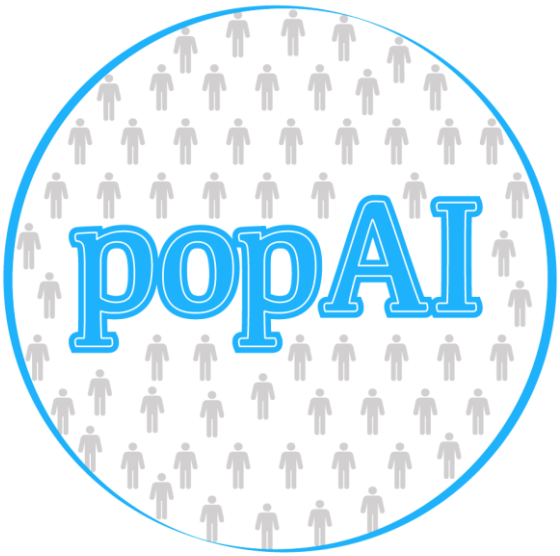


A European Positive Sum Approach towards AI tools in support of Law Enforcement and safeguarding privacy and fundamental rights

D2.6: AI meets organisational cultures: Human-machine interaction at the police station

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	ERI, NCSRD, TRI, KEMEA, CERTH/ITI, TUE, Z&P, HP, BayHfoD, ADM-PMM, APZ, PLTO		
Reviewers	Dimitris Kyriazanos, Andreas Ikonomopoulos (NCSRD)		

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 101022001.

Executive Summary

One of the most overlooked aspects of technology implementation is the issues that emerge when technology, and specifically AI, are incorporated into existing organisational structures and processes. This document is focusing on organisational and related issues such as the impact of technology processes on the health and safety, autonomy or responsibility of LEAs. The partners have broad expertise in working on the practical implementation of AI and data tools in the police sector and draw on this experience, the existing literature (both academic and grey literature, including press reports) and the input from the activities with stakeholders and citizens from empirical knowledge collection tasks and work package of popAI. The different case studies identified inform the conclusions of the report and shape the recommendations.

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

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.

One of the most overlooked aspects of technology implementation is the issues that emerge when technology, and specifically Artificial Intelligence (AI), are incorporated into existing organisational structures and processes. This task highlights the current and future organisational issues that LEAs have to face in their daily work. It also prioritises the use of AI systems from a human-centred perspective, which enhances the health and safety as well as the autonomy and responsibility of these professionals.

As a result, the Deliverable 2.6. provides a comprehensive mapping of the current and future challenges along three axes:

- How artificial intelligence (AI) is incorporated in LEAs organisation.
- Perception of AI by LEAs- E.g. what is AI for them then we have to look into:
    1. Legal aspects
    2. Ethical aspects - focus on responsibility-accountability
    3. Social aspects - citizens and AI
- Expectations around the introduction of AI:
    1. Legal aspects
    2. Ethical aspects
    3. Social aspects

In sum, the different case studies addressed in this deliverable serve to inform the conclusions of the report and shape the recommendation.

1.1 Scope and objectives of the deliverable

This deliverable pertains to the work conducted within the Work Package 2 (WP2): "Security AI in the next 20 years: trends, practices and risks". Thus, WP2 builds on the existing state of the art in relation to the use of AI by LEAs in the European Union to identify:

1. the actual AI use and technical characteristics of AI tools in the security domain (Task 2.1);
2. the legal frameworks and recent court rulings (Task 2.2);
3. how controversies have shaped technology adoption in the security domain (Task 2.3);
4. the ethical principles and challenges that can inform a practical ethics toolbox (Task 2.4);
5. the organisational issues around AI implementation in LEA contexts (Task 2.5).

This report covers D2.6 and systematises Task 2.5, being the organisational issues that emerge in the implementation of AI tools in LEA settings, including case studies and recommendations. As it stipulated in the Grant Agreement: "This task will tell the untold story of AI in the police forces by focusing on organisational and related issues such as the impact of technology processes on the health and safety, autonomy or responsibility of LEAs".

In sum, the scope of the report is framed within both theoretical and practical analytical mapping of these organisational issues, which ends up in an enriched and updated dialogue on benefits and challenges from both angles. In other words, the objective is to explore the overlooked aspects of technology implementation when AI is incorporated or aims to be incorporated into existing organisational structures and processes through the four primary goals:

- Introduce theoretically the existing literature on the implementation of AI and data tools in the police sector.
- Lay out the practical implementation of AI and data tools in the police sector.
- Analyse their convergences or discrepancies.
- Harmonise a set of best practices for LEAs based on the above content.

1.2 Structure of the deliverable

To achieve the objectives outlined above, this deliverable is organised into five main sections. Section 1 introduces the main topic discussed in the deliverable, outlines its scope and explains how this work relates to other popAI tasks and deliverables, as well as the working methodology employed.

Section 2 provides a theoretical discussion of the main literature debates integrating AI into LEAs. In this sense, the debates are mapped from the current and future challenges of human-AI interaction in LEAs. Likewise, emphasis is placed on predictive policing, automation bias and the role of Human in the Loop. Finally, some key conclusions of this new ecosystem policing are highlighted.

Section 3 outlines the practical insights gathered during different policy labs conducted at the Police Academy of Bratislava, the Hellenic Police, the Police Department of the University for Public Service in Bayern, the Municipal Police of Madrid and the Local Police of Turin. This section allows to demonstrate the existing dialogue between the theoretical debates explored in section 2 and the everyday AI-related uses of LEAs in section 3, either from the lived experiences in case AI systems have already been applied or from the expectations that LEAs may have in case AI systems have not yet been applied by LEAS.

Section 4 lays out the practical insights gathered also through interviews with the same actors mentioned in section 3, including insights from the Developers as well. This section allows to ratify that there is not only a link between theory and practice, but that there are some common challenges that are highlighted throughout the report, such as the concern to elaborate ethical and legal instruments that promote a responsible and justified use before the citizenship in constant human review of the AI systems, with the social benefit as the final purpose. Finally, section 5 offers a summary discussion and provides recommendations.

1.3 Relation to other tasks and deliverables

This report contributes to the popAI project by providing insights of the literature debates, the Policy Labs and interviews for LEAs stakeholders. The deliverable 2.6 “AI meets organisational cultures: Human-machine interaction at the police station” contributes directly to T2.5. The WP2 – T2.5 has the objective of to tell the untold story of AI in the police forces by focusing on organisational and related issues such as the impact of technology processes on the health and safety, autonomy or responsibility of LEAs. These combined efforts of academic research, LEAs interview, Policy Labs, partners experience and more, are going to be deployed in the WP3.

Additionally, T2.5 (D2.6) is one of the target-specific documents of a collection of the best practices among different disciplines within the T4.1 (D4.1), T4.2 (D4.2) and T4.3 (D4.3). Consequently, the contribution of the specific tasks facilitate the creation of a network of interaction among popAI (LEAs, CSOs, Industry), its Advisory Board and SU-AI-01-2020 and SU-AI-02-2020 Consortiums. The purpose is to create partnerships and synergies to communicate findings, validate the recommendations from T4.1-T4.3, identify best practices derived from various disciplines for the most efficient interaction among diverse stakeholder groups, leading to the appropriate design, use, monitoring of, and reaction towards AI tools in the security domain.

2 Mapping literature debates on integrating AI in LEAs

Technological advances, in continuous development, have brought about profound changes in modern societies in recent years. Lately, those prototypes that were confined to laboratories are being applied in different sectors, and Law Enforcement Agencies (LEAs) are not exempt from this transformation. To such an extent that it is even considered as a new phase of policing, Policing 4.0 (Deloitte, 2018), which is inscribed and defined as the fourth industrial revolution. Indeed, the deployment of new technologies for everyday use, in addition to some of the ethical and legal challenges addressed in this deliverable, also poses broader social and economic challenges depending on the use made of them.

Consequently, such developments and applications entail a distortion of old practices and even potential infringements of fundamental rights and EU values, such as the process of blurring public and private space that can lead to the misuse of video surveillance systems. It is therefore imperative to address the ethical dimension, and the new crossroads, that Policing 4.0 is generating.

Ultimately, this deliverable focuses on the practical implementation of IA and data tools in the police sector, drawing on theoretical debates in the existing literature, and inputs from stakeholder activities such as policy labs and interviews. The aim is to answer the following research question, aligned with the objective of Task 2.5. How can the experience of LEAs contribute to addressing current and future challenges of human-machine interaction at the police station?

To this end, we first present in the first section the state of the art of the literature focusing on such development and application of AI by LEAs, both in terms of the present and the future. An emphasis is placed on the implications, advantages and risks of a specific type of AI bias, the automation bias, and the role of the "human in the loop". This literature review on organisational cultures will serve as the basis for the analysis of the empirical work we have carried out, through policy labs and interviews, and which is presented in the following sections of the deliverable.

This review was generated through a comprehensive examination of both academic and non-academic sources, with contribution from all PopAI research collaborators. The sources of information can belong to broader five categories:

- Scientific Publications: Collection of publications in scientific journals, conference/workshops;
- proceedings and scientific book chapters;
- gray literature: magazines and newspaper articles;
- official report: work published by public and private institutions in a report format;
- legal Frameworks: Information related to regulations that regard technology and innovation;
- advocacy work: work produced by organizations for advocacy purposes.

Additionally, we have sought the input of crucial project entities (ALIGNER and STARLIGHT), who offered their insights on ethical frameworks throughout the entire work. PopAI partners have also liaised with INTERPOL and UNICRI and reviewed their ethics toolkit for AI in law enforcement.

2.1 Current challenges of human-AI interaction in LEAs

As the aim of this section is to present an overview of the current state of the art, the content focuses not on its history and development but on current trends. Artificial intelligence (AI) emerged in the first half of the 20th century. It was Wiener (1949) who coined the term cybernetics. Since then, it has been developing, ultimately at a dizzying pace to be defined as AI.

Nowadays, article 3(1) of the draft of the Artificial Intelligence Act[1] (AI Act) which is the first comprehensive European AI regulatory framework, with a human-centred and risk-based approach, states that 'artificial intelligence system' as follows: “software that is developed with [specific] techniques and approaches and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with”.

Similarly, Kitsos (2020) define AI as: “the field of computer science dedicated to solving cognitive problems commonly associated with human intelligence” (Kitsos, 2020:1). Furthermore, as the author states, this technological transformation through the development and implementation of AI systems is transforming advertising, finance, marketing, healthcare transformation, media, e-commerce, energy, and law enforcement activities.

Regarding their uses, the main AI-related applications stated by Kitsos (2020:2) are visual processing (e.g. facial recognition technologies, automated number plate recognition, lip-reading technologies, surveillance drones, body-worn cameras, or closed-circuit television (CCTV); audio processing; aural surveillance; autonomous research and analysis of identified databases; forecasting; behaviour detection tools; social media monitoring, International mobile subscriber identity (IMSI) catchers; automated surveillance systems; biometric identification, Natural Language Processing (NLP) or computational linguistics.

In terms of the benefits for LEAs in applying AI systems, Roksandić et al. (2022), highlight their potential to increase efficiency, data-driven processes and capabilities for concrete activities. Similarly, Campbell (2018) conclude likewise: “AI offers unprecedented capabilities to acquire and

[1] On 14 June 2023, the Members of the European Parliament adopted it. The next step is to reach an agreement by the end of the year on the final form of the law following negotiations with the EU countries in the Council. Available at: https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence?at_campaign=20226-Digital&at_medium=Google_Ads&at_platform=Search&at_creation=Sitelink&at_goal=TR_G&at_advertiser=Webcomm&at_audience=ai%20act&at_topic=Artificial_intelligence_Act&gclid=CjwKCAjw5MOlBhBTEiwAAJ8e1o5dILwP18VkanjWAcVeglkQB_vy-fcUFE2x1MZL8TZI2XXtTIoC1RoCOnQQAvD_BwE.

analyse big data, it is not surprising that the law enforcement community is interested in applying AI for its purpose".

Some authors highlight the following benefits for LEAs: "AI, and particularly Machine Learning (ML) and its emerging subset of deep learning (DL) algorithms play an important role in security functions due to its proactive threat mitigation capabilities. Particularly, computer vision methods based on DL have shown impressive results reaching human-level performance in several tasks" (Apostolakis et al., 2021:5).

We find a variety of methods being implemented in LEAs, for instance: "Methods of data analysis and interpretation based on AI are becoming common among LEAs. […]" Control applications: such as suspect policing (on social media), traffic control (automated license plate detection and vehicle identification), analyzing dark web money flows and, child pornography detection, and anomaly detection (Raaijmakers, 2019).

While other authors argue that AI has not only reached the level of human capabilities in some tasks but has even surpassed them: "Artificial intelligence is increasingly able to autonomously detect suspicious activities ('smart' law enforcement). In certain domains, technology already fulfils the task of detecting suspicious activities better than human police officers ever could" (Rademacher, 2019). However, this is not always the case, so the author calls for overcoming ethical, administrative and legal challenges with clear guidance based on three needs: regulatory provisions to maintain accountability; AI law enforcement needs to be used to overcome perpetuated discriminatory traits in human policing; smart law enforcement to decide whether we want to preserve the freedom to disobey the rule(s) of law.

In addition, the potential for cross-cutting technologies identified by Apostolakis et al. (2021) should also be highlighted: Augmented reality (AR) and AI are highly disruptive technologies that have revolutionised practices in a wide range of domains. As mentioned above, their potential has not gone unnoticed in the security sector, where several law enforcement agencies employ AI applications in their daily forensic investigation and surveillance operations (Apostolakis et al., 2021:1). Some of its uses include analysing digital evidence to detect objects or faces through deep learning algorithms, analysing recordings through machine-learning algorithms, or extracting text from documents to find clues to a crime.

However, as Roksandić et al. (2022) point out, the European Parliament Resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (European Parliament, 2021) warns that AI brings not only benefits but also many potentials for fundamental rights. The aim should be to enhance the well-being of people, human capabilities and security. Kitsos (2020) also notes that in the specific case of LEAs, the current technological growth has four implications for the use of AI: algorithmic bias, mass surveillance, privacy, and data protection.

There are currently two lines of literature. On the one hand, AI for the security and safety sector. The other body of literature, critical of the first, emphasises other intentions with a much broader scope that shapes security and safety reasons.

