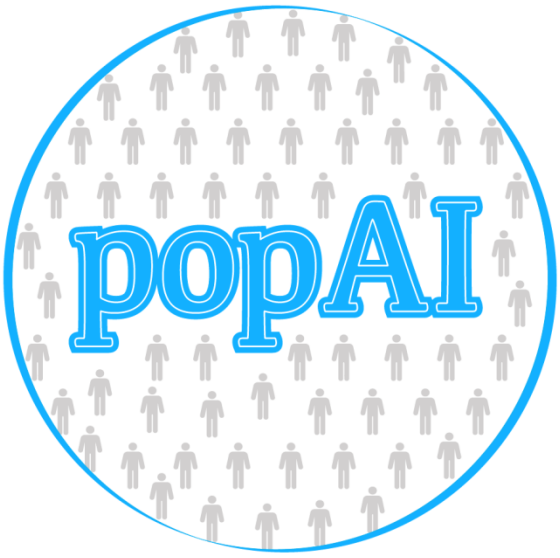


A European Positive Sum Approach towards AI tools in support of Law Enforcement and safeguarding privacy and fundamental rights

D3.5: Foresight scenarios for AI in policing

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	14/04/2023		
Nature	Document, report	**Dissemination Level**	Public
Author	Pinelopi Troullinou, Trilateral Research		
Contributors	Evan Fisher, Trilateral Research Fabienne Ufert, Trilateral Research Francesca Trevisan, ERI Simeon Stoyanov, ECAS Hellenic Police, Greece University of Applied Science – Police Affairs in Bavaria, Germany, Police Academy of Bratislava, Slovakia Dimitris Kyriazanos, NCSRD		
Reviewers	Paola Fratatoni, Z&P Andreas Ikonomopoulos, Dimitris Kyriazanos, NCSRD		

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

Executive Summary

Foresight Scenario methodology is increasingly used to support policy making processes. The methodology is adopted to fit the purposes and objectives of the popAI project and to specifically contribute to the Roadmap of AI in Law Enforcement 2040. For the scenarios to be credible and valuable for policymaking, it is important that diverse stakeholders are engaged in the scenario development process. To this end, Task. 3.5 entitled *Multi-Disciplinary Foresight Scenarios* provides the platform and methodology for diverse stakeholders to co-create an imaginary future for AI use in policing considering opportunities and constraints, potentials, and risks.

The report consists of six sections. The first section (Section 1) introduces Task 3.5 explaining its **purpose and the scope** as well as the **relation to other tasks and deliverables**. A **summary of the work methodology** is also provided.

Section 2 discusses the Foresight Scenarios as a methodology used nowadays to **assist policy making processes**. The various methods used for the development of the scenarios are discussed followed by the adjusted method adopted in popAI.

Section 3 presents the methodology as employed in the context of Task 5.5 following the main steps as defined by the European Commission JRC FOR-LEARN scenario building guidance, namely, **focal issue identification, identification and analysis of drivers, importance and uncertainties, selection of scenario logics, and fleshing out scenarios.** The analysis of the research activities that informed the scenario development is also presented as well as the analysis of AI Act and surrounding political discussions that contribute to the design of the scenarios.

Section 4 presents the **scenarios produced for each of the five broad contexts around which the civil security domain is structured**, as classified in Task 3.1, namely: crime prevention involving mainly predictive policing; crime investigation; cyber operations: migration, asylum, and border control; administration of justice. **The scenarios present a potential future in five years' time**.

Section 5 provides a **summary of the focal issues, the envisaged technology, the main drivers, and key factors** that are the most important and the most uncertain for each scenario. The scenarios are discussed underlying the common focal issue, the use of AI by LEAs, and how this is differentiated in different contexts. The section also discussed opportunities, risks, and obstacles depicted in different scenarios.

The final section of the deliverable (Section 6) provides a conclusion along with the next steps of foresight scenario methodology to be implemented in Task 5.5 *popAI roadmaps.*

Table of Contents

1 Introduction 5
1.1 Purpose and Scope 5
1.2 Relation to other Tasks and Deliverables 5
1.3 Work Methodology 6
1.4 Structure of the Deliverable 7
2 Foresight Scenarios 7
2.1 Foresight scenarios: Introduction 7
2.2 Foresight scenario: Methodology 8
2.3 popAI approach on foresight scenarios 10
3 Methodology 12
3.1 Identifying focal issues 12
3.1.1 Controversy Analysis 12
3.1.2 Policy Labs 13
3.1.2.1 Policy Lab 1 - Greece 13
3.1.2.2 Policy Lab 2 – Germany 13
3.1.2.3 Policy Lab 3 – Slovakia 14
3.2 Key factors 14
3.2.1 Computational methods 14
3.2.2 Crowdsourcing activities 15
3.3 Identification and analysis of drivers 16
3.3.1 AI Act provisions related to law enforcement 16
3.4 Scenario development 20
4 Foresight scenarios 21
4.1 Crime prevention/predictive policing 21
4.2 Crime investigation 22
4.3 Cyber Operations 22
4.4 Migration, Asylum, and Border control 23
4.5 Administration of justice 24
5 Discussion of the scenarios 25
6 Conclusions 28
7 References 29
8 ANNEX 30

List of Figures

Figure 1 Steps to take in policy scenario development workshops (Wright et al., 2020, p. 7).....10

List of Tables

Table 1 D3.5 Work Methodology.....7
Table 2 Comparison of existing foresight methods and their shortcomings for formulating policy recommendations.....9
Table 3 Summary of popAI foresight scenarios.....26

List of Terms & Abbreviations

Abbreviation	Definition
AI	Artificial Intelligence
FR	Facial Recognition
SAB	Stakeholder Advisory Board
LEAs	Law Enforcement Agencies
CSAM	Child Sexual Abuse Material
WP	Work Package

1 Introduction

popAI activities build towards a unified European view and recommendations for ethical, socially acceptable, and effective implementation of AI. To do so, Task 3.5 *Multi-Disciplinary Foresight scenarios* provides the platform and methodology for diverse stakeholders to co-create an imaginary future for AI use in policing to feed in popAI roadmaps and specifically the Roadmap of AI in Law Enforcement 2040 (T5.5) and policy making recommendations.

1.1 Purpose and Scope

This deliverable (D3.5) entitled *Foresight Scenarios for AI in Policing* discusses the adjusted methodology to fit the purpose and objective of the popAI project. The method has been used to build structured foresight narratives that support the exploration and understanding of diverse stakeholders' needs, concerns, and potential risks related to the implementation of innovative technologies in a critical area of application such as civil security. The aim of this activity is to facilitate the roadmap and policy making for an ethical use of AI and, therefore, the increase of public trust.

The creation of the foresight scenarios followed a collaborative approach. The scenarios were created based on the policy labs and crowdsourcing insights, the identification of controversies in Tasks 2.3 and 3.1 as well as dedicated activities bringing together different stakeholders. More specifically, research activities for the policy labs, the crowdsourcing task, and the controversy mapping identified focal issues and drivers and prioritised them based on citizen and expert perspectives.

The foresight scenarios are not an end themselves. They are a platform facilitating collaboration and communication between diverse stakeholders and disciplinary perspectives. They are also a valuable tool to support the development of a foresight strategy that will be credible, feasible, and socially acceptable.

