Bachelor Thesis

The Artificial Intelligence Act - The Impact of AI on Human Rights Standards in European Law Enforcement

Student: Katja Wiek

University of Twente, Enschede, NL

Management, Society and Technology

Thesis Supervisor: Dr. C. Matera

Second Supervisor: Dr. C. Fischer

Submission Date: 28.06.2023

Wordcount: 11998

List of Abbreviations

AI   Artificial Intelligence

AIA   Artificial Intelligence Act

CEPEJ   Council of Europe European Commission for the efficiency of justice

CFR   Charter of Fundamental Rights of the European Union

ECHR   European Court of Human Rights

Eurojust   European Union Agency for Criminal Justice Cooperation

GDPR   General Data Protection Regulation

NLP   Natural Language Processing

PRC   Permanent Representative Committee

Abstract

This thesis will address the topic of the AIA which is a proposed regulation of high-risk AI and aims at creating a unified AI strategy for the EU. Therefore, current practices using AI technologies, for example in the field of law enforcement and criminal justice, are at risk of disruptions. Hence, it needs to be determined how far-reaching the changes of the AIA are and their potential consequences are. This thesis aims to answer, "To what extend is the Artificial Intelligence Act coherent with the use of AI of Eurojust and what does this imply for Human Rights related to the administration of justice?". To address this, the thesis outlines the Human Rights in question, the current regulatory framework for AI within Eurojust, the proposed regulation through the AIA as well as how the changes will impact current practices and the impact on Human Rights. It will show that the regulation introduced is mostly geared towards empowering humans vis-à-vis technology which is in line with the democratic ideals of the EU. The analysis will also reveal that the exemptions included in the Act will have impact on various Human Rights which are at stake in the area of law enforcement.

Table of Contents

4

5

1. Introduction

1.1 Introduction

With a rising importance and wider use of AI in all areas of life governments need to adjust their strategies to regulate its use and safeguard citizens' interests and rights. These changes further need to be addressed at a supranational level, especially within institutions such as the EU a common position or general approach needs to be established to avoid conflicts when dealing with cross boarder issues or when coordinating organizations operating at an EU level. The current AI strategy of the EU includes a proposal of the Artificial Intelligence Act (AIA) which attempts to ensure "that artificial intelligence (AI) systems placed on the EU market and used in the Union are safe and respect existing law on fundamental rights and Union values" (European Council, 2022).

However, the current version of the AIA includes multiple exemptions to the rules it sets forth regarding issues such as national security which not only raises concerns within the branches of the EU such as the parliament but also within the general population (Skorik, 2022). Such exemptions need to be scrutinized with regards to any potential infringements on any fundamental Human Rights, or their proportionality within that specific context, as their protection is amongst the main prerogatives of the EU. Especially, in the field of law enforcement and criminal justices where organizations such as European Union Agency for Criminal Justice Cooperation (Eurojust) operate to combat cross boarder crime through various AI technologies such exemptions can critically impact a human's rights and their dignity. In the field of criminal justice, organizations employ both natural language processing technologies and AI for forensic analysis and anonymization (eu-LISA & Eurojust, 2022). These include technologies which under normal circumstances would be considered as prohibited under the AIA such as the "use of 'real-time' remote biometric identification systems in publicly accessible spaces" (European Council, 2022). Therefore, the exemptions ought to be examined to evaluate the potential impact the AIA has on the use of AI and the resulting implications for fundamental rights in the case an exemption is applicable.

Eurojust, as an institution of the EU, is mandated to coordinate the cooperation between national authorities in the process of investigation and persecuting a range of severe cross-border crimes. In fulfilling their mandate, they should act in an impartial and independent manner without meddling with the national legal systems of member states. Furthermore, Eurojust has the authority to communicate with national authorities, obtain information from them, expedite the implementation of international arrest orders, and manage collaborative investigation teams. Based on this, it needs to be questioned how national understandings of issues such as national security can impact the current framework of Eurojust and how these fit into the issue of the exemptions made by the AIA.

With the increasing interest in and use of AI not only legislative efforts were made to react to those changes, but there is also an increase in academic literature covering a wide range of issues regarding AI. Most research is geared towards understanding the impact AI has respectively on Human Rights Standards and the work in the field of law enforcement. This includes discussions by O'Flaherty (2020) and Dushi (2020) about the impact of facial recognition technology on fundamental rights and law enforcement or discussions about trustworthy and explainable AI in law enforcement by Sanz-Urquijo et al (2022) and Matulionyte and Hanif (2021).

Further, research critically assesses the AIA in terms of its impact, outlining risks and benefits and attempting to understand unclear issues that might be issues in the future when the AIA is implemented. Some authors such as Sunde (2022) analyze the general impact the AIA has on the field of law enforcement. While other research such as the one conducted by Veale and Zuiderveen Borgesius (2021) focus on making a general assessment of the AIA in terms of risks and benefits of the proposed regulation.

Another aspect represented in current research is the use of rights-based approaches to, for example assess current development. They offer a good basis for assessing AI within society since they offer an ethical and moral dimension to an analytical framework which is based on norms backed by international law (Nyamu-Musembi & Cornwall, 2004). There are four ways in which Human Rights

can be used in rights-based approaches: as normative principles, as instruments to assess, as components to programming, as justification for interventions which aim to strengthen institutions (Nyamu-Musembi & Cornwall, 2004). For a study such as this, Human Rights are used as a normative framework used to assess the appropriateness and proportionality of the proposed regulation.

While current research considers many relevant issues there are no assessments of the AIA that critically engage with its implication for Human Rights within the context of specific applications. This is especially critical and of importance for the general population when it is applied in situations where the people targeted by the AI are in a vulnerable position and their human dignity is at risk. This can be the case in criminal justice and law enforcement. Here the employment of surveillance devices can critically impact one's privacy and in instances even target innocent people, even in the case of a person being convicted of committing the crime it has to be questioned whether employment of such intrusive technologies are proportionally acceptable and justifiable in relation to the crime.

1.2 Research Question

On the basis of the above outlined gap in knowledge that is found on the potential impact that the enactment of the AIA can have in particular in the field of law enforcement, this thesis will aim at answering the following research question: *To what extend is the Artificial Intelligence Act coherent with the use of AI of Eurojust and what does this imply for Human Rights related to the administration of justice?*

In an effort to further structure the analysis several sub-questions will be addressed: (1) What are human right standards applicable in the field of law enforcement?; (2) What are the current regulatory framework and use of AI by Eurojust?; (3) How does the AIA plan to regulate the use of AI in the law enforcement and administration of justice sector?; (4) To what extent can the AIA uphold or disrupt the existing practice of AI use in law enforcement by Eurojust? Through these questions this thesis aims at creating an interpretative understanding of the changes that will occur due to the implementation of the AIA in Eurojust within the wider field of criminal justice in the EU and further what implications these changes have with regards to the proportionality of the regulations vis-a-vis the EU obligation to protect Human Rights. The relevance, purpose and the main ideas connected to the here identified sub-questions will be further explored in the following methodology section of this thesis.

2. Theory

2.1 Introduction

The following section will discuss the relevant theories which will be employed to inform the research design, namely AI Ethics as well as governance and politics of AI, and the foundational issue of law enforcement at stake of this thesis. Each issue will be presented in a separate sub-chapter and will form the basis for the coding scheme being developed in the following chapter.

2.2 Law Enforcement

Law enforcement can generally be seen as all activities that are undertaken by authorities to enforce the law. This includes the identification, investigation, countering and persecution of criminal offences and the apprehension of criminals as well as the prevention of criminal conduct to maintain public order and safety. While Eurojust offers support to national authorities in form of cooperative and coordinative efforts, it is not a law enforcement agency in the typical sense of its definition since they lack operational powers. This prevents Eurojust to make arrests or conduct and initiate investigations independently from national agencies. However, it plays a crucial role in the European law enforcement landscape by facilitating national efforts and providing necessary guidance for issues such as mutual legal assistance and extraditions.