2.1.1 The scope of AI for LEAs: security and safety

As for the first line of literature, focused on the security and safety for LEAs and the public, the starting point is the following liberal assumption:

> "Security and public safety are key prerequisites in the function of societies. Citizens expect governments to fight crime and disorder as a means to preserve a safe environment where private life is protected and respected and business is allowed to flourish" (Kitsos, 2020).

However, in the midst of globalisation, crime as well as new technologies are shaking the EU's defining principles, such as the subsidiarity principle established in the Maastricht Treaty (1992)[2]. This principle prioritises action by the European Union over the Member States in areas in which it is not intended to have exclusive competence. Already in the 1990s, David B. et al. (1993) pointed out this agitated character by arguing that from the very beginning this principle lacked precision in terms of application. Currently, AI is accentuating the atmosphere of change. Consequently, LEAs must face: "a complex ecosystem of traditional, cyber-dependent, and cyber-enabled crimes that is challenging and altering police work (Kitsos, 2020:2).

Authors such as Almeida (2022) aim to achieve greater efficiency in the detection and prosecution of crimes by reducing economic costs. In her work, she explores some of the most used methods, such as surveillance cameras or Facial Recognition Technologies (FRT). Nevertheless, beyond the benefits that these technologies bring, it is fundamental to examine, as this literature review aims to do in answering the research question, how the experience of LEAs can contribute to human-machine interaction. That is, positively, by sticking to purely security and safety purposes, or by extrapolating their functions and making misuse of AI systems.

In addition, all these systems, if they are not properly explained, with transparency and clarity, do not generate trust on the part of citizens and, consequently, are destined to fail. In this exploration of such interaction, the ethical question is essential, since in the process of developing and implementing such technologies lies the privacy of citizens. What is clear is that "despite technical and ethical challenges, the use of AI by LEAs is entering an inexorable state" (Campbell, 2018:7).

In short, an ethical analysis of these technologies offers a negotiation of accountability requirements for police practices, to find an ethical and legal balance between security and privacy for citizens. For this reason, the Cambell (2018) advocates for a citizen debate necessary to negotiate and establish requirements with greater transparency, audits and explanation of the uses of each

[2] Legal basis: Article 5(3) of the Treaty on European Union (TEU) and Protocol (No 2) on the application of the principles of subsidiarity and proportionality. Available at: https://www.europarl.europa.eu/factsheets/en/sheet/7/el-principio-de-subsidiariedad

technology. In the case of FRT, she exemplifies this in the following terms: “accountability and acceptable privacy limits is critical in terms of balancing rights and responsibilities for FRT” (Almeida, 2022: 378).

In this sense, another of the most burning issues, which is not exclusive for FRT but also to other AI systems used by LEAs, is the discrimination inherent in the configuration of input biases, widely criticised for being trained by white male faces (Dickey, 2009; Boulamwini et al., 2018) and therefore end up reflecting these biases. Yet, there is consensus on the need to reverse this tendency. Kitsos (2020), for instance, proposes potential solutions to these concerns through the establishment of ethical and legal rules and measures, as well as guidance on implementation, based on four principles: fairness, accountability, transparency and explicability. In his own terms:

> “the key here lies in the creation and coordination of an intertwined System of checks and balances supported by a complete set of rules aimed at the protection of the core of human rights and dignity that will bind both governments and LEAs, while at the same time establishing a sense of security and trust amongst the population” (Kitsos: 2020:5).

Ultimately, the goal remains the same, to achieve a balance between public trust and security (Kitsos, 2020). Otherwise, the future of policing may lead to further discrimination. For instance, as Almeida warns: “facial recognition algorithms without taking accountability for the consequences of this usage could not only lead to further discrimination and victimisation of specific communities, but also to an even greater loss of trust between the general population and law enforcement agencies” (Almeida, 2022:379).

To reverse these biases and power dynamics, there is a growing body of algorithmic literature exploring alternatives (Mc Gregor, 2018; Shah, 2018, Buchmann et al., 2020; Wang et al., 2020). In this regard, it is important to note that there are also actions by human rights activists to show how these technologies may be being misused by police officers (Hill, 2020). An example highlighted by Patton et al. (2017) is the police surveillance of social networks to identify criminal activity and, thus, to obtain evidence for criminal prosecutions. The authors argue that such digital surveillance is carried out based on everyday racism by LEAs. Thus, they speak of ‘everyday racism in social media policing’ in the United States. Such intrusion into mixed private and public life is described by other authors as “context collapse” (boyd, 2002; Marwich, 2011). Control must be omnipresent in all phases of its development and implementation, with the understanding that power relations are also omnipresent, i.e., one can be accountable for a particular technology, but that it is not ‘ethically viable’, as Almeida (2022) points out. Moving away from catastrophism, she concludes that “this is currently an ethical emergency requiring urgent global attention” (Almeida, 2022:386). However, it does not remain at a discursive level, but applies what it calls for, the imminent revision of the use of FRT systems by LEAs, as an example, based on the **practical reflection of the following ethical questions** (Almeida, 2022:378).

1. Who should control the development, purchase, and testing of FRT systems ensuring the proper management and processes to challenge bias?

2. For what purposes and in what contexts is it acceptable to use FRT to capture individuals' images?
3. What specific consents, notices and checks and balances should be in place for fairness and transparency for these purposes?
4. On what basis should facial data banks be built and used in relation to which purposes?
5. What specific consents, notices and checks and balances should be in place for fairness and transparency for data bank accrual and use and what should not be allowable in terms of data scraping, etc.?
6. What are the limitations of FRT performance capabilities for different purposes taking into consideration the design context?
7. What accountability should be in place for different usages?
8. How can this accountability be explicitly exercised, explained and audited for, for a range of stakeholder needs?
9. How are complaint and challenge processes enabled and afforded to all?
10. Can counter-AI initiatives be conducted to challenge and test law enforcement and audit systems?

2.1.2 The scope of AI for LEAs: beyond security and safety

As for the second line of literature, extending some of the challenges mentioned in the first line of literature, it is highly critical of the use of AI by LEAs, arguing that it extends the role of security and safety. In this sense, authors such as Ezzeddine et al. (2023) claim that: "AI use should be justified, legitimate and only used for declared purposes" Ezzeddine et al. (2023:8). Their recent study explores the views of 111 citizens through interviews on the use of AI in LEAs. The authors of the study aim to encourage citizen engagement, not only by considering them as beneficiaries of AI, but also as key actors in its development. Since if there is consent and support, as mentioned above, chilling effects can occur (Stoycheff, 2016), counteractions against LEAs (Bayerl et al., 2021) or even national and international movements opposing its deployment (Ezzeddine et al., 2023). Thus, the aim of the study is to avoid the negative effects of AI and the findings result in **113 recommendations compiled in the following areas to be assessed**:

1. Educational safeguards: for citizens and LEAs.
2. Technical safeguards: Regular Evaluations, anonymization of collected data.
3. Legal safeguards: National and international regulations and independent agencies.
4. Human safeguards: selectivity in employing AI-handling staff and importance of human validation of AI findings and decisions.
5. Privacy safeguards: Limited data collection and requests for consent.
6. Stop use of AI: use traditional means.
7. Inevitable vs. no negative effects: either not foreseeing any negative effects or assuming no safeguards can protect from them.

Other authors warn of the dangers of data collection and its consequent ethical and moral implications (Lyon, 2002), which can have psychological consequences for the population (Stoycheff et al. 2020). Some of the concerns it raises are alliances between independent private sector bodies (Trottier, 2017), lack of evidence of algorithmic-based decisions, accuracy, fairness and risks of predictive policing (Bushway, 2020; Quattrocolo, 2020; Završnik, 2020).

In short, in this first section on the state of the art of the use of AI in law enforcement, it has been demonstrated that there is currently great technical development but there is still a lack of ethical and legal development for the implementation of such technologies, as well as for their use and evolution. Therefore, this situation needs to be reversed, which will be discussed in the next section focusing on the future state of the art, through more human control by LEAs in collaboration with other expert actors, not forgetting the interaction of activists and the civilian population. Such a process will strike a fair balance between security and the fulfilment of fundamental rights.

2.2 Future challenges of human-AI interaction in LEAs

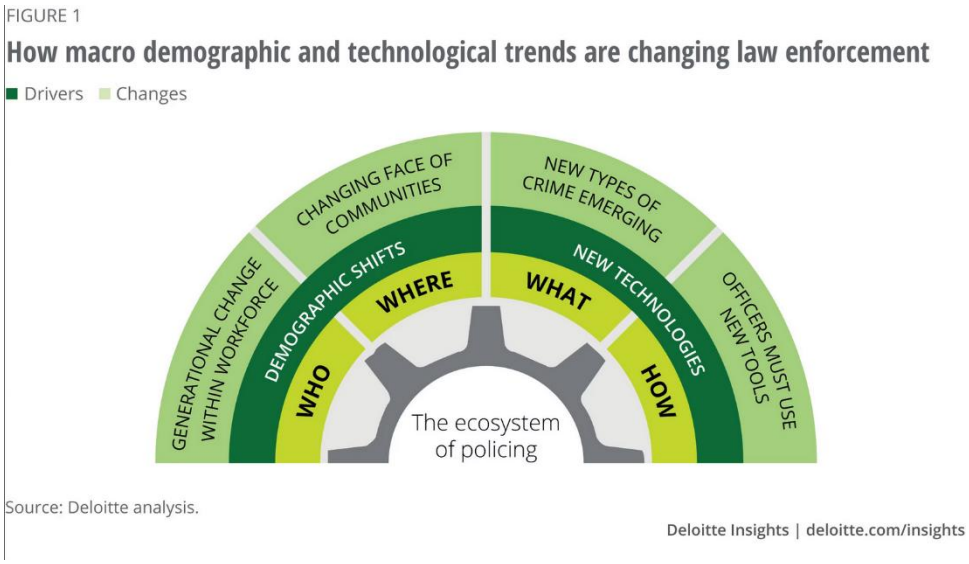
After exploring in the first section, in line with the objective of the deliverable, the organizational and security issues that LEAS encounter in their daily work, this second section will use this application to focus on future dilemmas and new tasks in this changing technological environment. They will also be complemented throughout the deliverable in collaboration with input from LEAS in the various case studies that make up the policy labs and interviews.

Indeed, when it comes to future of AI integration into police work, Kafteranis et al. (2023) make a very clear statement: “The planned decategorisation of AI-driven crime analytics as high-risk, as part of the ongoing negotiations on the EU AI Act (European Commission, 2021/0106, COD), may be aligned with the realities of police investigations in the digital age, but remains predominantly effectiveness-centred”. The authors criticise that a focus on effectiveness does not consider the potential risks and challenges, such as bias or errors in algorithms, the training and validation on datasets and data. It also fails to consider multiple social concerns such as privacy and non-discrimination to the fair trial principle. In their own terms: “Such concerns suggest that the exceptions suggested by the Council’s Compromise Texts and General Approach to the EU AIA should be treated with caution and require clear checks and balances”.

In sum, revision requires much more scrutiny of these processes. In addition, they claim the adoption of EU design standards for an ethical and responsible use of AI Applications in the future. This requires much more cooperation between stakeholders, including technology experts and end-users, policy- and law-makers, civil society, and affected individuals (Kafteranis et al. 2023).

Facing so many democratic and technological changes, with new crimes and new technologies, Gelles et al. (2019) examine how to respond to them proactively and positively, but also realistically. The fundamental change that law enforcement is undergoing is undeniable, and new policing strategies are therefore needed. They also point out that the often-polarised debates

between “enforcement” versus “community policing” are approaching each other with various nuances. In the end, the goal of policing should be to generate a safe community environment, so the mix between law enforcement and community engagement merges at different levels. The following graph shows the drivers and changes of the new ecosystem of policing.



Source: Gelles et al. (2019). Available at Deloitte Insights.

In this figure the future challenges in AI policing used by LEAs are visibly represented:

The how of policing: New tools. They are the ultimate exponent of change, also in the police station. The biggest challenge lies in how to adapt these technologies to their environment.

The what of policing: New forms of crime. Similarly, such developments are also at the disposal of criminals, taking advantage of them on several occasions.

The who of policing. A changing workforce. The problem is not the technology itself but the impacts it may have. It is also necessary to take into account the expectations of younger generations in the police forces in relation to technology and their profession.

The where of policing: Changing communities. Clearly, change is a social transformation, not just in policing. That is, demographic and technological changes distort interactions with LEAs as we knew them, so other relationships will have to be rebuilt to protect citizenship. This means many challenges at the communication level, with new media, for example.

In short, technological advances, and specifically the development and implementation of AI, must play a supportive and empowering role in human capabilities. It is therefore a question of finding a balance that generates holistic work, under human control, but with technological strengths that promote effective, respectful and transparent police work with and towards society. It is not a replacement for humans, but a complementary and empowering use that must be managed and

regulated based on a collective debate. Technology itself offers the tools for management under constant criticism of the population, and without its acceptance, there is no trust, and consequently, effectiveness is lost.

For instance, in the case of the aerial drones, Miliaikeala et al. (2018) study the perceptions of police legitimacy and public attitudes towards aerial drones. They demonstrate the importance of moral and positive affective feelings toward police, such as respect, obedience, and confidence, for public support of law enforcement in the use of Unmanned Aerial Vehicle (UAV) in various types of police activities. This supports the notion that police ought to increase and maintain positive and strong relations with community members to ultimately increase overall public receptivity and support for UAV use within policing. Further, having confidence in police will ultimately help make community policing and police-community relationships strong and effective (Hawdon et al., 2003). This study also adds to previous literature that demonstrates receptivity to UAV is highly contextual and varies by the way in which they are utilized. It is clear that UAV use within traditional police activities appears to garner higher support compared to applications that reflect a proactive, yet ambiguous, utility.

However, explicit and implicit social forces appear to be underlying factors that determine public support for police UAV use. Future research should continue to examine latent attitudinal variables to develop a framework that is able to assess public attitudes within a community where a law enforcement agency may implement UAV technology. Given the utility of this new technology for surveillance and the current level of tension in police-citizen interactions, it is critical for police departments to find effective ways of implementing UAV into police operations that will improve, rather than exacerbate, community relations. A relevant example is the Black Lives Matter movement. As it criticises the global campaign to ban the use of facial recognition systems as a form of mass surveillance, which, according to Amnesty International, "amplifies racist policing and threatens the right to protest" (AI, 2021). Thus, by demonstrating the value of this technology in dangerous situations and the transparency of its usage, UAV have the potential to enhance the fundamental mission of police to serve and protect the community.