1.2 Relation to other Tasks and Deliverables

The report presents the method and outcomes of Task 3.5 *Multi-Disciplinary Foresight scenarios* feeding specifically into Task 5.5 *popAI roadmaps*. Task 3.5 has also been closely interrelated to other tasks of the project as follows:

- Task 2.3 *The controversies and risks that have shaped innovation and will shape AI in the next 20 years*; controversies identified in this task were considered as focal issues for the development of the scenarios.
- Task 3.1 *Map the controversy ecosystems of AI tools in the security domain*; controversies identified in this task were considered as focal issues for the development of the scenarios.
- Task 3.2 *Understanding citizen discourses around AI and security controversies*; insights from computational activities carried out in the project informed the drivers[1] for the development of the scenarios.
- Task 3.3 *Crowdsourcing stakeholder attitudes and pro-active solution ideations*; insights of the crowdsourcing activities informed drivers and citizens' priorities for the development of the scenarios.

[1] The concepts "focal issues" and "drivers" in the context of the Foresight Scenario methodology are defined in the next section.

- Task 3.4 *Engaging LEAs and relevant experts through policy labs*; the structure of the lab was designed in accordance with the foresight scenarios approach. Analysis of the policy lab activities identified focal issues and drivers.
- Task 5.5 *popAI roadmaps*; foresight scenarios will be used to support popAI roadmap activities and specifically the development of the Roadmap of AI in Law Enforcement 2040 and its validation.

1.3 Work Methodology

The development of the foresight scenarios presented in this deliverable has been achieved and validated through diverse methods as will be discussed in the dedicated method section (Section 4). In fact, the collaboration with other tasks in WP3 started before the official kick-off of Task 3.5.

Task 3.4 *Engaging LEAs and relevant experts through policy labs* integrated the foresight scenario approach in their activities so as to increase LEAs' and other experts' engagement. This practically meant that the leading LEA for each policy lab would discuss internally and suggest two case studies of AI use in the civil security domain to be elaborated during the policy labs. Subsequently, the policy labs were largely organised as follows: a. presentation of a case study, b. discussion about the potentials, as well as ethical, social, legal, and organizational implications of AI in the security domain (in break-out sessions), c. elaboration on respective recommendations to overcome the identified challenges (in break-out sessions). The same steps were followed for the second case study. The insights of three policy labs have informed this report, namely the labs led by the Hellenic Police (Greece), the University of Applied Science – Police Affairs (HfoD) in Bavaria (Germany), and the Police Academy of Bratislava (Slovakia). The participants of each policy lab consisted of the respective LEA organising the event, as well as external experts from diverse backgrounds such as policy makers, civil organizations, technologists.

The case studies discussed in the policy labs provided the focal issues for the foresight scenarios as well as the drivers meaning the concerns, needs and so on. These insights were enriched and validated with desk-based research in Task 2.3 *The controversies and risks that have shaped innovation and will shape AI in the next 20 years* and Task 3.1 *Map the controversy ecosystems of AI tools in the security domain*, as well as the citizens' insights collected in the context of Task 3.3 *Crowdsourcing stakeholder attitudes and pro-active solution ideations*; insights of the crowdsourcing activities informed drivers and citizens' priorities.

The focal issues and drivers were discussed in a hands-on workshop with external experts and the participation of popAI's Stakeholders Advisory Board that took place in Rome on 14th March 2023. During this workshop, participants were split in four multi-disciplinary groups and created the scenarios that were further curated by Trilateral's team and presented in this report. The foresight scenarios will be further validated in Task 5.5. The table below summarizes the work methodology followed in this report.

Table 1 D3.5 Work Methodology

Deliverable Number	Title	Input from:	Output to:	Validation Methodology			
				Theoretical	Empirical		
				Literature review or Scientific Validation.	Experts	LEAs	Civil Society
D3.5	*Foresight scenarios for AI in Policing*	T2.3, T3.1, T3.2, T3.3, T3.4	T3.5	Literature Review to validate the approach. Computational methods in T3.2, and Crowdsourcing activities in T3.3 to validate drivers.	SAB and external experts engaged in Policy Labs and hands-on workshop to co-create scenarios	LEAs were involved in different phases; policy labs, validating activities in T3.2 and T3.3 and hands-on workshop to co-create scenarios	NGOs and CSOs were involved in policy labs and hands-on workshop to co-create scenarios. Citizens also participated in crowdsourcing activities

1.4 Structure of the Deliverable

The remainder of this deliverable is organised as follows:

Section 2 introduces the theory of foresight scenarios methodology and discusses its relevance and importance to the popAI project.

Section 3 reports on the research activities undertaken in Task 3.5 for the development of foresight scenarios.

Section 4 presents the foresight scenarios that emerged from the respective research activities.

Section 5 discusses the main findings of the research activity. The section also discusses the utilization of the findings for AI Act consultation and the development of the popAI roadmaps.

The final section provides a conclusion drawn from the Task findings along with a summary of the content.

2 Foresight Scenarios

This section introduces foresight scenarios as a methodology increasingly used to support policy making. The various methods used for the development of the scenarios are discussed followed by the adjusted method adopted in popAI to fit the needs and objectives of the project. The impact pathway of foresight scenarios in the project is presented assisting the development and evaluation of the popAI roadmaps while also providing recommendations for further shaping the AI.

2.1 Foresight scenarios: Introduction

The methodology of scenario building is more than half a century old. Foresight scenarios were first developed during the 1950s in the United States, most notably by Herman Kahn at RAND Corporation

(Kahn & Wiener, 1967). Since then, they have become a common tool for strategic decision-making in the public and private sectors, and there are now a plethora of existing methods serving specific objectives. In their original form, foresight scenarios are *story telling exercises that detail a sequence of events that may lead to an envisaged future on a given focus theme* (Kahn & Wiener, 1967). Starting and ending with strategic decisions related to their thematic focus, scenario narratives explore plausible and coherent, but fictional, accounts of what might be in store in the future. Importantly, foresight scenarios are not predictions. They rather consider different possible futures, exploring opportunities, as well as potential threats. Sometimes informed by science fiction writing and collectively organised speculation about what could happen, scenarios are often used when data is lacking[2], and as such, they are more imagination driven than data driven. In general, scenarios serve either as an exploratory tool or a normative tool[3]. As an exploratory tool, foresight scenarios start with what exists in the present and extrapolate on issues and themes for which there is little data. As a normative tool, foresight scenarios function by simulating possible futures and highlighting discontinuities between the present and future. Then, they look back on how these futures could grow out of the present – called *backcasting* – to develop transition pathways and specify the risks and opportunities associated with them[4]. By identifying trends, emerging issues, and potential implications, these scenarios allow strategic decisions to achieve or avoid these simulated futures.

The foresight scenario methodology allows senior policy sector executives to think about the future in a disciplined way. It gives them insight into the context in which their policy decisions are made and allows them to articulate different values in relation to these plausible futures. It challenges decision makers to move beyond common sense assumptions about what is possible, plausible, and desirable in order to shape creative and imaginative thinking. Foresight scenarios project policy propositions and decisions in the medium and long term, where many decision-making tools rivet policy thinking to the present and the short term. The European Commission embeds strategic foresight in its work towards "the transitions to a green, digital and fairer Europe"[5].

2.2 Foresight scenario: Methodology

Adopting a well-structured methodology is key for the development of foresight scenarios that will serve their objectives. As such, the methods and processes used to design scenarios must be transparent, well-documented, and robust. An ever-increasing number of foresight scenario methods are being developed based on different goals.

In contrast to older, more general approaches, these new methods are oriented towards specific outcomes and readerships. Wright, Stahl, and Hatzakis (2020) provided a review of the main existing methods, analysing their shortcomings when it comes to formulating policy recommendations and their findings are summarised in Table 2. Wright et al.'s (2020) methodology is specifically adjusted to respond to policy makers' requirements while considering the constraints of policy processes and assessments.