2.3 AI Ethics

AI ethics is a critical theory assessing the way AI should be used within the bounds of our society to protect human interest in the wake of a rising technological interest. Researcher in this field express a "fundamental concern for human emancipation and empowerment" (Waelen, 2022). This concern is central, however, it is not often made explicit. A connection is drawn to the way society treats technology where often skepticism towards the technology is expressed. While not all are sceptic, some even optimistic about prospects, the skepticism becomes more apparent when regarding the human AI relationship within a power dynamic. According, to researchers of AI ethics this can be seen in AI regulations (Waelen, 2022). They identified two not mutually exclusive categories, the first calls for empowerment from the machine, this includes regulation on transparency, privacy, freedom, and autonomy. The second one aims at protecting humans from "the power that could be exercised by means of AI" (Waelen, 2022), this includes regulation on trust, justice, responsibility and non-maleficent.

Regarding these categories, it can be questioned to what extent the AIA falls within these bounds. Analyzing the AIA with regards to which category it falls into and which aspects it predominantly focusses on creates a basis on which it can be compared to other regulations such as the current framework used by Eurojust to regulate the use on AI. Currently the ethical standard of AI systems can be measured using the European Ethical Charter on the use of artificial intelligence in the judicial system and their environment (CEPEJ, 2018). The Charter includes the following principles: respect for fundamental rights, non-discrimination, equality, transparency, impartiality, and fairness as well as Principle "under user control". Any changes in focus between the current framework and the AIA hint at changes that will occur due to the implementation of the AIA, thus, these areas are of interest when questioning whether it will uphold or disrupt the existing practice of AI use in law enforcement by Eurojust. In case that the representation of either of the two categories receive increasing or decreasing attention in the AIA compared to the preceding framework, those changes need to be analyzed to understand why they were made and what the larger implications are. For example, an increase in regulations aimed at protecting humans can show a general skepticism towards technology which necessitate additional measures to protect human interest and increase trust in the technological processes.

The paper by Fjeld et al. (2020) builds upon the theory of AI Ethics and with integrating rights-based approaches outline 47 actionable principles for AI systems. These principles are categorized by: privacy, accountability, safety and security, transparency and explainability, fairness and non-discrimination, human control of technology, professional responsibility, promotion of human values. These categories overlap in some parts with the concerns discussed in AI ethics while introducing different principles such as the promotion of human values which includes subcategories that state that AI ought to be used to benefit society and that "social norms, core cultural beliefs, and humanity's best interests" (Fjeld, et al., 2020) should prevail. The categories described in this paper offer a good framework for the coding scheme for the later analysis as it includes a broader set of key words compared to the theory of AI ethics. Yet, it is still similar enough to allow the key words used to be sorted into the border two categories set forth by the theory on AI ethics.

2.4 AI & Governance, Politics and Society

The differing viewpoints regarding technology, as alluded to in the theory on AI ethics, have informed various theories with respect to the relationship between technology and governance, politics and society. These different theories outline how technology is used, what values it is meant to enforce and the impact it has on society and while they have differing frames of focus, they are not mutually exclusive.

Theories surrounding governance and AI discuss how involved the government ought to be in the development process. The more leaning towards techno-optimism the less involvement is requested, techno-skepticism on the other hand, wands to heavily regulate the process as a safeguard against technology. Others such as techno-liberalism, techno- nationalism want to prioritize other issues such as the protection of freedom and autonomy or the use of technology for national interests (Dafoe, 2018). These stances towards technology outlined in both the governance of AI as well as in society and technology, especially the optimist vis-à-vis the pessimistic stance can be explanations for changes the AIA aims to enforce compared to the current framework. A suspension of regulation in an area could therefore indicate a high trust in technological advancements whereas increased regulations show an increased level of concern and a general pessimism regarding technological progress and the trust one can have in technological solutions.

Within the field of politics of AI theories outline that technologies might be used by the government to enforce the values attached to their ideology. This can range from techno-democracy to techno-authoritarianism both forms would aim at employing technology to further their values. However, the range is not limited to these two types of government, it can also include other types such as populism, liberalism, and socialism (Dafoe, 2018). Since the theories of politics of AI outline how technology can be used to enforce political values, these theories offer a general framework for the analysis to detect the underlying values concealed within the documentation of the AIA.

These theories offer as framework to uncover underlying intents and themes behind the AIA and the ongoing debate that surrounds it as well as the intent behind using AI in the field of law enforcement. It can show what values the AIA or Eurojust try to enforce through the means of technology whether these may be democratic aiming to reduce issues such as discrimination through technology to a minimum or whether they ignore those risks associated with the uses of these technologies. What needs to be questioned is what role Human Rights play in these theories and what the underlying intend means for the protection and enforcement of Human Rights within European law enforcement and criminal justice. Further, these theories can be used to assess the stance of different stakeholders such as the EU and Eurojust not only with regards to AI but also regarding their visions of prospects for society with a higher level of AI usage. Here it needs to be questioned whether they take an optimistic stance seeing AI as a solution, a skeptic stance by seeing AI as an issue form with society needs to be protected or whether it aims at protecting national interests by limiting Eurojust power and involvement either through AI or by limiting their scope of involvement potentially replacing their cooperative effort with technology.

2.5 Concluding Remarks

By combining the theory of AI Ethics and the theories revolving around AI and politic and governance one can reach conclusions on which underlying assumptions and beliefs about AI can impact the way policy document are produced. However, it is also possible to identify potential contradictions in the way policy documents are presented through the originally stated aims and goals vis-à-vis the underlying intents in the content of the document in question. These issues will be further elaborated on in the analysis.

3. Methodology

3.1 Introduction

The following sections of the thesis will outline the sub-questions as previously introduced and will further elaborate on their purpose regarding their contribution to the overarching analysis as well as through which means these questions will be addressed. Further, this chapter will highlight the relevant document, present the research design and the coding scheme which was developed for the analysis.

3.2 Research Design

This thesis paper aims at answering the primary research question: *To what extend is the Artificial Intelligence Act coherent with the use of AI of Eurojust and what does this imply for Human Rights related to the administration of justice?* To answer this as well as all four sub-questions this paper will adopt a qualitative research method in the form of a textual analysis. Textual analysis comprises multiple methods of analysis, such as content or discourse analysis, all of which have an interpretative focus aiming at understanding rather that explaining phenomena by closely examining "either the content or meaning of texts or their structure and discourse" (Given, 2008).

The four sub-questions will be answered by describing, evaluating and interpreting current standards and future prospect given that the AIA will be enacted. The first sub-question, *"What are human right standards applicable in the field of law enforcement?"*, has a descriptive focus and will contribute to set up the understanding of which human right are relevant within the context of Eurojust and therefore will be the primary focus of the analysis. To establish these Human Rights the analysis draws upon the CFR and determine which rights listed are of interest for law enforcement and state how this applicability can be understood. Similar to the first sub-question the second one, *"What are the current regulatory framework and use of AI by Eurojust?"*, has a descriptive nature. It aims at showcasing the current status quo of AI regulation prior to the potential enactment of the AIA by analyzing the charter of the CEPEJ and establishing which category of AI Ethics it represents and what can be deduced about the underlying assumptions about technology. Building upon the first two, the third question, *"How does the AIA plan to regulate the use of AI in the law enforcement and administration of justice sector?"*, will evaluate how the AIA will impact the current legal framework regarding the employment of AI within Eurojust by analyzing the AIA and similarly to the second question investigate its tendency with regards to the established categories of AI Ethics and underlying meanings and intents compared to the goals and aims. Lastly, the fourth sub-question, "*To what extent can the AIA uphold or disrupt the existing practice of AI use in law enforcement by Eurojust?"*, is both interpretative and evaluative in nature. It follows the analysis of the third question and evaluates how these changes would mean for the practice of Eurojust and ultimately what the impact would be on the Human Right as established in the first sub-question.

3.3 Data Collection

This analysis will be conducted by consulting relevant policy documents collected through the data bases of the EU related to the process of proposing the AIA as a policy, department publication of the EU and Eurojust as well as scientific publication regarding AI, Human Rights, and criminal justice assessments. The research and analysis will be based on documents and papers collected and published prior to the 14th of June. These documents will be analyzed to uncover themes within the policy documents to understand the implications of AIA for Human Rights in law enforcement.

