and specifically designed’.[66] These systems regulate generative models, which can be used for different applications and process different sources of data.[67]

[60] European Parliament and Council Article 69 (n 6)
[61] Pehlivan (n 4), 6; European Parliament and Council (n 6)
[62] Kouroupis (n 26)
[63] European Parliament and Council Article 52 (n 6)
[64] Bromhard and Merkle (n 8), 261
[65] European Parliament and Council Article 52a (n 6)
[66] Parliament, supra n. 20
[67] Thelisson and Verma (n 2), 2

Specifically, a model using over 10^25 floating point operations (FLOPs) for training is presumed to have high-impact capabilities. The Commission has the authority to revise these benchmarks and indicators through delegated acts, allowing adjustments in response to technological advances in AI.[68]

Using ChatGPT-4 as an example, its classification as a high-risk system presents a challenge due to its extensive capabilities and significant impact. As a powerful generative AI, ChatGPT-4 may be categorised under systemic risk because of its wide-ranging applicability across various domains and its ability to generate human-like text.[69] This classification could necessitate stringent compliance measures, including enhanced transparency and accountability, to ensure that its deployment does not violate ethical standards or fundamental rights.[70]

The AI Act also establishes several broad obligations that are applicable to all GPAI models, regardless of whether they pose systemic risks. For example, the providers will be required to comply with transparency requirements, which include drafting technical documentation.[71] Additionally, GPAI models must adhere to EU copyright law and furnish sufficiently detailed summaries regarding the content used for training.[72] While the exact definition of 'detailed' remains unclear, it is anticipated that the European AI Office will provide a template for clarification.[73]

Alternatively, if all generative AI systems were categorised as high risk due to the potential for use in high-risk areas, there could be a significant risk of over-regulation.[74]

[68] EU Parliamnet in Progress (n 3), 10

[69] Natali Helberger and Nicholas Diakopoulos, ‘ChatGPT and the AI Act’ (2023) 12 Internet Policy Review <https://policyreview.info/essay/chatgpt-and-ai-act> accessed 12 May 2024

[70] ibid

[71] EU Parliamnet in Progress (n 3), 10

[72] ibid; EU Parliamnet in Progress, ’Artificial intelligence act’ (n 3), 10

[73] Pehlivan (n 4).

[74] Helberger and Diakopoulos (n 68).

2.1.2.3 High-Risk Systems

There are systems that can be qualified as high-risk systems (Articles 6 to 7)[75], if the AI system is intended to serve as a safety component of a product or is itself considered as a product covered by the Union harmonisation legislation listed in Annex II, and if the said product, containing the AI system as a safety component or as a product itself, is subject to a third party conformity assessment (CA) for placing on the market or commencement of service in accordance with the Union harmonisation legislation listed in Annex II.[76] The Commission stated, that there is a need of ex-ante requirements, before any development in the EU market.[77]

When classifying a high-risk system, we have to distinguish between two main categories: first, AI systems which are used in products, which fall under EU product safety regulations, for example: toys, vehicles, medical devices and elevators and second, AI systems, which fall into specific areas, registered in a specific EU-database. These are for example: administration and operation of critical infrastructure, employment, access to and use of essential private and public services, law enforcement, administration and assistance with the interpretation and application of laws.[78] However, an AI system will invariably be classified as high-risk if it engages in the profiling of natural persons. Such high-risk AI systems will undergo assessment prior to market entry as well as throughout their lifecycle.[79] A lifecycle of AI comprises sequential stages essential for developing and deploying AI solutions. It begins with understanding the business context, followed by acquiring and analysing data, developing models, testing, and deploying them. Continuous monitoring and maintenance ensure ongoing performance, while feedback guides iterative improvements to keep the solutions aligned with evolving needs.[80]

[75] European Parliament and Council Article 6, 7 (n 6)

[76] European Parliament and Council (n 6)

[77] Bromhard and Merkle (n 8), 261

[78] EU Parliament, <KI-Gesetz: erste Regulierung der künstlichen Intelligenz | Themen | Europäisches Parlament (europa.eu)>; Kouroupis (n 9), 217

[79] Pehlivan (n 4)

[80] Jeff Saltz, 'What Is the AI Life Cycle?' (*Data Science Process Alliance*, 1 June 2023) <https://www.datascience-pm.com/ai-lifecycle/> accessed 12 May 2024

2.1.2.4 Differentiation between General Risk and High-Risk

Businesses often struggle to differentiate between GPAI systems and high-risk AI systems, leading to confusion about applicable compliance requirements and obligations. This lack of clarity can cause uncertainty among companies about which regulatory measures they need to follow.[81] Additionally, the specific obligations tied to GPAI models remain ambiguous. For example, the mandate to provide a ’sufficiently detailed summary’ of training data is open to interpretation, pending the establishment of standardised guidelines.[82] Furthermore, the categorisation of ChatGPT can be difficult, because it does not fit perfectly into any established category, because it is capable of handling such a wide range of tasks.[83]

However, it's important to recognise that ChatGPT operates purely based on algorithms and lacks any understanding of ethics or morals. This means it can generate a variety of outputs in response to prompts without any human oversight.[84] In essence, while ChatGPT may not appear to pose a significant risk on its own, its potential to generate various outputs without ethical considerations raises questions about its use and potential impact in different contexts.[85]

Furthermore, to ensure the correctness of implementation, the Commission has also introduced a high-level expert group on AI representing a wide range of stakeholders and has tasked it with drafting AI ethics guidelines as well as preparing a set of recommendations for broader AI policy.[86] The revised document from the stakeholders submitted to the Commission was highly appreciated for its practical guidelines and detailed guidance provided to developers, suppliers, and users of AI, ensuring the trustworthiness of AI systems.[87] Trustworthy AI should adhere to three key principles, compliance

[81] ‘Analysing the Impact of the EU AI Act Vote on Businesses’ (n 45)
[82] ibid
[83] ‘The EU AI Act: Concerns and Criticism’ (*Clifford Chance*) <https://www.cliffordchance.com/content/cliffordchance/insights/resources/blogs/talking-tech/en/articles/2023/04/the-eu-ai-act--concerns-and-criticism.html> accessed 12 May 2024
[84] Helberger and Diakopoulos (n 68)
[85] ‘The EU AI Act: Concerns and Criticism’ (n 81)
[86] Thelisson and Verma (n 2), 2; Kouroupis (n 8), 217
[87] ibid, 3

with legal standards and fulfilment of ethical principles. Moreover, mechanisms such as human oversight, technical robustness, safety, privacy, data governance, and transparency are essential to foster trust in AI technologies.[88]

2.1.2.5 Systems with Unacceptable Risk

The last category remains of systems with unacceptable risk, which are banned from sale on the European Market (Article 5).[89] These are for example, cognitive manipulation of individuals or specific vulnerable groups (such as voice-controlled toys that promote dangerous behaviour in children), social scoring (classification of individuals based on behaviour, socioeconomic status, and personal characteristics), biometric identification and categorization of natural persons; biometric real-time remote identification systems, such as facial recognition.[90]

Because some systems with unacceptable risks also bring significant benefits, they can be morally justified in certain situations. For example, facial recognition can be effective in tracking criminals and combating cyber threats.[91] The AI Act seeks to address such use cases and provides for exemptions under certain conditions, such as where the ex-post use of remote biometric identification is strictly limited to the targeted search of a person convicted or suspected of a serious crime.[92]

Nevertheless, real-time biometric identification systems will be under stringent regulations, including registering the system in the EU public database, conducting a fundamental rights impact assessment (FRIA), and obtaining validation for real-time usage from a judicial authority.[93] In addition, their usage will be restricted to specific timeframes and locations and permitted only for the following purposes, targeted searches of victims, prevention of a specific and present terrorist threat, or the localization or

[88] ibid, 3, 4

[89] Thelisson and Verma (n 2), 2; Kouroupis (n 8), 217

[90] Pehlivan (n 4), 6

[91] Bromhard and Merkle (n 8), 248

[92] ibid

[93] Thelisson and Verma (n 2), 6

identification of a person suspected of having committed one of the specific crimes mentioned in the regulation.[94] Similarly, ex-post use of remote biometric identification will be used strictly in the targeted search of a person convicted or suspected of having committed a serious crime.[95]

2.2 Scope of Regulation

2.2.1 Territorial Scope

The AI Act has an extraterritorial scope as detailed in Article 2 AI Act[96], and applies not only to AI systems or general-purpose AI models placed on the market or put into service in the EU, but also to systems deployed by entities established both inside and outside the EU, as long as the output is used in the Union.[97]

This reach tracks a similar approach of Article 3 GDPR[98], which applies to EU-based organizations and to entities established outside the EU where they offer goods and services to individuals in the EU or monitor the behaviour of such individuals.[99] If the AI Act applies to AI system providers in the EU, then providers from other countries who sell AI systems in the EU, as well as those in the EU who use these systems, must also follow this law.[100] Providers and users from third countries will also need to comply with the AI Act if the system's output is utilised within the EU.[101]

2.2.2 Personal Scope

The European Commission has adopted for a horizontal regularity approach. The AI Act is similar to the GDPR with regard to the personal scope. It is applicable to any natural or legal person, public authority, agency or other

[94] ibid
[95] Pehlivan (n 4), 6; retical 65
[96] European Parliament and Council Article 2 (n 6)
[97] Kouroupis (n 8), 218
[98] Regulation (EU) 2016/679 Article 3 GDPR
[99] Pehlivan (n 4), 3; Kouroupis (n 8), 218
[100] Thelisson and Verma (n 2), 13
[101] ibid; Pehlivan (n 4)

body using an AI system under its authority, unless the AI system is used in the course of a personal non-professional activity.[102] Providers of free and open-source models are exempted from the regulations outlined in the AI Act. According to Article 3(2) AI Act[103], the term 'providers' includes natural or legal persons, public authorities, agencies, or other bodies that either develop an AI systems or commission its development, with the intention of marketing or deploying it under their own brand or trademark.[104]

This exemption does not apply to systems which are classified as high-risk in accordance with Articles 6(1) and (2) AI Act related to products covered by Union harmonisation legislation.[105] This exemption does not cover obligations for providers of GPAI models with systemic risk.[106]

2.3 Enforcement

The AI Act furthermore establishes an enforcement framework, which is overseen by national competent authorities, designated by each EU Member State to supervise the application and implementation.