[2]European Foresight Platform, http://foresight-platform.eu/community/forlearn/how-to-do-foresight/methods/scenario/

[3] ibid

[4] European Commission. *Strategic foresight* https://commission.europa.eu/strategy-and-policy/strategic-planning/strategic-foresight_en

[5] ibid

Table 2 Comparison of existing foresight methods and their shortcomings for formulating policy recommendations

Method	Approach	Policy-relevant shortcomings
Best case, worst case, status quo	Kahn's method. Three scenarios are developed, depending on steps taken or not taken.	Too many possible outcomes.
Orthogonal futures	Four-quadrant matrix, with axes of likelihood and impact.	Formulaic, over-simplistic views of the world that lack nuance.
Dark scenarios	Focus on what can go wrong, serve as a warning.	Give little guidance on steps to take to reach a desired future.
Ethical dilemmas scenarios	Useful on controversial issues. By describing the ambiguities associated with a given set of futures, they provide the basis for stakeholder discussion and can contribute to consensus building.	Policy makers generally prefer to base their propositions on already existing consensus.
Narrative scenarios	Based on storytelling, with classic narrative structures and protagonists.	Can get caught up in developing a well-crafted story, which means not all relevant issues are discussed.
Trend scenarios	Start from what exists and forecasts into the future based on identified trends. They are meant to be realistic and non-normative.	Tend to ignore black swan events and other unexpected disruptions.
Normative scenarios	Define a desired future and backcast to the present to explore how it can be reached.	Normative scenarios are not realistic, read more like goals statements, and not a planning document.
Exploratory scenarios	Inspired by identified trends, critical zones of uncertainty, and expected policy decisions, these scenarios are meant to explore future possibilities.	Have been criticized for lacking realism and being out of touch with policy processes and assessments.

Wright et al.'s approach systematically explores ethical, legal, social, and economic issues. It develops scenarios that are plausible and probable. It builds on the expertise of a wide set of experts, intentionally targeted to represent contrasting perspectives and thereby achieving greater objectivity. Moreover, wide stakeholder engagement provides a basis for consensus building. These characteristics lend credibility to the scenarios developed. It achieves this by following a stepwise method, with iterative stakeholder consultation as can be seen in Figure 1. Each stakeholder workshop develops and refines foresight scenarios by:

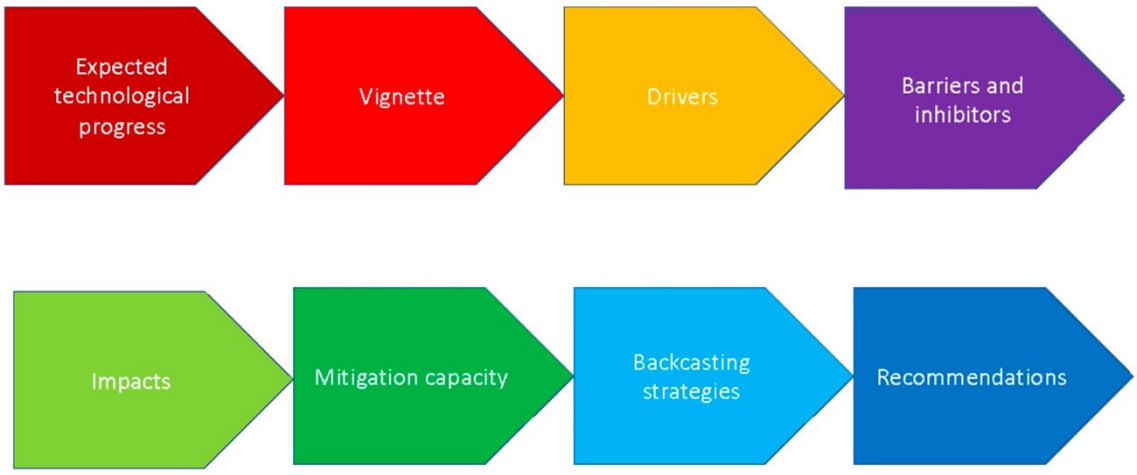


Figure 1 Steps to take in policy scenario development workshops (Wright et al., 2020, p. 7)

The first iteration of the scenarios and recommendations is based on workshops with small groups of domain experts. Subsequent iterations engage with a wider range of concerned individuals, progressively moving to include the general public for the final version. The objective is to obtain recommendations from the greatest number of stakeholders and potentially to establish a consensus.

Foresight scenarios can also be used as a method of a wider approach. For example, in computer science and AI projects, often under different names like vignettes or fictional/futuristic scenarios, foresight scenarios have also been employed to raise awareness on emerging social, ethical, and legal concerns and identify mitigation actions to build ethics-by-design systems (d'Aquin et al., 2018; Troullinou and d'Aquin, 2018; Troullinou et al., 2017). In short, the method used to build foresight scenarios depends on the purpose, context, and overall objective for which they have been employed for.

2.3 popAI approach on foresight scenarios

The foresight scenario methodology has a long history, and many approaches now exist. Their primary function is to provide results, namely scenarios, that are both rigorous and actionable (Ellis and Griffith, 2000; Ramirez et al., 2015) and will support systematic and creative analyses about potential futures. Foresight scenarios are of great relevance and importance to popAI's overall objective, namely, to foster trust in the application of AI in the civil security domain. The foresight scenario methodology has a two-fold role in the project. It serves as a platform for diverse stakeholders to come together and discuss, in a structured way, different and even opposing points of view, thereby assessing needs, preferences, and potential risks. Additionally, foresight scenarios actively inform and support the design and development of a dedicated Roadmap of AI in Law Enforcement 2040. The popAI roadmap aims to constitute a policy and practice-oriented resource towards building a responsible, ethical, and value-based AI application for LEA use. In short, foresight scenarios are an integral component of the overall project perspective of positive-sum thinking on AI in civil security.

In this context, the foresight scenarios methodology has been adjusted to fit the objectives of the project, recognising the complexity of this exercise and its interactive nature[6]. To this end, Trilateral Research followed an iterative, collaborative approach to co-produce the scenarios through wide stakeholder engagement in numerous occasions. The focal issues of the scenarios emerged and were validated via numerous activities considering all involved stakeholders and drawing upon controversies to ensure the inclusion of diverse views. Supplementing previous approaches, the foresight scenarios method in popAI was initiated with the controversy ecosystem mapping exercise in Task 3.1. This exercise was particularly important as it identified key controversies regarding the application of AI for civil security purposes, enabling then the mapping of all involved stakeholders and their respective discourses, as well as the charting of relevant legal frameworks[7]. Therefore, the task informed both focal issues, also enriched and validated by Task 2.3 and drivers meaning social, technological, ethical, and legal values that might impact the issue under consideration.

The engagement of diverse views from diverse stakeholders such as LEAs, citizens, researchers, and technologists through multiple methods, namely desk-based research, computational methods, and qualitative methods (policy labs, workshops)[8], informed and validated focal issues and drivers that shaped the foresight scenarios. A major outcome of the foresight scenario methodology adopted is to favour communication and connection between individuals, groups, and organisations with different perspectives and values. Indeed, as an integral part of the pop AI trans-disciplinary methodology, policy labs have been designed to facilitate knowledge exchange and improve understanding among EU LEAs along with experts, citizens, and relevant security domain stakeholders. Scenarios emerged from these policy labs as well as a dedicated workshop that is discussed in the next section.

The popAI project considers technology as a social construction that shapes and it is shaped by society in the broadest sense. This means that, to develop and regulate the use of AI in the security domain, it is crucial to comprehend the relevant factors, perspectives, needs, preferences, and risks by and posed to diverse stakeholders. To this end, the popAI project's method proposes the critical analysis of controversial cases of AI application in civil security as a key step to understand the social context within which technology is integrated and questions which technology, for what purposes and within which regulatory framework should be developed and used[9]. Including the results of controversy mapping in foresight scenarios affords recognition of real, widespread, and profound opposition to likely futures. By identifying and including such opposition in the narratives it allows formulating recommendations to assuage deep-seated societal concerns and better represent the full spectrum of societal values. In short, controversy mapping can turn foresight scenarios into a tool for techno-scientific citizenship in an era where "experto-cracy" tends to erode democratic process (see for example Jasanoff, 2012).