3.4 Data Analysis

Since the documents will be analyzed using interpretive research the coding scheme used will be grounded in theory to guide and frame the analysis. The coding scheme will be based upon theories and frameworks which were introduce in the theory section of the paper. Where necessary the coding scheme will be adjusted to ensure the findings accurately reflect the themes found in the empirical data and are not solely based on the assumptions made on the frame theories. One dimension of the coding scheme will be informed by the Human Rights in law enforcement as well as the framework of principled AI and AI ethics theories. These theories will be used by applying the coding scheme to the AIA and the documents describing the previous regulation of AI within Eurojust. By using the principles outlined by Fjeld et al (2020), such as the broad categories which includes 'privacy', 'accountability', 'safety and security', 'transparency and explainability', 'fairness and non-discrimination', 'human control of technology', 'professional responsibility' and 'promotion of human values', within the coding scheme it allows to sort regulations contained in the AIA and the previous AI framework into the categories outlined by the theory on AI ethics. Within law enforcement concepts such as the broad categories of privacy as well as safety and security are connected to the issue of data protection both of the data collected during the investigation as well as the personal data the person contributes during the investigation. Further, the principles of fairness and non-discrimination predominantly refer to the issue of biased algorithms while accountability as well as transparency and explainablity mainly refer to the issue of responsibility when working with AI and the potential lack of trust one can have in its results. Lastly, the categories of human control and protection of human values connect to the issue of responsibility and aim to protect human values from potential biases or mistakes through the algorithm.

Basing the analysis on the theory of AI Ethics creates a framework in which to compare the documents by assessing whether they have a focus on empowerment or protection or whether they leave out or include certain aspects regarding AI principles. The second dimension of the coding scheme will be focused on the theories of AI in relation to politics and governance. Here the codes be used to identify underlying values with regards to how AI is viewed and what values it will be used for. By coding the relevant literature for the stance on technology as it relates to humans and society through indications of optimism or skepticism it shows the intent behind the proposed legislation and whether it for example stems from an inherent fear of technology or a hope in technology as a solution. When coding for the values that are revealed, for example democratic, liberalist and socialist, it can reveal the latent values that are attempted to be enhance and what the focus of the AIA is.

Table 1: Coding Scheme

Theory	Theme	Codes
Law Enforcement		effectiveness, justice, security, fairness, victims, organised crime, cross border crime, terrorisms, national security, cyber crime, investigation, evidence, suspect, perpetrator, criminal justice system, surveillance, search, witness, evidence
Eurojust		coordination, cooperation, cross border crime, information exchange, joint investigation
Human Rights	Dignity	Human dignity (Art. 1), Right to life (Art. 2), Right to integrity of the person (Art. 3), Prohibition of torture and inhumane or degrading treatment or punishment (Art. 4)
	Freedoms	Right to liberty and security (Art. 6), Respect for private and family life (Art. 7), Protection of personal data (Art. 8), Freedom of thought, conscience and religion (Art. 10), Freedom of expression and information (Art.11), Freedom of assembly and association (Art. 12), Freedom of the art and science (Art. 13)

	Non-Discrimination and Equality	Equality before the law (Art. 20), Non-discrimination (Art. 21)
	Justice	Right to an effective remedy and to a fair trial (Art. 47), Presumption of innocence and right of defense (Art. 48), Principle of legality and proportionality of criminal offences and penalties (Art. 49), Right not to be tried or punished twice in criminal proceedings for the same criminal offence (Art. 50)
AI Ethics	empowerment from the machine	Transparency, explainability, privacy, freedom, autonomy, human control
	protecting humans	trust, (professional) responsibility, accountability, non-maleficent, human values, safety, security, fairness, non-discrimination
Governance of AI	techno-optimism	innovation, progress, digital transformation, smart solution, advancements
	techno-scepticism	privacy concerns, job displacement, pessimism, digital divide, algorithmic bias, risks
	techno-liberalism	free market innovation, digital democracy, open access, decentralisation
	techno-nationalism	digital sovereignty, protectionism, digital borders, national interests
Politics of AI	techno-democracy	digital governance, e-democracy, participation, open government, transparency
	techno-authoritarianism	digital surveillance, censorship, digital repression, oppression
	techno-populism	anti-elitism, national identity
	techno-liberalism	free market innovation, digital democracy, open access, decentralisation
	techno-socialism	digital cooperation, open source, collaborative, digital sharing, open knowledge

This analysis will be supported by using the software program Atlas.ti which is frequently used for coding in textual analyses. It features facilitate the analysis process by managing, structuring and the previewing in different visualizations of the data and the coding scheme that was applied (Friese, 2019). In this instance, all relevant documents such as the charter of the CEPEJ and the AIA and the have been imported into Atlas.Ti and through coding for the principles represented as well as the underlying intend with respect to the view on and use of AI within the context of governance, politics and society, Atlas.ti facilitates revealing the underlying narrative both within the former framework of Eurojust as well as in the current proposal of the AIA.

3.5 Concluding Remarks

The content analysis will be employed to juxtapose the aims and goals set by the European Union against the rules and regulations set forth in the AIA and the current framework employed by Eurojust to regulate the use of AI in the context of judicial systems. Moreover, it will be used to show the impact the changes the AIA entails will have as compared to the previous framework in place.

4. Analysis

4.1 Introduction

This chapter aims to address the previously outlined sub-questions respectively. First, this chapter will address the Human Rights at stake and then demonstrate how the European Ethical Charter by the CEPEJ regulates the use of AI and analyses how this is or is not consistent with the set-out goals and the way the document was presented. Further, the same will be done for the AIA which will then be compared the current regulatory framework. The last sub-chapter will address how the changes the AIA encompasses will impact the practices of Eurojust with respect to the obligation to protect the Human Rights at stake in law enforcement.

4.2 Human Right Standards in Law Enforcement

4.2.1 CFR

Human dignity is recognized as a guiding principle international Human Rights documents, including the Universal Declaration of Human Rights and the Charter of Fundamental Rights of the European Union (CFR) as well as in numerous national and regional Human Right frameworks. Therefore, human dignity is also foundational for all Human Rights applicable in law enforcement which implies that the dignity of all people involved, for example victims, suspects, perpetrators, and members of the public, must be "respected and protected" (European Union, 2012). This can include that law enforcement officials are obligated treat all individuals with respect and without discrimination, and they must uphold their basic rights and freedoms in all circumstances. They are obligated to refrain from using force when not strictly necessary, they ought to protect the privacy of individuals when interacting with law enforcement and any person of authority must be held accountable for any form of misconduct jeopardizing the principle of due process and the dignity of the person dealt with.

Further the CFR outlines in Article 2 the rights to life and in Article 3 the right to the integrity of the person, including physical and mental integrity, as well as in Article 4 the prohibition of torture and inhumane or degrading treatment. These rights are treated as an extension of the aspect of dignity and thus are foundational for all activities of law enforcement. The right to life entails not only that "no one shall be condemned to the death penalty, or executed" (European Union, 2012), it can also be understood to refer to the use of force where law enforcement officials only ought to use force when necessary and in proportion to the threat. Article 4 can be applicable in all aspects of law enforcement but can be seen to refer to the treatment of individuals during interrogations and during detainments. Chapter II of the CFR outlines all fundamental freedoms which are relevant for the area of law enforcement since no person ought to be persecuted for actions falling reasonably within their freedoms. This category of freedoms can include the right to marry and right to found a family, freedom of thought, conscience and religion, freedom of expression and information, freedom of assembly and association as well as freedom of arts and sciences (European Union, 2012). However, other freedoms are more directly related to law enforcement and are relevant for their practices. This includes the right to liberty and security as well as respect for private and family life, encompassing not only their life but also their home and communications. In the context of law enforcement this implies that law enforcement officials are not permitted to commit arbitrary or unlawful searches of individuals and their property. The right to have ones data protected entails that the data "must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law" (European Union, 2012). Further, it states that the person concerned has the right to access the data which has been collected and the have it corrected.