In the words of Kitsos (2020): “As we are heading towards a future of widespread adoption of AI technologies by many actors, it is becoming increasingly necessary to clearly define the data protection and privacy risks and the legal framework applicable in their use, even more so when LEAs are involved in the tasks” (Kitsos, 2020:5). This is precisely the overall objective of the European popAI project.

In conclusion, LEAs must take advantage of the mechanisms that AI offer to modulate them in a policing respectful of human rights, which protects without the costs being possible discrimination due to human carelessness in not controlling AI. To illustrate it, the following subsections exemplify the future challenges in predictive policing, automation bias and Human in the Loop.

2.2.1 Predictive policing

Algorithmic predictive policing systems are increasingly being used to prosecute criminal activity. The use of AI in predictive policing is defined in the following terms: "Its use in predictive policing to forecast crimes in time and space is largely an exercise in spatial statistics that in principle can make policing more effective and more surgical" (Berk, 2021:1). Furthermore, at the empirical level, the author emphasises that although these are modern predictive policing products that are analysed virtually, the content comes from crimes committed in the past, which would be the 'raw material' for future prediction. In other words, the probability of a crime occurring at a particular place and time is predicted from previous input data. Hence, there is a correlation between space and time. There are also systems that are person-based, predicting who will be involved, both as perpetrator and victim. Ultimately, you can change the variables, whether they are places, people, groups, or incidents (Castets-Renard, 2021).

McDaniel et al. (2021) explore how predictive and AI technologies are growing gaining in prominence and at an unprecedented rate. Powerful digital crime mapping tools are being used to identify crime hotspots in real-time, as pattern-matching and search algorithms are sorting through huge police databases populated by growing volumes of data in an effort to identify people liable to experience (or commit) crime, places likely to host it, and variables associated with its solvability. Facial and vehicle recognition cameras are locating criminals as they move, while police services develop strategies informed by machine learning and other kinds of predictive analytics. Many of these innovations are features of modern policing in the UK, the US and Australia, among other jurisdictions. AI promises to reduce unnecessary labour, speed up various forms of police work, encourage police forces to apportion their resources more, and enable police officers to prevent crime and protect people from a variety of future harms. However, the promises of predictive and AI technologies and innovations do not always match reality. They often have significant weaknesses, come at a considerable cost and require challenging trade-offs to be made.

As Berk (2021:1) summarises: "There are widespread concerns about the use of artificial intelligence in law enforcement. Predictive policing and risk assessment are salient examples. Worries include the accuracy of forecasts that guide both activities, the prospect of bias, and an apparent lack of operational transparency."

Two criticisms of predictive policing are as follows. On the one hand, as far as the dissemination and utilisation of crime forecasting are concerned, Ratcliffe and McCullagh (2001) argue that how information is transmitted, and officers' priorities are two key pieces of information that can be misrepresented. They also stress that accurate forecasts are not the only factor that guarantees improved police performance. On the other, Bennett Moses and Chan (2018) note that LEAs are purchasing predictive policing software when they see inefficiencies in their forecasts and to try to offload workload. However, such practices come with some concerns, if the algorithm is not well trained and the crime reported may not correlate with the crime committed. In addition, they

warn of the danger that over-policing in disadvantaged neighbourhoods may pose in terms of racial bias.

In the same line of indicting neighbourhoods under a surveillance state, Kaufmann et al. (2019) explore different empirical patterns that are subsequently translated into crime forecasts. In short, there is a body of literature, also from legal scholars such as Fuster (2020), who emphasises the concerns of predictive policing or fatal recognition, which allow for the automatic identification of individuals, and AI applications in criminal proceedings that also calculate the risk of recidivism. Moreover, the common point from all these works is that discussions need to be accompanied by ethical and legal regulations.

2.2.2 Automation bias: definition, characteristics and risks

Automation bias (AB) can be described as the "tendency to use automated cues as a heuristic replacement for vigilant information seeking and processing" (Mosier and Skitka 1999). Once again, in line with the thesis of Strauß (2021), AI carries a high potential for innovation, but also serious risks that need to be addressed if AI is not to become the worst technological threat ever. To this end, the author proposes a conceptual approach to approach AI in a more constructive, risk-aware way, understanding that Deep Automation Bias (DAB) is a problem inherent to the use of AI in societal contexts. In his own terms:

> "DAB represents a systemic metarisk that can be a useful reference point to assess the risks of AI systems. […] Apparently, it is always a matter of how technology is applied in particular application contexts and how its design relates to the corresponding individual, institutional, societal and ethical requirements. The crux is how to assess this and how to understand what kind of risks the use of AI bears" (Strauß, 2021:1).

Thus, it is from this conception as a starting point, as a sociotechnical meta risk, that this section begins. Indeed, Kupfer et al. (2023) describe the Automation bias in a similar way:

> "Automation bias has been found to be a serious problem in contexts of AI-based decision support systems (Mosier and Skitka, 1999; Goddard et al., 2012; Lyell et al., 2018; Davis et al., 2020), and violates ethical recommendations (Hunkenschroer and Luetge, 2022) as well as legal requirements like Article 22 of the GDPR (The European Parliament and the Council of the European Union, 2016) or the EU AI act (European Commission, 2021) that call for human oversight" (Kupfer et al., 2023:12).

The aim, therefore, is to create an alternative analytical framework, based on the conceptualisation of DAB, which improve practical problem awareness. The author warns that social problems cannot be solved by technological means alone, which seems to be the dominant trend. Therefore, there is literature that argues for the need to include social and ethical issues. In this regard, Kafteranis et al. (2023) argue that a holistic approach that protects the individuals affected (Mantelero, 2022) is essential when AI is linked to law enforcement. Indeed, human rights considerations must be

addressed, especially in terms of privacy and data protection, within an ethical and legal impact assessment (FRA, 2020). Other authors sharing this line of research are Strauß (2018), Edwards and Vaele (2017), Selbste et al. (2019), Wong (2020) and Tsamados et al. (2022).

Ultimately, societal concerns need to be addressed in a contextualised way, as there are different forms of automation depending on the use of AI. As stressed by Strauß (2018):

> "AI basically implies a higher degree of automation than any other technology. In other words, AI-based technology represents a sociotechnical system that enables and fosters automation at different levels. Consequently, a problem-oriented assessment of the sociotechnical impact of an AI system involves gaining knowledge on the basic functionality including the degrees of automation of the system. The crux is that this is not easy to determine and highly context-dependent" (Strauß, 2018:7).

However, the predominant literature advocates describing what should be automated, but the gap lies in why and where human scrutiny is needed, i.e., critically analysing each context to avoid "AI-based automation overrules human autonomy" Strauß, 2018:5). Furthermore, the authors justify this thesis as follows: "The severity of this risk depends not only on the overall explainability but also on the plausibility, reliability, predictability and intervenability of the automated system. Such problems cannot be solved by technical means alone" (Strauß, 2018:5-6).

Otherwise, without due critical reflection or scrutiny of the AI results, LEAs could fall into the risk of automation by accepting the computer-generated outcome, from a technical system, which is called automation bias (AB). This tendency will have societal impacts, not only in terms of individual human rights but also in a broader sense. As the authors claim: "as a wider consequence, society then becomes even more dependent on AI which increasingly produces an impact on society and individuals that hampers alternatives" (Strauß, 2018:7).

In sum, human control needs to be handled in AI systems. Indeed, Schemmer et al. (2022) highlight some of the added capabilities of humans, such as intuition, creativity, and commonsense. To this end, these authors also advocate for this perspective, which can be called 'hybrid intelligence' (Dellermann et al., 2019)". The authors define hybrid intelligence as the ability to achieve goals by combining humans and AI, thereby achieving results superior to what either could have achieved separately. As mentioned above, despite having multiple advantages, such as processing significant data volumes), but also challenging implications, 'evoking human bias that negatively affects the outcome of hybrid intelligence" (Challen et al. 2019).

2.2.3 The role of the Human in the Loop

The Human in the Loop (HITL) concept refers to human participation in the decision-making process of a machine learning model. In other words, it is an interaction in which preconditions are generated, thanks to the automatic learning algorithm, and subsequently, there is a human review. In this review process, the results can be corrected or adjusted. In short, it is a process that draws on technological

and human strengths, under the supervision of the latter, in the training of algorithms. It is important to note that human review in a loop is a human scale, as it can no longer increase the level of problem identification that automation achieves. Thus, Clyde (2021) highlights the current debate on the limited scope of the HITL for AI accountability. He asks the following question:

> "What is it about automated decisions that lead to this wide variety of issues? For some, the problem lies in that automated decisions lack scrutability. Scrutiny requires explainability and accountability. A party must speak on behalf of the algorithm and faithfully explain how the algorithm made a decision. Or the algorithm must be transparent and explainable to speak for itself. Essentially, an algorithm must be communicative with its questioners and engage in the kinds of justification humans do with each other naturally"

In the face of the current boom in automated decision-making systems, he proposes data protection and transparency (with due debate on how they work, with public and institutional scrutiny) in the use of these systems, in order to protect citizens.

In relation to police interrogations, Noriega (2020) analyses the effects of AI on racial and gender bias, cooperation, and false confessions. The latter suggests that the racial and gender bias influencing false confessions may be due to the two-fold bias occurring within the interrogator-to-suspect dynamic, referenced in this study as "the Bias-Uncooperative Loop." She argues that applying artificial intelligence AI within the interrogation room may minimize both the bias occurring in the dynamic. It also suggests the potential for cooperation between the two parties can be conditioned by programmable similarity; whereby artificial intelligence AI can mimic the racial, ethnic and/or cultural similarities of the suspect in question. This is reflected in research in different arenas (not inclusive of interrogations) to have an effect on enhanced improve comfortability and cooperation with AI. This study assumes similar results within interrogations.

2.3 Some key findings

In this section, the main current and future challenges of human interaction with AI in LEAs will be summarised. The literary mapping of the main debates has made it possible to highlight the thesis that Dechesne et al. (2019) point out, according to which it is impossible to fully anticipate the effects of the use of new technologies in the law enforcement domain. Nevertheless, in the particular case of the pop AI project, it has been suggesting foresight scenario based on social controversies as a good methodology to anticipate risks. It, therefore, helps if the introduction of new technologies is treated as a social experiment: a process that must be continuously evaluated. As a result, continuous ethical reflection and evaluation around the application of AI is required by the police, with emphasis already in the very first pilot phase.

In other words, despite the European ethical and legal contributions, mainly the AI Act, to achieving responsible or ethical use of AI by LEAs, there is not yet a long-term, grounded model. Therefore, there is a need to further develop a robust ethical framework, where such threats are

minimized while cultivating the benefits that AI can provide. In this sense, the ethical framework for the use of AI by LEAs provided by popAI's D2.4 can be considered a step in this long process.

In sum, a more cooperation and a holistic approach is claimed for the development and use of AI. New frameworks and guidelines are required for the development and use of AI within the police organization that will tackle all ethical concerns, risks, and vulnerabilities present in the police domain. These new tools should address the actions and responsibilities of all stakeholders in law enforcement; not just the police, but also the local government and the proper Ministry of Justice, Defence or Security, which sometimes makes high-level decisions on the business processes of the police organization. As a result, while designing an AI system, the broad picture of the contextualised criminal and security situation of each European Member State will be ensured, as well as their general societal impacts.

Furthermore, the use of AI systems must be properly explained not only to LEAs, but also to the public, since trust is only possible on the basis of understanding such systems. To this end, the transmission of information must be clear and transparent, not only in terms of objectives or uses but also in terms of the limits and scope of these new technologies. Citizens must feel involved not only in the benefits they can bring, but also in their challenges. The ethical and legal balance between security and privacy can be only found through a critical and participatory analysis of the situation among the above-mentioned actors.

In terms of the future, a new ecosystem of policing can already be envisaged (Gelles et al., 2019), with new tools, new forms of crime, changing workforces and changing communities. In the face of so much technological transformation, one premise is shared in most literature debates: AI should have a supportive and empowering role in human capabilities, but always under human control. As will be seen in the following sections on policy labs and police interviews, this premise is shared by the vast majority of people participating in the popAI project. Finally, the human control role, and the challenges it entails, has been exemplified by policing systems such as predictive policing, automation bias, or the role of Human in the Loop.

3 Insights from the policy labs

In this section are summarized the key points that emerged in the policy labs on the organizational aspects of incorporating police in the workforce (definitions, expectations, perceptions), the impact of tech on the police from a legal, ethical, social aspect.

3.1 Police Academy Bratislava

The policy lab conducted at the Police Academy in Bratislava assessed most aspects through one of the basic legal frameworks, which is the upcoming Regulation of the European Parliament and the Council, which lays down harmonized rules in the field of AI (Artificial Intelligence Act). Several

comments were made on the draft of this regulation, one of which was the Joint Opinion of the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) 5/2021. There are several aspects (among other things) important for the law enforcement in Slovak republic and/or using the AI tools in law enforcement:

- The use of AI in the field of police work and law enforcement requires precise, predictable and appropriate rules specific to the given area, which must take into account the interests of the persons concerned and the impact on the functioning of a democratic society.
- EDPB and EDPS call for a general ban on any use of AI for the automatic recognition of human features (face or gait, fingerprints, DNA, voice, keyboard typing and other biometric or behavioural signs) in public spaces in any context (therefore, in order to ensure compliance, according to Article 5 of the proposal, large-scale AI systems for remote identification should be prohibited in online spaces – point 23 of the opinion),
- An equally important point of the opinion is number 33, according to which the EDPB and EDPS recommend that both public authorities and private entities prohibit AI systems that categorize individuals based on biometric data (for example, facial recognition) into groups based on ethnic origin, gender, as well as political or sexual orientation or other grounds of discrimination prohibited under Article 21 of the Charter.

The participants agreed that AI tools daily help in law enforcement not only in the Slovak Republic, while this enforcement must have clear ethical and legal boundaries.