2.3.1 AI Management Board

The AI Management Board is tasked with ensuring that both the acquisition and creation of AI tools adhere to the ethical and fundamental rights principles.[107] The Board is also responsible for drafting an Ethics and Fundamental Rights Charter, which will serve as a foundational assessment tool for decision-making regarding AI tools. Additionally, the Board will implement a risk-based approach to proactively identify and set boundaries for high-risk sectors or tools that the organisation will avoid.[108]

[102] Bromhard and Merkle (n 8), 258
[103] European Parliament and Council Article 3 (n 6)
[104] ibid; European Parliament and Council (n 6)
[105] Ibid Aricle 6
[106] Pehlivan (n 4), 4
[107] CJEU (n 11), 20
[108] ibid

2.3.2 AI Office

In January 2024, the EU established an AI Office, which is part of the Commission and will be part of the administrative structure of the Directorate-General for Communication Networks, Content and Technology. It will therefore oversee AI-related purposes.[109] The decision of the Commission, which tasks the AI Office shall perform and how it will be financed, entered into force on 21st February 2024.[110] One of the Office main tasks is to ensure the uniform application of AI legislation in the Member States by setting up advisory bodies at EU level to provide support and exchange information. The AI Office will provide guidance and coordinate joint cross-border investigations as well as supervise the implementation of the tiered approach to foundational models.[111] It also focuses on developing tools and benchmarks for evaluating GPAI models and identifying models with systemic risks.[112] Additionally, the office collaborates with top AI developers and experts to create advanced codes that set regulatory standards. It investigates regulatory breaches, conducts capability assessments, mandates corrective actions, and drafts guidelines and acts to enforce AI Law compliance effectively.[113]

2.3.3 Fines

Furthermore, there can be fines for infringing the AI Act. Article 71, 72 state that, these can either be calculated as a percentage of the liable party’s global annual turnover in the previous financial year, or a fixed sum, whichever is higher.[114] The AI Act outlines specific fines for violations: up to €30 million or 6% of the total annual worldwide turnover for the most severe breaches. These fines vary depending on the severity of the infringement, focusing on violations of provisions related to prohibited AI practices or non-compliance

[109] Commission Decision of 24.01.2024; EU Legislation in Progress (n 3), 10

[110] ibid

[111] European Commission, Commission Decision of 24 January 24: Establishing the European Artificial Intelligence Office, C (2024) 390 final

[112] Commission Decision of 24.01.2024; EU Legislation in Progress (n 3), 10

[113] ibid

[114] Pehlivan (n 4), 11; Bromhard and Merkle (n 8), 260; European Parliament (n 6)

with data requirements. Lesser infractions incur fines of up to €20 million or 4% of annual worldwide turnover. These penalties are designed to enforce compliance with the Act's rigorous standards.[115]

2.4 Resume

First, a clear definition of AI is established, aligning with the OECD's principles. The AI Act's classification of AI systems, from low-risk to high-risk (risk-based approach), sets the stage for understanding the compliance requirements based on the potential impact on fundamental rights and safety.[116] This structure ensures that higher-risk AI applications, particularly those used in critical sectors like healthcare and judiciary, are subject to stringent regulatory oversight. A major concern here is the ambiguity of the regulations which can create uncertainty regarding the specific obligations for providers.[117]

Second, the AI Act is closely integrated with existing EU legislation, such as the GDPR and the Data Governance Act. This harmonization aims to create a cohesive regulatory environment that balances innovation with the protection of personal freedoms and rights.[118]

Third, there are detailed the mechanisms for implementing and enforcing the AI Act, including the roles of the AI Management Board and the AI Office. These bodies will ensure compliance, oversee CAs, and impose fines for violations.[119] These expected fines are comparatively high and can therefore have a significant financial burden. Such significant penalties might also be viewed as an overreach of regulatory power, possibly deterring companies from engaging in the AI sector in Europe.[120]

Therefore, there is the need for a precise legal framework that balances innovation with ethical considerations and market impacts.[121]

[115] Pehlivan (n 4), 11

[116] ibid

[117] Schwemer, Tomada and Pasini (n 1), 257

[118] Pehlivan (n 4), 8

[119] Commission Decision of 24.01.2024; EU Legislation in Progress (n 3), 10

[120] ibid

[121] Khalifa and Sabry (n 19), 105

3 High-Risk Systems in Depth

This chapter provides an overview of the requirements for high-risk systems and analyses the extent to which those AI systems used in judicial proceedings have an impact on the decision-making process. It also addresses whether the complete replacement of judges by AI is feasible or compatible with EU principles. This research includes a critical assessment of the impact of AI in the judiciary and its alignment with foundational legal standards. The sub-question: '*What are the specific challenges and implications of implementing high-risk AI systems within judicial processes, and how do these systems impact judicial decision-making and procedural fairness?'* will be answered.

3.1 Conditions for High-Risk Systems

The classification as a high-risk AI system is based on the intended purpose of the AI system in accordance with existing EU product safety regulations. Thus, the classification depends not only on the function of this system but also on its specific purpose and application modalities.[122] For such a classification, the conditions of Article 6 AI Act have to be fulfilled (see 2.1.2.3).[123]

A system will lose its high-risk classification, if it performs narrow procedural tasks, improves the outcome of previous human activities, such as merely providing an additional layer to human activities, does purely detect decision-making patterns and deviations and does not influence human decisions, such as identifying potential inconsistencies, or performs purely preparatory tasks, such as file handling.[124] Regulations must ensure that users understand how the AI systems work and what data is being processed.[125]

[122] Recital 27 AI Act

[123] European Parliament and Council Article 6 (n 6)

[124] Pehlivan (n 4), 6

[125] Reason 5.3 AI Act, 12

3.2 Requirements for High-Risk Systems

Every high-risk AI system is subject to stringent compliance requirements, with multiple specific obligations that must be met to ensure regulatory adherence.[126]

3.2.1 Risk Management System

Article 9 AI Act implements a risk management system, which is a continuous interactive process throughout the entire life of an AI system, requiring regular systematic updates.[127] The risk management measures reoffered to the last condition are designed to ensure that any residual risk associated with a specific hazard and the overall residual risk of high-risk AI systems can be deemed acceptable, when the system is used according to its intended purpose or in the context of reasonably foreseeable misuse.[128]

3.2.2 Data and Data Governance

High-risk cases, in which systems employing techniques where models are trained with data must be developed using training, validation and testing datasets that meet several criteria, which are described in Article 10(2-5) AI Act.[129] Especially Article 10(5) AI Act is relevant, when it comes to data protection and interference with the GDPR. Article 10(5) AI Act introduces a legal framework for processing special categories of personal data for debiasing purposes.[130] This clarification holds significant importance as, under the GDPR, modelers would have needed explicit and freely given

[126] Retical 51 AI Act
[127] European Parliament and Council (n 6)
[128] ibid
[129] European Parliament and Council Article 10 (n 6); Schwemer, Tomada and Pasini (n 1), 6
[130] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

consent for collecting and processing sensitive data.[131] While interpreting debiasing as falling within the realm of 'public interest' may offer some justification, potentially aligning with the exception outlined in Article 9(2)(g) GDPR allowing processing for reasons of substantial public interest, this provision could offer a clearer legal foundation.[132] Criteria for training, validation and testing data sets to be used for the training of models of AI systems.[133]

3.2.3 Technical Documentation, Record-keeping, Transparency and Provisions of Information

The AI Act also mandates through Article 11, that high-risk AI systems must be accompanied by technical documentation demonstrating compliance with the specified requirements.[134] Additionally, they have to be developed with logging capabilities enabling automatic event recording to ensure traceability of their functioning throughout their lifecycle (see Article 12 AI Act).[135] For providers meeting this obligation could become a balancing act, as the storage of data relating to the processes must simultaneously meet the requirements of the GDPR.[136] The operation of the AI system must be sufficiently transparent and accompanied by user instructions, as stated in Article 13 AI Act.[137]