Moreover, Chapter III outlines that everyone ought to be equal before the law and that no one should be discriminated on grounds such as "sex, race, color, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth,

disability, age or sexual orientation" (European Union, 2012).

Lastly, the CFR outlines specific rights with regards to the area of justice in Chapter VI constituting the principle of due process which includes Article 47 the right to an effective remedy and to a fair trial, article 48 the presumption of innocence and right to defense, article 49 principles of legality and proportionality of criminal offences as well as article 50 the right not to be tried or punishes twice in criminal proceedings for the same criminal offence. These fundamental rights directly apply to the functioning in law enforcement and the criminal justice system and are therefore to be expected to be the foundations upon which the functioning of institutions such as Eurojust are created. This also applies when considering the use of AI as it should not interfere but rather strengthen the adherence to these principles.

4.2.2   Concluding Remarks

This section established five categories of Human Rights which are applicable to the area of law enforcement to varying degrees. The relevant rights can be grouped as rights referring to human dignity, freedoms, non-discrimination and equality and justice related rights. It confirmed and extended upon the already established coding scheme based on the Human Rights relevant for the use of AI gathered through study by Fjeld et al. (2020). Based on the findings, it can be expected that most relevant document of this field will predominantly focus on these categories. Especially the category of justice which includes issues constituting the due process of the justice system such as a fair trial and the presumption of innocence as these are closest related to the issue of using AI in law enforcement. However, other issues such as of privacy and protection of personal data included in the category of freedoms are also closely related.

4.3 Eurojust's AI Framework

4.3.1   Eurojust

In accordance with Article 2 of the Regulation (EU) 2018/1727 of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), they are tasked with supporting and strengthening national cooperation and coordination relating to investigating and prosecuting serious crimes. They are acting when these affect two or more member states, or it "requires prosecution in common bases" (European Parliament, 2018). The investigations of Eurojust are based on operations conducted and the information they are supplied by member state authorities.

The competences of Eurojust fall within the bounds of serious criminal offences which are listed in the Annex of the Eurojust's regulation (European Parliament, 2018). This includes crimes such as terrorism, organized crime, drug trafficking, money-laundering, immigrant smuggling, murder and grievous bodily injury and computer crime. However, this list excludes crimes which fall within the group for which the EPPO exercises its competence. This excludes investigations that include Member states not participating in enhanced cooperation and that request participation or at the request of EPPO (European Parliament, 2018). Eurojust is expected to perform various operational functions including informing authorities of investigations and persecutions assisting in ensuring and improving coordination and cooperation, cooperating with other agencies, and providing support to Member states as well as institutions and bodies of the EU. When taking any of those actions Eurojust is expected to be acting through one or more Member States (European Parliament, 2018). This implies that Eurojust is limited in its independent actions which also applies in the case of employing AI under the regulation of the AIA. Therefore, Eurojust is bound to the national definition of what the countries they are cooperating with characterize as issues relevant for national security which can differ on a case-by-case basis or even be a conflict between two member states within the same case.

Eurojust is made up by its national members, the college, the executive board and the administrative director. National members and their respective deputies have the status of prosecutor, judge or representative within Eurojust with competences matching to those under their national law. They have the power to facilitate or support issuing or executing mutual legal assistance or recognition, contact

and exchange information and participate in joint investigations. Further, they have access to national crime records, investigation DNA and arrest registers and other registers of public authorities (European Parliament, 2018).

4.3.2   European Ethical Charter on the use of artificial intelligence in the judicial system and their environment

The charter established by the CEPEJ formulates five principles for employing AI on the basis on a study on the practices surrounding AI in the judicial system. In the first appendix, it discusses the state of use of AI algorithms, open data policies, operating characteristics, predictive and retrospective explanations of decisions, AI in the context of civil, commercial, and administrative justice as well as issues relevant in criminal justice. Further it assesses issues regarding protection of personal data, potential and limitations of predictive tools and the requirement of an in-depth public debate prior to the implementation of such tools. Lastly it discusses uses of AI within the European judicial systems. This includes uses that are encouraged, possible, can be considered or only considered with extreme reservations.

The introduction of the first appendix shows an even distribution between an optimistic and sceptic stance towards the technological transformation in the judicial sector. It depicts the transformation as great and the AI as spectacular and striking regarding the way it can be and is already used which, however, is currently predominantly in the private sector. The reality of the current uses, therefore, is viewed in a sceptic light, especially regarding the public sector alongside the still prevalent limitations of the technologies (CEPEJ, 2018).

The chapter on the state of the use shows that AI initiatives within the European judicial system are difficult to pinpoint because most "come from the private sector and are not often integrated into public policies" (CEPEJ, 2018). Contrary, parts of the chapter on open data policies alludes to a more positive stance as most member states have already established and implemented open data policies. Open data can be placed into the categories of techno-socialism or techno-liberalism both valuing open access and access to information. Lastly, it raises concerns for confidentiality, privacy and transparency, falling into the category of empowerment in AI Ethics. The pseudonymizing and anonymizing of personal data is an issue of the category of protection as responsibility needs to be established and thus far it appears to fall to the judicial personnel (CEPEJ, 2018).

The chapters on operating characteristics, prediction and explanation of judicial decisions add to the techno-skepticism stance as the further treatment of results through AI can result in "trade-off biases required to select one data over another" (CEPEJ, 2018). Regarding the prediction of decisions, while the study shows that AI could predict most cases within a particular court, this is not comparable with legal reasoning and they claim that no system could reasonably predict outcomes, especially of diverse European judges. In a similar vein, the document concludes that AI cannot retrospectively explain judicial decisions since more, not openly available input would be needed such as personal traits (CEPEJ, 2018).

The chapter on the use of AI in civil, commercial and administrative justice aims at recommending potential ethical uses AI in the system rather than criticizing specific practices. However, it does emphasis the importance of adhering to the fundamental rights and calls back to previous critiques stating that "AI can hide unacceptable design flaws and totally erroneous analysis results" (CEPEJ, 2018). This chapter highlights that AI could have "potentially desirable benefits" (CEPEJ, 2018) which showcases an optimistic stance on the theoretical application of AI.

The following chapter of the CEPEJ charter discusses uses of AI in criminal justice for prevention and danger assessment. It details concerns related to potential biases and discrimination through AI systems which is why it relates to the importance of the preservation of fundamental rights. This includes rights ranging from the category of justice such as the right to a fair trial to issues of non-discrimination to impacts on a person's private life and their integrity which could be seen as impacting their dignity, especially if the reliability of the AI system can be questioned.   Further, it is connected to the category of emancipation through the assessment of the importance of transparency, accountability and human oversight (CEPEJ, 2018).

The issue of data protection which is discusses throughout the entirety of the charter is addressed in chapter eight where recommendations are made for complying with data protection principles when employing AI, tying back to the protection of Human Right (CEPEJ, 2018).

The chapter on the potential and limitations of predictive justice tools states that they can improve the efficiency and accuracy of legal decision-making which can be deemed to be an optimistic assessment, however, there are limitations with regards to the complexity of legal situations. It relates back to previously discussed issues such as transparency, accountability and the issues of potential biases and discrimination (CEPEJ, 2018).

The last chapter highlights the importance of public debates and of developing AI frameworks protecting fundamental rights since employing AI will have potential impacts on society and on the justice system. The Human Rights discussed in this chapter regarding public debates are the right to privacy, a fair trial and to non-discrimination (CEPEJ, 2018).

Overall, the observations made and concerns that are being raised are not only consistent with the above-mentioned tendencies towards techno-liberalism and techno-socialism. The entirety of the discussion made in this document is in line with ideals of techno-democracy which becomes evident through the concern for issues which constitutes responsible AI, for example the concern for transparency. According to Rahman et al. (2022) establishing regulations geared towards responsible AI is indicative for democratic forms of government.

Whilst the document outlines instances of optimism, sceptic expressions outweigh these. The techno-skepticism which can be seen in this document is not an inherently pessimistic stance towards technology but is often regarding the capabilities of technology. Which would lead to belief that the policy makers would prefer regulations in place increasing the trust and establishing a clear responsibility as well as achieving a high level of transparency. This would mean that regulation of AI would be proportionally more geared towards protecting humans and their interests form AI rather than empowering human from the machine.