[6] European Foresight Platform, https://knowledge4policy.ec.europa.eu/foresight/topic/forlearn-online-foresight-guide_en

[7] D3.1 Map of AI in policing innovation ecosystem and stakeholders

[8] The methods will be further analysed in the dedicated method section (Section 3)

[9] D2.3 *The controversies and risks that will shape AI in the next 20 years* submitted on 30/11/2022 provides a detailed analysis on the importance of controversies' analysis.

The popAI foresight scenario method is informed by the overall project's positive-sum approach that promotes a consensus among European LEAs and involved stakeholders on AI in policing in developing a "European Common Approach". Broad acceptance of compliance and a future-focused roadmap aims at solid recommendations to policy makers with strong impact as they hash out an AI Act that ensures AI in policing is human-centred, socially driven, ethical and secure by design.

3 Methodology

Trilateral Research has adjusted the method to fit the purposes of the popAI project being in line with the European Commission JRC FOR-LEARN scenario building guidance[10] according to which for the scenarios to be effective, they need to be "plausible, consistent and offer insights into the future". Furthermore, external experts with different backgrounds need to be included in the process. The main steps of this approach are as following:

1. Identify the focal issue; start with a specific issue and considering key factors around it.
2. Identification and analysis of the drivers; identify the key drivers that will influence the key factors listed.
3. Importance and uncertainties; assess the drivers based on the degree of 'importance' of the focal issue identified in Step 1, and the degree of 'uncertainty' surrounding the factors and trends.
4. Selecting scenario logics; based on the ranking exercise select the scenarios logics.
5. Fleshing out the scenarios: Develop a number of internally consistent story lines which project as much as possible what learned through the process. Incorporate elements of both desirable and undesirable futures within the different scenarios.

The adjusted method enabled the collaboration between different tasks, promoting the engagement of diverse stakeholders through a variety of research activities. This section describes the different stages of the foresight scenario methodology as employed in the popAI project.

3.1 Identifying focal issues

In scenario development, it is essential to start with a focal issue based on which the scenario will be built. The focal issue can be generally understood as the question, or the problem, that we want to approach. The focus of the popAI project is the application of AI for civil security purposes which is quite broad to be used as a focal issue for the foresight scenario development. For this reason, more specific focal issues were necessary to create a set of scenarios that, together, can be used for the development of a credible roadmap. The focal issues of the scenarios were generated through the mapping and analysis of controversies and by the LEAs of the project.

3.1.1 Controversy Analysis

The controversies related to the use of innovation in policing have been mainly mapped in two tasks, namely Task 2.3 and Task 3.1.

[10] European Foresight Platform http://foresight-platform.eu/community/forlearn/how-to-do-foresight/methods/scenario/

Based on the civil security domain structure, Task 3.1 has organised controversies around six broad contexts: crime prevention involving mainly predictive policing; crime investigation; cyber operations; migration, asylum, and border control; LEAs' training; administration of justice[11]. The key controversial cases of AI application were identified for each context mapping and analysing the ecosystem around those: technology used, involved stakeholders, diverse discourses on risks and potentials. From the analysis conducted, no great controversies were identified in the training area.

Task 2.3 identified the most significant controversial technologies, namely: google glasses, smart meters, biometrics, facial recognition, CCTVs, encryption, body cameras, security scanners, and drones[12].

3.1.2 Policy Labs

Policy Labs have been designed as part of the foresight methodology approach. To this end, LEAs, when organising the labs, were instructed to identify case studies around which the discussions would take place. The respective activities in Task 3.4 have been extended and the first three policy labs out of the five planned were considered for the foresight scenarios in Task 3.5. However, the analysis showed that the case studies chosen and designed by the LEAs have been mainly around the same technologies and focal points, namely predictive policing for efficient resource allocation and automatic analysis of data.

3.1.2.1 Policy Lab 1 - Greece

The activities of the first Policy Lab were structured around two case studies prepared by the Hellenic Police. The case studies were formulated as follows:

a) predictive, research, and detection systems using crime data to improve policing and combat crime;
b) systems for predicting dangerous driving using video footage from traffic management cameras or other real-time footage to prevent traffic accidents.

The participants of the policy lab were from diverse backgrounds aiming to represent all the relevant stakeholder groups identified in Task 3.1. Representatives from the National Committee for Bioethics and Technology, Special Secretariat for Long-Term Planning and Research for the Future, European Union Agency for Asylum seekers, Hellenic Police, and local government, as well as companies providing integrated IT and communication solutions, and specialized lawyers actively participated in the event.

3.1.2.2 Policy Lab 2 – Germany

The second popAI Policy Lab was organised by the University of Applied Science – Police Affairs (HfoeD). Twelve participants attended the event with various expertise and backgrounds. The Policy Lab was structured around two use cases:

a) AI in support of mission control;
b) child pornography.

[11] Task's 3.1 outputs are reported in D3.1 Map of AI in policing innovation ecosystem and stakeholders
[12] Task 2.3 outputs are reported in D2.3 *The controversies and risks that will shape AI in the next 20 years*.

Participants were divided into groups to facilitate discussion and gathered later for a wrap-up session and some general comments. Each group consisted of participants from LEAs, ethics specialists, experts with a technical background and a moderator.

3.1.2.3 Policy Lab 3 – Slovakia

The third Policy Lab was organised by the Police Academy in Bratislava. The third lab was adjusted to include the popAI ethics toolbox. The group discussions concerned the LEAs' monitoring of social media based on a real case study from Slovakia regarding the murder of two people from the LGBTI+ community. Each working group was composed of a representative from the police practice or other law enforcement authority, a member working with the technological aspects of the AI tools, a member of the Police Academy in Bratislava and a member of another university or other authority that has an impact on law enforcement.

3.2 Key factors

Analysing the controversies and case studies discussed in the policy labs, the key factors that need to be considered when designing and developing foresight scenarios were also identified and discussed. These key factors have been enriched and validated through diverse methods such as computational methods namely: discourse overview via natural language processing (NLP) tagging and social listening (Task 3.2) as well as crowdsourcing activities (Task 3.3).

3.2.1 Computational methods

The computational methods were designed and informed by the findings of Task 3.1 and reported in D3.1 *Map of AI in policing innovation ecosystem and stakeholders*. The discourse overview via NLP tagging mainly indicated that the topics that were identified around the use of AI in LEAs were linked to phrases: 'human rights', 'free speech', 'against repression' and 'held accountable'.

The social listening activities[13] explored the key factors related to the main findings of Task 3.1 and prioritized by the project's LEAs. Here, the key findings related to the scenario development are presented in brief[14]. Social listening indicated that biometric identifiers produced the greatest volume of results. Even though biometrics is still the most discussed issue and has the highest number of negative results in absolute terms, mainly related to discrimination and bias, the discourse surrounding privacy was not overly negative. The discourse around predictive policing has been increasingly negative, especially with regards to algorithmic discrimination. Regarding police hacking, two subtopics generated most of the public discourse, namely: privacy and legitimacy, whereas discrimination also contributed to the topic with a highly negative sentiment. The representation of AI application in justice systems is dominated by the discussion surrounding the issue of

[13] Social listening is a way of monitoring web content for key themes and discursive trends. It is used by marketing professionals for their business purposes. Using mainly data from social media platforms, this allows them to then target users with very specific interests, maybe even specific people themselves for future campaigns. In the context of popAI, ECAS is conducting social listening in order to gather and assess the diverse citizen attitudes towards AI and policing. It should be noted that ECAS makes use of ethical social listening, which does not collect any data about the individuals, but is only interested in the content of the messages or conversations themselves. This prevents any possible biases about the data and respects the privacy of the people who voiced the opinions. popAI website. *Social Listening.* https://www.pop-ai.eu/social-listening/ [last accessed on 08/04/2023].