[131] ibid
[132] ibid
[133] ibid
[134] European Parliament and Council Article 11 (n 6)
[135] European Parliament and Council Article 12 (n 6); Schwemer, Tomada and Pasini (n 1), 6
[136] Bromhard and Merkle (n 8), 260
[137] European Parliament and Council Article 13 (n 6); Schwemer, Tomada and Pasini (n 1), 6; retical 49 AI Act

3.2.4 Human Oversight

AI systems must be effectively supervised by natural persons according to Article 14 AI Act, in order to prevent or minimise the risks that may arise when a high-risk AI system is used as intended.[138]

In general, AI systems have to be implemented in a way, that human can effectively oversee them, while using. Such manner includes appropriate human-machine interface tools.[139] Article 14(3) AI Act defines two requirements for this purpose, first, it must be determined by the provider before the AI system is placed on the market or put into service and, if technically feasible, integrated into the high-risk AI system. Second, it must be determined by the provider before the AI system is placed on the market or put into service and is capable of being implemented by the user.[140]

Additionally, Article 14(3) AI Act regulates measures aimed at enabling such supervision, such as: correct interpreting of results of AI, consider the characteristics of the system and the available interpretation tools.[141] Humans must have the necessary competence, training and authority to carry out the role of oversight.[142] The problem with Article 14 AI Act is that it does not distinguish between systems, which take and implement independent decisions without any human intervention, and systems that are used to support human decision-making.[143]

It is important to understand, that the obligation relates exclusively to the provider of such AI system, it does not stipulate an obligation for users to actually perform human oversight during operation.[144]

On the other side, users of such AI systems are required to use them in accordance with the accompanying instructions by the provider (Article 29(1) AI Act). A clear and concise documentation must inter alia include a detailed description of needed human oversight measures.[145]

[138] European Parliament and Council Article 14 (n 6); Recital 48 AI Act.

[139] Schwemer, Tomada and Pasini (n 1), 5

[140] European Parliament and Council Article 14 (n 6); ibid, 6

[141] ibid; European Parliament and Council (n 6)

[142] ibid; Schwemer, Tomada and Pasini (n 1), 6

[143] Joseph Srouji, 'Artificial Intelligence and Automated Decision Making: The New Frontier of Privacy Challenges and Opportunities' 163

[144] Schwemer, Tomada and Pasini (n 1), 6

[145] European Parliament Council Article 29 (n 6); Recital 46 AI Act.

3.2.5 Accuracy, Robustness and Cybersecurity

High-risk AI systems have to be designed and developed that they achieve an appropriate level of accuracy, robustness and cybersecurity and perform consistently in those respects throughout their lifecycle (Article 15(1) AI Act).[146] To this end, the Commission shall, where appropriate, encourage the development of benchmarks and measurement methodologies in cooperation with relevant stakeholders and organisations.[147]

3.2.6 Obligations

Article 16(a) AI Act requires the provider to ensure that the AI system is designed and developed in such a way, that it can be effectively overseen by a human to prevent or minimise the risk to health, safety or fundamental rights, and that it achieves an appropriate level of accuracy, robustness and cybersecurity throughout its lifecycle, taking into account its intended purpose.[148] The provider is required to fulfil the requirements set out in chapter 2 of Title III of the AI Act.[149] Before an AI system is made available for use or placed on the market, the provider or their authorised representative must register it in a new EU AI database (Articles 51, 60 AI Act).[150] In addition, if the provider uses datasets to train, validate, or test the AI system, they must ensure that these datasets are ’relevant, representative, free of errors, and complete’ (see also Article 10(3) AI Act).[151]

The requirements are to some extent unrealistic and hinder providers from acting in accordance with the functioning of the internal market. It is also difficult, to determine what obligations need to be met and how all these instruments relate to each other.[152] If all generative AI systems were to be

[146] European Parliament and Council Article 15 (n 6); Schwemer, Tomada and Pasini (n 1), 6; retical 51 AI Act

[147] European Parliament and Council (n 6).

[148] Tycho De Graaf and Gitta Veldt, ‘The AI Act and Its Impact on Product Safety, Contracts and Liability’ (2022) 30 European Review of Private Law 810

[149] ibid

[150] European Parliament and Council Article 51, 60 (n 6)

[151] Ibid Article 10

[152] Schwemer, Tomada and Pasini (n 1), 7

classified as high-risk due to their potential use in high-risk areas, there could be a significant risk of over-regulation.[153]

3.2.7 Conformity Assessments

If an AI system is identified as high-risk under the EU AI Act, it will require a Conformity Assessment (CA), which must be carried out regardless of the type of data processed, as set out in Article 3(2) AI Act.[154] CAs can be internal, carried out by the provider of the system or associated parties, which involves a self-assessment regulated under Annexes VI and VII, as outlined in Article 6(2) AI Act.[155] Alternatively, external CAs are mandated for certain AI systems under Article 6(1) AI Act, and are carried out by a designated external body meeting the criteria of Article 33 AI Act.[156] CapAI is a specialised tool developed to assist providers of high-risk systems in implementing CAs in accordance with the AI Act. It focuses on internal controls, to ensure that these systems meet rigorous safety, transparency, and ethical standards prior to deployment.[157] This tool not only facilitates the compliance verification process but also aligns with additional transparency requirements mandated by the AI Act.[158]

The AI Act also imposes additional transparency requirements on AI systems that interact directly with humans, such as chatbots and emotional recognition systems. Providers must clearly inform users when they are engaging with AI-generated content, as stated in Article 52 AI Act.[159] This comprehensive framework ensures that both internal and external CAs align with the broader regulatory goals of the AI Act, enhancing user awareness and ensuring AI compliance with existing legal standards.[160]

[153] Helberger and Diakopoulos (n 59), 3

[154] European Parliament and Council Article 3 (n 6); Thelisson and Verma (n 2), 6

[155] European Parliament and Council Article 6 (n 6); Bromhard and Merkle (n 8), 260; European Parliament and Council (n 6)

[156] Floridi and others (n 7), 12

[157] ibid

[158] ibid

[159] ibid, 13; European Parliament and Council Article 52 (n 6)

[160] ibid

3.3 Problematic High-Risk Cases

To address the research question, this study will first examine AI systems applicable to juridical processes. Subsequently, it will analyse the emerging challenges, particularly focusing on the interaction between the deployment of high-risk AI systems and GDPR compliance. This approach will help elucidate specific legal and regulatory issues arising from the use of AI in legal contexts in order to answer the sub-question:

'What are the specific challenges and implications of implementing high-risk AI systems within judicial processes, and how do these systems impact judicial decision-making and procedural fairness?'. Therefore, several questions have to be considered, such as, first, which AI systems are in discussion to be used by judicial authorities and in how far they do assist them? And second, which problems result therefrom, regarding the trustworthiness of AI, fair processes and the protection of personal data, while using AI?

3.3.1 AI Systems intended to be used by Judicial Authorities

Point 8(a) of Annex III classifies AI systems that are employed either by or on behalf of judicial authorities to assist in legal research, interpretation, and application of laws to specific cases, or similarly used in alternative dispute resolution processes, as high-risk.[161] In addition, judicial authorities are recognised under Article 47 of the Charter of Fundamental Rights as bodies capable of providing effective judicial protection, emphasizing their critical role in the administration of justice.[162]

A key issue with the AI Act is its definition of a 'provider' as articulated in Article 3 AI Act.[163] This broad definition encompasses a wide range of entities, potentially complicating compliance and regulatory enforcement.[164]

[161] European Parliament and Council (n 6)

[162] Charter of Fundamental Rights European Union (2012/C 326/ 02)

[163] European Parliament and Council Article 3 (n 6); See definition Section 2.2.2

[164] ibid

The implication, with respect to judicial independence, is that the provider should not be executive or legislative power.[165] If a national government were responsible for designing algorithms used in courts, it could potentially interfere with decision-making and undermine the external aspect of judicial independence. Similarly, if a private-sector provider were involved, it should operate independently of any influence from public authorities to prevent indirect manipulation of the judiciary.[166] Additionally, considering that the AI Act allows for the possibility of the provider being located in a third country, concerns arise regarding potential surveillance and control by foreign states.[167] Uncontested is, that the use of AI improves the efficiency and effectiveness of judicial processes, which is also the aim of the Commission itself.[168] Such improvement on effectiveness can be proven by several studies, for example from Harvard University and Boston Consulting Group (BCG)[169] as well as in juridical contexts.[170]

There are several AI systems under discussion. This thesis focusses on some of the most relevant and critical ones.