However, whilst relatively evenly distributed, on average the document leans more towards discussing issues falling into the category of empowering human vis-a-vis AI technology. When accounting for the fact that the category of protections holds more codes, it averages to 4.2 mentions per code while the category of empowerment averages out to 4.6. The most prominent issues within this document are transparency and privacy with 12 and 4 mentions of the category of empowerment and responsibility with 6, values and rights with 8 and security and protection with 15 of the category of protection. Further, not all codes encompassed by the category of protection are included in the discussions of the document. It leaves out the issues of trust and non-maleficence of technology. Based on this, compared to the techno-sceptic stance, it would be expected that the principles outlined in the main section would be geared to empowering humans rather than protecting them with the categories most often mentioned being integral parts of the principles as such.

The main section of the document, however, outlines five principles on the use of AI of which only two are aimed at protection and three are aimed at empowerment.

The first principle outlines the respect for fundamental rights which can be seen to fall into the first category of the theory of AI Ethics as it aim to protect human interest vis-a-vis the technological development. Further it is concerned with the Human Rights category of justice, specifically the right to a fair trial not influenced by prejudices or misdirected technology disregarding fundamental rights and freedoms. Secondly, the charter outlines the principle of non-discrimination which also falls within the bounds of the protection category. This principle is strongly related to the Human Rights category of equality and non-discrimination particularly Article 21 of the CFR. The principle of quality and security belong to the category of empowerment form the machine as it refers predominantly to the issues of privacy. Therefore, it seeks to protect Human Rights falling within the chapter on freedoms of the CFR, in particular Human Rights such as the protection of personal data in article 8. The fourth principle addresses the issues of transparency, impartiality and fairness and thus it fall within the category of empowerment. Particularly regarding the issue of impartiality which refers to an absence of bias and fairness this principle can be seen to protect Human Rights of the category of justice and are aimed at preserving the principle of due process. Lastly, the principle of "under user control"

matches to issues covered by the category of empowerment of AI Ethics. It calls for transparency of information and for the autonomy of the people participating (CEPEJ, 2018).

In addition to the five principles, the charter also outlines various uses of AI within the criminal justice system and categorizes them in accordance with the level of which they are encouraged to be used. The first category of uses to be encouraged included case-law enhancement, access to law and creation of new strategic tools. The second category of possible uses which require methodological precautions include "help in the drawing up of scales in certain civil disputes" (CEPEJ, 2018), "Support for alternative dispute settlement measures in civil matters" (CEPEJ, 2018), online dispute resolution and "the use of algorithms in criminal investigation to identify where criminal offences are being committed" (CEPEJ, 2018). Judge profiling and the anticipation of court decisions belong to the third category which outlines uses only to be considered after additional scientific studies. Lastly, the fourth category details uses only to be considered "with most extreme reservations" (CEPEJ, 2018). It includes quantity-based norm and the "use of algorithms in criminal matters in order to profile individuals" (CEPEJ, 2018).

4.3.3   Concluding Remarks

The section provided insights into the current functioning of Eurojust and principles applicable to their current use of AI systems. The current framework, while not harmonized and binding, grants insights into the perception and way AI was attempted to be regulated prior to the AIA. In the principles outlined in the previous section, the trend towards empowerment-oriented regulation is in line with the prediction made through the coding based upon political tendency which coincided with the observation made by Rahman et al. (2022). On the other hand, the sceptic stance has a limited impact on the amount of protectionist principles which would have been anticipated since the stance would warrant aiming at protecting human interest in the face of a technological transformation.

4.4 The AIA Regulating AI Use in Law Enforcement

4.4.1   The AIA

The AIA is set up to aim at creating a comprehensive and harmonized framework for the use and development of AI within the EU. It is establishes in this legal framework that it is supposed to ensure that any development of AI systems do not compromise existing laws on Human Rights, or the values set forth by the EU. However, it is not solely intended to safeguard human values and protect the interests of individuals, but it also recognizes the importance of innovations and ensuring equality of smaller contributors within the process of innovating AI. Thus, the regulation needs to be able to balance both aims without compromising either objective.

AI systems as defined by the AIA encompasses all systems that are developed through the means of machine learning as well as logic- and knowledge-based approaches. These systems then are differentiated between high-risk and general-purpose systems. The AIA is set up to create guidelines for the development and use of high-risk systems as well as establishing prohibited practices to create a safety and protection network of fundamental rights.

Similarly to the current AI charter of the CEPEJ, the AIA presents a higher average use of terminology or concepts falling into the category of empowerment of human vis-à-vis technology which averages at about 10.7 whereas the category of protection of human interests averages at 9.8. codes per concept included in the category. While the distribution is similar in terms of a higher importance of empowerment, the difference between these categories is more apparent in the AIA which would allude to a greater importance granted to empowerment of humans vis-a-vis the technological development. The concepts of both categories which are predominantly discussed in the document are either concerned with the protection of human values in form of the fundamental rights and ensuring high security standards or discuss the importance of transparency in relation to design of the algorithms and data used. This can be seen in the text of the draft regulation which demands high levels of transparency

from all parties involved in creating, producing, testing and allowing the AI system onto the market by means such as thorough technical documentation.

As seen in the distribution between the categories of AI Ethics the distribution between techno-skeptic and techno-optimistic concepts is the same as compared to the charter of the CEPEJ with a higher representation of sceptic notions towards technology. Therefore, similarly to the charter this would lead to the assumption that a more protection-oriented stance would be taken in regulating the use of AI which is supported by the number of references to the fundamental rights which outweighs the other issues raised in the categories of AI Ethics.

The AIA displays signs which are consistent with techno-democracy as well as techno-liberalism and techno-socialism which is in line with values usually displayed by the EU. These tendencies towards these particular sets of values can be seen through the discussion of issues such as transparency, free market innovation, open access and knowledge sharing. This is in line with observations made by Rahman et al. (2022) who concluded that democratic entities can uses principles of responsible AI which included transparency, human agency and oversight to strengthen their values. However, some aspects of the AIA are also partially consistent with values conveyed in techno-populism. The notion of anti-elitism can be seen in the way that the AIA aims to support smaller enterprises and by giving them advantages against large scale corporations aiming at diversifying input into the innovative pool for the further development of AI system.

4.4.2   Regulatory Changes for AI in Law Enforcement

The AIA compared to previous drafts of this regulation made modifications which allow for a level of flexibility regarding the use of high-risk AI systems within the context of law enforcement as well as to "reflect on the need to respect the confidentiality of sensitive operational data in relation to their activities" (PCR, 2022).
Of the AI systems that are categorized as high-risk the practice of biometric identification when conducted in "real-time" is prohibited in most instances as outlined in Article 5. Even within the area of law enforcement the practice is seen as "particularly intrusive" (PCR, 2022) in a way that it might impact the private life of the population due to the fact of feeing surveilled which can discourage their exercise of their rights such as the right of assembly. Therefore, the practice is prohibited with the exception of instances where the use is deemed to be critically necessary for the pubic safety where the importance of investigation is seen as overriding the risks (PCR, 2022).
When employing the AI system there are limits to the use with regards to the time and space and the data collected of an individual ought to be proportionately appropriate to the severity of the situation. This would be the case if the risk and consequences of the committed or the potential crime outweigh the risks associated with the use of AI systems ant the potential impact they can have on the individual in question. Further, to conduct the identification of an individual and the access to their personal data by using AI the agency requires authorization which should be obtained prior to employing the system. The rule can only be disregarded in case of emergencies, however, the authorization should be obtained as timely as possible while providing reasoning of why the authorization was not obtained prior. In case the authorization is not granted prior the use is restricted and is subjected to the appropriate safeguards and conditions. Nevertheless, the practice is only possible in instances in which the Member State allows them and provides the possibility of authorization (PCR, 2022).