[14] For a detailed analysis, please read D3.3 *Citizens produced priorities and recommendations for addressing AI in the security domain*.

discrimination, indicating great concern on the algorithmic-assisted decision-making process being biased and discriminatory.

The topics were ranked based both on the average sentiment and the percentage of negative results as follows:

1. Police Hacking
2. Predictive Policing
3. Decision Making in the Justice System
4. Biometric Identifiers

The volume of discourse under "Cyber Operations" was not significant, therefore, is not discussed here.

3.2.2 Crowdsourcing activities

The crowdsourcing methodology has been employed in the popAI project to actively engage citizens so to understand their perceptions on the use of AI in the security domain. For the purposes of the foresight scenarios, the prioritization of the topics and key factors will be presented here.

Based on the controversy identification and taxonomy activities conducted in popAI, a range of topics and aspects of AI systems in the civil security domain was selected for the citizens to prioritize[15]. The same topics that were used for the computational methods presented above, namely: biometric identification, AI systems used to prevent crime (predictive policing), AI systems used in cyberoperations, police hacking, and justice decision-making tools.

For each of the five topics, citizens were asked to rate their level of agreement on eleven aspects of their implication and management:

1. Respect to human rights
2. Human oversight
3. Accuracy
4. Reliability
5. Respect to privacy
6. Legitimate access to people's data
7. Transparency
8. Prejudice and discrimination
9. Benefit to society
10. Sustainability
11. Accountability

In agreement with the social listening findings, the five topics were ranked from most to least concerning, with the contribution of 189 responses:

1. Police Hacking
2. Predictive Policing

[15] For a detailed analysis, please read D3.3 *Citizens produced priorities and recommendations for addressing AI in the security domain.*

3. Decision Making in the Justice System
4. Biometric Identifiers
5. Cyber Operations

3.3 Identification and analysis of drivers

To develop scenarios that are feasible and credible and thus useful, it is important to analyse the environment within which the technology is being developed and implemented. In these lines, the key drivers that will have great influence and impact on the issue in question – in this case, the application of AI in the civil security domain – needs to be identified. Drivers in a nutshell are factors that play a role in the future evolution of the landscape. In the context of popAI, the key drivers emerged from the policy labs where challenges and constraints were pointed out besides opportunities for AI use and the analysis of the Artificial Intelligence Act, proposed by the European Commission in April 2021 and currently under discussion in the European Parliament[16].

The policy labs have been presented above as well. In regard to key drivers' identification, it was evident in all policy labs discussions that LEAs expect from AI applications to support their work. AI systems can automatically conduct data analysis that is not possible with a manual approach. Such analysis can lead in pattern identification providing valuable insights to support their decisions. At the same time, organizational processes and lack of training were identified as obstacles for the use of AI systems and tools.

For the development of effective scenarios, it is important to also analyse the Artificial Intelligence Act that will significantly influence the application of AI in security domain. Furthermore, considering AI Act will result in the development of an effective roadmap and appropriate recommendations.

3.3.1 AI Act provisions related to law enforcement

Following the rational of the controversy approach discussed above, the proposed AI Act and political discussions surrounding it were analysed to support the development of scenarios. It is key to identify the controversies that exist in the current version of the AI Act and the political discussions surrounding it to inform the scenarios and understand potential impact. The steps for identifying the AI Act controversies related to law enforcement are as follows:

- Classification of the most recent version of the AI Act, the Council's General Approach of 6 December 2022 (Council, 2022), into its individual provisions, including a summary of each provision for easier accessibility.
- Identification of provisions directly addressing LEAs and/or concerning law enforcement.
- Mapping of the political landscape regarding these law enforcement provisions through the identification of the changes that the Council proposed in comparison to the previous version of the AI Act European Commission Proposal of 21 April 2021 (EP & Council, 2021), as well as supervising the ongoing discussions between the legislators as monitored by the press.

Through this process the following controversies have been identified and briefly discussed below.

[16] The text of the proposal is available at this link: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206

AI systems for activities concerning military, defence, or national security fall outside the scope of the AI Act

The most recent version of the AI Act excluded AI systems for activities concerning military, defence, or national security from its scope.[17] However, AI systems used for military purposes may be the ones that are most controversial and the ones to which the least transparency obligations apply. Still, their application is excluded from the scope of the AI Act. For a long time, Article 346 of the Treaty on the Functioning of the European Union (TFEU) was read as excluding the whole defence sector from the remit of EU law (Randazzo, 2014, p. 1). On the basis of established case law of the Court of Justice, however, it is now clear that this is – instead – a case-by-case derogation that is to be applied strictly in exceptional situations (Randazzo, 2014, p. 1). The key conditions for the application of Article 346 TFEU are necessity and proportionality (Randazzo, 2014, p. 1). This shows that the rigorous exclusion of AI systems for activities concerning military, defence, or national security from the scope of the AI Act was purely political, which adds to its controversiality.

High-risk AI systems: Remote biometric identification systems

As mapped in more detail in popAI deliverable D2.3, remote biometric identification systems – listed as high-risk systems in the AI Act – bear multiple controversies, especially facial recognition (FR). They most prominently include bias in FR technologies and misidentifications.[18] However, the main controversy is that these systems give authorities the ability to track people and collect their personal data which is considered incompatible with democracy because it raises moral questions, compromises privacy, leads to mass surveillance and infringes civil liberties.[19] Generally, human right campaigners and civil societies argue that this technology might be easily abused to spy on societies and marginalised individuals like migrants, people of colour, or residents in low-income neighbourhoods.[20]

The AI Act makes a difference between remote biometric identification systems and real-time remote biometric identification systems. While the former systems are classified as high-risk[21], the latter systems are generally prohibited, unless certain exceptions apply[22], as it's discussed below.

Real-time remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement are prohibited unless and as far as such use is strictly necessary for one of the objectives listed in Article 5.

The use of real-time remote biometric identification systems, defined as "remote biometric identification system whereby the capturing of biometric data, the comparison and the identification all occur instantaneously or near instantaneously"[23], in publicly accessible spaces for the purpose of law enforcement is prohibited, unless and as far as such use is strictly necessary for one of the following objectives:

- The targeted search for specific potential victims of crime;

[17] Article 2(3) AI Act of 6 Dec 2022
[18] popAI D2.3, pp. 28-29
[19] popAI D2.3, pp. 29-30
[20] popAI D2.3, p. 30
[21] Article 6(3) AI Act of 6 Dec 2022
[22] Article 5 AI Act of 6 Dec 2022
[23] Article 3(37 AI Act of 6 Dec 2022

- The prevention of a specific, substantial, and imminent threat to the critical infrastructure, life, health, or physical safety of natural persons or of a terrorist attack;
- The localisation of a natural person for the purposes of conducting a criminal investigation, prosecution or executing a criminal penalty for offences referred to in Article 2(2) of the European Arrest Warrant Council Framework Decision[14], or other specific offences punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least five years.[24]

The use of real-time remote biometric identification systems falling under any of these three exceptions must, however, take into account the nature of the situation giving rise to the use of the system, the consequences of the use of the system for the rights and freedom of all persons concerned, and necessary and proportionate safeguards and conditions in relation to the use.[25] In any case, the use of such a system must be subject to prior authorisation by a judicial or independent administrative authority of the Member state in which the use is to take place.[26] Consequently, the approach of Article 5 demonstrates a valid compromise of allowing the use of real-time remote biometric identification systems by LEAs in a very safeguarded manner only.