3.3.1.1 SIGA

First, an AI system called SIGA, which is a case management system that aims to be the unique platform in which all cases are managed end-to-end, for the Court and the General Court. This system could at first be developed internally and will be tested under close user supervision.[171] The objective of this module is to aid users in enhancing the handling of original documents. For instance, it may provide automated recommendations on topics or keywords, identify references within the text, or aid in processing text related to pending cases for decisions and conclusions. An advantage of using such

[165] Aziz Z Huq, ‘A RIGHT TO A HUMAN DECISION’ 106 Virginia Law Review

[166] Eugene Volokh, ‘Chief Justice Robots’ 68 DUKE LAW JOURNAL

[167] ibid, recital 10 AI Act

[168] CJEU (n 11), 6

[169] ‘Harvard And BCG Unveil The Double-Edged Sword Of AI In The Workplace’ <https://www.forbes.com/sites/danpontefract/2023/09/29/harvard-and-bcg-unveil-the-double-edged-sword-of-ai-in-the-workplace/?sh=13a22ef83f9f> accessed 12 May 2024.

[170] Jonathan H Choi and Daniel Schwarcz, ‘AI Assistance in Legal Analysis: An Empirical Study’ (13 August 2023) <https://papers.ssrn.com/abstract=4539836> accessed 12 May 2024

[171] CJEU (n 11), 6

a system would be to save time and minimise errors, enabling the ECJ staff to concentrate on more advanced tasks.[172] The aim of SIGA is, that people are working together, not separately. Furthermore, this technology helps to organise information better. It has to be made sure, as always while working with AI systems, that the data is of good quality to improve the work. Therefore, an institution should be implemented to overview the implementation of the data to such systems, that the used data is accurate and reliable.[173]

3.3.1.2 Speech-to-Text Machine

Second, a speech-to-text machine, this type of AI could be used to automatically generate transcripts of the hearing.[174]

This AI system would also save time to produce texts. However, it could be problematic to protect personal data. Speech-to-text machines often process highly sensitive data information, which must be stored afterwards. Therefore, the in- and output of this system must be under secure circumstances, to ensure that the content of the court hearing remains secret.[175]

3.3.1.3 Search Engines

Third, search engines, which could be used by the Court staff for searching juridical documents.[176] Through this AI system, they would also have the opportunity to use AI. They would benefit from a search engine for legal documents, including semantic search, where the machine is able to understand the context and meaning behind a user's query.[177]

On the other hand, these systems present several challenges that need to be addressed to ensure fair and effective legal outcomes. AI search engines can reflect and amplify biases in their training data. Historical legal data used to

[172] ibid, 7

[173] Khalifa and Sabry (n 19), 107

[174] CJEU (n 11), 6

[175] ibid

[176] ibid

[177] Khalifa and Sabry (n 19), 107

train these systems may contain biases that, if not carefully managed, could lead to discriminatory practices and unfair decisions. This could also lead to incorrect outcomes that could undermine the legal process.[178]

In addition, AI search engines process large amounts of sensitive information, raising significant privacy and security concerns. These systems will need to comply with data protection laws, such as the GDPR, in order to maintain the confidentiality and integrity of legal proceedings.

3.3.1.4 Natural Language Processing

Fourth, through Natural Language Processing (NLP), AI could be used to analyse and understand judicial documents.[179] This system would allow the user to have a faster and more accurate analysis as well as automatic summaries. This would presume, that the AI used is well trained and uses sufficient quality data.[180] Furthermore, it would have the possibility to break language barriers in communication, which would mean that people from all over the world can be understood perfectly during court hearings.[181] No specific interpreter would be needed. This in consequence would also reduce costs. NLP is able to do: multimodal translations, contextual translation as well as cross-language retrievals.[182] When using such an AI, it has to be made sure, that the outcome is correct, meaning that the specific AI system is not leaving out relevant information, which could be important for a judicial process, especially regarding empathy and personal information.[183] On the other hand, it is observed that eyewitness testimonies in court do not always reflect the true circumstances completely but are inherently subjective, which leads to a distortion of the facts.[184]

[178] Forgó (n 36), 43
[179] CJEU (n 11), 15
[180] ibid
[181] ibid
[182] ibid
[183] Forgó (n 36), 48
[184] ibid

3.3.1.5 AI-Powered Virtual Assistant

Last, through AI-powered virtual assistants, the Court staff could improve doing administrative tasks. This could be possible with daily tasks, such as scheduling, preparing of documents or letters, as well as taking care of administrative duties.[185] Such an AI system is not deeply connected to sensible personal data regarding the content of court hearings or decisions of judges, this kind of AI would help to save time and could, for example, detect overlapping of court hearings.[186]

3.3.2 Assistance of AI

AI systems generally assist humans by conducting research, interpreting facts and law, and applying the law to specific facts. It is crucial to emphasise that such systems should not only aid in interpretation but also in the thorough research of facts.[187] What exactly this entails remains vague. In any case, legal information retrieval and case law search systems are unlikely to be covered.[188] Even if AI systems for case law search and information retrieval are used directly by judicial authorities, they do not as such assist the authority in fact-finding or in the direct application of the law to the facts, although the design of search algorithms may present a risk of bias in terms of what would be considered a relevant case and the information that they display to the user.[189] A literal interpretation implies furthermore that intertwined tasks of a judge can be compartmentalised into decision-making and non-decision-making parts, which may not necessarily be the case.[190]

To delineate the classifications of AI systems in terms of risk, it is crucial to understand who employs the system and for what purpose, as outlined in Annex III, point 8(a) and Article 7(2)(a) of the high-risk framework.[191] This framework highlights the intended use of an AI system as defined by the

[185] Khalifa and Sabry (n 19), 107

[186] ibid

[187] ibid

[188] Khalifa and Sabry (n 19), 107

[189] ibid

[190] Khalifa and Sabry (n 19), 108

[191] European Parliament and Council (n 6)

provider, which includes the specific context and conditions under which the system is to be utilised.[192] This intent is detailed in the accompanying documentation provided by the provider, such as usage instructions, promotional materials, and technical documents. This distinction is critical for classifying a system as high-risk.[193] This implies that such purpose is unilaterally defined by the provider of an AI system. Consequently, if an AI system is directly marketed towards judicial authorities, it would fulfil the first part of the requirement of the use case in Annex III point 8(a).[194] Conversely, if an AI system is marketed exclusively towards private practice (but unintendedly used by a judge or people working for judicial tasks) it would likely not fulfil the requirement and thus not be considered high-risk.[195]

3.3.3 Upcoming Problems of Using AI Systems in Judicial Processes

3.3.3.1 High Quality Data

A significant concern arises when AI systems are trained on low-quality data or fail to meet established criteria for accuracy and robustness. Inadequate design and testing prior to deployment can result in AI systems that operate unfairly, potentially leading to discriminatory outcomes or other forms of injustice against individuals.[196] This underscores the necessity for rigorous development standards and validation processes to ensure equitable AI functionality.[197] Moreover, the term ’high-quality data’ must be contextualised. Even databases on court cases include cases that were decided at times when different moral standards prevailed or when judicial precedents had not yet adapted to modern social structures.[198] This in consequence has an impact on the decision-making process itself. It has to be ensured, that the

[192] ibid

[193] CJEU (n 11), 14

[194] European Parliament and Council (n 6)

[195] Schwemer, Tomada and Pasini (n 1), 107; retical 40 AI Act

[196] Nikolaus Forgó, ‘Zur Regulierung Künstlicher Intelligenz, Auch in Der Strafverfolgung’ (2023) 106 Monatsschrift für Kriminologie und Strafrechtsreform 48

[197] ibid

[198] ibid

use and outcome of AI based information is transparent and maintains public trust to ensure effective legal protection.[199]

The thought of employing AI in the actual decision-making process implies that those who create and oversee the algorithm hold sway over the outcomes.[200] Therefore, it's imperative to ensure transparency in algorithms and allow for third-party scrutiny before implementing AI systems, especially within governmental functions.[201]

3.3.3.2 Responsibility

Moreover, the existing legal framework operates under the assumption that humans are the active agents behind court and administrative decisions. Ultimately, humans bear responsibility for the consequences and societal implications of their decisions.[202] It can be inconceivable and legally untenable to attribute responsibility to machines regarding processes.[203] Instead, laws often assign operational or organizational responsibility to humans when utilizing machines, technology, or organizational structures.[204] To understand the upcoming problems through using AI in decision-making process, it is elementary to understand the difference between machine decisions and human decisions. It lies fundamental in their operational basis and impact.[205] Machine decisions, driven by algorithms and machine learning, excel in handling large data sets quickly, identifying patterns, and providing predictions with consistency and scalability.[206] These decisions are primarily correlational rather than causal, optimised for specific performance metrics without necessarily understanding underlying reasons.[207]

[199] European Parliament and Council (n 6)
[200] ibid
[201] Forgó (n 164), 48
[202] Rita Matulionyte and Ambreen Hanif, 'A Call for More Explainable AI in Law Enforcement' [2021] 2021 IEEE 25th International Enterprise Distributed Object Computing Workshop (EDOCW), Enterprise Distributed Object Computing Workshop (EDOCW), 2021 IEEE 25th International, EDOCW 75
[203] ibid
[204] Gentile (n 36), 12
[205] Huq (n 160), 672
[206] ibid
[207] Huq (n 160), 673

Conversely, human decisions incorporate intuition, ethical reasoning, and flexibility, allowing for individualised judgment and adaptability to context.[208] This ability to consider moral and social implications, alongside nuanced reasoning, marks a critical difference from the more data-driven, objective approach of machines.[209] Machine decisions excel in efficiency, consistency, and scalability, effectively managing vast datasets and delivering quick, uniform results. However, they lack the nuanced judgment and ethical considerations inherent to human decision-making, which can interpret complex contexts and incorporate moral reasoning.[210]

While human decisions benefit from deep contextual understanding and creativity, they suffer from potential inconsistencies, slower processing times, and scalability limitations. This dichotomy underscores the need for a balanced approach that leverages the strengths of both methods while mitigating their weaknesses.[211]

If AI tools should be used in judicial processes, they have to comply with several principles, particularly the requirements of independence and impartiality. Furthermore, there can be a disruption with some national laws.[212] This is why human oversight of AI systems plays a significant importance.

