A European Positive Sum Approach towards AI tools in support of Law Enforcement and safeguarding privacy and fundamental rights

D2.5: Practical Ethics Toolbox for the Use of AI by LEAs

Grant Agreement ID	101022001	Acronym	PopAI
Project Title	A European Positive Sum Approach towards AI tools in support of Law Enforcement and safeguarding privacy and fundamental rights		
Start Date	01/10/2021	**Duration**	24 Months
Project URL	https://www.pop-ai.eu/		
Document date	30/09/2023		
Nature	R = Document, report	**Dissemination Level**	PU = Public
Authors	Virginia Bertelli, Matteo Mastracci, Luis Rodrigo González Vizuet, Judith Jordà Frias (ERI)		
Contributors	Pinelopi Troullinou, Francesca Trevisan (TRI), Dimitris Kyriazanos (NCSRD), Sofia Segkouli, Porfiriou Nikolaos (CERTH)		
Reviewers	Pinelopi Troullinou (TRI), Dimitris Kyriazanos, Andreas Ikonomopoulos (NCSRD)		

Abstract

The D2.5 "Practical Ethics Toolbox for the Use of AI by Law Enforcement Agencies" is a novel document presenting a set of resources for anyone involved in the implementation of AI in the LEAs context. Nevertheless, the resources presented by the report are accessible to everyone interested in the topic. The Ethics Toolbox is composed of three main sources, educational videos, ethics briefs and taxonomies visualisation. These three resources are based on past popAI tasks (T2.1, T2.2, T2.3, T3.4) with a comprehensive view of the use, implementation, ethics, policies and challenges of AI in the LEAs context. The Ethics Toolbox is a novel document because is one of the first documents that compiles a set of legal frameworks, guidelines, recommendations, academic research and study cases of use and implementation of AI in LEAs. This compilation can be founded on the Taxonomy and motivated by the educational videos bringing the main questions and challenges of AI. Additionally, the document offers three ethics cases of AI in LEAs scenarios where ethics challenges are behind complex decision-making process.

Table of Contents

List of Terms & Abbreviations

Abbreviation	Definition
AI	Artificial Intelligence
AI HLEG	High Level Expert Group on Artificial Intelligence
D	Deliverable
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
FRT	Facial Recognition Technologies
HRIA	Human Right Impact Assessment
LEAs	Law Enforcement Agencies
UN	United Nations
VR	Virtual Reality
WP	Work Package
NCSRD	National Centre for Scientific Research "Demokritos"
TU/e	Technische Universiteit Eirndhoven
KEMEA	Kentro Meleton Asfaleias
TRI	Trilateral Research Ltd
GDPR	General Data Protection Regulation
ERI	Eticas Research and Innovation

1. Introduction

PopAI is the EU H2020 project that aims to increase awareness, boost trust, and encourage a constructive dialogue on the ethical use of AI in policing between EU policymakers, LEAs, technology providers, and civil society. popAI follows a comprehensive, cross-disciplinary, and inclusive approach, mapping and engaging all ecosystem stakeholder groups through a series of knowledge sharing modalities and collaboration tools. The project results include AI policy recommendations and multidisciplinary best practices as well as an ethics toolbox for law enforcement agencies, organising the knowledge around AI within functionality, ethical and legal taxonomies. These practical tools are part of popAI's blueprint for a European AI hub for LEAs, a hub facilitating exchange of knowledge between stakeholders and supporting the responsible use of AI by law enforcement.

The Practical Ethics Toolbox respond to the crucial necessity of AI introduced in Law Enforcement with the potential to generate benefits in efficiency and accuracy, bringing positive change to European LEAs operational capacity. However, at the same time, AI generates also great risks for fundamental rights and democracy. To mitigate risks and create a just, sustainable and inclusive European AI culture for Law Enforcement, it is important to understand what AI ethics is and how it applies to Law Enforcement.

The Toolbox becomes the first resource that integrates the multiple perspectives of Ethics and AI through LEAs space. In this sense, the ethics toolbox is composed by three main products. The first product is a collection of educational videos regarding to explore the intricate relationship between artificial intelligence (AI) and ethics within the context of policing. These videos have been selected to offer valuable insights and facilitate a deeper understanding of the ethical implications surrounding the use of AI technologies in law enforcement.

The second product is a series of three ethics briefs. The briefs explore how artificial intelligence is used in law enforcement, specifically focusing on predictive analytics, natural language processing (NLP), and image recognition. The aim of the briefs is to provide law enforcement personnel with better awareness and information about the various uses and applications of artificial intelligence, including the potential benefits and risks of these technologies in policing, and to consider the ethical implications of their use.

Lastly, the third product is the visualisation of the taxonomies. The interactive visualisation serve as a translation tool for the work accomplished under the four PopAI project deliverables, namely: D2.1 Functionality taxonomy and emerging practices and trends, D2.2 Legal framework and casework taxonomy: emerging trends and scenarios, D2.3 The controversies and risks that have shaped innovation and will shape AI in the next 20 years, and D2.4 Ethical frameworks for the use of AI by LEAs. The website will show users in which of the four taxonomies they can find their specific terms and in which specific items/docs under the taxonomies. This living tool for analysis and

discussion will be an important resource for anyone interested in the ethical implications of AI in law enforcement.

1.1 Scope and objectives of the deliverable

This deliverable pertains to the work conducted within Work Package (WP) 2 "Security AI in the next 20 years: trends, practices and risks" which builds on the existing state of the art in relation to the use of AI by LEAs in Europe and elsewhere to identify:

1. the actual AI use and technical characteristics of AI tools in the security domain (T2.1);

2. the legal frameworks and recent court rulings (T2.2);

3. how controversies have shaped technology adoption in the security domain (T2.3);

4. the ethical principles and challenges that can inform a practical ethics toolbox (T2.4);

5. the organisational issues around AI implementation in LEA contexts (T2.5).

Task 2.4 "The Ethical Principles and Challenges that can Inform a Practical Ethics Toolbox" explores current ethical frameworks in the LEA and AI space, drawing on published materials and internal reports used by security actors and technology providers. It is divided into two deliverables: D2.4: "Ethical frameworks for the use of AI by LEAs" and D2.5 "Practical ethics toolbox for the use of AI by LEAs". This report covers D2.5 which provides a practical ethics toolbox for the use of AI by Law Enforcement Authorities (LEAs). It is organized into three main sections:

1. Introduction to Educational Videos on AI and Ethics

- Introduces the aim of creating eight educational videos on AI and ethics based on ten questions from LEAs.

- Provides clear and concise answers to these questions in an accessible and engaging manner.

- Targets a wide range of audiences, including students, educators, and the general public.

2. Technology Ethics Briefs

- Focuses on three specific AI applications: predictive analytics, natural language processing, and image recognition.

- Covers definitions, examples of usage, and ethical considerations for each application.

- Enables better-informed decision-making by providing a comprehensive overview of technology ethics related to these AI applications.

3. Interactive Web Page on AI and LEAs Ethics Taxonomies

- Translates four AI taxonomies: ethics, legal, functionalities, and social controversies.

- Provides a categorization framework for understanding the field of AI and LEAs ethics.

- Offer an interactive visualization for searching and accessing relevant documents, supporting researchers, practitioners, and policymakers in navigating AI and LEAs ethics.

1.2 Structure of the deliverable

This deliverable is structured into **three main sections**. **Section 1** will focus on introducing the project's aim of creating **8 educational videos** on AI and ethics. The videos are based on ten questions compiled by the project team from the feedback received from Law Enforcement Authorities (LEAs). These questions form the basis for the video scripts and cover topics related to AI and ethics. The aim of the videos is to provide an accessible and engaging introduction to these complex topics, with each video being no longer than two minutes. The questions are likely to cover a broad range of topics, including but not limited to the definition of AI and ethics, the ethical implications of AI, the role of ethics in AI development, and the potential benefits and risks of AI. The videos aim to provide answers to these questions in a clear, concise, and engaging manner, making the content accessible to a wide range of audiences, including students, educators, and the public.

Section 2 would consist of **three technology ethics briefs** related to specific AI applications, such as predictive analytics, natural language processing, and image recognition. The briefs would cover the definition, examples of usage, and ethical considerations related to each AI application. For instance, the predictive analytics brief would include details on its use in policing, ethical implications, and examples of its usage in Europe. The aim of these briefs is to provide a comprehensive overview of technology ethics related to specific AI applications, enabling better-informed decision-making.

Finally, **Section 3** would serve as a basis for creating an **interactive taxonomy visualization** on the PopAI web page of the four AI taxonomies: ethics, legal, functionalities, and social controversies. Each taxonomy would provide a categorization framework for better understanding the field of AI and LEAs ethics. For example, the ethics taxonomy would include a collection of relevant documents about AI in policing from an ethical perspective. Users can search the taxonomies around the visualization in the four different categories. This tool pretends to be a hub of multiple documents or cases valuable for researchers, practitioners, and policymakers. The main objective of this visualization is to help the multiple final users to get a quick, accessible and useful tool to get the main discussions, applications and cases of AI and LEAs.

1.3 Relation to other tasks and deliverables

This deliverable has been implemented as part of WP2 "*Security AI in the next 20 years: trends, practices and risks*" and of Task 2.4 "*The Ethical Principles and Challenges that can Inform a Practical*

Ethics Toolbox". Task 2.4 is divided into two deliverables: D2.4: "*Ethical frameworks for the use of AI by LEAs*" and D2.5 "*Practical ethics toolbox for the use of AI by LEAs*". The current PopAI Practical Ethics Toolbox (D2.5) is, then, closely connected to the PopAI Functionality taxonomy and emerging practices and trends (D2.1), legal taxonomy (D2.2), the controversies report (D2.3) and the ethical frameworks for the use of LEAs (D2.4).