Despite this seemingly well-balanced compromise, the scope of the use of real-time remote biometric identification systems by LEAs seems to continue to be a controversial point of discussion among the legislators. Interestingly, the latest version of the AI Act removed the particular reference to 'missing children' from "specific potential victims of crime", suggesting that a debate concerning the protection of children took place between the legislators but seems like it was decided against referencing children as a vulnerable group of persons. Additionally, "other specific offences punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least five years" were added to the exceptions listed above, thereby expanding the options for using real-time remote biometric identifications systems by LEAs.

The EP's co-rapporteurs want live biometric identification in publicly accessible spaces to be banned altogether (Bertuzzi, AI Act: EU Parliament's crunch time on high-risk categorisation, prohibited practices (EURACTIV), 2023). In this case, the high-risk use case would be limited to ex-post identification (Bertuzzi, AI Act: EU Parliament's crunch time on high-risk categorisation, prohibited practices (EURACTIV), 2023).

Some AI systems for law enforcement purposes are no longer included in the list of high-risk AI systems in the most recent version of the AI Act

Some AI systems for law enforcement purposes are no longer included in the list of high-risk AI systems in the most recent version of the AI Act, such as:

- AI systems for the detection of deepfakes
- AI systems for crime analytics regarding natural persons, allowing LEAs to search complex related and unrelated large data sets available in different data sources or in different data formats to identify unknown patterns or discover hidden relationships in data.

[24] Article 5(1)(d) AI Act of 6 Dec 2022
[25] Article 5(2) AI Act of 6 Dec 2022
[26] Article 5(3) AI Act of 6 Dec 2022

This controversy speaks more or less for itself, but it remains to be seen if this offers a better or worse protection of citizens and other stakeholders. The debate on which AI systems should be included in the list of high-risk AI systems or even be prohibited is certainly ongoing (Bertuzzi, AI Act: EU Parliament's crunch time on high-risk categorisation, prohibited practices (EURACTIV), 2023).

Potential controversies relate to the exceptions LEAs enjoy if they are users of high-risk AI systems, such as:

- Comply with instructions of use – human oversight and monitoring of AI system – and inform the provider or distributor and suspend the system when identifying a serious incident (**exception:** sensitive operational data of users of AI systems which are LEAs);[27]
- Users that are public authorities, agencies or bodies (**exception:** law enforcement, border control, immigration or asylum authorities) must comply with registration obligations as per Article 51);[28]
- Transparency obligations for users of certain AI systems that LEAs are mainly exempted from.[29]

Complete ban of AI-powered predictive policing methods (Bertuzzi, AI Act: EU Parliament's crunch time on high-risk categorisation, prohibited practices (EURACTIV), 2023)

The placing on the market, putting into service or use of AI systems for the evaluation or classification of natural persons over a certain period of time based on their social behaviour or known or predicted personal or personality characteristics, with the social score leading to either or both of the following:

a) detrimental or unfavourable treatment of certain natural persons or groups thereof in social contexts which are unrelated to the contexts in which the data was originally generated or collected;
b) detrimental or unfavourable treatment of certain natural persons or groups thereof that is unjustified or disproportionate to their social behaviour or its gravity.[30]

German Constitutional Court strikes down predictive algorithms for policing: The systems used by the Hessen Police were deemed unconstitutional because they violated the right to informational self-determination (Killeen, 2023). The application of AI-driven tools by law enforcement, as in the case of the Hessen Police, is a controversial point in the discussions on the AI Act (Killeen, 2023). The EU Council of ministers has been pushing to give police forces more leeway, whilst progressive MEPs are arguing for a more restrictive approach (Killeen, 2023). Most recently, upon the request from left-to-centre lawmakers in the EP, the list of prohibited practices was significantly expanded to include biometric categorisation, predictive policing, and facial recognition databases based on indiscriminate scaping, as per the controversial company Clearview AI (Bertuzzi, AI Act: European Parliament headed for key committee vote at end of April, 2023). The amendment is yet to be adopted with the EP's vote on the Act by the end of April 2023.

[27] Article 29(4) AI Act of 6 Dec 2022
[28] Article 29(5a) AI Act of 6 Dec 2022
[29] Article 52 AI Act of 6 Dec 2022
[30] Article 5(1)(c) AI Act of 6 Dec 2022

3.4 Scenario development

The scenario development followed a collaborative approach with the Task 3.5 research team being in close collaboration with the task leaders of the aforementioned activities. The purpose was to analyse the findings to further develop, refine, and adjust the scenarios that were defined in the three policy labs presented above and the workshop held in Rome where popAI LEAs, members of the Stakeholder Advisory Board and external experts participated. In total, eight external experts participated in the workshop with expertise in ethics, law, security, and IT representing areas of academia and research, policy, industry, and civil society.

The workshop lasted 1.5 hours with the twofold objective of foresight scenarios in popAI, namely, to bring together diverse stakeholders discussing the short-term (5 years) future of AI application in policing and the creation of the scenarios themselves.

Participants were briefly introduced to the foresight scenario methodology and a sample scenario as a tangible example was presented. Following, four areas of AI application by LEAs were presented as classified in Task 3.1, namely: predictive policing; crime investigation; migration, asylum, and border control; cyber operations. Participants were split in four groups and assigned one of the above areas each.

An interactive presentation (ANNEX) had been created which participants could advise and use to support the discussions and development of the scenarios. Three groups were physically present, whereas a fourth group participated virtually. The presentation was organised as follows for each area of AI application:

- expectations and risks (identified in the activities discussed above);
- sample controversial case study;
- working sheet to support discussion on the expectations of diverse stakeholders;
- working sheet to support identification of relevant technology;
- working sheet to support identification of diverse stakeholders involved;
- working sheet to support identification of potential risks;
- working sheet to compile their scenario.

The leading researcher from Trilateral Research grouped the scenarios developed at the workshop with the ones produced for and at the policy labs as there were overlaps from diverse stakeholders. Subsequently, the scenarios were refined and enriched by the analysis described in this methodology section. More specifically, an assessment of the importance and uncertainties was carried out and based on this exercise the scenarios logics were selected. Next, the scenarios were fleshed out following the criteria of the "EFP European Foresight Platform – supporting forward looking decision making"[31] and specifically the following criteria:

1. **Plausibility:** the scenarios to be finally selected need to be plausible, meaning they need to describe a future that is possible to occur.
2. **Differentiation:** the set of the scenarios need to consist of diverse stories, structurally different, so they are not perceived as simple variations of a central story line.

[31] http://foresight-platform.eu/community/forlearn/how-to-do-foresight/methods/scenario/

3. **Consistency:** the scenarios need to have an internal consistency to support their credibility.
4. **Decision making utility:** each scenario separately, and all of them as a set, should highlight potential issues in the future that need to be considered when making decisions.
5. **Challenge:** the scenarios should challenge the conventional wisdom existing about the future.

4 Foresight scenarios

This section will present the scenarios produced for each of the five broad contexts around which the civil security domain is structured, as classified in Task 3.1, namely: crime prevention involving mainly predictive policing; crime investigation; cyber operations: migration, asylum, and border control; administration of justice[32]. The scenarios present a potential future in five years' time.

4.1 Crime prevention/predictive policing

Past will always define future.

AI algorithms for civil security purposes use police data, combined with other datasets such as demographic, abstracted data from mobile phones, and socio-economic data, as well as data that come from hotspot methods to predict when and where criminal activities are most likely to occur. Interoperability of diverse data sources is authorised in support of crime prevention and community safety. Several local 'blacklists' have been created among European Member States that can be linked, compared, and updated in a European level. Based on advanced algorithmic processes, AI-powered surveillance systems are installed in areas flagged as high-risk while drones often circle over.