3.3.3.3 Human Oversight

The necessity of human oversight in AI-driven decision-making juxtaposes the challenges in establishing a legal mandate for such oversight. Human involvement is critical due to ethical considerations, accountability, error correction, and maintaining public trust, as these aspects often lie beyond the capability of current AI technologies.[213] However, formulating a normative foundation for mandating human decisions legally is elusive.

[208] Michaels (n 44), 1082
[209] Huq (n 160), 673
[210] ibid
[211] Michaels (n 44), 1082
[212] European Parliament and Council (n 6)
[213] Huq (n 160), 673

This difficulty arises from the increasing reliability of AI, the variable impacts of AI decisions, and the complexity of integrating stringent oversight without curtailing the benefits of technological advancements.[214] Thus, while human oversight is indispensable in certain contexts, a universal legal requirement remains a complex, unresolved issue.[215]

3.3.3.4 Interfere with EU Principles

When considering the possibilities of the use of AI in the judiciary, it is important to emphasize from a constitutional perspective that for example in Article 6(1) ECHR the law refers to 'judges' and a right to a statutory 'judge'.[216] The principle of judicial independence is an expression of the wider EU principle of ensuring effective judicial protection. Within this framework, Member States are required to provide effective legal remedies in areas governed by EU law, which encompasses ensuring the existence of impartial courts.[217] Judicial independence has both, internal and external dimensions under EU law. While the internal dimension maintains an impartial attitude towards the parties of the litigation, the external dimension requires judges to be free from interferences.[218]

Should AI be utilised, for instance in research or data processing, courts must transparently validate how such usage could potentially influence or compromise decision-making responsibility. [219] The independence of judges, as mandated by EU law, could be at risk if AI-dependent decisions are biased by underlying data. European and international laws guarantee the right to legal hearings or consultations in judicial and administrative contexts. This right should not be curtailed by the integration of AI in procedural tools.[220] While using AI in courts, it has to be ensured, that judges are free from external pressures that could influence their decision-making processes.[221]

[214] ibid

[215] ibid

[216] Europen Court of Human Rights (2012/C 326/02) Article 6

[217] AK, C-824/18), 118

[218] Gentile 1 (n 33).

[219] Aviv Ovadya, 'Reimagining Democracy for AI' (2023) 34 Journal of Democracy 162

[220] ibid

[221] Gentile (n 33), 2

Furthermore, there is a risk by adopting automated decision-making tools by the government because it could potentially disrupt the traditional balance between legislative, executive and judicial powers by introducing non-transparent, unaccountable decision-making processes.[222]

3.3.3.5 Benefits

On the other side, the quality and consistency of judicial decisions can be enhanced. Using AI will allow the Courts employees to process their tasks more quickly and more efficiently.[223] For example, using SIGA will automatically extract references and enrich texts, as well as generate descriptors automatically. SIGA would also be able to recognise case correlations.[224] Especially this recognition could lead to a fairer decision by judges, because they have access to similar cases and can refer to them, instead of deciding completely independent.[225] Controversy, this use then could also lead to the risk, that judges rely on the correlations, and don't have a deep look on the differences of the facts of the case or personal circumstances.[226]

Furthermore, legal searching could be improved by AI, to ensure a broad range of facts, to come to a decision. AI could assist judges, legal officers, or colleagues in legal research by quickly analysing vast amounts of data, finding relevant cases, and providing recommendations.[227] This could make the research process more efficient and uncover insights that might not be obvious at first.[228] Looking ahead, as national databases become more interconnected or widely available, AI could also help overcome language barriers using advanced translation algorithms.[229]

[222] Huq (n 160), 674
[223] Ovadya (n 188), 165
[224] CJEU (n 11), 13
[225] ibid
[226] Gentile (n 36), 12
[227] ibid
[228] Ovadya (n 188), 165
[229] ibid

However, it's important to note that for these algorithms to be effective, they need to be extremely accurate. While current technology hasn't yet reached this level of accuracy, rapid advances in AI suggest that this could soon change.[230]

Important will therefore be in the future, that it is clearly visible from where information is from and that the source is transparently disclosed.

3.3.4 Replacement of Judges through AI

The prospect of replacing human judges entirely with AI poses significant concerns. Professor Eugene Volokh articulates that if an AI system consistently delivers decisions that are deemed sound, we should be open to accepting its judgments without rigidly adhering to traditional methods of decision-making.[231] This statement criticises in some way, the acceptance of decision based on AI. Professor Volokh favours the use of AI during judgements. But on the other hand, we also have to consider, that there is a significant value in the human involvement in the process leading to the production of the opinion.[232] Human society actively participates in shaping the law by presenting legal arguments in court, influencing judicial decisions, and thereby influencing the legal system. This involvement distributes power among judges, legal professionals, and to some extent, the public, allowing them to contribute to legal developments.[233] It also encourages a well-informed legal community to closely engage with the law. Unlike a system where humans collectively shape the law through reasoned debate, an AI judge operates as an opaque authority, less responsive to persuasion, even if it provides explanations similar to human judges.[234]

The function of a judge is to shape the law and adapting it to a constantly changing society. Judges make law in a more measured way than

[230] ibid

[231] Eugene Volokh, 'Chief Justice Robots' 68 DUKE LAW JOURNAL 1135; Michaels 1083 (n 16)

[232] Michaels (n 44), 1082

[233] ibid, 1083.

[234] ibid, 1084

legislatures.[235] They have to balance respect for precedent and stability against the need for law to adapt to changing and unforeseen circumstances through adjudication. The disagreements between judges or litigants can help to clarify and publicise debates about what is the best law or policy.[236] The human legal system encourages a dialogue between law and society, and it is beneficial to have judges who are part of that society.[237] In addition to that, without human judges the society could lose much of the community of professionals paying attention to the law. There will be a replacement of legal human thoughts of artificial, databased thoughts. This could hinder the ability to adjust the law to changing societal circumstances.[238]

Furthermore, there can be a risk of the loss of ethical reasoning that human judges provide, which AI may not fully replicate due to its reliance on data-driven processes without moral considerations. In consequence there could be a lack of empathy and fail to consider broader societal impacts.[239]

Some scholars contend that there is no inherent right to a decision made by humans; rather, they argue for the legitimacy of ’a well-calibrated machine decision’ as a sufficient alternative.[240] This stands clearly against the current law of Article 6(1) ECHR, which refers to human judges (see section 3.3.3.4).[241] Furthermore, in Europe it will be difficult to establish a full AI decision system, because there would be the need to change the whole EU and national law. When a judge writes an opinion, they are essentially explaining their reasoning so that everyone, including the legal community and society, can understand why they made their decision.[242]

This interaction fosters a dialogue between society and the judicial system, enhancing the legal process. The involvement of judges, as members of both the legal community and society, is beneficial in facilitating this exchange.[243]

[235] Huq 107 (n 160)
[236] ibid.
[237] Michaelis (n 44), 1085
[238] Volokh (n 192), 1138
[239] Huq (n 160), 675
[240] ibid
[241] Europen Court of Human Rights (2012/C 326/02) Article 6
[242] Michaels (n 44), 1083
[243] ibid, 1098; Ashley S. Deeks, ’Secret Reason-Giving’, 129 YALE L. J. 675

If understanding of the law is limited, there may be little response to executive branch lawlessness.[244] The introduction of AI into the judiciary poses a significant challenge to the division of powers by potentially undermining checks and balances, introducing opacity into decision-making processes, opening the door to external control, and raising constitutional concerns about the judiciary's role in resolving legal disputes.[245]

When comparing the use of AI for helping lawyers doing their work more efficiently and replacing judges through AI, to have more consistent decisions, there is a massive difference to record. In any event, efficiency arguments do not adequately account for the increased risks due to the loss of redundancy, nor do they answer the related separation of powers concerns.[246]

The shift from human judges to AI in judicial roles prompts substantial concerns. Although AI may enhance consistency in decisions, as noted by Eugene Volokh, it cannot match the nuanced understanding and adaptability of human judges to changing societal norms. Human judges play a pivotal role in interpreting and shaping laws in response to societal dynamics.[247] Their participation ensures a vital dialogue between law and society, crucial for legal relevance and fairness. Furthermore, replacing judges with AI could centralise power, diminish transparency, and inhibit public participation in the judiciary, jeopardizing the system's checks and balances.[248]

3.3.5 Data Protection

Furthermore, the proper protection of data can be seen difficult, during the implementation of high-risk systems as well as while using AI to improve the decision-making process, because of the inference of the EU AI Act within the GDPR.