- Information systems: Several of the information systems used by the police in the Slovak Republic are standard databases without AI features. However, there are some exceptions: for example, the system from the company SOITRON, which is installed in several police patrol cars, meets the characteristics of an AI system and recognizes the license plates of all vehicles that come into its field of vision. Following this, the workshop participants agreed that it is crucial to take into account ethical aspects when using this and similar systems, as, for example, taking photos of recognizable drivers' faces in vehicles exceeding the speed limit may interfere the GDPR.
- Social networks: Some participants of the workshop presented information about the fact that at the level of the Ministry of the Interior of the Slovak Republic, in cooperation with some other authorities in the field of law enforcement, tools with AI elements are being prepared, through which they will search and evaluate information found on social networks. In this context, it is often considered in the Slovak Republic that, for example, contributions to discussions on the internet should only be allowed if it is a so-called verified user account (i.e., it must be clear who is the user). In this regard, too, the question arises as to whether this requirement is in line with ethical principles and freedom of speech. Law enforcement agencies must have effective AI tools to monitor social networks in order to prevent crimes.

- Drones: On the use of drones in law enforcement, it has been pointed out that if the drones are equipped with a device that makes a video recording, the face of individual persons may be recognized, which may violate their personality rights (in Slovak republic these are mainly governed by the Civil Code).
- Prevention: Participants highlighted that it is necessary to use AI tools in law enforcement, but there should also be an emphasis on prevention at all levels to reduce the risk of criminal acts, not only on the Internet. The question arises whether prevention should not be started as soon as possible, i.e., at elementary schools (familiarity with law, ethics, risks of social networks, etc.). For this purpose, appropriate technical equipment is needed that can process and evaluate a large volume of data. If AI tools were able to collect and evaluate data on social networks on the basis of relevant algorithms so that prevention would be more effective, appropriate ethical standards for the use of AI tools must be created too. The use of AI tools and the creation of relevant ethical standards is also crucial because a large part of criminal activity is moving from the "physical world" to the world of social networks.

In sum, in this policy lab we can find some points in common with the theoretical debates of the literary bodies seen above, such as the need to create ethical standards to address the new challenges of AI, such as new actors and crimes in the current ecosystem of policing (Gelles et al., 2019). In this way, the current polarised landscape of debates between 'enforcement' versus 'community policing' can be broken. This also requires exploring new networking coalitions between different actors, not just LEAs. As Kafteranis et al. (2023) point out, this demands much more cooperation between stakeholders, including technology experts and end-users, policy- and law-makers, civil society, and affected individuals.

3.2 Hellenic Police

In the stakeholder policy lab conducted with the support of the Hellenic Police, it was argued that predictive capabilities based on machine learning (ML) and AI would improve the existing system of crime recording that provides statistics based on collected data including type of crime, location, gender, and age of offender, etc. The objective was argued to be the appropriate and targeted allocation and distribution of resources minimizing potential human biases. Data bases could be enriched with additional types of data and further parameters creating a new data ecosystem which is not easily processed manually.

As a result, an advanced AI system could advise or support decision making on different levels of policing. The potentiality of explaining and understanding crimes would be of social benefit. Thus, it would assist organizations not only to predict but also to act preemptively and even guide policy making through evidence-based approach. However, developing and implementing such a system could raise great concerns on the foundations of democracy.

In addition, the risk of impartial control and bias of the system was also discussed, highliting that there is a general problematization around data-driven systems: they rely on existing statistical data, collected, and interpreted by the police, leading to a negative feedback loop. Furthermore, over-reliance on a system carries great risk. A regular practice may entail the risk of producing an overconfidence of the LEAS towards the system, and therefore, undermine the need for a critical analysis of the outcomes, assuming them as valid without carrying out an evaluation process with the due experience and critical thinking. Another issue that was raised and is often overlooked is the necessary sensitivity regarding the crimes committed by children.

AI systems need to support the decision making not to make the decisions. There should always be human supervision in the whole lifecycle of the AI system and the final decision to be made by humans. Some of the organizational recommendations stated are the following:

- Sandboxes for the implementation of the systems in protected environments/settings should be developed. In this way, explainability and cyber security could be further explored without putting risks on data subjects.
- Regulation to promote and ensure citizens' awareness regarding the existence and implementation of an AI system and enable objection to potential unjust decisions.
- Establishment of AI observatory body: potentially an independent authority with technical, organizational, and practical capabilities to assess the system's compliance with legal and ethical rules and regulations set by interdisciplinary committees and stakeholders.
- Certification of system accountability through specific processes and frameworks; algorithm audit: "democratic" data - "robust" algorithm; what data are collected, for what purpose, qualitative assessment, potential bias etc.
- Need for qualified staff/users and model/technology designers with continuous training processes in place. Relevant certifications to be described in the legal framework.
- Legal harmonization of AI usage at the national and European level. Legal framework to ensure data protection and enable judges' intervention regarding permission for the data usage.
- Interdisciplinary assessment of the whole process of development, implementation and regulation of the system ensuring also ethical processing of data.
- Before system procurement, the technical specifications must be accepted by social organizations and agencies while during the implementation, it needs to be checked by representatives of social and other bodies and to give an opinion that the system covers the institutional framework.

Participants also discussed how an AI approach would benefit the prevention of traffic accidents and the ethical dimensions of a potentially emerging mass surveillance systems. Profiling and targeting a driver before an accident or highway code offence has been committed is controversial

as is the creation of such a cameras network that includes body worn cameras (as emerged from the discussion). Archival data related to verified offence of highway code -especially causing accidents- can be used to train algorithms in scoring driving behaviour as low, medium, and high risk.

Participants discussed that interoperability, traffic data in relevance to population intensity for example, could be utilized by Road Traffic Police Division and the Ministry of Transport. For instance, the system could identify locations where highway code offence has been repetitively occurred patterns- so potential correlations can emerge to inform the respective governmental bodies.

Furthermore, such a system would allow the localization and prevention of illegal car races. DIts developing involves technical difficulties, as the translation of highway code in an algorithm is very challenging, including exceptions in algorithmic parameters; i.e, dangerous maneuvers. The potential risk of profiling was also raised in the discussion threatening human rights. This system could be used as mass surveillance restricting liberty, freedom of movement and freedom of expression as well as privacy and autonomy. In any case, drivers should be aware of what data is collected and for what purpose. The described system also carries the risk of abusing sensitive personal data, i.e biometrics. Risks on potential bias based on driver's gender and make/model of the car were also raised.

In addition, participants discussed potential abuses of the system as third parties, i.e insurance companies could use it for different purposes. From a legal perspective, there is a data ecosystem created that challenges the ownership of the data. It would be unclear who owns the relevant data, i.e., if some cameras on a motorway are public owned by the ministry of transport, but police body cameras are owned by the police so the data wouldn't be in one place, and the data controller would be unclear. Challenges to privacy and data protection emerge also in the case of data collected by body worn cameras.

Regarding further organizational and regulative recommendations, the main ones are:

- Creation of data intermediaries: bodies that provide -free of charge- their services to citizens to manage third parties' data based on their preferences. In this way, when police use data originally collected for other purposes, citizens will be notified regarding the process, the purpose, storage, etc. This process describes the right to informed consent in an automatic way.
- Open data for accountability and transparency purposes and an entity/civil society organization for data benchmarking.
- Operators' training and supervision and a clear institutional operating framework justifying access to the system and describing the process of an accountable regular control of the use of the system (how, who, and why can use the system data).
- Clear legal framework on protection/restricted use of biometric data and copyright issues.

- Legal frameworks relevant to data protection in the context of the case study: GDPR, AI Act, Data governance act.

Concluding the discussion similarly to the first case study, **participants concluded that the focus should be social benefit.** In this context, the system could be interoperable with other governmental bodies. The system could produce statistical reports and provide specific classifications (e.g., traffic accidents signaling a lack of infrastructure) that can indicate potential causes of accidents.

In this case, the Hellenic policy lab begins and concludes with the same thesis: the objective of IAs should be to promote social benefit. To this end, human and preeminently impartial control and risk must be critically reversed by LEAs but also by fostering citizens awareness. Moreover, all this must be regulated in legal frameworks and conveyed in continuous training. In other words, as mentioned in the literature review section, control must be translated into practice with ethical and legal instruments that are applied to the constant, critical and contextualized review of the AI systems in LEAs. In their own terms:

"Apparently, it is always a matter of how technology is applied in particular application contexts and how its design relates to the corresponding individual, institutional, societal and ethical requirements. The crux is how to assess this and how to understand what kind of risks the use of AI bears" (Strauß, 2021:1).

In short, the goal remains to strike a balance between public trust and security (Kitsos, 2020) to overcome potential discriminations that could arise without proper human supervision.

3.3 The Police Department of the University for Public Service in Bayern

The policy lab conducted by the University of Applied Science – Police Affairs (HfoeD) first focused on how command and control centers face significant challenges in the deployment of units for operations. Following a discussion on how an AI-based suggestion mechanism on which units to deploy could help make relevant and pertinent decisions for the best possible management of an operation, participants concluded that:

- AI should be used to ensure police officer receive timely information about the crime scene.
- The legal dimension needs to be taken into account to see to what extent automated queries can be used; clear limits are essential.
- Traceability must always be given - no black-box approach.
- Automated processing must always ensure the possibility of human intervention.
- LEAs representatives recognised no game-changer role of AI in mission control, although it could be more useful in metropolitan areas.

Moreover, participants discussed how processing dozens, even hundreds, of suspected Child Sexual Abuse Material (CSAM) cases poses challenges to LEAs on a daily basis, both emotionally-psychologically and organisationally. On the use of AI-based solutions that can help with both case processing and documentation, as well as identifying potentially substantive leads of relevance to investigation, participants conclude that:

- AI can help identify perpetrators more easily, although it cannot replace the competencies of the investigators.
- AI systems should not be a black box: process tracking, and human intervention must remain possible. It is therefore crucial to educate people.
- A lot of negative perceptions are due to the way public media report AI issues (e.g. job killer, surveillance state).

In conclusion, it emerged that the second scenario is more likely to see the implementation of AI-based solutions, as AI allows the analysis of a greater amount of data. In both cases, participants agreed that black box approaches should be avoided and recognised the need to ensure human intervention if and where necessary.

AI-related Key points addressed during the policy lab:

1. **Actors:**
    a. Public media feeding negative perceptions on surveillance and unemployment
    b. Citizens
    c. Policymakers
2. **AI characteristics:**
    a. AI should not be a black box: Traceability and human intervention should be made possible.
    b. Education is crucial
    c. Minimizing potential human biases when providing statistics
    d. AI systems need to support the decision making not to make the decisions. There should always be human supervision in the whole lifecycle of the AI system and the final decision to be made by humans
    e. Focus should be the social benefit
3. **Legal dimensions:**
    a. Need to be taken into account

b. The use of AI in the field of police work and law enforcement requires precise, predictable and appropriate rules specific to the given area, which must take into account the interests of the persons concerned and the impact on the functioning of a democratic society

c. Regulation to promote and ensure citizens' awareness regarding the existence and implementation of an AI system and enable objection to potential unjust decisions.

d. Establishment of AI observatory body

e. AI tools daily help in law enforcement not only in the Slovak Republic, while this enforcement must have clear ethical and legal boundaries

4. **Ethical dimensions:**

a. Concerns on the foundations of democracy. The risk of impartial control and bias of the system was also discussed

b. Systems rely on existing statistical data, collected, and interpreted by the police causing negative feedback loop

c. Over time, end users might feel "too comfortable" with the system so that they do not challenge the outcomes and they don't use their critical thinking and experience

d. Profiling and targeting a driver before an accident or highway code offence has been committed is controversial as is the creation of such a cameras network that includes body worn cameras

e. State surveillance

5. **Type of crime:**

a. AI can help to cope with the emotional, psychological and also organisational burden in cases of CSAM material

b. Crimes committed by children

c. Help to identify perpetrators but not a substitute of human

d. AI should give timely information about the crime scene

e. AI would improve the existing system of crime recording that provides statistics based on collected data including type of crime, location, gender, and age of offender, etc.

f. Support decision making

g. Explaining and understanding crimes would be of social benefit. Such a system would assist organizations not only to predict but also to act preemptively and even guide policy making through an evidence-based approach.

6. **Functions:**

h. AI approach would benefit the prevention of traffic accidents

i. License plates readers

j. Social network analysis

k. Drones equipped with video recording

In conclusion, the session highlights different scenarios with a plurality of actors, characteristics of AI systems, legal and ethical dimensions, types of crimes and functions. Thus, through these scenarios, it is possible to see in practice the main theoretical debates discussed above, both the potentialities the challenges of AI. Regarding this unbalanced concern, Campbell (2018) conclude likewise: "AI offers unprecedented capabilities to acquire and analyse big data, it is not surprising that the law enforcement community is interested in applying AI for its purpose". However, as stated in the policy lab, legal and ethical limits need to be regulated in order to overcome some of the implications outlined by Kitsos (2020) in the specific case of LEA: algorithmic bias, mass surveillance, privacy, and data protection. Once again, the policy labs are not only in dialogue with each other, but also with the main literature debates, in advocating for a human control that does not divert the positive potential of AI's supportive role from the negative and thus lose the scope of such technologies, which is social benefit.

3.4 Municipal Police of Madrid

The Spanish Policy Lab was organised by the Municipal Police of Madrid with the aim of serving as a platform to share knowledge, experiences and perspectives on the impacts of AI in police practice. The event was divided into two parts, each with a case study, and the conclusions. On the one hand, the use of closed-circuit television (CCTV) systems and, on the other hand, the application of drones for the search and location of individuals.