Federico is an Italian political activist. He has studied chemistry but is unemployed. When he was a teenager Federico was a musician and through his music, he was protesting xenophobia and racism. Due to his beliefs, he was often victim of far-right extremists. He never gave up on his ideas. Last year, Federico visited some family friends in Barcelona with his parents for two weeks. During their stay, his mother was feeling rather weak and therefore they mainly relaxed at their friend's hotel without visiting tourist attractions. At the same time of the year, in Spain's capital, there were riots on the streets against austerity. Several people were prosecuted. On their way back to Italy, Federico and his parents were asked a few questions by the airport security staff.

Two weeks after their return in Italy, Federico bought online a ticket for a big concert that didn't match his music taste. Political figures from the government would also attend this concert. In the same afternoon, Federico joined a telegram group calling for action against European austerity policies. Some of the concert's technicians were also members of this group as well as left wing extremists.

The night of the concert Federico noticed that a drone was following him. He had already a difficult day. Suspecting his past might be still triggering algorithmic systems to surveil him he gets angry. The sensors in his car record Federico's tension. The algorithm flags Federico as a high-risk case. The AI-powered system sends a signal to the next available operational unit based on the distance as well

[32] Task 3.1 classified six areas including LEAs' training. However, training has not been included here as the focus is the use of AI for civil security.

as their available equipment, skills, and experience. A police car approaches him a few minutes later and the police officer asks him to follow them to the nearest police station. Federico reacts but complies with the request. Federico is soon released as his case was a false positive. Police officers insert the new data in the system and Federico's scoring is updated.

4.2 Crime investigation

AI investigator. Case closed.

A woman is found dead in her house. Mary was 36 years old, single, and a lawyer. A friend of hers has called the police. Mary didn't show up at their meeting, nor responded to her phone. Her friend went to her house and even though her car was in her parking space, Mary wouldn't open the door. The police arrive and secure the scene. The investigative police officers collect evidence. They are equipped with advanced AI-assisted technology. They have body-worn cameras that scan the space and digitalise evidence that can be analysed in real time and compared with other relevant databases, local, national, and European to evaluate the reliability of evidence and also make suggestions based on potential patterns.

The police system grants access to her phone and analyses the extracted data like her journey home, who she contacted in her last hours and the location of relevant activities and communications. The system also gets access to her messages. All evidence collected is stored in a digital archive. AI systems run through databases of similar crimes looking for patterns. The system suggests further investigation practices to police officers and flags potential suspects. The system scans potential suspects' digital archives and provides their ranking to the police officers. LEAs do not always have complete data. However, the scan runs through diverse databases, including those from private data providers, and adjusts the algorithm to minimize any false positives.

Police investigators use the insights of explainable AI to understand the criteria of the suspects and assess the evidence. They upload their assessment in the system and the ranking is further adjusted. Further evidence is collected from CCTV cameras in the main suspects' area, their mobile phones, and smart devices of their houses. The system produces reports for the main suspects highlighting the evidence that flags each of them and potential interrogation questions that can complete the data.

Police officers send the case files of the suspects for prosecution. During the interrogation, an AI-based CCTV camera analyses the emotions and facial expressions of the suspects, informing the system in real time and assisting the process. The perpetrator confesses and is arrested.

4.3 Cyber Operations

Don't shoot the artist.

Crimes of child pornography and exploitation have been rising with the increased use of the internet and the widespread use of the dark web. At the same time, the cases of human operators experiencing post-traumatic disorder and other mental health issues due to daily exposure to child pornography are rising dramatically. Therefore, LEAs have been using an AI system that crawls the web, including social media sites, for images of child sexual abuse. The system allows automated processing, assessment, and prioritisation of child sexual abuse material (CSAM). In addition, once such material is flagged the system records the 'journey' of the material and identifies all internet

users, including dark web and peer-to-peer file sharing networks, who interacted with it, including posting, reposting, downloading, saving, processing and so on.

The system then runs an automatic crawling of online sources for complementary information for investigations in compliance with the national legal requirements and provides a score flagging those representing a high risk. The algorithm that provides the scoring is based on their history, online activity, and other factors such as demographics, network, and others. The criteria used by the algorithm are not public. LEAs have access to private databases for the flagged users.

The use of the system has proved efficient in many cases and now, the human operators have to assess much less volume of child abuse material, especially in cases of objection to the automated results and further investigations. A huge volume of such material has been removed from the internet and many abusers are jailed.

John is a 42-year-old Englishman who has moved to Greece since Brexit. John works as a photographer. He is homosexual and last year he adopted a 2-year-old child with his partner. John mainly promotes his work through social media such as Instagram, TikTok, and YouTube. He shares photos, as well as snapshots "behind the scenes" sharing photography tips. John is inspired by the seaside. This is why he chose to live on a small Greek island. Since he became a father though, his main inspiration are the children and their relationships with adults, with the environment, and so on. In this context, he shares pictures online depicting young children in swimsuits with adults nearby. Recently, he joined online communities for parents and children. He is preparing an exhibition on the empowerment of children through photography and conducts some research.

The automatic system falsely identifies some of his photos as CSAM as an algorithm embedded in the web crawler proved unfairly biased against specific characteristics – sexual orientation, age, background, etc. All of his photos are removed, and his accounts are suspended. A police officer appears at John's house and takes him to Athens for further investigation. He is falsely accused, and these accusations have terrible effects on his work and life. Even though he is discharged, this whole situation has ruined both his professional fame and his relations on the small island. He and his family decide to move to another place, and he slowly starts working again using a nick name. Along with other photographers, cartoonists, and other artists, they form a campaign group to make the algorithm fairer.

4.4 Migration, Asylum, and Border control

Crossing the invisible borders.

Brussels' airport has installed an AI-based intelligent video surveillance system to monitor travellers' entire trip from check-in to boarding, using solely their face as a form of identification. The system uses a facial recognition system with CCTV cameras installed in the airport. Biometric templates created with the camera footage are used for comparison with the travellers' passports. Besides, the system monitors behaviour within the border control areas, with the purpose of producing warnings for potential anomalies and suspicious events. The system also analyses a combination of behaviour and appearance risk indicators which contribute to an aggregated risk calculation, from both negative and positive indicators. In cases where the system is triggered, the biometric templates are also compared to datasets of criminals and suspects of crime.

Joe enters Brussels' airport to catch his return flight home after a business trip. He is a journalist in the Netherlands. In Brussels, he covered a special European Council meeting regarding EU migration and asylum policy. Joe is himself a migrant from Syria. His family managed to migrate when Joe was just two years old. Even though he only briefly lived in Syria, he was often treated differently because of his ethnicity. He managed to study nevertheless and for the last three years, he has been working as a freelance journalist.

Joe arrives early at the airport and instead of proceeding to the security check, he wanders around the arrivals area as he talks on the phone with a colleague. Without realising it and in pursuit of a quiet place, he walks just inside of a restricted area of the airport as he makes phone calls and checks his messages, emails etc.

Video surveillance analysis based on AI triggers and raise an alert based on a combination of risk indicators triggered by his appearance, behaviour, and current location. The alert activates the process of automated analysis across multiple datasets. Joe's full history comes up including his passport information, articles he has published, public posts on his social media, as well as CCTV footage from the demonstrations outside the European Parliament where the special meeting took place.