[244] Michaels (n 44), 1086
[245] ibid, 1100
[246] ibid, 1101
[247] Volokh (n 192), 1138
[248] Michaels (n 44), 1101

4 Comparison between GDPR and AI Act

The AI Act will be compared to the GDPR, followed by an explanation of the impact on the use of AI through in the courts. The research question: '*How do the regulatory requirements of the AI Act intersect with those of the GDPR, particularly in terms of data governance, transparency, and human oversight, and what conflicts or synergies arise from this interplay?'* will be answered.

4.1 General Data Protection Regulation

The GDPR regulates that 'personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed' (= data minimisation).[249] This principle requires that organisations and governments collect only data that is needed to achieve the purpose at hand.[250] Furthermore, the GDPR requires a Data Protection Impact Assessment (DPIA) to be conducted if the processing of personal data, which is likely to result in a high-risk to the rights and freedoms of individuals.[251] If personal data are processed, a DPIA may also be required in addition to the CA of AI Act, and both can be conducted by the same organisation, such as the data controller.[252] The documentation of a DPIA enables the data controller to demonstrate that they acted in a diligent and responsible manner before processing the data in the event of damage or a lawsuit.[253]

Additionally, the general aim of data protection regulations is designed to serve mankind and the right to informational self-determination. Every decision underlays the principle of proportionality and has to respect fundamental rights.[254]

[249] Regulation (EU) 2016/679 GDPR (n 125)

[250] Abigail Goldsteen and others, 'Data Minimization for GDPR Compliance in Machine Learning Models' (2022) 2 AI and Ethics 477

[251] Regulation (EU) 2016/679 GDPR (n125)

[252] Pehlivan (n 4), 10

[253] Thelisson and Verma (n 2), 5

[254] Retical 4 GDPR

The challenge lies in the fact that AI often requires personal data as a basis for learning, while simultaneously respecting the boundaries of data protection.[255] This issue remains, how the use of AI applications poses the risk of formerly considered anonymous or anonymised databases being de-anonymised through AI, potentially revealing information about individual people.[256] This in consequence leads to another question: who is then responsible for the lack of data?

4.2 Interplay between GDPR and AI Act

The interplay between the GDPR and AI Act is crucial for understanding how these frameworks complement each other.

There is an interplay in the scope of application. The AI Act is applicable to public and private entities across the entire AI value chain, including providers and deployers of AI systems that are placed on or utilised within the EU market, irrespective of their geographical location. Conversely, the GDPR applies to controllers and processors that handle personal data within the context of activities conducted by an establishment in the EU, or that offer goods or services to, or monitor the behaviour of, data subjects within the EU.[257]

The primary focus of the AI Act is to ensure the safe and lawful use of AI systems, while focusing on high-risk systems. On the other side, the GDPR protects personal data and privacy of individuals. [258]

A potential conflict can be, that the AI Act's broader scope may apply to AI systems that do not process personal data or are placed outside the EU, which can potentially lead to regulatory complexities.[259]

[255] Goldsteen and others (n 215), 478

[256] ibid

[257] Pehlivan (n 4), 10; Srouji (n 120), 164

[258] Rack (n 29)

[259] European Parliament and Council (n 6)

Additionally, the AI Act mandates a risk management framework for high-risk AI systems, including requirements for data governance, transparency and human oversight as well as CAs, which verify that high-risk systems have been designed and developed according to the specific requirements.[260]
The GDPR takes also a step further and requires a DPIA for processing activities that pose high-risk to individuals rights and freedoms (Article 35 GDPR). Therefore, Article 29(6) AI Act tries to bring both regulations together.[261] Both regulations aim to identify and mitigate risks, though they focus on different risks.[262]

Moreover, the AI Act regulates the adoption of data governance and management practices, including the training, validation, and testing of suitable datasets. This aligns with the GDPR's principles ensuring that personal data is processed lawfully, fairly, and transparently, minimally and appropriately relevant, and accurately (see Article 9(1) and 10(5) AI Act).[263]

Article 6 GDPR establishes a fundamental principle for data handling, which is also applicable to the use of any AI system and adheres to stringent legal standards for consent and necessity.[264] It specifies that data processing is lawful only if the data subject has consented to the processing for one or more specific purposes, or if the processing is necessary for reasons detailed in Article 6 subsections (b) to (f) AI Act.[265] AI systems operate by aggregating personal data from diverse sources such as user inputs, online interactions, sensors, and third-party data providers. This data can range from basic identifications like names and addresses to more sensitive information such as biometrics and personal preferences.[266] Once gathered, this data is

[260] Thelisson and Verma (n 2), 4
[261] European Parliament and Council Article 29 (n 6); reason 1.2. AIA, 4
[262] Rack (n 45), 45
[263] Pehlivan (n 4), 10; Regulation (EU) 2016/679 GDPR (n 125)
[264] Regulation (EU) 2016/679 GDPR (n 125); Kouroupis (n 28), 218
[265] European Parliament and Council (n 6)
[266] James Clark Kettas Muhammed Demircan, Kalyna, ‘Europe: The EU AI Act’s Relationship with Data Protection Law: Key Takeaways’ (*Privacy Matters*, 25 April 2024) <https://privacymatters.dlapiper.com/2024/04/europe-the-eu-ai-acts-relationship-with-data-protection-law-key-takeaways/> accessed 12 May 2024

processed using machine learning algorithms for various purposes, including pattern recognition, prediction, and decision-making.[267] Organisations might face overlapping compliance obligations, particularly concerning data governance and transparency. Clear guidelines are needed to navigate these overlaps effectively.

The paramount consideration is human oversight. The AI Act mandates that high-risk systems be designed to facilitate effective human oversight, thereby preventing or minimizing risks.[268] This principle is echoed in the GDPR through Article 22, which stipulates that individuals must not be subjected to decisions based solely on automated processing without meaningful human intervention.[269] Both frameworks mandate human oversight to safeguard individual rights, though they approach this from different angles – GDPR from a data processing standpoint and the AI Act from an AI operational perspective.[270]

Table 2: Comparison of the AI Act and GDPR[271]

Aspect	**AI Act**	**GDPR**
Scope of Application	Applies to providers and users of AI systems in the EU, regardless of their location, as long as the AI system's output affects individuals in the EU.	Applies to controllers and processors handling personal data of individuals within the EU or targeting individuals in the EU.
Primary Focus	Ensures the safe and lawful use of AI systems, focusing on high-risk AI applications.	Protects personal data and privacy of individuals.

[267] ibid

[268] ibid

[269] Bygrave, 'Article 22 Automated Individual Decision-Making, Including Profiling' (n 35), 22

[270] Reason 1.2. AIA, 4

[271] For having a better overview of the different aspects of the AI Act and the GDPR, there was a table created out of different sources regarding both regulations.

Risk Management	Mandates a risk management framework for high-risk AI systems, including requirements for data governance, transparency, and human oversight.	Requires a DPIA for processing activities that pose high risks to individuals' rights and freedoms.
Data Governance	Stipulates that training, validation, and testing datasets for high-risk AI systems must be relevant, representative, free of errors, and complete.	Emphasises data minimization, accuracy, and lawfulness of processing.
Transparency Requirements	Requires providers of high-risk AI systems to ensure transparency through technical documentation and logging capabilities.	Obligates controllers to inform data subjects about data processing activities and their rights.
Human Oversight	Requires high-risk AI systems to be designed for effective human oversight to prevent or minimise risks.	Article 22 ensures individuals are not subject to decisions based solely on automated processing without meaningful human intervention.
Accountability	Providers and users of high-risk AI systems are accountable for adhering to the AI Act's requirements and ensuring system compliance throughout its lifecycle.	Controllers and processors are accountable for complying with GDPR principles and must demonstrate compliance.
Enforcement and Penalties	National authorities, supported by the AI Office, enforce the AI Act with fines up to €30 million or 6% of global annual turnover for severe breaches.	Supervisory authorities enforce the GDPR with fines up to €20 million or 4% of global annual turnover for violations.

4.3 Data Protection in Decision-Making Processes

If issues regarding the protection of personal data in the use of AI by legal authorities or the use of AI in decision-making processes may arise, Article 22 GDPR has to be considered.[272] This will also give an answer to the last sub-question: '*What are the ethical and legal considerations associated with the use of AI in judicial contexts, and how can effective human oversight and accountability be ensured to uphold fundamental rights and maintain public trust?'*.