The aim of Task 2.4 is to document in a systematic and extensible taxonomy of all the possible published materials and internal reports used by security actors and technology providers regarding LEAs and AI. In this sense, D2.5 integrates the work done in T2.1, T2.2, T2.3, T3.2, and T3.4 with a more applicable and practical perspective for the use of LEAs. The visualisation of the Taxonomies is totally developed from previous deliverables and complemented by the integration of real examples or cases of the LEAs context.

Regarding to the educational videos, their development was based on crucial input of T3.2 and T3.4. These tasks were relevant to understand the most important discussions, doubts and challenges of AI and LEAs. The development of the educational videos is a direct contribution on the dissemination tasks of WP5. Additionally, their development contributed to construct a constant synergy between popAI partners and LEAs by resuming and represent the main challenges of AI in the LEAs context.

2. Educational Videos on AI and Ethics

This section introduces a comprehensive collection of educational videos that explore the intricate relationship between artificial intelligence (AI) and ethics within the context of policing. These videos have been carefully selected to offer valuable insights and facilitate a deeper understanding of the ethical implications surrounding the use of AI technologies in law enforcement. These videos aim to provide valuable insights and enhance comprehension of the ethical considerations regarding AI's use in law enforcement. Each video tackles various aspects of AI in policing, answering crucial questions and providing clarity on its implications. With these videos, viewers can gain fundamental knowledge to understand the ongoing debates in the field, participate in well-informed conversations, and contribute to the discussion on AI's role in law enforcement. The educational videos are designed for everyone interested in the topic. Consequently, each video includes keywords and main ideas to raise the challenges and implications of AI in the LEAs space considering ethical perspectives, algorithm auditing, system accountability, role of the society in AI, and more.

The first video introduces the concept of AI in law enforcement and explores its practical applications. It is the presentation of the series of eight educational videos with the objective to spotlight the main doubts, implications, debates and topics regarding ethics in the implementations of AI in the Law Enforcement Agencies. The second video, aim the necessity to understand the difference between two concepts: ethics and morality. These two terms are crucial to develop the further videos and the relationship between ethics and AI.

The third video dives deeper into the complex relationship between AI and ethics. It explores the ethical considerations arising from the use of AI in policing, offering key principles and real-life examples to illustrate their intersection. Consequently, this video tries to resume the experience of popAI partners and the most common cases of AI and ethics. The fourth video correspond to the questions: how to address bias in AI? It explores the significance of avoiding bias and discriminatory treatment in AI systems, especially in law enforcement.

The fifth video, the spotlight is on ensuring traceability and accountability in AI systems. It emphasizes the importance of human oversight and responsible decision-making in AI applications. The sixth video tackles the question of responsibility in advancing and monitoring AI development. It highlights the need for collaboration among society, law enforcement agencies, and technology companies. Investigating public perceptions, the seventh video examines how citizens view AI usage by the police. It delves into whether AI is seen as a helpful tool or a control mechanism, fostering transparency and democratic accountability. Lastly, the eighth video focuses on the impact of AI on police organizational needs. It addresses the effectiveness, efficiency, and ethical implications of integrating AI into police work.

Through this collection of educational videos, we aim to provide viewers with a comprehensive overview of AI and its ethical implications in policing. The viewer can be anybody interested on the topic, this is a main goal of the videos. The use of a common language and explanation of key concepts foster the debate and discussion around AI. Additionally, the contributions from our partners enrich the discussions and help to develop informed decision-making, ensuring the responsible and beneficial deployment of AI in law enforcement practices.

The developing of the videos was realized by Gorilla Agency (https://www.gorilla-agency.uk/) in association with ERI to construct the eight videos. The eight videos can be visualised on the popAI webpage (https://www.pop-ai.eu/ethics-toolbox/). The creation of the multimedia is divided in six phases:

1. validation of graphic identity;
2. script writing;
3. realisation of the storyboard;
4. animation;
5. mounting; and
6. delivery.

The graphic identity was developed using the popAI web page and the logos of the project. For the script writing, each script was reviewed and enriched by different partners and contributors. Nevertheless, Gorilla Agency realized a final version of each script to ensure a video of one or two minutes maximum. Additionally, the agency worked with copyrights to avoid possible legal issues according to the content of the videos or phrasing. For the realisation of the storyboard and animation, Gorilla made a design of the animation for each different transition and image used in the video. These scenes of the videos were also developed with the help of multiple partners and the

LEAs' approval. Subsequently, the mounting phase corresponds to the integration of the sound. In this case, the videos will use voice and background music to communicate the videos. Lastly, the delivery of the final version of the videos. The next sections explain the main topics and questions engaged by each video with their final scripts. The initial scripts are included in the annexe section of the document.

2.1 Unveiling the Meaning of AI and Its Applications in Policing

The first video was created with the knowledge and expertise of NCSRD. As the largest multidisciplinary research centre in Greece, NCSRD is comprised of five distinct institutes, each dedicated to advancing knowledge and innovation in different scientific fields. Leveraging their expertise, NCSRD contributed significantly to the development of the video, providing valuable insights and perspectives on the ethical implications of artificial intelligence. This collaboration highlights NCSRD's commitment to fostering public understanding and awareness of AI ethics, making important contributions to the ongoing dialogue surrounding responsible and ethical AI development.

The inclusion of the questions "*What is AI? What are the current capabilities for policing? In which areas? Where?*" in the educational video on AI and ethics is of utmost importance. These questions provide vital information to the audience, enabling them to grasp the fundamental concepts of AI and its practical implications in law enforcement. By addressing the question of "What is AI?" in the video, viewers can gain a clear understanding of the technology and its potential applications in policing. Explaining the current capabilities of AI in law enforcement allows individuals to comprehend the advancements and benefits that AI brings to the field. Moreover, discussing the specific areas where AI is being employed in policing highlights the practical contexts in which AI systems are utilized. This knowledge provides insights into the diverse applications of AI, such as digitalizing tasks, analysing data, and offering recommended actions. Understanding the scope and reach of AI in law enforcement enhances the viewers' awareness of its potential impact. In summary, addressing these key questions ensures that the educational video provides a comprehensive overview of AI in policing. It equips the audience with the necessary knowledge to engage in meaningful discussions about the ethical considerations and responsible use of AI in law enforcement.

FINAL SCRIPT VERSION

Welcome!

In this video, we explore AI in policing, a field of computer science developing intelligent systems for tasks needing human intelligence. AI boosts policing in various areas and decision-making. Predictive policing uses crime data to identify high-risk areas for prevention. AI tools analyse surveillance data, aiding crime investigations. In cyber ops, AI prevents cyberattacks and identifies online crimes. AI's in migration and border control verify identities and surveil borders. VR simulators enhance law

enforcement training; AI aids case management and court proceedings. The USA prioritizes case clearance and predictive policing; Europe utilizes facial recognition, speech analysis, and more. However, ethical, privacy, and legal frameworks must guide AI for fair and transparent policing.

Thank you for watching!

2.2 Understanding ethics

The second educational video on AI and ethics was created as a result of the answer provided by the PopAI partner, TU/e, a research-led university specialising in engineering science & technology based in the Netherlands. The video will explore the meaning of ethics in detail and seek to answer the question of who defines what ethics is. Through discussion and analysis, we will aim to provide a comprehensive understanding of the fundamental principles of ethics and how they relate to policing practices. By the end of the video, viewers will have gained a better understanding of the complexities of ethics and how it applies to the field of policing.

This section emphasizes the importance of addressing fundamental questions surrounding ethics in the context of policing, namely "*What in detail does 'ethics' mean? Is there any fixed definition of ethics and of how to behave ethically (in policing)?*" These questions form the basis for understanding the ethical dimensions of AI technology in law enforcement. By delving into the complexities of ethics, and questioning its definition, origin, and applicability in policing, we can navigate the ethical landscape of AI technology with clarity and responsibility. Ethics encompasses a broad range of principles, values, and moral guidelines that shape our understanding of right and wrong conduct. Understanding the depth of ethics is crucial for comprehending the underlying principles and philosophies that guide ethical decision-making in policing.

Defining ethics involves exploring the perspectives of various stakeholders involved in shaping ethical frameworks. Ethics is not a static concept but evolves over time, influenced by diverse perspectives, cultural contexts, and societal norms. Ethics is a dynamic field subject to ongoing philosophical debates and contextual considerations. Acknowledging the absence of a rigid ethical framework allows for a nuanced exploration of diverse perspectives and evolving challenges when integrating AI technologies in law enforcement.

FINAL SCRIPT VERSION

Welcome!

In this video, we explore the intricacies of ethics in policing. Ethics is the compass that guides our actions, distinguishing between right and wrong. While morality shapes our personal beliefs, ethics involves critically evaluating the impact of our actions on various stakeholders and adhering to relevant moral values and duties. It transcends legal boundaries, as legality doesn't always align with moral appropriateness. Institutions like the International Association of Chiefs of Police have codes of

conduct that define the values and duties for law enforcement professionals. Upholding ethics means making challenging decisions that prioritize doing what's right, even when it exceeds legal obligations. It requires us to consider the broader implications of our actions. By understanding and embracing ethics, law enforcement can maintain trust and integrity while navigating complex situations.

Thank you for watching.

2.3 Exploring the intersection of AI and ethics

The third educational video on AI and ethics has also been drafted following the answers given by PopAI partner, TU/e. Eindhoven University is a leading research university specializing in engineering science and technology. Situated in the Eindhoven Brainport region, TU/e is committed to developing knowledge and innovative technologies to tackle societal challenges in health, mobility, and energy. Their Innovation Lab facilitates technology transfer and the commercialization of research, supporting the creation of spin-off companies and patents. With their expertise, TU/e contributes valuable insights to the development of the educational video on AI and ethics, bridging the gap between academia and practical applications in law enforcement.