The focus of both discussions, in an interactive format, was on privacy protection, ethics and accountability, citizen participation and good practices in the training and education of officers. It was attended by 30 participants, mostly police officers, some of them withAI experience, but also a postdoctoral researcher, NGO's working on the protection of civil rights and privacy and technical advisors from the Madrid City Council. The event was held online, with an initial combination of cases studies, followed by debate and open discussion sessions with active participation and additional information and communication channels provided in order to future collaboration and information exchange. Their resulting conclusions and recommendations are set out below:

First case study: use of CCTV in police activity

In order to address the first case on the use of CCTV in police activity, the following generic aspects were addressed earlier:

Privacy protection should be promoted by establishing protocols that clearly define who and for what purposes can access the data and by protecting personal data while using recorded images. As far as personal and confidential information is concerned, the uses of personal biometric data should be defined on a context-specific basis. On data accountability, participants point to the need for a data controller is needed to promote and control proper use and discuss which profile would be more reliable between the police or the politics sphere. In this sense, the proper use of data is highlighted through the potential application of restrictive or utilitarian approaches, depending on the context. In contrast, misuse, which is often about using rather than obtaining data, implies a loss of privacy on the part of the citizen. To overcome this challenge, information and transparency should go hand in hand to explain the proper use of data and to raise citizens' awareness of their evolving perception of privacy. It is necessary to establish levels of data protection. In addition, AI systems must be under human supervision and participation should be encouraged to assess the balance between privacy and security.

Regarding the CCTV systems specifically, the following conclusions can be drawn:

In terms of their use, CCTV systems highlight this imbalance between increased security and loss of privacy, so it is necessary to address what this loss of privacy entails and what constitutes privacy in public spaces. In terms of legislation and protocols, the participants find it relevant. Finally, with regard to the data collected, there is a need for them to be safeguarded.

With regard to AI in general, there are bias in the development of the systems and there is a need to justify the purposes of their use, to conduct citizen information campaigns and to build a relationship of trust between citizens and the use of AI, but also in police judgement. For this, it is needed to inform citizens about the use of AI and drones, respecting the premise of transparency and involvement in decision-making about their possible use. Furthermore, it is necessary to overcome the lack of training and knowledge, and to break the persistent dichotomy between the technical part and the tool to combine it. Finally, an ethical approach to training is needed.

Second case study: use of drones to search for people

Firstly, in comparative terms, drones resemble CCTV cameras in their privacy concerns, but their mobility and versatility increase the related challenges. Secondly, it is proposed to create platforms or commissions for the use of AI in security that include civilian, police, technical and political representatives to regulate and supervise it. Thirdly, there is a need to establish proportionality in the use of AI and its purpose. Security forces in particular need to establish a scale of proportionality. Fourthly, participants highlighted how technology has impacted on the lives of society, which is why there is a need to inform society about the uses of AI at all levels of security. Finally, regarding the involvement of police officers in the development of algorithms, they discuss the fact that they want reliable and safe AI, and also that they need to be involved in the process so that they can provide their expertise in determining what is detected and thus improve the reliability of the AI. Finally, the importance of AI-related training and education is stressed.

Conclusions

The event represented a space to address the following challenges and opportunities for the integration of AI in the police field. Fundamental aspects for a responsible and ethical application of AI in public space have been discussed on the use of AI in policing, in particular through the cases of CCTV and drones. In particular, the importance of protecting privacy and ensuring data protection, the need to establish clear protocols and adequate security levels as well as human control of AI and the fostering of a relationship of trust with society based on transparency and clear communication. Also, their participation in decision-making on the uses of technology and the importance of creating participatory and representative platforms or commissions from different sectors. Another relevant factor is the proportionality of the uses of AI, also in police forces. This should be translated into information for society, explaining the specific application and its benefits.

The relevance of police officers for training and education in the use of AI, due to their expertise, is highlighted when developing trustworthy algorithms.

To summarize, the Spanish policy lab format is divided into two concrete case studies, which represents the logic described by Ezzeddine et al. (2023:8) when they admit: "AI use should be justified, legitimate and only used for declared purposes" Ezzeddine et al. (2023:8). Ultimately, in advocating for the justification of uses, the participants start by putting it into practice in the session itself through these two case studies. On both occasions, the starting point is a resolute approach, with an emphasis on data protection regulated by clear rules and a human data control post to provide this oversight. Such parameters would foster information transparency for citizens and thus understand the balance between privacy and security. It is also intended to overcome the dichotomy between technical training and knowledge, understanding that both are self-consistent and depend on an ethical understanding of the proportional uses of such AI systems, both for LEAs and citizens. Throughout, it starts from the individual and collective liberal premise mentioned previously, according to which: "Security and public safety are key prerequisites in the function of societies. Citizens expect governments to fight crime and disorder as a means to preserve a safe environment where private life is protected and respected and business is allowed to flourish" (Kitsos, 2020).

3.5 The Local Police of Turin

The policy lab organised by the Local Police of Turin was launched from a concrete case study: the implementation of an AI in video surveillance network following a brutal murder in the city. The aim of the first part of the session was to discuss the advantages, disadvantages, regulations, ethical complexities, as well as propose some recommendations on the introduction of AI software in the video surveillance system. Subsequently, in the second part, the aim was to evaluate assess both the benefits and recommendations for the Ethics toolbox, conceived as an outcome that provides accessible and understandable resources for LEAs and civil society. The participants were divided into three multidisciplinary groups composed of local police, legal experts and ethical experts.

Case Study: AI software in the video surveillance system

1. **Advantages:**
- Significant reduction in investigation times for low enforcement
- Enhance the public's perception of safety (still without direct correlation)
2. **Disadvantages:**
- Risk of misuse for social scoring, labeling individuals/groups, and creating prejudices and biases
- Lack of clear regulations regarding data collection, retention and access
- Indiscriminatory collection of information (although only a fraction is involved in the research)
3. **Regulations:**
- Need for clear norms and regulations (emphasizing the minimization of data collection and metadata in order to mitigate associated risks)
- Resolving specific doubts about the access of which persons and the duration of the data retention have been solved
4. **Ethical Complexity:**
- Complex ethical concerns on individual data protection, and individual and collective freedoms as well.
- Emphasis on the social relevance of the decision to implement such a project.
- Detailed examination of the invasive nature of AI usage in surveillance systems, especially by vulnerable groups of people.
5. **Recommendations:**
- Share and use existing best practices
- Conduct contextual assessment of each case by a multidisciplinary team with different experts, defining the specific purposes for which the technology will be used
- Consider the ethical dilemma that carry the unclear technological process (not biometric data collection, but latter biometrical analysis for individual identification purposes)
- Enact comprehensive legislation (including laws determining administrative offenses and the legality of these systems under specific conditions)
    - Principles of transparency, functionality, and procedural requirements
    - Principle of maintenance to prevent and correct algorithms errors and non-exclusivity of decision-making algorithms (avoiding a disproportionate focus on individuals with specific physical characteristics or in certain territories)
    - Technical and public nature, with a control based on ethical values
- Exame professionalism and ethical conduct of those carrying out the assessments through training courses and adherence to professional codes of conduct
- Verify constantly the technological progress
- Enhance transparency and clear communication with the public, fostering trust and ensuring that citizens know how their privacy and security are protected
- Adopt an ethics-by-design approach during the design phase with external stakeholders to minimise risks during the programming phase, although there is always a risk of discovering concerning aspects of the technology

In sum, this list of recommendations advocated by all the stakeholders responds to a human-controlled approach to this supporting tool, as opposed to a fully automated decision-making process because of the risks involved. Thus, this human-controlled approach to explaining systems in a transparent and clear way counteracts the perception as "black boxes" and promotes greater understanding which helps not only to protect but also to defend oneself.

Ethics toolbox

1. **Benefits**

- Responsible and effective utilisation of AI technology. To this end, training and information aspects are considered as primary safety measures, with comprehensive training to operators on the objectives and significance of their actions in the system
- In-depth academic research on the utility and impact of artificial intelligence in surveillance systems for further informed discussions and decision making between academics, policymakers, and civil society. Collective participation promotes a more conscious and responsible approach.

2. **Recommendations**

- Provide technical specifications and details regarding the toolbox's AI tools. A comprehensive understanding of is crucial for critical evaluation and scrutiny of its capabilities and data collection; and a basic training to the proficiency and responsible use of the ai system by the average user.

Conclusions

A holistic approach is needed to overcome the complexities of integrating ethical AI surveillance systems. As Kafteranis et al. (2023) argue, the scope of a holistic approach is the protection of the individuals affected (Mantelero, 2022), especially in law enforcement. To this end, human rights considerations must be addressed, especially in terms of privacy and data protection, within an ethical and legal impact assessment (FRA, 2020).

Thus, training and information play a central role in introducing an AI system into the surveillance network, not only in terms of responsibility but also of effective utilization. In addition, academic research is also essential to analyse the potential benefits and risks which need to be regulated by means of robust regulations and technical specifications to ensure proper data handling and privacy protection. In other words, as mentioned in the literature review, there is no such thing as responsible or ethical AI, only responsible or ethical human use of AI. Therefore, there is a need for a robust ethical framework, where such threats are minimized while cultivating the benefits that AI can provide.

4 Interview development and structure

The interview followed a semi-structured approach integrating multiple LEAs profiles and partners, focusing on organisational and human factor issues and the impact of potential AI-driven processes on the health and safety, autonomy or responsibility of LEAs.

In order to integrate all possible perspectives of LEAs institutions the interviews were applied to different profiles, at least five:

1. experience and recent police officers;
2. different departments (criminalist, law, security, information technologies, administrative, policy, etc.);
3. experience with AI in police department;
4. developers of AI algorithms or technologies; and
5. experience in AI policy or public policy in LEAs.

Taking into account the different profiles of the interviewees and the diverse context around the LEAs partners (Policy Academy of Bratislava, Hellenic Police, The Police Department of the University for Public Service in Bayern, Municipal Police of Madrid and The Local Police of Turin), the semi-structure interview methodology is the better option to integrate the numerous views, experiences, backgrounds and contexts. All of the interviews are anonymous but the main findings are described in the next section.

The interview is composed of four main sections (complete questionnaire at annex section). The first section is to make the first interaction with the interviewee and know if they are involved with the AI systems or their definition. This section has the objective to open the conversation and guide following questions based on the participant profile. The next set of questions inside the section of AI impact on police officers and individual work: changes, expectations and needs; is based on the individual perspective according to the officers and personnel of LEA's institutions. This section has the objective to deep inside the effects, challenges, responsibilities, boundaries or feelings about the AI systems and the individual. In this sense, this section refers more to personal experiences, individual responsibilities and background.

The third section is based on the role of the whole LEA's to open the scope to the entire organization. Consequently, each interviewee can answer from multiple perspectives according to their antiquity, job position, future vision, background, etc. Additionally, the section wants to emphasize the future responsibilities and adoption of the AI systems into LEA's organizations. Lastly, the final section talks about the perception of civil society of these new technologies, remarking on the role of the LEA's as responsible for AI and their effective application in real-world scenarios.

5 Interviews results

The objective of the interviews is to better understand what Law Enforcement agents think about Artificial Intelligence and what are the benefits and challenges of incorporating AI applications in the police workforce. The next sections cover the main results of each Law Enforcement Agencies and two AI developers' interviews. The results are mainly focused on the four main subjects: understanding of AI, AI impact on police officers and individual work, AI impact on law enforcement's organizational structure, and Relationship between AI, law enforcement and civil society. Most of the LEA's agencies were composed of multidisciplinary profiles, with multiple perspectives and, in some cases, mixed opinions.

5.1 Police Academy Bratislava

Most of the interviewees understand the AI is a tool in law enforcement as something that can search for relevant information, evaluate it, and provide LEAs with feedback that will be useful in the decision-making process of law enforcement. Most of the participants have contact with some LEA's new technologies like systems of car vehicle plates detection. Nevertheless, the application of AI systems in the institution is limited for the moment. The interviewees perceive the AI tools as useful and functional, even though in the beginning of its use it had some errors in recognizing numbers or letters. All participants agree that the use of AI tools itself does not bring any substantial risks, real risks arise more from "who" and "how" will use the AI tools and how they will deal with the information obtained from AI tools. In other words, the participants consider potential professional or moral failure on the part of humans to be the main risk when using AI tools.

All participants agree that AI tools are effective in assisting them in law enforcement so, they will welcome any additional AI tools that the future brings. The proper use of AI tools, by all means, requires a number of basic aspects to be fulfilled. On the one hand, there are personnel aspects, that means everyone who will act as a police officer and work with AI tools must be qualified, must be continuously educated and must have a high personal integrity. On the other hand, the use of AI tools by police officers must be subject to multi-level control, meaning that the "first decision" to use an AI tool as well as the "last control" of how the AI tool was used should be up to the person.

Another necessary aspect is the creation of corresponding rules at the level of the National Council of the Slovak Republic as well as at the level of the Ministry of the Interior, as well as a "timeless" general ethical framework for the use of AI tools. Additionally, adequate funding becomes a relevant factor. LEA's needs funds for the purchase of AI tools and funds for appropriate salaries of police officers.

Regarding the role of the police institutions, the interviewees associate challenges and needs in law enforcement with sufficiently high-quality and gradually developing legal regulation, specifying internal regulations, especially at the level of the Ministry of the Interior, and with the formulation of a general ethical framework for the use of AI tools. Another challenge will be the provision of

adequate funding for the purchase of AI tools and, at the same time, a motivating salary assessment for police officers. Respondents agree that the use of AI tools will be necessary in the future, especially in cyberspace. They also shared the view that although they are aware that an AI regulation is being prepared at the European level, which is likely to ban the use of AI for facial recognition in public spaces, respondents think that the public interest should prevail in this case on enabling LEA's to use AI tools to identify as many risks as possible and protect public order. The increasing use of AI tools in law enforcement may be problematic for older generation of police officers who are not used to work with more sophisticated modern technologies, but this may not be a major issue for the future personal structure of LEA's.

Lastly, corresponding to the relationship between AI, law enforcement and civil society, the interviewees agree that the use of any modern technology, not only in law enforcement, will be associated with a certain degree of mistrust on the part of civil society. In this context, however, it will be decisive whether current and future AI tools will help law enforcement, that is, whether they will continue to prove effective and reliable. If this happens - and the respondents have no doubt about it - then it will be important to transparently inform civil society about these results, which will contribute to the gradual increase of trust in AI tools. According to the participants, this trust is likely to increase naturally as young generations work with modern technologies from a young age, therefore they trust modern technologies, from their basic functionalities to sophisticated AI tools.

In conclusion, the focus must be on increasing society's trust. As previously mentioned, Almeida warns:

> "facial recognition algorithms without taking accountability for the consequences of this usage could not only lead to further discrimination and victimisation of specific communities, but also to an even greater loss of trust between the general population and law enforcement agencies" (Almeida, 2022:379).