Law enforcement agencies are granted exemptions for numerous regulations set forth by the AIA. This includes the requirement to seek informed consent in the case that this procedure would prevent the proper testing of the AI system (Article 54) and they are not required to comply with the registration obligations of Article 51 (PCR, 2022). The derogation from the conformity assessment (Article 43, Article 47) is allowed for reasons including public security and the protection of life and health. AI systems are allowed to be tested outside of the provided regulatory sandboxes (Article 53, Article 54) under given conditions which include that the system is to be used in areas such as law enforcement and the test subjects have given their informed consent which can excluded as a condition when the

system is to be used for law enforcement and the fact that the subject is informed about the test would impact the testing procedure. However, this necessitates that the testing does not negatively impact the test subject. Further, high-risk system used in areas such as law enforcement or by judicial authorities require specifically designated market surveillance authorities who should not interfere or affect the independence and activities of the agencies. Moreover, law enforcement agencies get granted exceptions by this regulation to the information exchange between national authorities and the Commission based on potentially endangering public and national security (PCR, 2022).

The necessary technical documentation of high-risk AI systems when used by law enforcement authorities must remain with these agencies while ensuring that the responsible market surveillance authorities are capable of accessing the documentation. Accessing this information should only be allowed for members of these agencies with the necessary security clearance (Article 70) (PCR, 2022). However, law enforcement agencies such as Eurojust still must adhere to Article 72 where it is laid out that Union institutions, agencies and bodies can be subjected to administrative fines. These are determined by issues such as "the nature, gravity and duration of the infringement and of its consequences" (PCR, 2022).

In addition to other high-risk systems the AIA categorizes all applications intended for the use of law enforcement as high-risk since they are seen as having a "significant degree of power imbalance and may lead to surveillance, arrest or deprivation of a natural person's liberty as well as other adverse impacts on fundamental rights" (PCR, 2022). This dynamic is indicative of the power relation introduced by Waelen (2022). There it is stated that in a situation in which an individual is subjected to such a power relation this person ought to be protected. Therefore, based on this a high level of protective measures regarding the regulation of AI in law enforcement should be expected.

This is particularly evident in the case where such systems have not been trained by quality data or do not meet specific requirement regarding accuracy and robustness which is heavily regulated if they are classifies as high-risk. In case of not transparent or explainable systems rights such as the presumption of innocent or the right to a fair trial can be impacted (PCR, 2022). The exemptions to the set regulation are, therefore, only granted in circumstances in which national security is concerned.

The systems included in this list are: individual risk assessment, polygraphs, tools detecting emotional states, evaluation of evidence reliability, prediction of occurrence or reoccurrence of criminal offences, personal trait and characteristic and past criminal behaviors assessments, profiling and investigating or prosecution of criminal offences (PCR, 2022).

This list does not include systems intended to for administrative proceedings by tax and customs authorities or by financial intelligence units carrying out administrative tasks relating to anti-money laundering legislation due to the "purposes of prevention, detection, investigation and prosecution of criminal offences" (PCR, 2022).

Further in the area of administration of justice similar issues are raised which impact fundamental rights which are connected to the issues discussed in law enforcement such as the impact on the right to an effective remedy and to a fair trial. Therefore, additional systems are categorized as high-risk such as systems assisting judicial authorities. These systems could have direct impact on the functioning of law enforcement, for example, since agencies require authorization from judicial authorities for the usage of "real-time" biometric identification systems (PCR, 2022).

4.4.3   Concluding Remarks

This section of the analysis indicated how AI in law enforcement and criminal justice would be regulated under the AIA and what underlying intends and purposes with regards to AI might have impacted the way the regulation is constructed. Even though the AIA establishes all systems intended for the use of law enforcement as high-risk which should imply that these are subjected to the same level of necessitated transparency, technical scrutiny and operational obligations. However, the area of law enforcement with respect to issues such as national security is granted numerous exemptions or easement of regulation regarding the high-risk systems. Further, some aspects of use are left to the individual member states this includes what is constituted as a national security risk and the ultimate decision of whether some practices are allowed under national jurisdiction. In terms of the tendency of

the document, the AIA leans towards empowerment regulation and shows value indicators that are consistent with common European values such as a consistency with techno-democracy.


4.5 Impact on Existing Practices

4.5.1 Changes in Regulations

Both the AIA and the charter of the CEPEJ display a similar distribution of traits consistent with optimistic and sceptic stances regarding technology. In both cases a sceptic stance is more predominant which is not geared towards the possibilities of technology but rather towards their current capabilities and the risks attached to their general application. Nevertheless, both encourage the use and innovation of AI systems under the given regulations or guidelines in the respective documents.

In the same vein as their stance towards technology, both document showcase traits in line with similar political values which indicates according to the theories of politics of AI that the intended use of AI system will enforce those values. Therefore, no drastic changes of the value systems are to be expected particularly since most of the political orientations represented in the documents are in line with the values generally set forth in the EU. The charter and the AIA include notions of techno-socialism and techno-liberalism. In addition to that, the AIA discusses issues falling into the categories of techno-democracy and techno-populism regarding the general application of AI systems while the regulation of systems within the bounds of law enforcement and criminal justice appears to have a focus more geared towards a nationalistic regulation of practices and definition of issues which are the frameworks for the use of high-risk AI systems.

With regards to their respective principles and regulations both documents show that the priorities empowerment related issues over issues concerning protecting human interests vis-a-vis the technology being employed. On average the difference between the empowerment and protection is smaller in the current framework of the charter with a 0.4 difference between the averages compared to the AIA with a difference of 0.9 which, however, can be explained by the difference in the length of the respective frameworks and does not necessarily imply a change in stance of the people establishing the new regulation. Therefore, both regulatory frameworks exhibit some discrepancies regarding their techno-skeptic stance which would lead to the assumption that the regulation would aim at supporting and protecting fundamental rights and human values. This is supported by the number of instances in which rights and values are being discussed especially in the context of potential threats. On the other hand, the higher level of empowerment regulation is in line with the techno-democratic political tendency of both documents.

Figure 1

21
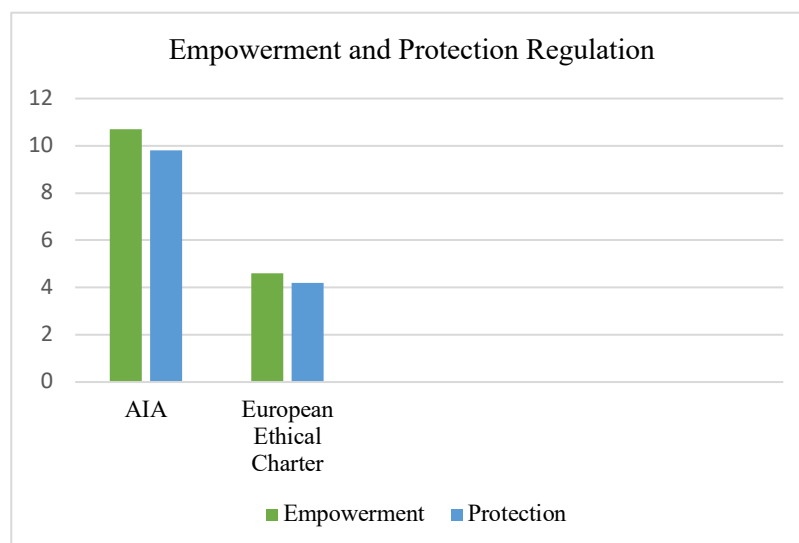
In both the AIA and the charter AI practices related to law enforcement and criminal justice are being outlined and categorized. The AIA focuses on a risk-based approach while the charter lists practices ranging from those, they encourage to uses which can be considered only with the most extreme reservations. The AI practices listed in the AI, specifically in Annex III, only include high-risk systems. Therefore, other practices related to law enforcement and criminal justice are either categorized as general-purpose systems or they have yet to be added to the list with later amendments.

Both documents include the profiling of natural persons and issues surrounding judicial decisions. The AIA categorizes all practices as high-risk related to judicial decisions that use AI to interpret facts and the law and then apply these to cases. In the charter quantity-based norm in relation to judicial decisions and the profiling of natural persons is included in the last and least encouraged category whereas the profiling of judges and the prediction of judicial outcomes can be considered after additional scientific studies into their reliability amongst other issues discussed prior in the document.