The effort by the Commission to regulate the use and implementation of AI with the data protection regulations is evidenced when comparing the AI Act with the White Paper on AI.[273] This comparison illustrates how the White Paper's discussion of human oversight under Article 22 GDPR is expanded upon in the AI Act. It offers legal protections for the various stages of AI system development that are align with the principles of GDPR. [274]

Although the GDPR does not explicitly mention AI, its provisions on automated decision-making indirectly regulate AI systems that engage in such processes, impacting individuals. Article 22(1) asserts that data subjects have the right to not be subjected to decisions based solely on automated processing, including profiling, that have significant legal effects on them or similarly significant impacts.[275] This clause serves as a critical safeguard, ensuring that decisions made by AI systems are subject to oversight and appropriate legal standards.[276]

[272] Regulation (EU) 2016/679 Article 22 GDPR

[273] Kouroupis (n 8), 225

[274] Regulation (EU) 2016/679 Articcle 22 GDPR; Guillermo Lazcoz and Paul De Hert, 'Humans in the GDPR and AIA Governance of Automated and Algorithmic Systems. Essential Pre-Requisites against Abdicating Responsibilities' (24 January 2022) <https://papers.ssrn.com/abstract=4016502> accessed 12 May 2024

[275] Regulation (EU) 2016/679 Article 22 GDPR (n 125)

[276] ibid

Therefore, it sets out three cumulative conditions: (1) a decision is taken which (2) is based exclusively on automated processing or profiling and (3) has either legal effects or equally significant effects.[277]

A decision, in this context, refers to a stance or position taken towards an individual that carries a binding effect, meaning it either must be implemented or is likely to be implemented.[278] The term ’automated’ implies that the individual affected has no influence over the digital decision-making process.[279] When decisions are based on 'profiling' rather than mere 'automated processing,' they necessitate the automated processing of personal data as defined under Article 4(4) GDPR, which includes any automated operations on personal data. This process significantly impacts or alters an individual's rights.[280]

When comparing Article 22 GDPR with the AI Act, it becomes evident that the AI Act imposes additional constraints and requirements for the deployment of AI, particularly in contexts where AI systems execute automated decisions that impact individuals.[281] Article 22 focuses on ensuring that individuals have the right not to be subject to decisions based solely on automated processing, particularly when such decisions have a significant effect on them. In contrast, the AI Act extends the regulatory framework specifically tailored to AI systems, focusing on high-risk AI applications across various sectors. It introduces requirements for transparency, accountability, and data quality that AI systems must meet before deployment (Article 52 (1) AI Act).[282] This act aims to ensure that AI systems are safe, transparent, and traceable while also respecting EU standards for privacy and data protection.[283]

[277] Bygrave, ‘Minding the Machine v2.0’ (n 35)

[278] Bygrave (n 18), 523

[279] Bygrave, ‘Minding the Machine v2.0’ (n 35)

[280] Regulation (EU) 2016/679 Article 4 GDPR; Bygrave, ‘Article 22 Automated Individual Decision-Making, Including Profiling’ (n 35) 22

[281] Regulation (EU) 2016/679 GDPR (n 125)

[282] European Parliament and Council Article 52 (n 6)

[283] ibid

The extent of human oversight and intervention in the use of an AI system can determine whether the system falls within the scope of the automated decision-making framework outlined in the GDPR.[284]

Essentially, if a human intervenes meaningfully at a crucial stage of the AI system's decision-making process, the decision may no longer be considered fully automated according to Article 22 GDPR.[285] However, it's more probable that AI systems will indeed make fully automated decisions, but effective human oversight will serve as a protective measure to ensure fairness in the automated decision-making process and uphold individuals' data protection rights.[286] When employing AI in decision-making, particularly in areas protected under data protection laws like the GDPR, there is a critical need to balance the efficiency and breadth of data processing capabilities of AI with the necessity for individualised consideration. This is important to prevent outcomes that might unfairly categorise or disadvantage individuals based on broad, impersonal data sets.[287]

There can also be drawn a line between Article 22(3) GDPR and the AI Act. Article 22(3) GDPR introduces a set of qualifications on two of the derogations in Article 22(2) GDPR, those for contract and consent.[288] The enumeration of rights outlined in Article 22(3) GDPR is not exhaustive. There is disagreement regarding the additional rights it may entail. Specifically, there were debates from different scholars, whether Article 22(3) mandates the provision of a ex post explanation of automated decisions impacting data subjects.[289] This discussion extends to the interpretation of several other provisions within the Regulation (Articles 13(2)(f), 14(2)(g), and 15(1)(h) GDPR).[290]

[284] ibid
[285] ibid
[286] Kettas (n 261), 3
[287] Huq (n 160), 678
[288] Regulation (EU) 2016/679 Article 22 GDPR (n 125)
[289] ibid
[290] ibid

In turn, the regulations of the GDPR are converse to the ones regarding the AI Act. Individuals will possess the right to file complaints regarding AI systems and obtain clarifications regarding decisions stemming from high-risk AI systems affecting their rights, (Articles 68(a) and (b) AI Act).[291] Another crossing point of the GDPR with the AI Act, is human oversight. Article 14 AI Act requires high-risk systems to be designed and developed in such a way that they can be effectively overseen by natural persons. [292]

Important to discuss regarding the protection of data, will be systems such as SIGA and speak-to-text machines. AI in general, entails the collection of vast amounts of data and has a broad range of application, which makes it difficult to oversee the data.[293] It is concerning that AI systems allow users to manipulate and analyse previously decided cases, storing relevant personal data that can be cross-referenced with new cases. This raises significant privacy concerns, as historical data is not only preserved but also actively compared, potentially affecting the integrity of new judicial assessments.[294] Judicial authorities must ensure that AI systems access only the personal data designated within a protected space and cannot interact with publicly accessible data sources.[295] All databases, especially those from various public authorities, should be interconnected while adhering to uniform safety standards compliant with GDPR, particularly Articles 6 and 22.

Furthermore, it is crucial that these databases safeguard individual rights without causing harm or discrimination.[296] For AI-driven speech-to-text systems, security measures must guarantee the confidentiality of court hearing transcripts to uphold procedural rights such as a fair trial and the principle of presumption of innocence (*in dubio pro reo,* Article 6(2)

[291] Srouji (n 120), 164
[292] Schwemer, Tomada and Pasini (n 1), 5
[293] ibid
[294] CJEU (n 11), 13
[295] European Commission, 'Communication from the Commission to the European Parliamnet, the Cpuncilm the European Economic and Social Committe, and the Committee of the Regions, buliding trust in Human-Centric Artifcicial Intelligence' (8 April 2019) 5
[296] ibid

ECHR).[297] Additionally, defendants should be informed about the use of AI in their legal processes and must consent to its application in decision-making.[298]

[297] ECHR Article 6; Srouji (n 120), 164

[298] European Parliament and Council (n 6)

5 Conclusion

More than four years passed by, until the European Court of Justice started to embrace AI. This technology is a rapidly evolving and advancing field. Consequently, it is possible that by the time the AI Act is implemented into both EU and national law, some adjustments may be necessary. Some regulations may already have become obsolete, and the legislation could potentially even be outdated.

Moreover, the AI Act might be regarded by some nations as a model for their own implementation of AI laws. This scenario underscores the need for a flexible and adaptive regulatory framework that can accommodate the fast-paced developments in AI technology, ensuring that regulations remain relevant and effective in promoting safe and ethical AI deployment.[299]

Furthermore, the integration of the AI Act with existing data protection requirements, particularly those outlined in the GDPR, is crucial. As AI systems often process vast amounts of personal data, it is imperative that they comply with GDPR principles of data minimization, transparency, and accountability. The intersection of the AI Act and GDPR will require continuous monitoring and potential updates to ensure that data protection standards are upheld, even as AI technologies advance. This alignment is essential to safeguard individual privacy rights and maintain public trust in AI applications.

The question, *'What can be seen as AI and how can AI be classified?'* is answered. In a nutshell, AI is the simulation of human intelligence processes by machines, especially computer systems and can be classified into several groups based on the risk it poses to operators and users, ranging from minimal to unacceptable in four levels.[300] Each level is associated with different requirements. The process of classifying AI systems is complex and not always straightforward, which can pose challenges in both commercial and

[299] CJEU (n 11), 24

[300] European Parliament and Council (n 6)

regulatory contexts, particularly in line with the risk-based approach.[301] In addition, these obligations are to some extent unrealistic and hinder providers from acting in accordance with the functioning of the internal market.[302]

In the discourse on the integration of AI in judicial systems and in accordance of answering the research question: '*What are the specific challenges and implications of implementing high-risk AI systems within judicial processes, and how do these systems impact judicial decision-making and procedural fairness?'* and '*How do the regulatory requirements of the AI Act intersect with those of the GDPR, particularly in terms of data governance, transparency, and human oversight, and what conflicts or synergies arise from this interplay?'*, several problematic facts arise.