Indeed, technology itself offers management tools under constant criticism from the population, and without its acceptance, there is no trust, and consequently, effectiveness is lost. In the case of the older generations, it will be necessary to strengthen communication-based on familiarity and respect, as proposed in practice in the contributions to these interviews.

5.2 Hellenic Police

Regarding the Hellenic Police, most of the interviewees have a firm understanding of AI and defined it as the capability of computers to make decisions on behalf of humans. AI was mostly described positively as a tool that would increase the efficiency and productivity of police officers. Some of them described AI not only as a tool to make jobs easier for practitioners but also to create new crime-preventing services that humans cannot perform. One example of this is using facial recognition to identify criminals. The commonly identified threats of AI were mostly related to the

harm they could cause to citizens, mainly due to inaccurate and unsupervised results. Additionally, two of the interviewees mention the risk of bias.

None of the interviewees had worked with AI before, and the system most known to them was machine learning; nevertheless, a few gave other examples like voice and face recognition or language processing models. Most believe the enforcement agents were not ready to use AI, saying it was "too early," highlighting the need for training and specialization. However, they perceive AI as a positive change in their daily work, improving efficiency and productivity. Opinions concerning the changes in autonomy and responsibility due to AI are varied. Some said their responsibility would remain the same, as they are always responsible for the activities they carry out, while others argue it would broaden their responsibilities. Similarly, some believe their autonomy would be restricted, while others think AI would complement their labour. Additionally, some interviewees mention that AI could not replace specific activities in their job related to emotional intelligence, creativity, or critical thinking skills but would replace administrative tasks, call center responses, case allocation, and data analysis.

The interviewees answer that AI is not in use in their law enforcement agencies, and they have no knowledge of efforts in this sense. However, they believe legal framework will be needed if these systems are introduced, ensuring compliance with present laws. Thus, legal frameworks would be necessary to enable the use of AI in courts and to protect law enforcement authorities as well as citizens.

Finally, the mentioned risks are numerous, for instance, privacy concerns, ethical concerns, and security issues. However, to improve the benefit of AI integration, the interviewees highlight the importance of protecting privacy, ensuring accountability and transparency, and working with stakeholders to provide continuous feedback and monitoring. An interviewee mentioned the importance of these efforts to maintain a trusting relationship between law enforcement and citizens. Many interviewees think that citizens are hesitant about artificial intelligence because of concerns about their personal information being used, the potential increase in surveillance, and the possibility of making mistakes. Nevertheless, they are also confident that AI could help build a better relationship between law enforcement agents and citizens as they could provide timely and responsive services, as well as efficiency in policing for crime rate reduction.

To conclude, the insights from these interviews, despite the multiple challenges to be overcome collectively, in the interaction between LEAs and citizens, are along the lines of authors such as Almeida (2022) who underlines the potential to achieve greater efficiency in the detection and prosecution of crimes by reducing economic costs.

5.3 The Police Department of the University for Public Service in Bayern

The interviewees from the Police Department of the University for Public Service in Bayern describe AI in various ways, some referring to the capability of computers to think as humans would. In

contrast, others focus on the applications like analyzing larger amounts of data, automatization, and "self-learning". A positive feature of AI they found in everyday police work is that it makes the job easier. They mention applications of AI in image analysis and video evaluation. However, they identify some moral and ethical limitations and the unreflective use of AI-generated results, highlighting the importance of transparency and comprehensibility. Some believe that AI depends on the application area, while others thought it should be used in early detection to filter larger amounts of data.

Most of the interviewees declare that there are no AI applications currently used in the Bavarian Police Force. The focus would be much more on first creating an infrastructure for it. Additionally, the actual police law and criminal proceeding law don't handle AI. Nevertheless, the police would be ready for an introduction, or even more open to it, because the AI systems can make their work easier in certain areas.

Regarding the relationship between AI systems and autonomy at work there are four main discussions:

1. **Decision-making:** AI systems can assist in providing relevant information and recommendations during the decision-making process of humans.
2. **Resource allocation:** AI systems can analyze data on crime patterns and predict where crimes are likely to occur, which could help LEAs to allocate their resources more effectively.
3. **Automated decision-making:** in some cases, AI systems may be able to make decisions autonomously without the need for human intervention. This could potentially reduce the autonomy of LEAs if they are required to follow the decisions made by the AI system.
4. **Accountability:** as AI systems become more prevalent in law enforcement, there will be a need to ensure that we are used ethically and in accordance with the law. This may require LEAs to maintain a level of human oversight and accountability over the use of AI systems, which could impact our autonomy.

Continuing with the role of the police institution and the AI systems, most of the interviewees declare three main points. First, the rule of law is always in the foreground for the police and independent work and action should therefore also be guaranteed with the use of AI. This implies a clear legal framework of regulations, operational frameworks, distribution of responsibilities and check and balances. Secondly, the institution needs to ensure that its employees have the knowledge and skills necessary to use AI systems effectively. This requires training and education programs that teach how to operate AI systems and enable employees to properly interpret data and make decisions based on insights generated by AI systems. Lastly, there should be no blind trust in AI. Humans would be necessary and decisive in the final decision-making and the evaluation of the generated results.

Finally, the interviewees have different opinions about the relationship between AI, law enforcement and civil society. On the one hand, AI systems could help police officers make more informed decisions and thus increase citizens' trust in policing. For example, AI systems can help analyze security cameras, identify suspects more quickly, and thus possibly lead to a higher rate of

crimes being solved. In addition, AI systems could help to better prepare police officers for potentially dangerous situations and thus increase their safety. On the other hand, AI systems could also have a negative impact on the interaction between police and citizens. If AI systems are inaccurate or flawed, innocent citizens could be misidentified as suspects, which could lead to a negative perception of the police. In addition, citizens may feel that their freedoms and rights are being restricted by the use of AI systems.

In summary, these interviews put into practice the controversial debate about the functions and scope of AI. That is, as mentioned in the literature review, at the theoretical level, and as seen here in practice, some of the participants argue along the lines of Rademacher (2019). The author keeps that AI has not only reached the level of human capabilities, but even surpassed them in terms of autonomy, also in detecting suspicious activities much better than LEAs, which is known as, "smart" law enforcement.

5.4 Municipal Police of Madrid

There is a wide range of interviewee profiles. Few of them are involved in the development of new technologies or AI systems. Nevertheless, all of them are aware of the new policies like drone population density model, vehicle detection cameras, automatic traffic lights or facial recognition. Most of the interviewees consider AI systems like a tool useful for complex problem-solving scenarios.

AI is mostly considered as a tool with multiple advantages like fast analysis of high amount of data, fast data management, help in the decision-making process, efficient in resources allocation, better social security perception, etc. All the interviewees recognize that the Spain Police Department does not have currently AI system. Nevertheless, they contemplate a future with more application of these technologies. Equally important, all the participants agree that the current officers are ready and with the knowledge to adapt and use new technologies and approaches. One of the participants in particular emphasizes the adaptability of the LEAs to their ever-changing context. Therefore, most of the actual current officers' claim to be prepared to use and apply the new technologies in their jobs.

One of the questions with more differences relates to the relationship of dependency between the officers and the AI systems. On the one hand, a group of interviewees are worried about the possible dependence of the institution and the officer's decision if the computer is quite good to learn and predict results in complex scenarios. On the other hand, some interviewees do not consider that this relationship can exist by the level of detail and experience of the colleges. Even so, it is possible that in the future, AI systems can develop better-trained algorithms and more decision-making participation causing dependent relationships between humans and computers.

Regarding the role of police institutions, there are two common points. First, the institutions are slower to adopt new technologies because the level of responsibility is totally different from an

academic institution or company, etc. Therefore, the integration and development of AI systems in the Police Departments need to be gradual and with caution because the possible system errors or spillover effects can provoke social damage. Secondly, most of the interviewees agree that the Institution needs, with the help of others, to ensure the security, not harmful, and privacy of the data used by these systems. Additionally, there must be a legal framework to regulate all the possible scenarios, adverse effects, assign clear responsibilities, accountability processes and check and balances protocols for the algorithms. One of the interviewees mention that it could be beneficial to have a pool of multidisciplinary experts to check and evaluate the output of the AI systems. In addition, this pool of experts should be modified periodically to ensure a decentralization of power and decision-making.

Lastly, all the participants agree that society has a good perception of technologies. One clear example of the perception was the implementation of street cameras. Currently, citizens are asking for more cameras in their neighborhoods. Ultimately, the key element of society's good response is the clear benefit of technology. In the case of Madrid Police, the perception of security and the decrease of time response were key factors for social acceptance of body cameras and street cameras. In this sense, if the communication of data usage, privacy policy, limits of the system, benefits expected, and implications of policy are well explained to the civil population, they will have a good reception of these new policies and systems.

In conclusion, adaptation to change and review of protocols and responsibilities are the characteristics that could describe such interviews. A relevant aspect that has emerged is the rotation of the pool of multidisciplinary experts. Once again, this aspect recalls the call made by Kafteranis et al. (2023) to foster cooperation between stakeholders, including technology experts and end-users, policy- and lawmakers, civil society, and affected individuals.

5.5 The Local Police of Turin

The AI's knowledge translates from (lack of) familiarity with its uses. Some of them are the following: video surveillance, which is the best-known AI system, but also others such as modular video, facial recognition, behavioral pattern recognition or license plate reading. In contrast, participants who have not worked with it show a high level of expectations. Starting with the definition, there is some confusion in describing AI as an everyday tool or as a very advanced concept. Only in two cases is it described accurately, as a system that provides and processes data by means of an algorithm or as a series of information from datasets. The common feature of AI is the reproduction of human actions in a simpler way to optimize police activities.

In terms of assessment, on the one hand, AI is positively valued for addressing the lack of resources of police forces and for its objectivity without human error or bias. Paradoxically, much emphasis is placed on human supervision precisely because of this supposed neutrality of technologies. On the other hand, AI is negatively valued for its risk of addiction and for the challenges of data processing. Furthermore, it highlights the complexity and the lack of information, especially

for the end-users, on the development of algorithms. In other words, how can they be trained and have bias.

In general, emphasis is placed on the impact of AI on LEAs, mainly in prevention, research and analysis activities. As for readiness, there is a range from easy introduction through training in the younger officers (considered the pivot for the introduction of AI) to more difficult due to the digital age gap, and even lack of readiness. The main expectation is a learning process, in which these challenges can be solved by transmitting not only technical knowledge, but also practical use between LEAs and the public. Consequently, awareness of the responsibilities involved in their use can be promoted.

Regarding the influence of AI, there are two common points stated by the participants. One is that uselessness and complementary support to policing, which will continue to maintain human relationships as irreplaceable. Metaphorically, AI should be a support in the same way that dogs are an aid to drug operations. The other common point is the greater influence in terms of security and prevention, not only for LEA's but also for end-users. However, some criticisms are levelled at the superficial approach to introducing and implementing these technologies, and the delay in formalizing universal guidelines of political institutions, despite being the most important industrial revolution ever experienced, as a participant mentions. Ethical guidelines are urgently needed because of the quick development of these technologies. Thus, the ethical implications of the perversion nature of AI must be addressed and framed in legal instruments. In addition, the new AI regulations must be translated into privacy education. In sum, more control, regulation and education on how to use AI systems is needed, especially if it affects the freedom of citizens, by processing and storing their data with a video surveillance system, for instance.

In this sense, satisfactory communication with the public is crucial to overcome some of the main concerns, which are the absence of human control or the loss of confidentiality. To this end, civil society should therefore be informed. Police interviewees advocate that only this will bring a positive perception of AI. Right now, despite the belief that there will be a gradual transition to AI, there are a variety of positions on current public perceptions, from those who believe that acceptance of AI will be more difficult in older generations and easier, or conversely uncomfortable, with youngers. In conclusion, a collective understanding of AI-related uses in policing through information campaigns is key to gain public trust in police-civilian interactions.

In conclusion, these Italian interviews contribute to the main themes discussed by other participants in the rest of the interviews. This fact leads to reaffirm the urgent need, also mentioned in the literature review, that new frameworks and guidelines are required for the development and use of AI within the police organization that address all the ethical concerns, risks and vulnerabilities present in the police domain. Based on Rademacher (2019) warning, there is a need administrative and legal challenges with clear guidance based on three needs: regulatory provisions to maintain accountability; AI law enforcement needs to be used to overcome perpetuated discriminatory traits

in human policing; smart law enforcement to decide whether we want to preserve the freedom to disobey the rule(s) of law.

5.6 Developers interviews

In the latter case, interviews have been conducted with two AI developers with experience in LEAs. The developers interviews focused on the three different moments of the system life cycle: pre, in and post processing of the information. The pre-processing is all the data management, training, data cleaning, variable selection, etc. The in-processing grasp the application and executing of the AI system or model. Lastly, post-processing is the leverage and use of the system or model output. In this sense, the developer's interviews have the purpose to cover the whole cycle of the system and the implications of their use through the ethical perspective, responsibilities, decision-making process or possible effects on the LEA's.

Regarding the in-processing and LEA's, there are four main challenges. The interviewees agree that data quality, information veracity, development of legal framework and budget constraints are the LEA's biggest challenges. The data quality can be acquired from internal sources like surveys, administrative processes, criminal report, etc.; but also, from external sources like private companies, other government institutions, non-governmental organizations, etc. Therefore, any system would be worried about the quality of the data to get the best accuracy and the best performance through multiple cases and scenarios. Besides the data quality, there is a need to answer if the data can effectively represent the real world. As with all the model representations, AI systems and the available data are needed to manage the dilemma of the real-world representation. For the interviewees, the security topic is quite difficult to cover with an AI system. The actual available data is not enough to assure a representation of real-world scenarios, for example, real time risk situations of street officers.

The third main challenge the interviewees mention is the legal framework background. Actually, there is no legal framework to clarify the limits of responsibilities, development, application or even guides for AI systems into LEAs[3]. Consequently, the interviewees consider that the LEA's are taking small steps to not commit mistakes with the citizens. Additionally, these institutional changes have a budget constraint. Like security institutions, they cannot totally trust remote services, clouds or external servers. Therefore, each research department, like criminology, ballistics, forensics or more, needs to make a high level of investment in hardware and software. Finally, the interviewees consider that all the steps can be taken with the support of multiple institutions and national policies to boost the development and adoption of new technologies.