This section will explore the complex relationship between AI and ethics, focusing on the ethical considerations that arise when using AI, such as in policing. While legislation is important for upholding ethical standards, it may not address all concerns. We will discuss key principles in AI ethics and examine how AI systems can be designed to be inherently ethical, going beyond the ethics of the end user. Real-life examples will illustrate the nuanced ethical implications of AI, fostering a comprehensive understanding of its intersection with ethics. The video will also explore the ethical acceptability of using AI software in policing, considering factors like individual rights, fairness, and accountability. It emphasizes that legislation alone does not fully reflect ethical standards, urging a broader perspective encompassing societal values, human rights, and the risks and benefits of AI deployment. These questions contribute to a holistic exploration of AI and ethics, providing viewers with a comprehensive understanding of the ethical considerations in various contexts, including policing.

FINAL SCRIPT VERSION

Welcome!

In this video, we explore the relationship between AI and ethics, particularly in policing. AI technology has revolutionized various fields, including law enforcement, but its use raises ethical concerns that must be addressed. The moral appropriateness of AI-supported actions should align with professional or institutional codes of conduct, emphasizing values and duties. However, AI systems can be biased, opaque, unsafe, and unsustainable, undermining values like fairness, transparency, privacy, and

security. During development and procurement, choices regarding algorithms, data processing, and performance standards impact the ethical implications of AI systems. Existing regulations may not provide clear guidance, emphasizing the need for careful ethical reflection to ensure positive outcomes. By critically evaluating the moral implications of AI technology in policing, we can utilize it for good.

Thank you for watching.

2.4 Addressing bias in AI

The fourth educational video on AI and ethics is based on the contribution by ERI, a Spanish non-profit organisation focused on research, training and dissemination at the intersection of technology, data, society and responsibility. Eticas Research and Innovation is dedicated to research, training, and dissemination in the realm of technology, data, society, and responsibility. Eticas's primary objective is to enhance public awareness regarding the implications of digital technology and empower individuals and communities to safeguard their data. ETICAS assists decision-makers in formulating policies that maximize the benefits of technology while minimizing its negative impacts. The Eticas Foundation is currently spearheading cutting-edge projects across various domains, including the development of responsible data sharing mechanisms, ethical solutions, and GDPR compliance assessment for sensitive projects.

The question "*How could AI bias be avoided?*" is crucial in the context of AI and ethics. The video will discuss AI bias, which is the unfair treatment of certain groups of people due to their race, gender, age, religion, or other characteristics. Bias can enter the AI model during different phases, and historical imbalances and patterns of discrimination in the data can cause harm. To reduce bias, it is important to identify protected groups, proactively search for bias in the data or model, build awareness, hire a diverse workforce, and be transparent about the algorithm. Responsible AI principles should also be followed when buying third-party data or AI-related services.

FINAL SCRIPT VERSION

Welcome!

In this video, we address the question: "How could AI bias be avoided?" AI has transformative potential but can perpetuate bias and discrimination. To reduce bias, we need to understand its origins and take proactive measures. Bias can enter AI models in any moment of its development, through biased data, technical factors, model construction and more. We must identify protected groups vulnerable to discrimination and consider them throughout the AI pipeline. Open discussions about potential bias are crucial during product design and use. Exploratory data analysis helps detect and mitigate bias. Open source toolkits like Fairness 360, among others offer metrics and algorithms

to address bias. Building awareness through bias training and diversifying the workforce is essential. Transparency in algorithm use encourages scrutiny and error correction. Responsible procurement involves choosing vendors adhering to Responsible AI principles. Reducing AI bias requires collaboration, awareness, and transparency. By following these steps, we can create ethical, transparent, and inclusive AI that benefits society.

Thank you for watching.

2.5 Ensuring traceability and accountability in AI systems

The fifth educational video on AI and ethics is also based on the contribution by ERI. Without human oversight, AI systems can potentially make decisions that are biased, discriminatory, or even harmful, without anyone knowing or being able to intervene. Human supervision and monitoring can help to prevent these issues from arising and can help to identify and address them if they do. Overall, the aim of the video is to foster a discussion about the importance of designing and using AI systems that are traceable, accountable, auditable, and subject to human supervision and monitoring. By emphasizing these principles, the video encourages developers and users of AI systems to prioritize transparency, fairness, and ethical decision-making when working with AI.

FINAL SCRIPT VERSION

Welcome!

In this video, we address the questions: "Is the system designed for traceability, accountability, and auditability? Does it allow for human supervision and monitoring?" AI systems should be responsibly developed and used, which includes traceability, accountability, and auditability. Let's explore these terms and their importance. Traceability involves tracking inputs, outputs, and decisions made by the AI system. It enhances transparency, helps identify biases and errors, and builds trust. Accountability holds people responsible for AI systems, managing risks, and addressing harm or unfairness. Regular audits, unbiased data, and measures to mitigate biases ensure accountability. Auditability allows evaluation of AI system performance. It ensures proper functioning, prevents harm and discrimination. Conducting audits is essential to maintain trust. Designing AI systems with traceability, accountability, and auditability is crucial for responsible development and use. It fosters trust, confidence, and benefits society.

Thank you for watching.

2.6 Who should be responsible for advancing and monitoring the development of AI?

The sixth educational video on AI and ethics is based on the answers given by PopAI partner, TRI, consulting and technology development company which specialises in research and the provision of policy, regulatory and certification advice and recommendations for new technologies and systems. The video will touch base on the growing debate around who should have the responsibility of advancing and monitoring the technological development of AI. With the rapid advancements in AI technology, it is becoming increasingly important to consider who should be responsible for ensuring that these technologies are developed and used in a responsible and ethical manner.

The question of "*Who should advance and monitor the technological development of AI? Society, including law enforcement agencies, or technology companies?*" is of significant importance in the context of AI and ethics. It highlights the need for a collaborative approach involving multiple stakeholders. Society, including law enforcement agencies, should play an active role in advancing and monitoring AI technology. This is because AI systems have far-reaching implications for society, and decisions about their development should consider the values, needs, and concerns of the people they affect. Law enforcement agencies have a unique perspective, particularly in the context of policing, and their involvement is crucial to ensure that AI technologies are used ethically, responsibly, and in compliance with legal frameworks. At the same time, technology companies also have a role to play, as they possess the technical expertise and resources to drive AI innovation. However, it is essential to balance their involvement with the interests and well-being of society as a whole. Ultimately, a collaborative and inclusive approach that includes society, law enforcement agencies, and technology companies is necessary to navigate the complex ethical landscape of AI development and ensure its responsible and beneficial use.

FINAL SCRIPT VERSION

Welcome!

In this video, we address the question: "Who should advance and monitor the technological development of AI? Society, including law enforcement agencies, or technology companies?" The development of AI should be driven by societal needs, not just the capabilities of tech companies. Leaving it solely in the hands of technology companies may prioritize corporate interests over societal ones. Law enforcement agencies using AI tools must ensure transparency and accountability. Communicating their role to the public is essential to maintain trust and support. Society's interests, such as privacy and security, should be fundamental when developing and deploying new AI tools. Co-creation with diverse stakeholders ensures ethical and appropriate use of AI. Collaboration among society, law enforcement agencies, and technology companies is crucial. This approach ensures ethical, transparent, and public-interest-driven development and use of AI.

Thank you for watching.

2.7 Investigating public perceptions: Is AI in policing a useful aid or a means of control?

The seventh educational video on AI and ethics was made by TRI's contribution and aims to explore the impact of AI on citizens, particularly in relation to its use by law enforcement agencies. It seeks to examine the effects of AI technology on individuals and society, including its potential benefits and drawbacks. Furthermore, the video aims to delve into the attitudes and perceptions of citizens towards AI-driven policing, exploring whether it is viewed as a helpful tool for improving public safety or as a means of exerting control over the population. Through this exploration, the video seeks to shed light on the ethical and societal implications of AI use in law enforcement and how it affects citizens' trust in the justice system.

The question of "*What is the impact of AI on citizens, and what is their perspective on the use of AI by the police? Do citizens see artificial intelligence as a helpful tool or a control mechanism?*" is crucial for understanding the broader societal implications of AI in policing. It is essential to consider the perspectives and experiences of citizens as the primary stakeholders affected by the use of AI by the police. By exploring the impact of AI on citizens, we gain insight into the potential benefits and concerns associated with its deployment. Understanding the positive aspects helps us recognize AI's potential as a helpful tool in enhancing law enforcement capabilities, improving efficiency, and increasing public safety. Conversely, addressing citizens' concerns about AI as a control mechanism is equally important. It allows us to identify potential risks, such as privacy infringements, biases, and the potential for undue surveillance, which may erode trust between the police and the communities they serve.

Taking citizens' perspectives into account helps ensure that the development and implementation of AI technologies align with societal values, respect individual rights, and address public expectations. It allows for the development of AI systems that are not only effective but also ethically and socially acceptable. Engaging citizens in discussions about the use of AI by the police also fosters transparency and democratic accountability. It enables a participatory approach, where citizens have a say in shaping the policies and guidelines governing AI deployment. By considering citizens' perspectives, we can build a more inclusive and responsible AI ecosystem that respects the rights, needs, and expectations of the communities being served.

FINAL SCRIPT VERSION

Welcome!

In this video, we explore the impact of AI on citizens' perspective regarding its use by the police. AI in law enforcement can enhance policing efficiency and safety. However, it's essential to consider citizens' viewpoints. While AI can assist officers, it should be used responsibly to maintain public confidence. Biometric identification and predictive policing raise concerns and must be regularly reviewed and trained to ensure compliance. Transparency is vital to avoid controversies like the Clearview AI breach. Officers should understand AI systems they use to avoid unintended

consequences. Despite rational public wariness, AI will benefit criminal justice systems and enhance safety. AI tools complement human decision-making but can affect citizens differently, demanding genuine public understanding for the full potential of law enforcement AI.