First, the central challenge lies in ensuring effective human oversight. The AI Act mandates that high-risk systems be designed for such oversight, a principle mirrored in Article 22 GDPR.[303] However, implementing meaningful human intervention in automated processes remains complex and requires clear guidelines to balance efficiency and accountability.[304]

Second, AI applications often clash with the GDPR's stringent data protection requirements. High-risk AI systems must navigate the delicate balance between utilizing large datasets for training and maintaining compliance with data minimization and consent principles. Ensuring that personal data is protected while allowing for AI innovation is a critical concern.[305]

Third, both the AI Act and the GDPR emphasise transparency, but AI systems often suffer from a lack of explainability. This opacity complicates accountability, making it difficult to ensure that AI decisions are fair and understandable to affected individuals. Enhanced transparency measures and clearer documentation requirements are needed to address this issue. [306]

[301] EU Legislation in Progress (n 3); Michaelis (n 131), 1083
[302] Srouji (n 120), 164
[303] Bygrave (n 233), 5
[304] Choi and Schwarcz (n 143), 3
[305] Srouji (n 120), 164
[306] De Graaf and Veldt (n 34), 13

Fourth, the AI Act and GDPR have overlapping requirements, particularly concerning data governance and risk management. Organizations may face challenges in complying with both frameworks simultaneously, leading to regulatory complexities. Harmonizing these regulations to provide clear, cohesive guidance is essential for effective implementation.[307]

Last, the use of high-risk AI systems in judicial processes raises ethical and legal concerns. While AI can enhance efficiency, it is imperative to ensure that AI systems do not undermine fundamental rights, such as the right to a fair trial. Human judges cannot be fully replaced by AI, and maintaining the integrity of judicial decisions requires careful integration of AI tools.[308]

In conclusion, the AI Act establishes a regulatory framework for the use and implementation of AI technologies. However, it raises several questions and reveals certain gaps, particularly in areas requiring ongoing adjustments to stay relevant with technological advancement. Despite these challenges, the regulations are a positive first step and effectively integrate with existing legislative measures, such as the GDPR, to promote the safe and ethical deployment of AI.

[307] Regulation (EU) 2016/679 GDPR (n 125)
[308] Kettas (n 261), 12

Bibliography

Primary Law of the European Union:

European Commission, 'Accompanying the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts; and Annexes' (21 April 2021).

European Parliament and Council, 'Proposal for a Regulation on European data governance (Data Governance Act) COM/2020/667; Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, PE/28/2019/REV/1, OJL 172' (26 June 2019) 56–83.

European Parliament and Council, 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and certain Union Legislative Acts; Brussels' (21 April 2021).

European Parliament and Council, 'Provisional Agreement resulting from International Negotiations of the European Parliament, Committee on the Internal Market and Consumer Protection Committee on Civil Liberties, Justice and Home Affairs' (2 February 2024).

European Parliament and Council, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Secondary Law of the European Union:

Court of Justice of the European Union, ‘Artificial Intelligence Strategy’ (11 July 2023) Directorate-General for Information, 1-25, <cjeu_ai_strategy.pdf (europa.eu)> accessed 18 April 2024.

European Commission, Commission Decision of 24 January 24: Establishing the European Artificial Intelligence Office, C (2024) 390 final.

European Commission, ’Communication from the Commission to the European Parliamnet, the Cpuncilm the European Economic and Social Committe, and the Committee of the Regions, buliding trust in Human-Centric Artifcicial Intelligence’ (8 April 2019) 1.

Academic Papers:

Bromhard D and Merkle M, ‘Regulation of Artificial Intelligence – The EU Commissions proposal of an AI Act’ (08 April 2021) 6 EuCML 257, <CitationPDFURL (lu.se)> accessed 10 April 2024

Bygrave LA, ‘Minding the Machine v2.0: The EU General Data Protection Regulation and Automated Decision Making’ (6 February 2019) <https://papers.ssrn.com/abstract=3329868> accessed 30 April 2024

Bygrave LA, ‘Article 22 Automated Individual Decision-Making, Including Profiling’ in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press February 2020) <https://doi.org/10.1093/oso/9780198826491.003.0055> accessed 30 April 2024

Choi JH and Schwarcz D, ‘AI Assistance in Legal Analysis: An Empirical Study’ (13 August 2023) <https://papers.ssrn.com/abstract=4539836> accessed 5 May 2024

De Graaf T and Veldt G, ‘The AI Act and Its Impact on Product Safety, Contracts and Liability’ (March 2022) 30 European Review of Private Law 803

Floridi L and others, ‘capAI - A Procedure for Conducting Conformity Assessment of AI Systems in Line with the EU Artificial Intelligence Act’ (23 March 2022) <https://papers.ssrn.com/abstract=4064091> accessed 12 April 2024

Forgó N, ‘Zur Regulierung Künstlicher Intelligenz, Auch in Der Strafverfolgung’ (7 February 2023) 106 Monatsschrift für Kriminologie und Strafrechtsreform 44

Gentile G, ‘AI in the Courtroom and Judicial Independence: An EU Perspective’ (22 August 2022) <https://papers.ssrn.com/abstract=4198145> accessed 12 April 2024

Goldsteen A and others, ‘Data Minimization for GDPR Compliance in Machine Learning Models’ (January 2022) 2 AI and Ethics 477

Huq AZ, ‘A RIGHT TO A HUMAN DECISION’ (2020) 106 Virginia Law Review

Khalifa M and Sabry M, ‘The Challenges of The Artificial Intelligence of Law in The Context of Technological Development’ [2024] 2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS), Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS), 2024 ASU International Conference in 1

Kouroupis Konstantinos, ‘The AI Act in Light of the EU Digital Agenda: A Critical Approach’ (5 (3) 2022)

Lazcoz G and De Hert P, ‘Humans in the GDPR and AIA Governance of Automated and Algorithmic Systems. Essential Pre-Requisites against Abdicating Responsibilities’ (24 January 2022) <https://papers.ssrn.com/abstract=4016502> accessed 30 April 2024

Matulionyte R and Hanif A, ‘A Call for More Explainable AI in Law Enforcement’ [2021] 2021 IEEE 25th International Enterprise Distributed Object Computing Workshop (EDOCW), Enterprise Distributed Object

Computing Workshop (EDOCW), 2021 IEEE 25th International, EDOCW 75

Michaels AC, ‘Artificial Intelligence, Legal Change, and Separation of Powers’ (March 2020) 88 University of Cincinnati Law Review

Ovadya A, ‘Reimagining Democracy for AI’ (February 2023) 34 Journal of Democracy 162

Pehlivan CN, ‘The EU Artificial Intelligence (AI) Act: An Introduction [Pre-Publication]’ (June 2024) 5 Global Privacy Law Review 1

Rack F, ‘Rechtsfragen zur generativen KI’ (7 January 2024) 44 ABI Technik 39

Ramos S and Ellul J, ‘Blockchain for Artificial Intelligence (AI): Enhancing Compliance with the EU AI Act through Distributed Ledger Technology. A Cybersecurity Perspective’ (February 2024) 5 International Cybersecurity Law Review 1

Schwemer SF, Tomada L and Pasini T, ‘Legal AI Systems in the EU’s Proposed Artificial Intelligence Act’ (21 June 2021) <https://papers.ssrn.com/abstract=3871099> accessed 12 April 2024

Srouji Joseph, ‘Artificial Intelligence and Automated Decision Making: The New Frontier of Privacy Challenges and Opportunities’ (December 2016)

Thelisson E and Verma H, ‘Conformity Assessment under the EU AI Act General Approach’ (January 2024) 4 AI and Ethics 113

Articles (Block posts):

Analysing the Impact of the EU AI Act Vote on Businesses' <https://www.twobirds.com/en/insights/2024/global/analysing-the-impact-of-the-eu-ai-act-vote-on-businesses> accessed 24 April 2024

'Harvard And BCG Unveil The Double-Edged Sword Of AI In The Workplace' <https://www.forbes.com/sites/danpontefract/2023/09/29/harvard-and-bcg-unveil-the-double-edged-sword-of-ai-in-the-workplace/?sh=13a22ef83f9f> accessed 5 May 2024

Helberger N and Diakopoulos N, 'ChatGPT and the AI Act' (16 February 2023) 12 Internet Policy Review <https://policyreview.info/essay/chatgpt-and-ai-act> accessed 5 May 2024

Kettas JC Muhammed Demircan, Kalyna, 'Europe: The EU AI Act's Relationship with Data Protection Law: Key Takeaways' (*Privacy Matters*, 25 April 2024) <https://privacymatters.dlapiper.com/2024/04/europe-the-eu-ai-acts-relationship-with-data-protection-law-key-takeaways/> accessed 5 May 2024

Saltz J, 'What Is the AI Life Cycle?' (*Data Science Process Alliance*, 1 June 2023) <https://www.datascience-pm.com/ai-lifecycle/> accessed 10 May 2024

'The EU AI Act: Concerns and Criticism' (*Clifford Chance*) <https://www.cliffordchance.com/content/cliffordchance/insights/resources/blogs/talking-tech/en/articles/2023/04/the-eu-ai-act--concerns-and-criticism.html> accessed 5 May 2024

Table of Cases

CJEU Opinion 1/15, Opinion of 26 July 2017 (Grand Chamber) (ECLI:EU:C:2017:592)

Cour de Cassation, Chambre criminelle, audience publique du 24 septembre 1998, No. de pourvoi 97-81.748, Publié au bulletin

Bundesgerichtshof(BGH), Urteil vom 28.1.2014, VI ZR 156/13