Regarding the in-processing moment, the interviewees agree that are quite similar points with the pre-processing moment like: data quality, bias testing, optimization of the model, veracity, etc. Nevertheless, they consider that the selection of the model is crucial for the multiple problems

[3] In this sense, this is because the interviews were conducted before the adoption of the AI Act.

presented in LEA's. Additionally, they agree that the research and the constant exchange of ideas between academia and LEA's will create new models and new adaptations for complex scenarios.

Lastly, the interviewees accord three main challenges for the post-processing moment. First, the AI systems still being a black box for multiple people and even for researchers. These black boxes reduce the confidence in the algorithm, and they can mislead to incorrect assumptions or reductions of the real world. Consequently, the confidence of the AI systems is the second challenge, how can we convey trust to citizens. AI, machine learning applications or statistical models can be seen positively or negatively in society. It is critical for LEA's effective communication between the citizens and to make tangible the benefits of new technology. Lastly, the interviewees mention the challenge of who is going to be responsible for AI outputs. In this sense, they agree that a multidisciplinary team must exist to evaluate and constantly monitor the outputs of the system to improve it and double-check the results.

In conclusion, in terms of the benefits for LEAs in applying AI systems, the participants hold the same thesis as Roksandić et al. (2022), who highlight their potential to increase efficiency, data-driven processes and capabilities for concrete activities. However, and in line with the LEAs interviewed, they point out the four major challenges to be faced from an analytical perspective, but also resolutive and cooperative between different multidisciplinary actors. Once again, adapting and promoting transparency in order to train and transmit accurately which are the uses of AI systems to the population is essential to gain their trust. Indeed, as mentioned in the literature review, if they are not adequately explained, with transparency and clarity, they do not generate trust on the part of citizens and, consequently, are destined to fail. In this exploration of such interaction, the ethical issue is essential, since in the process of developing and implementing such technologies lies the privacy of citizens. What is clear is that "despite the technical and ethical challenges, the use of AI by LEAs is entering an inexorable state" (Campbell, 2018:7).

6 Conclusion

The mapping of the organisational issues, both theoretically and practically, around the AI implementation in LEA context, are an ongoing process that must be systematised and updated due not only to the rapid advancement of the conception of new AI systems, but also due to the multiplicity of new and intersecting challenges involved in their implementation.

Thus, the objective of this report was to explore the overlooked aspects of technology implementation when AI is incorporated or aims to be incorporated into existing organisational structures and processes. The report aimed to:

- Introduce theoretically the existing literature on the implementation of AI and data tools in the police sector.
- Lay out the practical implementation of AI and data tools in the police sector.
- Analyse their convergences or discrepancies.
- Harmonise a set of best practices for LEAs based on the above content.

From the above, the following conclusions can be drawn. Despite the vertiginous growth of new technologies and the distortion of old policing practices, the benefits and impacts of such transformations need to be assessed. The common threads related to the implementation of AI in the LEA context that can be drawn not only from the various bodies of literature but also from policy labs and interviews are the following:

- **Role:** AI systems in LEAs should have a supportive role, which enhances human capabilities. However, control must at all times be human. To exemplify this, the potential Human Rights concerns of the focus on algorithmic predictive policing systems, Automation Bias (AB) and the Human in the Loop role have been highlighted.
- **Use:** Starting from the above-mentioned regulation as a basis, responsible use of AI systems by LEAs requires holistic education, based on technical, ethical and legal knowledge and trainings.
- **Goal:** The ultimate goal should be social benefit, enhancing the security and privacy of the population by reducing the biases that AI system algorithms may have.
- **Transparency:** In order to promote and familiarise the population with AI and its implementation in the security field, the systems and their uses need to be explained to the population in a clear and transparent manner.
- **Acceptance:** Only with the above factors can trust be achieved in order to establish the necessary balance between security and privacy. This balance must be negotiated in a multi-stakeholder and multidisciplinary manner.

However, some divergences in the implementation of AI in LEA context that have generated debate are as follows:

- **Misuse:** at the theoretical level, and even at the practical level, the misuse of AI systems, especially in data processing, has been pointed out. For this there must be accountability internally within LEAs but also externally, by way of evaluation, to other governmental and supra-governmental institutions, as well as to the rest of the population. Such misuse may be deliberate, to pursue other offences that diverge from criminal or security activity, or unconsciously due to lack of knowledge of how to use AI systems.
- **Economic features**: While some participants and authors of the literature review point to an optimisation of resources thanks to the ease of processing metadata with AI data analysis systems, others point out that the human management of review is residual and entails high costs, as do the costs of such systems for their proper implementation.
- **Adaptation:** The reluctance of the population may be a direct consequence of the lack of transparency of AI systems, the narratives conveyed by the media, or a lack of readiness due to the digital divide in terms of age. In this sense, there are participants and authors who point out that younger generations are more likely to adapt and older generations are more reluctant. On the other hand, there are other participants and authors who point out the opposite, that the younger generations perceive AI systems as a means of mass surveillance and as a deflagration of their rights and freedoms. In any case, the common point is the binary homogenisation by age.

In conclusion, what emerges clearly is that we are facing a 'new ecosystem of policing' (Gelles et al. 2019) that unveils many challenges of how, what, who and where to carry out policing. That is, through new tools, forms of crime, a change of work processes and communities. For this, in line with the objectives of the European popAI project, analytical rigour to help establish ethical and legal regulations through multidisciplinary expert groups, as well as the participation of LEAs and the civil population through different organisations, so that their expectations, concerns and wishes can be considered, is of vital importance.

7 Annex

7. 1 Interviews discussion guide

The aim

To explore and analyze the interviewee's perception of the impact, benefits, and challenges of incorporating AI into existing police forces' organizational structures and processes and on the relationship of the interviewee with AI in the workplace.

The context

Artificial Intelligence and predictive technologies are gaining popularity at an unprecedented rate. As pattern-matching and search algorithms sort through enormous police databases filled with growing volumes of data in an effort to identify people likely to experience (or commit) crime, places likely to host it, and variables associated with its solvability, powerful digital crime mapping tools are being used to identify crime hotspots in real-time. Criminals are being tracked by facial and vehicle recognition cameras as they travel, and police departments are developing tactics based on predictive analytics and machine learning. Numerous of these ideas are components of contemporary policing in the US, Australia, the UK, and other countries. Studies reveal that AI is shaping the way police officers will perform their jobs as well as the police-to-civilian interactions. Police officers are generally enthusiastic about AI; however, they also see certain risks and acknowledge the need to handle them. When smart policing technologies are introduced, the public and police perceive more utility in the prevention and investigation of cybercrime, respectively. In fact, few studies in this field separate the prevention and investigation of crimes or compare perceptions of the public and police toward the introduction of smart policing technologies.

Regarding the implications of incorporating these technologies into existing law enforcement's organizational structures and processes and the perception of the stakeholders involved, the literature (and the results of popAI policy labs on the matter) report that should meet specific characteristics and requirements: AI should not be a black box, so traceability and human intervention should be made possible. In fact, AI systems need to support the decision making, not to make the decisions. There should always be human supervision in the whole lifecycle of the AI system and the final decision should be made by humans. For this reason, education, as well as a thorough understanding of the legal and ethical framework and boundaries is crucial. The focus should always be the social benefit: use of artificial intelligence in the field of police work and law enforcement requires precise, predictable and appropriate rules specific to the given area, which must take into account the interests of the persons concerned and the impact on the functioning of a democratic society. Regulation is needed to promote and ensure citizens' awareness regarding the existence and implementation of an AI system and enable objection to potential unjust decisions. Moreover, continuous ethical reflection and evaluation around the application of AI is

required by the police, with emphasis already in the very first pilot phase. Main concerns are related to the foundations of democracy. The risk of impartial control and bias of the system needs to be taken into account for several reasons: for example, systems rely on existing statistical data, collected, and interpreted by the police causing negative feedback loop; over time, end users might feel "too comfortable" with the system so that they do not challenge the outcomes and they don't use their critical thinking and experience; profiling and targeting before the commission of an offense is controversial.

Reported uses of AI into police forces include prevention of traffic accidents; license plates readers; social network analysis; aerial drones equipped with video recording; body worn cameras; facial recognition systems. Research around aerial drones implementation revealed that receptivity to aerial drones is highly contextual and varies by the way in which it is utilized. It is clear that aerial drones use within traditional police activities appear to garner higher support compared to applications that reflect a proactive, yet ambiguous, utility. It is critical for police departments to find effective ways of implementing aerial drones into police operations that will improve, rather than exacerbate, community relations. On the other hand, a study reported that the public is overwhelmingly supportive of body worn cameras but found more mixed opinions for police. Officers seem to believe in the citizen-related benefits of body worn cameras, but only 31% of the officers surveyed support the citywide adoption of body worn cameras. Furthermore, support for body worn cameras and their potential benefits seems to increase significantly once officers gain hands-on experience with the cameras. Officers who have used the cameras believe that they can decrease citizen complaints, maintain police-community relations, and are relatively easy to use. However, officers are less likely to believe these cameras can increase officer safety, make their jobs easier, or are comfortable to wear, but they resoundingly do not believe body worn cameras can decrease paperwork.

Interview guide

Thank you for having agreed to participate in this interview. We are interviewing you to better understand what Law Enforcement agents think about Artificial Intelligence and what are the benefits and challenges of incorporating AI applications in the police workforce. Your point of view is incredibly valuable to us to better understand how you feel that AI technologies affect your work, responsibility and health and safety. So, there are no right or wrong answers to any of our questions, we are interested in your own experiences.

Participation in this study is voluntary and your decision to participate, or not participate, will not affect you in any way. The interview should take approximately one hour. With your permission, we will be taking notes. The interview responses will be anonymised and there will be no way to trace the answers back to you or to your organization. The interviews will be used to write up a report outlining LEA's perspective on the benefits and challenges of incorporating Artificial Intelligence in law enforcement. Findings will be extremely useful for the community to understand what needs to

be improved in the way AI is built, regulated and integrated in the police workforce. You may decline to answer any question or stop the interview at any time and for any reason. Are there any questions about what I have just explained?

Please note that this guide only represents the main themes to be discussed with the participants and as such does not include the various prompts that may also be used (examples given for each question). Non-leading and general prompts will also be used, such as "Can you please tell me a little bit more about that?" and "What does that look like for you".

Questionary

Understanding of AI

1. Can you tell me how do you define Artificial Intelligence?

Prompts:

a) What is your understanding of AI?
b) How do you see it?
c) What are the positive characteristics of AI for Law Enforcement?
d) What are the negative characteristics of AI in law enforcement?

2. What types of AI systems have you heard of?
3. Have you worked with any AI system?

Prompts:

a) If yes, how did it go? Who was part of the team?
b) If not, how would you expect it to go?

AI impact on police officers and individual work: changes, expectations and needs

4. Do you think law enforcement agents are ready to work with AI?
   a) Why?
   b) What could be done differently?

5. How do you see your daily job affected by AI?
6. Do you think that the way you perform your job has changed since the introduction of Artificial Intelligence?
   a) If yes, how and why?
   b) If not, why?
   c) Has this change been positive or negative?

***Note**: If the interviewees do not have experience with AI systems, we can ask them to tell us their expectations of how AI might change their job. Also ask them if this AI is more beneficial or maybe a risk for their jobs or interpretation of the contexts and decision-making process.*

7. How did you experience the introduction of Artificial Intelligence in your work?
    a) What stands out for you about your first experience with Artificial Intelligence?
    b) Any challenges? Any benefits? Any risks?
    c) Were you provided with any resources that helped you to understand the system?
    d) Were you provided with any resources that helped you to use the system?

8. How would you describe your approach to AI?
9. Do you think Artificial Intelligence tools are understandable by the police? You can think of some AI systems that you use or know.
    a) If not, why what can be done?
    b) If yes, why what was done to make it understandable?

10. How do you think AI affects your responsibility at work?
    a) Is there any mechanism in place to clearly allocate responsibilities when decisions are taken after considering an AI output?
    b) Do you have any examples?

11. How do you think AI affects your autonomy at work?
    a) If yes, why and how?
    b) If not, why?

12. In your day-to-day work, do you think that there is an activity that cannot be replaced by an AI?
    a) Why?
    b) Which activities do you consider can be made by an AI?

13. How do you think AI affects your health and safety at work?

<u>AI impact on law enforcement's organizational structure: changes and needs</u>

14. Do you think that law enforcement organisations are ready to introduce and use AI?

a) Why?
b) What could be done differently?

15. How would you describe your organisation approach to AI?
16. How has AI been introduced in your organisation?
    a) How would you describe the process through which AI was introduced?
    b) Were you provided with any resources or training? If yes, how did it work? If not, why?

17. Do you think AI has brought changes in the law enforcement organizational characteristics and mechanisms?

Prompts:

a) If so, what are these changes?
b) Are they positive or negative?

18. What do you think should be the role of AI in law enforcement structures and processes?
19. Do you think AI systems bring with them some kind of risk?
    a) If so, what type of risks are you concerned about?
    b) How do you think these risks could be mitigated?

20. Which activities can be done by an AI in your work?
    a) Are there activities that you wouldn't trust in an AI model?

21. What do you think is needed from an organizational perspective to improve the benefit of AI integration into law enforcement?
22. What do you think is needed from an ethical perspective to improve the benefit of AI integration into law enforcement?
23. What do you think is needed from a legal perspective to improve the benefit of AI integration into law enforcement?
24. What role do you think ethics has for AI in law enforcement?

<u>Relationship between AI, law enforcement and civil society</u>

25. How do you think civil society/the public perceive the introduction of AI into law enforcement processes?
26. Do you think the introduction of AI system in law enforcement has influenced the police-to-civilian interactions in some way?

a) If yes, how have police-to-civilian interactions changed since the introduction of AI?