Thank you for watching!

2.8 AI and Police Organizational Needs

The eight educational videos on AI and ethics features an important collaboration with KEMEA. KEMEA, established in 2005 within the Hellenic Ministry of Citizen Protection, is a renowned think tank and research centre dedicated to supporting security policy implementations in Greece at a strategic level. Their activities encompass research and development in collaboration with LEAs, practitioner training, certification in private security professions, and advisory services to various public and private authorities on safety and security matters.

The questions explored in this video - "*How well does AI meet the needs of the police? Should the police receive specific AI training? What are the repercussions of AI on police work in terms of effectiveness and efficiency?* - are crucial for understanding the impact of AI in policing. These questions assess the suitability of AI for meeting police requirements and the necessity of specialized training for law enforcement personnel. They also examine the effects of AI on the effectiveness and efficiency of police operations. Additionally, they highlight the importance of ensuring that AI systems used by law enforcement align with ethical guidelines and serve the agency's objectives. Finally, they consider the potential benefits and challenges associated with AI implementation in policing. By addressing these questions, the video provides insights into the opportunities and considerations associated with integrating AI into law enforcement practices. It promotes a comprehensive understanding of how AI can be leveraged effectively while upholding ethical standards, maximizing effectiveness, and minimizing potential risks.

FINAL SCRIPT VERSION

Welcome!

In this video, we address: "How well does AI meet police needs? Should police receive specific AI training? What are the repercussions of AI in terms of effectiveness and efficiency? How can AI use be ensured ethically? To what extent can AI help or hinder?" AI supports law enforcement, saving time and digitalizing tasks. Specific AI training for police, including ethics and well-being, is crucial. Assessing AI's impact involves human rights, ethics, data protection, and democracy assessments. Clear problem definitions, compliance, and human oversight are essential. Establishing mechanisms to protect citizens' rights, including the right to appeal AI decisions, is vital. Balancing security and democracy are crucial. By considering these factors, we harness AI's potential while upholding ethics, rights, and safety. Responsible and ethical AI use is our responsibility. Even, if the AI is powerful tool let's enhance security while respecting values and ethics.

Thank you for watching.

3. Technology Ethics Briefs

The rapid advancement of technology brings with it countless opportunities to improve various aspects of society, such as predicting crime hotspots and digitizing old documents, to enhance public safety and efficiency. However, the use of technology in these areas also raises ethical dilemmas and considerations that must be carefully examined. This is particularly true in the field of law enforcement, where the application of technologies like predictive analytics, image recognition, and natural language processing can significantly impact privacy, civil liberties, and the potential for biased outcomes.

In this series of three ethics briefs, we will explore how artificial intelligence is used in law enforcement, specifically focusing on predictive analytics, natural language processing (NLP), and image recognition. The selection of these main topics is based on previous tasks and deliverables. The work developed on the D2.2, D2.3, D2.4 and D3.1 (T2.1, T2.2, T2.3) were key insight to select the three main uses of AI in LEAs context with specific algorithms or actual systems. In this sense, we understand the next relevant applications:

- **Data analytics and prediction**: AI technologies can analyse large datasets, identify patterns and extract insights from the data fed into the systems. In law enforcement, data analytics powered by AI are used to predict crime spots, offenders, perpetrators' identities or victims of crime.

- **Machine vision & recognition**: AI technologies can identify or understand images and videos. Facial recognition technologies and licence plate readers are examples of this class of tools that can trace and track individuals and objects.

- **Natural language processing (NLP):** NLP techniques can analyse and generate language data to extract insights. AI powered chatbots using NLP can be used to interact with the public and provide information about crime prevention and reporting.

The aim of including these common examples and applications is to provide law enforcement personnel with better awareness and information about the various uses and applications of artificial intelligence, including the potential benefits and risks of these technologies in policing, and to consider the ethical implications of their use. Each brief mentions actual algorithms that have been implemented in LEAs that can have ethics concerns, risks and challenges.

3.1 Predictive Analysis

What are Predictive Analytics (in Policing)?

Predictive analytics in policing is the use of advanced data analysis techniques to identify patterns and predict future events related to crime and public safety. These techniques involve the application of machine learning algorithms to historical crime data, along with other relevant data to identify potential crime hotspots or individuals who may be at risk of committing a crime.

Some examples of how predictive analytics can be used in policing include:

- **Predicting crime hotspots**: By analysing historical crime data and other relevant data sources, predictive analytics can identify areas that are at higher risk of crime. This information can be used to guide the deployment of police resources to those areas, allowing law enforcement agencies to be more proactive in preventing crime.

- **Predicting repeat offenders**: Predictive analytics can be used to identify individuals who are at higher risk of committing a crime based on their past behaviour. By focusing resources on these individuals, law enforcement agencies can intervene before a crime is committed.

- **Identifying emerging crime trends**: By analysing data on crime patterns and trends, predictive analytics can help law enforcement agencies identify new or emerging crime trends that may require a proactive response.

Overall, the use of predictive analytics in policing holds the promise to improve public safety and enhance the effectiveness of law enforcement agencies, while also raising important questions about bias, privacy, fairness, and accountability.

How is predictive analytics being used in Europe?

- **ProKid 12_SI** is used by the Dutch police and intends to assess the criminality of children under 12 years old and is used. ProKid employs a combination of historical data and statistical analysis to assign a risk to a child. It utilizes available police data on children, including information on their address, police contacts, and "living environments" which includes information about parents and cohabitants, their police contacts, and whether they have been victims of violence, to categorize them into one of four colour-coded risk categories for future criminal activity. The system assesses children based on their relationships with others and their supposed risk levels, allowing individuals to be classified as higher risk if they are associated with others who have a high-risk assessment, such as siblings or friends. Additionally, a parent's assessed risk can also affect a child's risk level (La Fors, 2020).

- **Key Crime Delia** has been used by the Italian State Police in Milan. The software analyses data on past criminal events to predict future events and help allocate police resources. Based on previous crimes, targets and repeating patterns Delia purports to help to plan their routes, Radar. The German Federal Criminal Police Office and the University of Konstanz have developed a risk assessment tool to assess the risk of individuals committing serious acts of violence related to terrorism.

- **RADAR-iTE** compares an individual's behaviour with data on the behaviour of people who committed crime. The evaluation procedure consists of two stages. The initial stage involves the police officer in charge collecting all available information about the extremist individual, while the second phase comprises a questionnaire consisting of 73 questions. The questionnaire includes queries about personal and social life events, social network, proof of terrorism-inspired travel, history of violence, with response options of "Yes," "No," or "Unknown."

Ethical dilemmas and considerations

The use of predictive analytics in policing raises important ethical considerations that need to be carefully addressed. One major concern is the potential for **biased outcomes**, particularly if the algorithms used to analyse the data are trained on biased historical data. This could lead to unfair profiling of certain groups, exacerbating existing social inequalities. Another concern is the impact on **individual privacy**, as predictive analytics relies on collecting and analysing large amounts of personal data. There is also a risk that individuals may be **stigmatized or falsely accused** based on predictions that are not accurate. Additionally, there are questions around **accountability and transparency**, particularly regarding the use of proprietary algorithms and the lack of oversight or regulation. **Finally**, the use of predictive analytics can lead to a shift in the role of police officers from being reactive to proactive, potentially leading to a loss of community trust if not implemented in a fair and transparent manner.

3.2 Natural Language Processing (NLP)

What is Natural Language Processing (in Policing)?

Natural language processing (NLP) is the field of AI covering knowledge and techniques involved in the processing of linguistic data by a computer (ISO, 2019), used to determine and identify key words and phrases within processing audio data (e.g. call centres) and free-form text (e.g. the body of an email) (ISO, 2018; ISO, 2021). The purpose of this technology is to make machines capable of reading and reasoning with human language and therefore, automatically process it. Some common tasks involving NLP include information extraction, document categorization and semantic text matching (European Commission, 2022), which can help police agencies in crime investigations, intelligence gathering, and public safety operations. The ultimate goal of NLP in policing is to improve the

efficiency and accuracy of police operations by automating the analysis of linguistic data and facilitating the decision-making process.

Some examples of how NLP can be used in policing include:

- **Crime analysis:** Police agencies can use NLP algorithms to analyse crime data and extract useful insights, such as identifying patterns and trends in criminal activity, analysing the language used in social media posts to detect threats or identify potential suspects, and identifying high-risk areas for criminal activity based on text data from various sources.

- **Investigative support:** NLP can be used to automatically extract and categorize data from police reports, interviews, and other sources, making it easier for investigators to quickly identify key information and potential suspects. NLP can also help in identifying the language patterns used in crime reports, such as determining the level of risk and severity of the incident, which can help in prioritizing investigations.

- **Community engagement**: Law Enforcement Authorities can use NLP algorithms to analyse social media and other online platforms to gauge public sentiment and detect potential threats or unrest. This can help authorities to anticipate and respond to potential public safety issues, as well as to identify areas where community outreach and engagement may be needed.

Overall, NLP has a range of potential applications in Law Enforcement, from improving crime analysis and investigative support to enhancing community engagement and predicting the risk of recidivism. As NLP technology continues to evolve, it is likely that we will see even more innovative and effective uses of this technology in the field of Law Enforcement.

How is NLP being used in Europe?