Compared to the charter the AIA includes regulations on technologies used for remote biometric identification, risk assessments for offending or reoffending as well as the risk of a person to become a victim, polygraphs and comparable systems, the assessment of evidence, the prediction of occurrence or reoccurrence of offences based on profiling of natural persons and for the assessment of traits, characteristics and past criminal behavior of people or groups.

The charter, on the other hand, included AI systems used to detect where offences are being committed, alternative ways of dispute resolution and settlement, access to the law, create new strategic tools, and for case-law enhancement. These issues are included in the categories of encouraged uses and possible uses which require precautions. Therefore, it is possible that these issues have been excluded for the AI because these practices do not fall into the parameters set up for high-risk systems.

4.5.2 Impact on law enforcement activities and practices of Eurojust

Based on the observations regarding the theory of AI Ethics, the assumption can be formed that the use of AI systems in law enforcement should be regulated in terms of their capabilities and should be attached to regulations which safeguard the user and the persons under investigation from potential risks or impacts on their fundamental right. Further it is to be expected that the use in law enforcement should only uphold democratic values and should adhere to values such as digital cooperation, open access and open knowledge with regards to the innovative processes and the transparency of the criminal justice systems as it is represented in the tendency towards techno-liberal and techno-socialist ideas. However, the area of law enforcement is still heavily regulated by the national level, in line with the European principle of subsidiarity, this also includes the regulation of which systems will be allowed to be used even if allowed under the AIA and the definition of what situation constitutes a threat to national security as there is no concrete, general definition on the EU level. However, based on European case law some factors have been identified which constitute the concept of national security. According to the European Court of Human Rights this includes "the protection of state security and constitutional democracy from espionage, terrorism, support for terrorism, separatism and incitement to breach military discipline" (ECHR, 2013). Lastly based on the tendency toward the category of empowerment it is to be expected that values such as transparency, privacy, autonomy and human control will be prioritized in the practices of law enforcement while still maintaining a level of protection as the discrepancy between both categories relatively minor. Nonetheless, the difference has increased from the current framework to the current version of the AIA indicating a higher value of empowerment that before which can be seen, for example in the amount of transparency standards that are being introduced.

The practice of Eurojust regarding their use of AI will be mostly impacted by the definition and the use of national security as a reason for exemptions for parts of the regulation. While Eurojust currently is already limited in their independent action, they now are required to adapt their work to the definition of what the different members constitute as a risk to national security. This does not only impact the ways in which they are allowed to use AI technologies during investigation but also impacts their tasks of facilitating cooperation and coordination between member states. Given a circumstance where two

member states are affected by cross border criminal activity and Eurojust is involved, they need to balance the investigation in accordance with the regulation of both member states or the country with the higher regulatory standards might refuse to cooperate in the investigation to protect national interests. In this scenario it is possible that either of the countries has additional restrictions in terms of the usage of for example real time biometric identification systems. Additionally, both countries could categories the same criminal offences differently according to their national definition of the term national security. Both issues would necessitate either a compromise, a situation in which cooperation is refused or ultimately would lead to a different treatment for the same criminal offence depending on the country of the perpetrator. A different treatment of people, who are for example part of the same criminal organization, during an investigation leads to advantages or disadvantages later on during the trail and can cause unnecessarily strong or comparatively weak punishments for the same offences. In the circumstance in which cooperation is refused the investigation is severely hindered by limiting the access to evidence which in turn can impact the later trial and charge of the offenders.

Since the issue of civil protection is a competence of the respective member state, the EU cannot prohibit them from refusing cooperation. However, since the issue of fundamental rights and justice is a shared competence, the EU could take steps towards a more harmonized systems with the aim of achieving improved conditions for upholding high Human Rights standards within law enforcement.

The use of AI and the way it is regulated through the AIA can have several implications of various fundamental rights applicable in law enforcement as discussed in chapter 4.1. A higher involvement of AI system in law enforcement can impact human dignity and changes the way of how humans are treated in a dignified way throughout the process of investigation. This incorporates but is not solely limited to the risks of technological based discrimination and bias, loss of human interactions, invasion of privacy and the potential of dehumanization. Using AI systems can lead to the phenomenon that the individuals dealt with can be reduced to data points and simple statistics. This can be seen in chapter 4.4 dealing with the practices the AIA categorizes as high-risk which includes systems used to assess likelihood of criminal offences or people becoming victims of crimes based on statistical analysis.

Another Human Right which can be impacted is the protection of personal data and privacy. While the AIA establishes different safeguards aimed at transparency of the systems and protection of data, there are instances in which personal data as well as the privacy of potentially innocent people are put at risk. An example of this is the exemption from seeking prior authorization in cases of emergencies. In case the situation has been misjudged and the authorization post employing the AI is not granted, the privacy of the individual has been breached and the data has been exposed to an unjustified risk even though the agency is necessitated to use appropriate safeguards. The concern for privacy and personal data protection is also raised by Dushi (2020) regarding the use of face recognition technology as these allow for a more detailed account of a person's life and habits that previously possible which leads to lacking anonymity and freedom.

The use of AI systems further risks the rights of equality and non-discrimination due to potential biased in the data. This particularly applies to technologies such as facial recognition or biometric identification. These types of technologies are proven to "not always have a high accuracy rate, especially on moving videos, and it tends to wrongly identify women and people of color" (Dushi, 2020).

Further equality is put at risk due to the national differences in cross border issues. While two individuals might be part of the same group and have committed comparable crimes, they can be tried differently if there are different standards applied during the respective investigations. Moreover, this impacts additional rights of the category of justice, for example the right to a fair and impartial trail which is jeopardized if there are different standards of evidence with regards to the use of AI systems.

4.5.3 Concluding Remarks

The last section of the analysis focused on the specific changes in the way the AIA regulates the use of AI systems within law enforcement and criminal justice. Using these changes as the baseline the chapter explored whether the introduction of the AIA would uphold or disrupt the current practices of Eurojust. While both documents are relatively similar in their tendencies, the AIA clearly distinguishes itself not

only due to it being a legally binding regulation but also on the basis of being more thorough and exhaustive in its set standards and the categorization of practices. The implementation not only holds implications for Eurojust in terms of their dependence on member states and their additional standards and definitions but also for the Human Right standards in law enforcement. While the degree of impact may vary, the regulations set up in the AIA have impacts on rights included in all four relevant categories.

5. Conclusion

This thesis aimed to answer the research question: To what extend is the Artificial Intelligence Act coherent with the use of AI of Eurojust and what does this imply for Human Rights related to the administration of justice?

To conclude, this thesis shows that the regulations of AI systems in law enforcement as established by the AIA are largely coherent with the current practices and frameworks of Eurojust. Nevertheless, the use of AI and the exemptions included in the AIA for the purpose of national security pose some threats to all Human Rights related to law enforcement and criminal justice to varying degrees. Therefore, a balance needs to be found in which national security concerns can be solved as efficiently as possible without impacting Human Rights of individuals disproportionately. This can be achieved by, for example, establishing more centralized parameters of national security which would counteract most risks of inequal treatment and by setting up guidelines for which level of threat would justify the use of high-risk AI systems.

In order to reach this conclusion, this paper respectively focused on identifying which Human Rights are applicable to law enforcement, the current framework for the use of AI by Eurojust, the regulation of AI in law enforcement and administration of justice through the AIA and on analyzing to what extent the AIA upholds or disrupts existing practice of Eurojust with regards to their use of AI.

The thesis showcased that the relevant Human Rights set forth by the EU in the CFR for law enforcement and criminal justice fall into the categories of human dignity, individual rights and freedoms, non-discrimination and equality and justice. Currently, the use of AI systems by law enforcement agencies such as Eurojust is not regulated through a harmonized legal framework. The analysis of the charter highlighted a tendency towards empowerment-oriented regulation and values in line with techno-liberalism, techno-socialism and techno-democratic ideals. Similarly, while introducing a harmonized framework, the AIA keep in line with the empowerment-oriented form of regulation and highlighted issues surrounding transparency, privacy and human control of AI systems. Despite the strict regulation of high-risk systems, the AIA set up exemptions relevant for the area of law enforcement given the issue of potential threats to national security. Further, some aspects of the regulation are set up to be ultimately determined by the individual member states such as the approval to employ real time biometric identification systems or what constitutes as a threat to national security, therefore, deciding in which concert circumstances the exemptions take effect. The AIA upholds existing structures and dynamic between Eurojust and the member states in the sense that the practices and actions taken by the agency are dependent on the member states approval. While the regulation on the use of AI systems would be harmonized to some extend the exemptions and the influence on of the national governments definition and categorizations. Some of the exemptions and parts of the regulation in general, further pose threats to fundamental rights which would be disruptive to the general aim and self-set purpose of the EU and its agencies to uphold and protect high standards of Human Rights.