27. Can you think of any benefits for citizens?

Conclusion

28. Is there anything else you would like to comment on that I haven't already asked you about?

8 References

Almeida, D., Shmarko, K., & Lomas, E. (2022). The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks. *AI and Ethics*, *2*(3), 377–387. https://doi.org/10.1007/s43681-021-00077-w

Amnesty International (2021). Ban dangerous facial recognition technology that amplifies racist policing. *Amnesty International*. https://www.amnesty.org/en/latest/press-release/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing/

Apostolakis, K. C., Dimitriou, N., Margetis, G., Ntoa, S., Tzovaras, D., & Stephanidis, C. (2021). DARLENE – Improving situational awareness of European law enforcement agents through a combination of augmented reality and artificial intelligence solutions. *Open research Europe*, *1*, 87. https://doi.org/10.12688/openreseurope.13715.1

Bennett Moses, L., & Chan, J. (2018). Algorithmic prediction in policing: assumptions, evaluation, and accountability. *Policing & Society*, *28*(7), 806–822. https://doi.org/10.1080/10439463.2016.1253695

Benvenisti, E. (2019). Toward Algorithmic Checks and Balances: A Rejoinder. *European Journal of International Law*, *29*(4), 1087–1090. https://doi.org/10.1093/ejil/chy089

Berk, R. A. (2021). Artificial intelligence, predictive policing, and risk assessment for law enforcement. Annual Review of Criminology, 4(1), 209–237. https://doi.org/10.1146/annurev-criminol-051520-012342

boyd d. (2002). *Faceted id/entity, Managing representation in a digital world* (Doctoral dissertation). Massachusetts Institute of Technology, Cambridge. http://www.danah.org/papers/Thesis.FacetedIdentity.pdf

Buchmann, M., Schach, E., Leißner, T., Kern, M., Mütze, T., Rudolph, M., Peuker, U. A., & Tolosana-Delgado, R. (2020). Multidimensional characterization of separation processes – Part 2: Comparability of separation efficiency. *Minerals Engineering*, *150*(106284), 106284. https://doi.org/10.1016/j.mineng.2020.106284

Bushway, S. D. (2020, April 15). *Nothing is more opaque than absolute transparency*. Harvard Data Science Review. https://www.rand.org/pubs/external_publications/EP68132.html

Campbell, T. (2018, July 20). Opportunities and challenges from artificial intelligence for law enforcement. *Futuregrasp.com*. https://www.futuregrasp.com/opportunities-from-artificial-intelligence-for-law-enforcement

Castets-Renard C. (2021) Algorithms, freedom, and fundamental rights. In Micklitz H., Pollicino O., Reichman A., Simoncini A., Sartor G., & de Gregorio G. *(eds.) (2021), Constitutional challenges in the algorithmic society (pp. 25-128). Cambridge: Cambridge University Press.* https://doi.org/10.1017/9781108914857

Challen, R., Denny, J., Pitt, M., Gompels, L., Edwards, T., & Tsaneva-Atanasova, K. (2019). Artificial intelligence, bias and clinical safety. *BMJ Quality & Safety*, *28*(3), 231–237. https://doi.org/10.1136/bmjqs-2018-008370

Clyde, A. (2021, December 1). *Human-in-the-loop systems are no panacea for AI accountability*. Tech Policy Press. https://techpolicy.press/human-in-the-loop-systems-are-no-panacea-for-ai-accountability/

David B., Crémer J., Danthine J. P., Edwards J., Grilli V., Neven D., Seabright P., Sinn H. W., Venables A. and Wyplosz C. (1993), Making Sense of Subsidiarity: How Much Centralization for Europe? CEPR, London

Davis, J., Atchley, A., Smitherman, H., Simon, H., & Tenhundfeld, N. (2020). Measuring automation bias and complacency in an X-ray screening task. *2020 Systems and Information Engineering Design Symposium (SIEDS)*, 1–5.

Dechesne, F., Dignum, V., Zardiashvili, L., & Bieger, J. (2019). AI & ethics at the police: Towards responsible use of artificial intelligence in the dutch police. In *AI & Ethics at the Police: Towards Responsible use of Artificial Intelligence in the Dutch Police*. https://scholarlypublications.universiteitleiden.nl/handle/1887/85954

Dellermann, D., Ebel, P., Söllner, M., & Leimeister, J. M. (2019). Hybrid intelligence. *Business & Information Systems Engineering*, *61*(5), 637–643. https://doi.org/10.1007/s12599-019-00595-2

Deloitte (2018). Policing 4.0 deciding the future of policing in the UK. London, UK: Deloitte.

Edwards, L., & Veale, M. (2017). Slave to the Algorithm? Why a Right to Explanationn is Probably Not the Remedy You are Looking for. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2972855

European Commission (2021). "Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts", COM (2021) 206 final, art. 3 (1).

European Parliament (2023, June 8). *EU AI Act: first regulation on artificial intelligence*. https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence?at_campaign=20226-Digital&at_medium=Google_Ads&at_platform=Search&at_creation=Sitelink&at_goal=TR_G&at_advertiser=Webcomm&at_audience=ai%20act&at_topic=Artificial_intelligence_Act&gclid=CjwKCAjw5MOlBhBTEiwAAJ8e1o5dILwP18VkanjWAcVegIkQB_vy-fcUFE2x1MZL8TZI2XXtTIoC1RoCOnQQAvD_BwE

European Parliament *(2021). Texts adopted - Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters - Wednesday, 6 October 2021*. https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html

European Parliament (2021). *The principle of subsidiarity | Fact sheets on the European Union.* April 2023. https://www.europarl.europa.eu/factsheets/en/sheet/7/el-principio-de-subsidiariedad

Ezzeddine, Y., Bayerl, P. S., & Gibson, H. (2023). *Citizen perspectives on necessary safeguards to the use of AI by Law Enforcement Agencies.* En *arXiv* [cs.CY]. http://arxiv.org/abs/2306.01786

FRA (2020). "Getting the future right – Artificial intelligence and fundamental rights". https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights/

G.G. Fuster, G. G. (2020). "Artificial Intelligence and Law Enforcement. Impact on Fundamental Rights" European Parliament. https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU(2020)656295_EN.pdf

Gelles et al. (2019, October 22). *The future of law enforcement*. Deloitte Insights. https://www2.deloitte.com/us/en/insights/focus/defense-national-security/future-of-law-enforcement-ecosystem-of-policing.html

Goddard, K., Roudsari, A., & Wyatt, J. C. (2012). Automation bias: a systematic review of frequency, effect mediators, and mitigators. *Journal of the American Medical Informatics Association: JAMIA*, *19*(1), 121–127. https://doi.org/10.1136/amiajnl-2011-000089

Hawdon, J. E., Ryan, J., & Griffin, S. P. (2003). Policing tactics and perceptions of police legitimacy. *Police Quarterly*, *6*(4), 469–491. https://doi.org/10.1177/1098611103253503

Hill, K. (2020, October 21). Activists turn facial recognition tools against the police. *The New York Times*. https://www.nytimes.com/2020/10/21/technology/facial-recognition-police.html

Hunkenschroer, A. L., & Luetge, C. (2022). Ethics of AI-enabled recruiting and selection: A review and research agenda. *Journal of Business Ethics*, *178*(4), 977–1007. https://doi.org/10.1007/s10551-022-05049-6

Kafteranis, D., Sachoulidou, A., & Turksen, U. (2023). Artificial Intelligence in Law Enforcement Settings : AI Solutions for Disrupting Illicit Money Flows. *Eucrim*. https://doi.org/10.30709/eucrim-2023-006

Kaufmann, M., Egbert, S., & Leese, M. (2019). Predictive policing and the politics of patterns. *The British Journal of Criminology*, *59*(3), 674–692. https://doi.org/10.1093/bjc/azy060

Kitsos, P. (2020). The Limits of Government Surveillance: Law Enforcement in the Age of Artificial Intelligence. *ResearchGate*. https://www.researchgate.net/publication/351528399_The_Limits_of_Government_Surveillance_Law_Enforcement_in_the_Age_of_Artificial_Intelligence

Kupfer, C., Prassl, R., Fleiß, J., Malin, C., Thalmann, S., & Kubicek, B. (2023). Check the box! How to deal with automation bias in AI-based personnel selection. *Frontiers in Psychology*, *14*, 1118723. https://doi.org/10.3389/fpsyg.2023.1118723

Lyell, D., Magrabi, F., & Coiera, E. (2018). The effect of cognitive load and task complexity on automation bias in electronic prescribing. *Human Factors*, *60*(7), 1008–1021. https://doi.org/10.1177/0018720818781224

Lyon, D. (2002). Everyday Surveillance: Personal data and social classifications. *Information, Communication and Society*, *5*(2), 242–257. https://doi.org/10.1080/13691180210130806

Mantelero, A. (2022). *Beyond data: Human rights, ethical and social impact assessment in AI*. T.M.C. Asser Press.

Marwick, A. (2012). The public domain: Surveillance in everyday life. *Surveillance & society*, *9*(4), 378–393. https://doi.org/10.24908/ss.v9i4.4342

McDaniel, J. L. M., & Pease, K. G. (Eds.). (2021). *Predictive policing and artificial intelligence*. Routledge. https://doi.org/10.4324/9780429265365

Miliaikeala, S. J., Heen, J. D., & Lieberman Terance, D. (2018). *The thin blue line meets the big blue sky: perceptions of police legitimacy and public attitudes towards aerial drones*. Criminal Justice Studies, 31:1, 18-37, DOI: 10.1080/1478601X.2017.1404463

Montag, L., Mcleod, R., De Mets, L., Gauld, M., Rodger, F., & Pe, M. (s/f). *A legal analysis of biometric mass surveillance practices in Germany, the Netherlands, and Poland*. Edri.org. Recuperado el 10 de julio de 2023, de https://edri.org/wp-content/uploads/2021/11/EDRI_RISE_REPORT.pdf

Mosier, K. L., & Skitka, L. J. (1999). Automation Use and Automation Bias. *Proceedings of the Human Factors and Ergonomics Society . . . Annual Meeting*, *43*(3), 344-348. https://doi.org/10.1177/154193129904300346

N., E., & Wiener, N. (1949). Cybernetics. Or Control and Communication in the Animal and the Machine. *The Journal of Philosophy*, *46*(22), 736. https://doi.org/10.2307/2020260

Noriega, M. (2020). The application of artificial intelligence in police interrogations: An analysis addressing the proposed effect AI has on racial and gender bias, cooperation, and false confessions. *Futures*, *117*(102510), 102510. https://doi.org/10.1016/j.futures.2019.102510

Patton, D. U., Brunton, D.-W., Dixon, A., Miller, R. J., Leonard, P., & Hackman, R. (2017). Stop and frisk online: Theorizing everyday racism in digital policing in the use of social media for identification of criminal conduct and associations. *Social Media + Society*, *3*(3), 205630511773334. https://doi.org/10.1177/2056305117733344

Quattrocolo, S. (2020). *Artificial intelligence, computational modelling and criminal proceedings: A framework for A European legal discussion*. Springer International Publishing.

Raaijmakers, S. (2019). Artificial intelligence for law enforcement: Challenges and opportunities. *IEEE security & privacy*, *17*(5), 74–77. https://doi.org/10.1109/msec.2019.2925649

Rademacher, T. (2019). Artificial Intelligence and Law Enforcement. En *Springer eBooks* (pp. 225-254). https://doi.org/10.1007/978-3-030-32361-5_10

Ratcliffe, J. H. (2001). Chasing ghosts?: Police perception of high crime areas. *The British journal of criminology*, *41*(2), 330–341. https://doi.org/10.1093/bjc/41.2.330

Roksandić, S. (2022). *Trustworthy Artificial Intelligence and its use by Law Enforcement Authorities: where do we stand?* https://www.semanticscholar.org/paper/Trustworthy-Artificial-Intelligence-and-its-use-by-Roksandi%C4%87-Protrka/6cd98c2023da827f9eecbcc35fb2f4d99e8e576f

Schemmer, M., Kühl, N., Benz, C., & Satzger, G. (2022). *On the influence of explainable AI on Automation Bias.* https://arxiv.org/ftp/arxiv/papers/2204/2204.08859.pdf

Selbst, A. D., Boyd, D., Friedler, S. A., Venkatasubramanian, S., & Vertesi, J. (2019). Fairness and Abstraction in Sociotechnical Systems. *Proceedings of the Conference on Fairness, Accountability, and Transparency*. https://ssrn.com/abstract=3265913

Shah, H. (2018). Algorithmic accountability. *Philosophical Transactions of the Royal Society A*, *376*(2128), 20170362. https://doi.org/10.1098/rsta.2017.0362

Stoycheff, E. (2016). Under surveillance: Examining Facebook's spiral of silence effects in the wake of NSA internet monitoring. *Journalism & Mass Communication Quarterly*, *93*(2), 296–311. https://doi.org/10.1177/1077699016630255

Stoycheff, E., Burgess, G. S., & Martucci, M. C. (2018). Online censorship and digital surveillance: the relationship between suppression technologies and democratization across countries. *Information, Communication & Society*, *23*(4), 474-490. https://doi.org/10.1080/1369118x.2018.1518472

Strauß, S. (2018). From big data to deep learning: A leap towards strong AI or 'intelligentia obscura'? *Big data and cognitive computing*, *2*(3), 16. https://doi.org/10.3390/bdcc2030016

Strauß, S. (2021). Deep automation bias: How to tackle a wicked problem of AI? *Big Data and Cognitive Computing*, *5*(2), 18. https://doi.org/10.3390/bdcc5020018

Trottier, D. (2017). 'Fear of contact': Police surveillance through social networks. *European Journal of Cultural and Political Sociology*, *4*(4), 457-477. https://doi.org/10.1080/23254823.2017.1333442

Tsamados, A., Aggarwal, N., Cowls, J., Morley, J., Roberts, H., Taddeo, M., & Floridi, L. (2022). The ethics of algorithms: key problems and solutions. *AI & Society*, *37*(1), 215–230. https://doi.org/10.1007/s00146-021-01154-8

Wang, Y., Wang, L., Chen, G., Cai, Z., Zhou, Y., & Xing, L. (2020). An improved ant colony optimization algorithm to the periodic vehicle routing problem with time window and service choice. *Swarm and Evolutionary Computation*, *55*(100675), 100675. https://doi.org/10.1016/j.swevo.2020.100675

Wong, P.-H. (2020). Democratizing algorithmic fairness. *Philosophy & Technology*, *33*(2), 225–244. https://doi.org/10.1007/s13347-019-00355-w

Završnik, A. (2020). Criminal justice, artificial intelligence systems, and human rights. *ERA Forum*. https://doi.org/10.1007/s12027-020-00602-0