- **VeriPol**, is a model developed for the detection of false robbery reports based solely on their text, which combines Natural Language Processing and Machine Learning methods in a decision support system[1]. The tool was developed in collaboration with the Spanish National Police and provides police officers the probability that a given report is false. The tool has been tested on more than 1000 reports from 2015 provided by the Spanish National Police, and empirical results show that it is extremely effective in discriminating between false and true reports with a success rate of more than 91% (Quijano-Sánchez et al., 2018).

- **Automatic speech analysis software** is being used by Germany's Federal Office for Migrants and Refugees to verify the dialects of refugees seeking asylum, with the aim of reducing the number of language analysis experts needed for the process. The software works by analysing the refugees' speech patterns and providing a report on the probability of the dialect they speak[2].

---

[1] https://eticasfoundation.org/veripol-spotting-false-complaints-made-to-the-police/

[2] https://www.dw.com/en/automatic-speech-analysis-software-used-to-verify-refugees-dialects/a-37980819

- **Kamu[3]**, a chatbot developed by the Finnish Immigration Service that helps citizens with general advice related to immigration processes and application procedures. The chatbot uses NLP and machine learning algorithms to understand user queries and provide appropriate responses, enabling the Immigration Service to provide more efficient and timely support to citizens.

- The **Swedish Land Registry** (SLR) developed by border authorities to increase efficiency in handling land registry requests[4]. Many old handwritten documents cannot be digitized easily as the text is hard to read. The SLR uses NLP and AI to analyse and interpret these documents, thereby making the process of digitization faster and more accurate. This has improved the quality of service provided to citizens by reducing the processing time for requests and ensuring the accuracy of records.

Ethical dilemmas and considerations

When implementing NLP technology in policing or other fields, it is important to consider the ethical implications and potential risks associated with its use. For instance, there may be concerns regarding **privacy** and the use of **personal data**, as well as the **potential for bias and discrimination** in the algorithms used. Additionally, there is a **risk of over-reliance** on NLP technology, which could lead to a decrease in human decision-making and critical thinking skills. Therefore, it is crucial to ensure that NLP systems are designed and implemented with transparency, fairness, and accountability in mind. Policymakers, law enforcement agencies, and developers should work together to establish ethical frameworks and guidelines for the use of NLP technology in order to ensure its responsible and effective use in society.

3.3 Image Recognition

What is Image Recognition (in Policing)?

Image recognition or image classification is a computer vision process that involves identifying, detecting, and categorizing objects, patterns, or concepts in digital images or photographs. This process typically involves the use of machine learning algorithms and deep neural networks to train a model on a large dataset of labelled images. Once trained, the model can be used to analyse and classify new images based on the patterns and features it has learned. Google's definition of image recognition or image classification is "*a process that classifies object(s), pattern(s), or concept(s) in an image.*"[5] This definition emphasizes the key role of classification in image recognition, which involves identifying and categorizing objects or patterns within an image. The ISO/IEC 22989:2022 standard provides a similar definition of image recognition, describing it as "*a process that classifies object(s),*

---

[3] https://migri.fi/en/chat1

[4] https://www.gov.uk/government/case-studies/natural-language-processing-for-land-registry-documentation-in-sweden

[5] See, https://developers.google.com/machine-learning/glossary/image

pattern(s), or concept(s) in an image." However, the ISO standard goes into more detail, defining image classification as "*a process that assigns a label or multiple labels to an image based on its content or a portion of its content.*" This definition emphasizes the role of labels in image classification, which are used to identify and categorize different objects, patterns, or concepts within an image.

Thus, image recognition in policing is a technology that utilizes computer vision algorithms and machine learning to analyse and classify images or video footage obtained from cameras or other visual sources. This technology can help law enforcement agencies in a variety of ways, such as identifying suspects, tracking criminal activity, and monitoring public safety. Image recognition systems can be used to automatically detect and recognize faces, license plates, and other objects of interest, allowing police to quickly and accurately identify individuals and track their movements. In addition, these systems can be trained to identify specific types of criminal behaviour, such as gun violence or drug trafficking, enabling police to respond more quickly and effectively to these incidents. However, image recognition in policing also raises concerns about privacy and potential biases in the algorithms, which must be carefully monitored and regulated to ensure that they are used in a fair and ethical manner.

Some examples of how Image Recognition can be used in policing include:

- **Crime Scene Analysis**: Image recognition technology can be used to analyze crime scenes and help investigators identify potential evidence, such as weapons or other objects. This can help to solve crimes more quickly and efficiently.

- **Crowd Surveillance**: Image recognition can be used to monitor crowds and identify individuals who may be acting suspiciously. This can be useful in detecting potential threats or criminal activity.

- **Predictive Policing**: Image recognition can also be used in conjunction with machine learning algorithms to predict areas where crime is likely to occur based on past data. This can help police departments allocate resources more effectively.

Overall, image recognition technology is increasingly being used in policing to aid in investigations and improve public safety. The technology can be used for various purposes such as facial recognition, license plate recognition, crime scene analysis, crowd surveillance, and predictive policing. However, it's important to ensure that the technology is used ethically and with appropriate safeguards in place to protect individual privacy and civil liberties.

How Image Recognition is being used in Europe?

- **ANPR system**, which stands for Automatic Number Plate Recognition, is a software used by the Dutch police that is designed to recognize and read number plates of vehicles[6]. It has a

---

[6] https://www.politie.nl/onderwerpen/anpr.html

wide range of applications including paid parking, traffic control, tax avoidance, environmental protection and many more. This software is currently being used in over 2000 administrations and is considered to be a powerful and versatile AI technology.

- **Henri Coandă International Airport** in Bucharest has awarded a contract worth EUR 4.675.000 (excluding VAT) for the modernization and expansion of its video surveillance system[7]. As part of the project, a face recognition system will be implemented to alert security personnel of the airport when a wanted person or terrorism suspect listed by intelligence services is detected. The system aims to help detect and prevent terrorism, and it will be integrated with the existing video surveillance cameras at the airport. In addition, an intelligent image analysis system will be implemented to detect suspicious behavior and alert security staff. The security systems deployed will use state-of-the-art technology, while maintaining data protection and confidentiality mechanisms in compliance with GDPR regulations.

- **S.A.R.I.** (Sistema Automatico di Riconoscimento Immagini), or Automated Image Recognition System, is an algorithmic facial recognition tool used by Italy's national police force. The software has the capacity to process live footage and identify recorded subjects through a process of facial matching (AlgorithmWatch 2019). In 2018, SARI made headlines when it correctly identified two burglars in Brescia as a result of its algorithmic matching process. Despite being successful in that instance, questions have been raised regarding the accuracy of the software (the risks it poses to justice and safety due to a susceptibility to create false-positives and false-negatives), as well as cybersecurity and privacy guidelines it follows (AlgorithmWatch, 2019).

Ethical dilemmas and considerations

When it comes to image recognition in policing, there are ethical dilemmas and considerations that need to be addressed. In Europe, image recognition technology is being used in various applications, such as ANPR systems, face recognition systems at airports, and algorithmic facial recognition tools used by national police forces. However, there are concerns around **privacy** and **potential biases** in the algorithms, which must be carefully monitored and regulated to ensure that they are used in a fair and ethical manner. Moreover, the **accuracy of the software** and its susceptibility to create false-positives and false-negatives pose risks to justice and safety, which need to be addressed through proper cybersecurity and privacy guidelines. Therefore, it's essential to ensure that the technology is used ethically and with appropriate safeguards in place to protect individual privacy and civil liberties.

---

[7] https://www.uti.eu.com/press-releases/uti-will-implement-face-recognition-and-intelligent-image-analysis-systems-with-otopeni-airport/

4. AI and Law Enforcement Ethics: An Interactive Taxonomy

The use of AI in LEAs has become increasingly prevalent in recent years. However, the use of AI in policing raises many ethical concerns that need to be addressed. In order to better understand and organize the field of AI and LEAs ethics, an interactive taxonomy has been developed. This taxonomy is not intended to be a comprehensive list, but rather a categorization framework for organizing relevant documents around AI in policing from four different perspectives: ethics, legal, functionalities, and social controversies. These taxonomies will be integrated into an online webpage, which will serve as an open database that can be consulted through an interactive visualization on the PopAI webpage. The interactive webpage will serve as a translation tool for the work accomplished under the four PopAI project deliverables, namely: D2.1 Functionality taxonomy and emerging practices and trends, D2.2 Legal framework and casework taxonomy: emerging trends and scenarios, D2.3 The controversies and risks that have shaped innovation and will shape AI in the next 20 years, and D2.4 Ethical frameworks for the use of AI by LEAs. The website will show users in which of the four taxonomies they can find their specific terms and in which specific items/docs under the taxonomies. This living tool for analysis and discussion will be an important resource for anyone interested in the ethical implications of AI in law enforcement.

The legal taxonomy is composed of laws, conventions, rights, guides or recommendations regarding the use of AI by Law Enforcement Agencies. Additionally, most of the elements is supported by an example of their application of study. In some cases, these contributions can cover more than LEAs' topics. Nevertheless, they can be useful as general guidelines or initiatives to improve the regulation and comprehension of AI. The main advantage of this visualisation is to integrate in the same place all the efforts developed in past research, discussions with LEAs, Policy Labs, etc. (D2.1, D2.2, D2.3, D2.4 and D2.6) with an accessible language to researchers, practitioners, and policymakers in navigating AI and LEAs ethics. However, the development of the final set of taxonomies was reviewed and supervised by popAI partners and approved by LEAs partners to ensure their usability in their context.