The thesis provides insights into how the political tendency can be predictive for the way AI is regulated which is in line with observations made by Rahman et al. (2022). As both documents display democratic values through measures on issues which are central to democratic values such as transparency, it can be assumed that this orientation can be indicative for the tendency displayed in the regulative measures taken.

Predicting the tendency towards empowerment or protection-oriented regulation through the technological stance of the policy maker, however, is based on this analysis inconclusive since the distribution between optimistic and pessimistic stances was relatively equal. Nevertheless, in both document the pessimistic stance was slightly more prevalent and despite that the regulation was geared towards empowerment. Further, this thesis establishes with regards to power relations (Waelen, 2022) that these do not automatically lead to exclusively protective measure or even a regulatory framework that is heavily geared towards protective regulations. Nevertheless, the fact that in law enforcement there is a power relation with individuals subjected to it can be an explanation for the protective measures that are put in place even if they do not make up the majority.

Ultimately, this thesis showcased that there are risks associated with the use of AI in law enforcement and criminal justice this can have an impact on the European directive of upholding all fundamental rights. While the potential impact was highlighted further research is needed to determine how severe the impact would be for the respective rights.

However, this thesis is not a complete assessment of the AIA as it is limited by its focus on law enforcement and Human Rights. While Human Rights offer a basis on which to asses risks and harms of regulation there are still other factors which could have negative impacts "that are not identifiable or anticipated in terms of Human Rights" (Latonero, 2018). Therefore, to fully assess the potential impacts of implementing the AIA more research outside of the frame of Human Rights-based approach needs to be conducted.

Bibliography

Dafoe, A. (2018). AI Governance: A Research Agenda. Retrieved from: https://www.fhi.ox.ac.uk/wp-content/uploads/GovAI-Agenda.pdf.

Dushi, D. (2020). The use of facial recognition technology in EU law enforcement: Fundamental rights implications.

Eu-Lisa, Eurojust. (2022). Artificial Intelligence Supporting Cross-Border Cooperation in Criminal Justice: Joint report prepared by eu-Lisa and Eurojust. Retrieved from: https://www.eurojust.europa.eu/sites/default/files/assets/artificial-intelligence-cross-border-cooperation-criminal-justice-factsheet.pdf

European Commission for the Efficiency of Justice. (2018). European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment. Retrieved form: https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c

European Court of Human Rights. (2013). National Security and European Case-Law. Retrieved from: https://rm.coe.int/168067d214

European Council. (2022). Artificial Intelligence Act: Council calls for promoting safe AI that respects fundamental rights. Retrieved from: https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/

European Union. Aims and Values. Retrieved form: https://european-union.europa.eu/principles-countries-history/principles-and-values/aims-and-values_en.

European Union. Human Rights and Democracy. Retrieved from: https://european-union.europa.eu/priorities-and-actions/actions-topic/human-rights-and-democracy_en

European Union Agency for Criminal Justice Cooperation. Retrieved from: https://www.eurojust.europa.eu/about-us/who-we-are

Friese, S. (2019). Qualitative Data Analysis with ATLAS.ti. London, Sage.

Fjeld, J., Achten, N., Hilligoss, H., Nagy, A., & Srikumar, M. (2020). Principled artificial intelligence: Mapping consensus in ethical and rights-based approaches to principles for AI. *Berkman Klein Center Research Publication*, (2020-1).

Given, L. (2008). The SAGE Encyclopaedia of Qualitative Research Methods. London: Sage.

Latonero, M. (2018). Governing artificial intelligence: Upholding Human Rights & dignity.

Matulionyte, R., & Hanif, A. (2021, October). A call for more explainable AI in law enforcement. In *2021 IEEE 25th International Enterprise Distributed Object Computing Workshop (EDOCW)* (pp. 75-80). IEEE.

Nyamu-Musembi, C., & Cornwall, A. (2004). What is the" rights-based approach" all about?: perspectives from international development agencies.

O'Flaherty, M. (2020). Facial recognition technology and fundamental rights. *Eur. Data Prot. L. Rev.*, *6*, 170.

Permanent Representatives Council. (2022). Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts

Sanz-Urquijo, B., Fosch-Villaronga, E., & Lopez-Belloso, M. (2022). The disconnect between the goals of trustworthy AI for law enforcement and the EU research agenda. *AI and Ethics*, 1-12.

Skorik, V. (2022). The AI Act should not contain exemptions for 'national security'. Retrieved from: https://euobserver.com/opinion/156421

Sunde, I. M. (2022). AI-based Law Enforcement Online: The Impact of the European Artificial Intelligence Act (AIA). *Bergen Journal of Criminal Law & Criminal Justice*, *10*(2), 29-50.

Veale, M., & Zuiderveen Borgesius, F. (2021). Demystifying the Draft EU Artificial Intelligence Act—Analysing the good, the bad, and the unclear elements of the proposed approach. *Computer Law Review International*, *22*(4), 97-112.

Waelen, R. (2022) Why AI Ethics Is a Critical Theory. *Philos. Technol.* 35, 9. https://doi.org/10.1007/s13347-022-00507-5

Appendix I

Permanent Representatives Council. (2022). 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

European Commission for the Efficiency of Justice. (2018). European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment

Appendix II

<u>Table 1: Coding Scheme</u>

Theory	Theme	Codes
Law Enforcement		effectiveness, justice, security, fairness, victims, organised crime, cross border crime, terrorisms, national security, cyber crime, investigation, evidence, suspect, perpetrator, criminal justice system, surveillance, search, witness, evidence
Eurojust		coordination, cooperation, cross border crime, information exchange, joint investigation
Human Rights	Dignity	Human dignity (Art. 1), Right to life (Art. 2), Right to integrity of the person (Art. 3), Prohibition of torture and inhumane or degrading treatment or punishment (Art. 4)
	Freedoms	Right to liberty and security (Art. 6), Respect for private and family life (Art. 7), Protection of personal data (Art. 8), Freedom of thought, conscience and religion (Art. 10), Freedom of expression and information (Art.11), Freedom of assembly and association (Art. 12), Freedom of the art and science (Art. 13)
	Non-Discrimination and Equality	Equality before the law (Art. 20), Non-discrimination (Art. 21)
	Justice	Right to an effective remedy and to a fair trial (Art. 47), Presumption of innocence and right of defense (Art. 48), Principle of legality and proportionality of criminal offences and penalties (Art. 49), Right not to be tried or punished twice in criminal proceedings for the same criminal offence (Art. 50)
AI Ethics	empowerment from the machine	Transparency, explainability, privacy, freedom, autonomy, human control
	protecting humans	trust, (professional) responsibility, accountability, non-maleficent, human values, safety, security, fairness, non-discrimination
Governance of AI	techno-optimism	innovation, progress, digital transformation, smart solution, advancements
	techno-scepticism	privacy concerns, job displacement, pessimism, digital divide, algorithmic bias, risks
	techno-liberalism	free market innovation, digital democracy, open access, decentralisation
	techno-nationalism	digital sovereignty, protectionism, digital borders, national interests
Politics of AI	techno-democracy	digital governance, e-democracy, participation, open government, transparency
	techno-authoritarianism	digital surveillance, censorship, digital repression, oppression
	techno-populism	anti-elitism, national identity
	techno-liberalism	free market innovation, digital democracy, open access, decentralisation
	techno-socialism	digital cooperation, open source, collaborative, digital sharing, open knowledge

Data Appendix III

Empowerment and Protection Regulation