The visualisation of the Taxonomy tries to be a novel repository of multiple resources regarding ethics, AI and LEAs. It is the central hub for multiple resources like guidelines, recommendations, principles, policies, application cases, etc. The taxonomies are the one of the first efforts to compile, describe and contribute to understanding a whole and vast space of AI, LEAs and ethics sphere open to anyone. The next figure represents all the sources and components of the taxonomies.
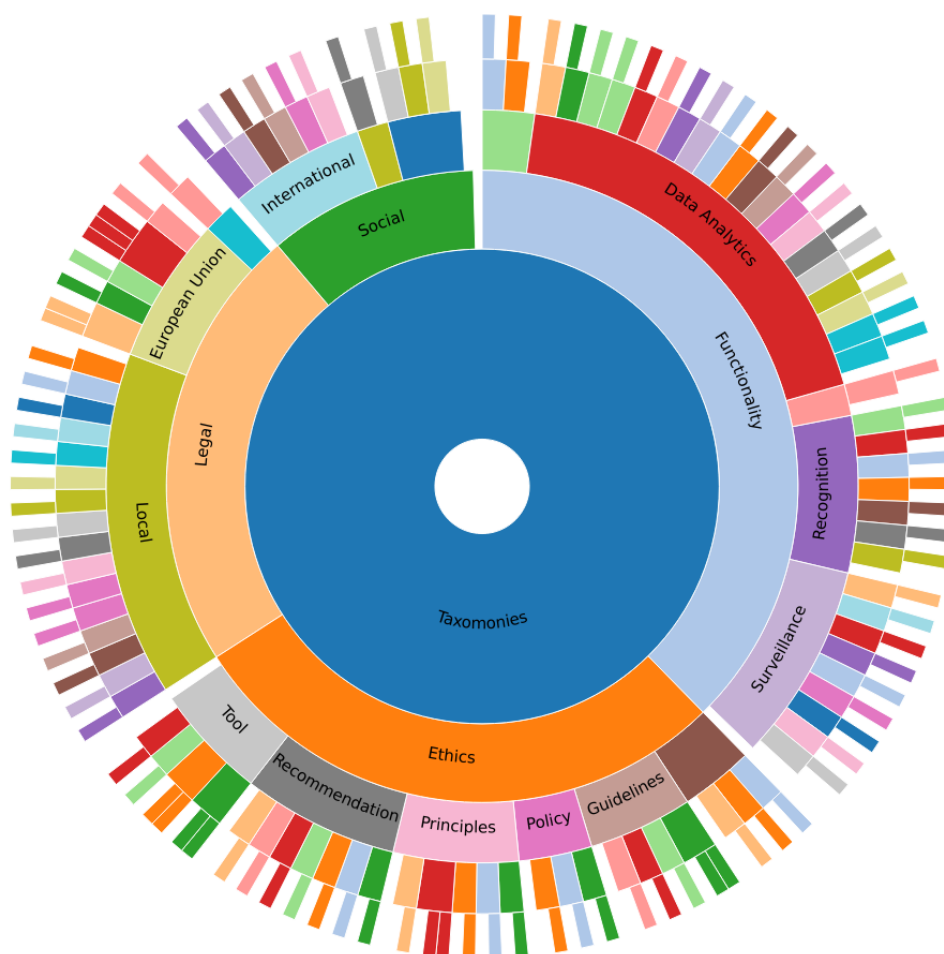
Figure 1: Taxonomies visualization

In each field of the legal, ethical, social and functionality taxonomies, you will find different aggregations of the information. The legal taxonomy consists of four main levels of information. Each level is represented like a ring inside the pie graph. First, the level of these regulations, guides or rules, for example if they are from the European Union, or at the Federation level etc. Secondly, the taxonomies include the Entity information, for example the European Parliament, European Council, local governmental agencies or other institutions. Lastly, the two remaining levels or rings are the title and the link to the related contributions. In this final ring or branch, the user can find more information like the direct reference of the document, links, examples or cases of study.

The ethical taxonomy is structured in the same four levels or rings inside the pie. First, the contributions are classified into six classes: code of ethics, tool, recommendations, principles, policy and guidelines. These classifications correspond to the character of each taxonomy contribution. Second, the taxonomy considers different actors or main contributors to these taxonomies like government agencies, academia, civil society, professional bodies, etc. Third, when it is possible to know this information, the third level shows if the actual contribution is completed, ongoing or an initial draft. At the final level, the taxonomy includes the name of the contribution and its year of publishing.

The social taxonomy is divided into three main levels. The first level is the scope of the contribution, e.g., if it is a global, national, local or regional contribution. Secondly, the taxonomy identifies the origin of the main contributor, if it is a governmental source or a private sector source. The third level is the title of the contribution. Lastly, the taxonomy includes a brief description of the contribution and its status of development.

Lastly, the functionality taxonomy has the objective to collect most of the terminology, developments, models or methods applied in the law enforcements field. In this sense, the taxonomies are grouped into four levels. First, the contributions are classified into different topics such as data analysis, surveillance studies, communication, etc. The next level includes a classification of the main methods used, e.g., natural language processing, neuronal network, machine learning, computer vision etc. The third level corresponds to the name of the algorithm, or the main topic addressed: biometric validation, social network analysis, anti-money laundering, etc. Finally, the taxonomy includes the status and the link to the related contribution.

As a result, the visualisation of the taxonomies tries to concentrate multiple sources of information divided in multiple topics, with an easy access for the diverse profiles of users. In this sense, the visualisation is the first attempt to give a holistic vision of AI and Ethics through LEAs challenges. Hopefully, in the future this first visualisation keeps growing in a more comprehensive and active platform of new resources, updates and applications of AI and LEAs.

5. Conclusions

The *Practical Ethics Toolbox for the Use of AI by LEAs* is the first resource that integrates multiple perspectives of Ethics and AI through LEAs space. The development of three main products: educational videos, ethics brief cases and visualisation of taxonomies; are the key components to open the discussion about AI and its interaction with ethics and Law Enforcement Agencies around Europe. Is not trivial to mention that AI can motivate ethical dilemmas, privacy issues or harmful spillovers to the society if the algorithms are not developed on a democratic, ethic, law supported and transparency frameworks to understand their use, application, effects, outputs and implications through the society.

The ethics toolbox pretends to be a useful product, approachable to all kind of users like academy researchers, policy makers, civil society, organisations, LEAs and more. This toolbox is composed by three key components that attends to different approaches. The educational videos engage the main questions and doubts about AI and LEAs: what is AI?, who develops AI?, how this affects to the society?, how these changes modify de LEAs role?, etc. In this sense, the educational videos present the big debates and actual discussions about AI-Ethics-LEAs sphere.

Regarding to the present context, the toolbox includes three brief cases where the application or AI in the security institutions can be done with their limits and ethical accountability. Using the cases of predictive criminal analytics, natural language processing (NLP), and image recognition; the case explores the potential benefits and risks of these technologies in policing. Consequently, the toolbox includes real cases of AI application in LEAs, ethical dilemmas and considerations regarding their use in real case scenarios.

Lastly, the visualisation of legal, social, functionalities and ethics taxonomies are the first repository of multiple resources regarding ethics, AI and LEAs. The taxonomy visualisation is the resume of multiple efforts regarding to other PopAI deliverables (D2.1, D2.2, D2.3 and D2.4) to allocate in an ordered and structured way all the possible resources of legal guidelines, ethical approaches, recommendations, frameworks, examples, cases studies, and more products regarding LEAs and AI. This first approach to the literature, study cases and expertise of multiple partners is the pioneering integration of resources and knowledge form multiple backgrounds and now open to the public in an easy and approachable content.

During the final presentation made at the "Towards a European AI hub for LEAs supporting the ethical use of AI in policing" event in Brussels, the Ethics Toolbox had a favourable reception from the public and stakeholders. The Toolbox was seen as a useful resource and a complete integration of multiple sources of information open to multiple users and profiles. However, the Ethics Toolbox can be complemented by additional efforts as does the EU AI Innovation Hub. Consequently, the Toolbox can be complemented and enriched by other sources of information and keep it updated with further legal frameworks, experiences, challenges and study cases.

6. Annex

First video initial transcript

Hello and welcome. In this first video, we will be answering the following questions: "*What is AI? What are the current capabilities for policing? In which areas? Where?*"

[Opening shot of a police officer patrolling a neighborhood]

Narrator: We live in a world where technology is advancing rapidly, and one of the most transformative fields is Artificial Intelligence, or AI. But what exactly is AI, and how is it being utilized in policing today?

[Cut to a shot of a computer screen displaying AI algorithms]

Narrator: Artificial Intelligence, or AI, is a broad field of computer science focused on developing intelligent systems that can perform tasks typically requiring human intelligence. It involves creating algorithms and models that enable machines to learn, reason, problem-solve, perceive, and make decisions. Machine Learning, a subset of AI, allows computers to learn and make predictions from data, similar to how humans learn from experience.

[Cut to footage of police officers in action]

Narrator: In the realm of policing, AI is being leveraged to enhance operational capabilities and improve decision-making in various areas. Let's explore some of these capabilities and the areas in which they are applied.

[Cut to an animated visualization of predictive policing]

Narrator: One area where AI is making an impact is in crime prevention. Through predictive policing, historical crime data is analyzed and interpreted to generate predictive models. This helps law enforcement agencies identify high-risk areas and strategically allocate resources to prevent crime before it happens.

[Cut to surveillance camera footage]

Narrator: AI is also being used in crime investigation. Law enforcement officers can rely on AI tools to analyze various types of information, such as images, videos, texts, and sounds, extracted from surveillance cameras, drones, and personal devices. This aids in extracting meaningful insights and supporting investigative procedures.

[Cut to a cybersecurity operations center]

Narrator: Another crucial application is in cyber operations, where AI plays a role in cyberattack prevention, network monitoring, and cybersecurity. AI techniques are employed to track online content, analyze social media, and identify potential criminal activities such as child abuse, terrorism, and radicalization.

[Cut to footage of border security]

Narrator: AI is also deployed in migration, asylum, and border control. It assists in identity verification, passport control, and border surveillance. Biometric identification, emotion detection,

algorithmic risk assessment, and AI tools for migration monitoring, analysis, and forecasting contribute to secure and efficient border management.

[Cut to police training simulations]

Narrator: Training and skill development of law enforcement agencies are also being enhanced through AI applications. Virtual reality (VR) simulators offer realistic and immersive training scenarios that are difficult or impossible to recreate in real-life situations. This helps improve the preparedness and decision-making abilities of officers.

[Cut to court proceedings]

Narrator: Administration of justice is another area where AI is utilized. AI-powered functionalities support case management, evidence management, and court proceedings. These tools increase efficiency, ensuring the validity of digital evidence and facilitating the retrieval and analysis of mobile phone data.

[Cut to shots comparing USA and Europe]

Narrator: The implementation of these AI applications varies between regions. In the United States, technologies such as improving case clearance rates through AI, predictive policing, and VR simulators are widely employed. In Europe, facial recognition, speech and text analysis, image and video analysis, automated license plate recognition, cyber operation techniques, and more are already being used by law enforcement agencies.

[Closing shot of a police officer and a computer screen displaying AI algorithms]

Narrator: While AI technologies offer valuable capabilities for policing, it is crucial to ensure their implementation is guided by ethical considerations, privacy safeguards, and adherence to legal frameworks. By harnessing the power of AI responsibly, law enforcement agencies can leverage its potential while upholding fairness, accountability, and transparency in their practices.

[Fade out with educational message on screen: "AI in Policing: Balancing Innovation and Ethical Considerations

Second video initial transcript

Hello and welcome. In this video, we will be answering the following questions: "*What in detail does 'ethics' mean? Who defines what ethics is? Is there any fixed definition of ethics and of how to behave ethically (in policing)?*"

[Opening shot of a city skyline with a voiceover]

Narrator: We all want to do good and avoid doing harm, but sometimes it's not clear what the right thing to do is. Take for example, monitoring an individual's financial activity to detect possible financial crimes. On one hand, it could prevent harm to others, but on the other, it could infringe on their right to privacy. This is where ethics and lawcomes into play.

[Cut to a shot of a person deep in thought]

Narrator: But what exactly is ethics? Who defines it, and is there a fixed definition of ethical behavior, particularly in policing?

[Cut to a shot of a bookshelf with various books on ethics]

Narrator: Ethics, or ethical reflection, is a tool that helps us distinguish good from bad actions, helping us to make the right decisions. It involves thinking critically about the impact our actions may have on different stakeholders and whether they conform to relevant moral values and duties.

[Cut to a shot of a person writing in a journal]

Narrator: Ethics is different from morality, which is a system of beliefs used to guide or evaluate actions. These beliefs may refer to values like fairness, justice, and transparency, or duties like doing no harm. While morality may be personal, it may also be institutional, with relevant values and duties described in a code of conduct.

[Cut to a shot of police officers standing in a line]

Narrator: For instance, the International Association of Chiefs of Police has a code of conduct that describes the values its members should uphold and their duties when exercising their profession.

[Cut to a shot of a gavel]

Narrator: However, what is considered morally appropriate may not always align with what is legal. Actions that are legal, like lying to your spouse about smoking, may be considered morally inappropriate, while actions that are considered morally appropriate, like exceeding the speed limit to escape an immediate danger, may be illegal.

[Cut to a shot of a police car with sirens]

Narrator: That's why merely obeying the law isn't enough for doing good. We must always consider the ethical implications of our actions.

[Closing shot of the city skyline with a voiceover]

Narrator: In the end, ethics is about doing what's right, even when it's difficult, and even when it requires us to go beyond what the law requires.

Third video initial transcript

Hello and welcome. In this video, we will be answering the following questions: "*How are AI and ethics related to each other? Are there any examples? When and how would the use of certain software (including AI) in policing be ethically ok or not ok?Doesn't our legislation completely reflect ethical standards?To what extent should ethical issues be considered beyond the legal framework? What are the most important principles in AI ethics?How can an AI system be used ethically and not depend on the ethics of the end user?*"

[Visuals of a computer screen showing data being analyzed by an AI program]

Narrator: Welcome to our educational video series on AI and ethics. In this video, we will explore the relationship between AI and ethics and discuss some of the most important principles of AI ethics. We will also examine how the use of certain software, including AI, in policing can be ethically justified or not.

[Visuals of AI technology and police officers in action are shown]

Narrator: AI technology has revolutionized many aspects of our lives and has become an essential tool in various fields, including law enforcement. However, the use of AI in policing raises several ethical concerns that must be addressed.

[Visuals of AI-supported policing activities, such as surveillance, are shown]

Narrator: First, let's consider the relationship between AI and ethics. Like all other technology, AI technology should be used to do good rather than bad. It is essential to reflect ethically on the actions performed with the help of such technology. If a relevant professional or institutional code of conduct is available, such actions should accord with the values and duties described therein.

[Visuals of professional codes of conduct related to AI are shown]

Narrator: However, the use of AI technology is not always value-neutral. AI systems have been known to undermine values such as fairness, transparency, privacy, sustainability, and security. For example, AI systems used by parole boards to predict recidivism have been shown to be systematically biased against racial minorities, while face-recognition systems have been known to be opaque even to experts.

[Visuals of AI systems and their potential biases are shown]

Narrator: The moral appropriateness of AI-supported actions must be evaluated during development, procurement, and use. During development, engineers make choices about the kinds of algorithms that an AI system should use and the kinds of data it should process. These choices have previously contributed to the development of systems that were biased, opaque, unsafe, and unsustainable. Similarly, during procurement, law enforcement agencies make choices about the standards against which to measure an AI system's performance, and about the task environments in which to apply it.

[Visuals of engineers and law enforcement agencies working on AI systems are shown]

Narrator: Finally, existing regulatory and legislative frameworks may not be specific enough to offer clear guidance about the moral appropriateness or legality of AI-supported actions. In such cases, careful and critical ethical reflection is particularly important to ensure that these actions do good.

[Visuals of laws and regulations related to AI are shown]

Narrator: In conclusion, the use of AI technology in policing raises several ethical concerns that must be carefully evaluated. By reflecting ethically on the actions performed with the help of AI technology, we can ensure that AI is used to do good rather than bad. Thank you for watching.

Fourth video initial transcript

Hello and welcome. In this video, we will be answering the following question: "*How could AI bias be avoided?*"

[Opening shot of a person typing on a laptop with a voiceover]

Narrator: Artificial intelligence has the power to transform the world we live in, but it can also perpetuate bias and discrimination if not monitored and addressed appropriately. In this video, we will discuss how bias can enter an AI model and what we can do to reduce it.

[Cut to a shot of a diverse group of people working in an office]

Narrator: Bias can enter the process right from the beginning. The data that we use to train these algorithms comes from the real world, which is not always fair or equal. This means that historical imbalances and patterns of discrimination can show up in the data and cause harm. Also, when we create an algorithm or adapt it to a specific context, bias can be introduced by technical and statistical factors, or by the developer team choices and interpretation.

[Cut to a shot of a person analyzing data on a computer]

Narrator: So, what can we do about bias?

[Cut to a shot of a person leading a team meeting]

Narrator: Bias can be reduced at each phase of the AI pipeline, and it starts with identifying the protected group. A protected group is any group of people who may be vulnerable to discrimination according to law, policy, or other authority. Any subgroup that could be treated unfairly should be considered a protected group in the AI system.

[Cut to a shot of a person discussing potential bias with a team]

Narrator: During the product design phases or use, we must be mindful of protected groups and have open discussions about the potential risks of bias. We can conduct a comprehensive exploratory data analysis process to explore the structure and patterns within our data. If any potential bias is discovered, data scientists should not hesitate to voice their concerns.

[Cut to a shot of a person using an open source toolkit to detect bias]

Narrator: There are open source toolkits, like Fairness 360 by IBM that contain a comprehensive set of metrics, metric explanations and algorithms to detect and mitigate bias in the dataset and models. We can use descriptive statistics such as mean, median, standard deviation, and range to describe the distribution of our variables. We can also use visualizations such as histograms, boxplots, and scatter plots to explore the distribution of our variables. We can also use fairness metrics and test the accuracy of our system across different groups.

[Cut to a shot of a person leading a training session]

Narrator: Building awareness is also essential. We can offer regular bias training to help people understand what bias is and how it affects technology. We can hire a diverse workforce that helps us to see reality from different angles and spot new problems.

[Cut to a shot of a person discussing transparency with a team]

Narrator: We must be transparent about the algorithm we build and how it is used. In this way, people can help us spot errors and address them. And finally, we should buy responsibly or talk to "responsible" vendors. We must make sure that any third-party providers of data or AI-related services adhere to Responsible AI principles and provide their staff with regular and appropriate bias training.

[Closing shot of a person looking thoughtfully at a computer screen]

Narrator: In conclusion, reducing bias in AI is a complex process that requires collaboration, awareness, and transparency. By following these steps, we can build AI that is more ethical, transparent, and inclusive, and that benefits society as a whole.

Fifth video initial transcript

Hello and welcome. In this video, we will be answering the following questions: "*Is the system designed for traceability, accountability and auditability? Does the system allow for human supervision and monitoring?*"

AI systems should be designed to be traceable, accountable, and auditable, but it ultimately depends on how they are developed and used. So, what exactly do these terms mean and why are they important in the development and use of AI systems?

[Opening shot of a computer screen with a voiceover]

Narrator: AI systems are becoming increasingly prevalent in our lives, and it's important that they are developed and used in a responsible manner. This includes designing them to be traceable, accountable, and auditable. But what do these terms mean, and why are they important?

[Cut to a shot of a person working on a computer]

Narrator: Traceability is the ability to track what goes in and what comes out of an AI system, as well as the intermediate steps or decisions made by the system. This can be achieved through detailed logging and record-keeping of the system's activities. It's important because it provides a clear

understanding of how an AI system is making decisions, including the data inputs and algorithms used. This can help to build trust and confidence in the system among stakeholders and can also improve the AI system itself by allowing it to identify and address biases and errors.

[Cut to a shot of a person signing a document]

Narrator: Accountability means that people are responsible for creating, using, and controlling AI systems, and that we need ways to manage and reduce the risks involved in using AI. If an AI system causes harm or unfairness, we need ways to hold people accountable and make things right. For example, if a company is using an AI algorithm to screen job applications, accountability means that the company has mechanisms in place to ensure that the algorithm is not discriminating against any specific group of applicants based on factors like race or gender. This might involve conducting regular audits of the algorithm's decision-making process, ensuring that the data used to train the algorithm is representative and unbiased, and implementing measures to mitigate any potential biases that the algorithm may be inadvertently picking up.

[Cut to a shot of a person reviewing a report]

Narrator: Finally, auditability refers to the ability to review and evaluate the performance of an AI system. Being able to evaluate the system and access records of those evaluations can help to make sure that the AI is trustworthy. For example, if a bank is using an AI system to make decisions on loan applications, auditability means that the bank can conduct an audit of the system to ensure that it is working properly and not causing any harm or discrimination.

[Closing shot of a computer screen with a voiceover]

Narrator: In conclusion, designing AI systems to be traceable, accountable, and auditable is crucial in ensuring that they are developed and used in a responsible manner. By doing so, we can build trust and confidence in AI systems and ensure that they are being used to benefit society.

Sixth video initial transcript

Hello and welcome. In this video, we will be answering the following questions: "*Who should advance and monitor the technological development of AI? Society, including law enforcement agencies, or technology companies?*"

[Opening shot of a person typing on a laptop with a voiceover]

Narrator: Artificial intelligence is transforming our world, and as it becomes more prevalent, we need to consider who should be driving its development and how we can ensure that it is monitored effectively.

[Cut to a shot of a technology company office]

Narrator: Leaving the creation of AI solely in the hands of technology companies can lead to prioritizing corporate and technical priorities over societal interests. Therefore, the development of AI should be driven by the needs of society, not just the capabilities of tech companies.

[Cut to a shot of people walking on a city street]

Narrator: In terms of law enforcement, AI tools must be transparent and accountable. There is a particular concern that law enforcement agencies use AI tools ethically and communicate their role to the public to ensure their trust and support.

[Cut to a shot of a person holding a protest sign]

Narrator: Citizens have interests such as privacy and security that must be fundamental when new AI tools are developed, tested and deployed. If society's needs are not met, AI may be rejected or used in ways that do not benefit the public.

[Cut to a shot of a person reading a book about AI]

Narrator: Additionally, while regulations such as the upcoming European AI Act have an important role to play, co-creation with diverse stakeholders from across society is required to ensure that AI is safe, ethical and appropriate.

[Closing shot of a person looking thoughtfully at a computer screen]

Narrator: In conclusion, the advancement and monitoring of AI must be a collaborative effort involving society, law enforcement agencies, and technology companies. This approach will ensure that AI is developed and used ethically, transparently, and in the public interest.

Seventh video initial transcript

Hello and welcome. In this video, we will be answering the following questions: "*What is the impact of AI on citizens, and what is their perspective on the use of AI by the police? Do citizens see artificial intelligence as a helpful tool or a control mechanism?*"

[Opening shot of a police car with sirens]

Narrator: Artificial intelligence is becoming increasingly prevalent in law enforcement, and it has the potential to make elements of policing easier and more efficient, ultimately making communities safer. However, it is important to consider the impact of AI policing tools on citizens and to acknowledge their perspectives. While AI systems can be beneficial, they can also cause problems if conceived or implemented inappropriately, not least for public confidence. Therefore, it is crucial to build genuine public understanding and acceptance to reduce risks and enable the revolutionary benefits of law enforcement AI.

[Cut to a shot of an officer working at a computer]

Narrator: AI tools can assist officers in many ways, such as interpreting data, simplifying processes, and automating gruelling work like categorizing child abuse images. This not only reduces the damaging impacts on officer wellbeing but also benefits how they approach their work and interact with the public. Artificial intelligence is a helpful tool to assist officers, and citizens should see it as a valuable resource rather than a control mechanism to unlock these benefits.

[Cut to a shot of people protesting with banners]

Narrator: However, different types of AI systems pose different risks, with biometric identification systems in public spaces and predictive policing tools being particularly contentious. These systems can jeopardize public trust and raise understandable concerns about the power of these hi-tech tools and the credibility of their conclusions. Regular training and review are essential to ensure that AI tools are compliant and effective and avoid controversies, such as the Clearview AI facial recognition system breach, which violated data protection rules.

[Cut to a shot of an officer in training]

Narrator: Additionally, officers need to understand how AI systems operate to avoid being in the dark about the tools they are using. The UK's HART risk assessment tool, which attributed a higher risk of reoffending to offenders with poor socio-economic backgrounds, raises legitimate questions about the power that impenetrable technology can exert over citizens.

[Closing shot of an officer talking to a member of the public]

Narrator: In conclusion, while public wariness of artificial intelligence is rational, new technologies will relieve pressure on criminal justice systems and make citizens, including law enforcement agents, safer. Effective AI tools assist human decision-making, they do not replace it, but citizens can be affected unequally, and blind spots have emerged during design and delivery. Therefore, building genuine public understanding and acceptance is crucial to reducing risks and enabling the revolutionary benefits of law enforcement AI.

Eighth video initial transcript

Hello and welcome. In this video, we will be answering the following questions: "*How well does AI meet the needs of the police? Should the police be given specific training on AI? What repercussions would have AI in police work in terms of effectiveness and efficiency? How could it be ensured that the use of an AI system fulfils the purposes of the law enforcement agency while being within an ethical framework? To what extent can AI help or hinder?* "

[Opening shot of a computer screen with a voiceover]

Narrator: In the context of law enforcement, the use of AI systems can serve as valuable support for police operations. They can assist in digitalizing tasks, saving time for law enforcement agencies (LEAs), and providing recommendations based on the vast amount of information they analyze.

[Cut to a shot of a person working on a computer]

Narrator: To ensure effective and responsible use of AI, specific training procedures should be implemented for LEAs. This includes providing qualifications or certificates to users and operators of AI systems, which should be periodically renewed. Ethical considerations and the psychological well-being of those interacting with AI systems should also be part of the educational programs for LEAs.

[Cut to a shot of the narrator summarizing the impact of AI in law enforcement]

Narrator: It is essential to assess the impact of AI on law enforcement practices in terms of effectiveness and efficiency. This involves conducting assessments such as human rights impact

assessments, ethics impact assessments, data protection impact assessments, social impact assessments and democracy impact assessments or a combination of those before introducing AI systems into everyday use by officers.

Narrator: To ensure the proper use of AI systems, clear problem definitions and goals must be established by LEAs. The proportionality test and compliance with applicable frameworks should be conducted throughout the development, deployment, and use of AI systems. Human oversight should be maintained, allowing for intervention, evaluation, and the ability to halt processes when necessary.

Narrator: Additionally, mechanisms should be established to support citizens' rights, including the right to appeal decisions made by AI systems. It is crucial to strike a balance between utilizing AI for security purposes and ensuring it does not hinder democracy or encroach upon the public sphere.

[Cut to various shots highlighting the impact of AI in different fields]

Narrator: By considering these factors, we can harness the potential of AI while upholding ethical principles and safeguarding the rights and well-being of both law enforcement agencies and the public.

[Closing shot of the narrator speaking directly to the camera]

Narrator: Remember, AI can be a powerful tool, but it's our responsibility to ensure its responsible and ethical use. Let's strive for a future where AI enhances our safety and security while respecting fundamental values.

7. References

AlgorithmWatch. (2019). Automating Society Report 2019: Taking Stock of Automated Decision-Making in the EU. Retrieved from https://algorithmwatch.org/de/wp-content/uploads/2019/02/Automating_Society_Report_2019.pdf

European Commission (DIGIT, Directorate-General for Informatics). (2022). Natural Language Processing for Public Services. Retrieved from https://joinup.ec.europa.eu/sites/default/files/inline-files/D02.01_Natural%20Language%20Processing%20for%20Public%20Services_4.pdf

International Organization for Standardization. (2018). ISO/TR 22957:2018(en), Artificial intelligence -- Categorizing and tagging [Technical Report]. https://www.iso.org/standard/64728.html

International Organization for Standardization. (2018). ISO 31000:2018 Risk management – Guidelines. https://www.iso.org/standard/74296.html

International Organization for Standardization. (2019). ISO 24613-1:2019(en), Language resource management -- Semantic annotation framework (SemAF) -- Part 1: Time and events [Standard]. https://www.iso.org/standard/72582.html

International Organization for Standardization. (2021). ISO/TR 24291:2021(en), Artificial intelligence -- Learning, education and training -- Guidance [Technical Report]. https://www.iso.org/standard/78787.html

La Fors, K. (2020). Legal Remedies For a Forgiving Society: Children's rights, data protection rights and the value of forgiveness in AI-mediated risk profiling of children by Dutch authorities. Computer Law & Security Review, 38, 105430. https://doi.org/10.1016/j.clsr.2020.105430

Quijano-Sánchez, L., Liberatore, F., Camacho-Collados, J., & Camacho-Collados, M. (2018). Applying automatic text-based detection of deceptive language to police reports: Extracting behavioral patterns from a multi-step classification model to understand how we lie to the police. Knowledge-Based Systems, 150, 102-116. https://doi.org/10.1016/j.knosys.2018.03.010