Joe walks towards his gate where he attempts to scan his ticket. However, his attempt fails and, in the meantime, a security officer appears and asks him to follow her/him. Joe is not surprised as he is aware of the AI-based intelligent video surveillance system installed in the airport. Using his journalist hat, he is asking for a report on the algorithmic decision. The officer cannot disclose the AI explainability report he received as the indicators are classified on the basis of public safety. However, he displays the EU certification which has assessed and validated the AI system as operating in a responsible and trustworthy manner. Joe is filing an official report asking for full disclosure before he continues his journey.

4.5 Administration of justice

Guilty till proven innocent.

AI systems have been gradually employed in the courts of the European Member States. Indeed, the use of AI to support the decision making at every stage of the criminal justice system is encouraged given the large number of cases to be judged. In this line, algorithmic tools have been assisting the decision-making process on whether a prosecuted person should be immediately released as innocent, if they should have a financial penalty, or the case should be assessed in court. The AI system at this stage is built on data from diverse sources, including the history of the prosecuted persons that exist in police database, the national databases, as well as all the evidence collected throughout the investigation process. Data can be completed by social media and the web depending on the seriousness of the crime.

If the case goes to court, the system is further fed with the evidence presented in court in real time. At the end of the hearing process, the system makes the calculations based on all the data, looking for patterns and comparing the case with similar past ones. Finally, it suggests to the judge the risk of reoffending within the following five years and indicates if the risk for an individual is low, medium, or high. The scoring is accompanied by a report that indicates the data and the criteria based on which the score emerged.

Nadia is approaching a jewellery store when a man passes by her, falling into her in his rush. She ignores the situation and enters the store to buy a present for her mother's birthday. As soon as she enters the security door closes behind her and a police officer arrests her. Nadia is totally confused. She tries to protest but everything happens very quickly. In her bag, they find a stolen ring with a diamond. She knows she did not steal the ring, but she cannot prove it. Nadia has been raised in a rather problematic household. Her father was an alcoholic with a history of committing intimate partner violence. They were often in trouble with the police. She knows that she has a police record even though she was the victim. Similarly, as a teenager, she also ended up at the police station following a fight with some girls that were bullying her at school.

The AI system assigned her a high-risk scoring suggesting two years in prison. Nadia objected and her lawyer asked for the CCTV footage of the area. The scene where the man falls into her while he is exiting the jewellery store is captured. The system runs a check using the facial recognition to compare the man's face with other databases. The person is identified but the system gives low scoring. He is a middle-class businessman with no record with the police.

5 Discussion of the scenarios

The five scenarios presented in section 4 depict plausible futures in the next 5 years. Therefore, the scenarios reflect the existing technocentric approach that aims at collecting and analysing data from diverse databases including private data providers. The scenarios showed how different technologies already in the making or in pilot phase might be used collaboratively in different areas to assist the LEAs' work on different levels based on their current needs. Also, the scenarios consider the AI Act as the regulatory framework as it is currently designed and is expected to be binding for LEAs use of AI.

The focal point of the scenarios can be perceived as common, namely the application of AI in civil security domain. A common focal point between the scenarios provides consistency and coherency for the role they are to play in the roadmaps' development. At the same time, the stories are differentiated as they depict AI use in different LEA contexts which is key for the legal justification of the technology and the social acceptance. Specifically, the scenarios are based on the application of AI powered systems in the five main domains of the civil security, namely, crime prevention, crime investigation, cyber operations, migration, asylum, and border control, and administration of justice. Furthermore, the storyline chosen aims at telling the story from different perspectives raising different points for discussion in terms of technology development, organizational processes, and regulation as well as risks and opportunities for diverse involved stakeholders such as LEAs and citizens. The table below (Table 3) summarises the focal issues, the envisaged technology, the main drivers, and key factors that are the most important and the most uncertain for each scenario. This list is not exhaustive but provides a general picture for a primary discussion that is to be more detailed as described in the next section.

Table 3 Summary of popAI foresight scenarios

Title	Focal issue	Envisaged Technology	Drivers	Importance	Uncertainties
Past will always define future.	Use of diverse databases and AI-powered technology for predictive policing	AI algorithms, combined datasets, AI-powered surveillance systems, drones, sensors, social scoring	Advanced AI systems, interoperability, LEAs' desire for effective prediction, AI Act, mass surveillance	Predictive policing assisted by AI-powered technology, increasingly advanced technology, mass surveillance	Maturity of technological development in the next 5 years, AI Act
AI investigator. Case closed.	Use of diverse databases and AI-powered technology for crime investigation	body-worn cameras, digitalization of evidence, AI algorithms to analyse and compare evidence with other relevant databases, local, national, and European, identify patterns and compare with similar cases, AI-powered ranking of suspects , emotional detection	Advanced AI systems, interoperability, LEAs' need for AI assistance in crime investigation, AI Act	Crime investigation assisted by AI-powered technology, advanced technology to enable comparison between diverse archives of past crimes	Maturity of technological development in the next 5 years
Don't shoot the artist.	Use of AI systems crawling the web for cyber operations and specifically child pornography and exploitation	AI enabled crawling, automated processing, assessment, and prioritisation of CSAM, identification and scoring of CSAM users	Human operators experiencing post-traumatic disorder and other mental health issues, Advanced AI systems, potential biased technology, AI Act, Human Rights such as privacy and	Assistance of human operators' work, effective identification of CSAM and criminals, discrimination	Human rights and AI Act, technological advancement to crawl and analyse data on dark web

			freedom of expression		
Crossing the invisible borders.	Use of AI-powered technologies to enable border control with minimal human interference	AI-based intelligent video surveillance system, facial recognition, biometric templates, CCTV cameras, AI assisted risk assessment.	LEAs desire for AI assisted border control using less human resources, AI act, interoperability of diverse databases	Border control with less human interference, AI Act	AI Act, advancement of technology to enable such levels of interoperability
Guilty till proven innocent.	Use of algorithmic tools to assist court decision-making process	AI algorithms for risk assessment, interoperability between different databases	AI tools to support criminal justice system due to large volume of cases, advanced algorithmic technology, AI Act	Assistance of criminal justice system in. regards to primary assessment of cases to reach the court, assistance on decision making regarding sentences.	AI Act, human rights, biased technology

The main technological advancement that is key in all different scenarios is the capacity of the algorithms to be informed by diverse databases and provide predictions, rankings, and recommendations based on identified patterns or specific design. The constant update of the databases described in the scenarios through any activity of our lives, digital or not, poses discussions around mass surveillance in the name of security. Even more so, the resulting predictions regarding the potential crime and/or criminals are of great significance and raise uncertainties regarding both the technological feasibility and the regulatory framework. Furthermore, it is important to underline that AI assistance in crime investigation raises less concerns than in the case of predictive policing that might result in a surveillance society where human rights are at stake. Also, the scenarios depict cases where AI innovation can be driven by the LEAs and/or societal needs as is the case of manual assessment of CSAM, or the AI pattern identification of past crimes to assist the investigation efforts. In these cases, it is easier to identify the technological developments required to respond to the specific need and develop it following ethics- and privacy-by-design approach. Other scenarios, such as AI use for predictive policing or border control, depicted a more technocentric approach. In this context, the focus is on the technology and how it can be applied to support in general LEAs domains raising more risks and with not many tangible criteria for assessment.

The scenarios depicted key factors identified in previous research activities such as the probable discrimination against specific groups of people based on the bias of the systems as well as the need for transparency and accountability regarding the systems in use and the processes followed. The

detailed analysis and assessment of the scenarios will be conducted in the next phase in the context of Task 5.5 as it will be discussed in the next section.

6 Conclusions

Foresight Scenario is a widely used methodology that is increasingly relevant and important for policy making processes. The methodology was adopted to fit the purposes and objectives of the project contributing to popAI roadmaps (T5.5) as a resource towards building a responsible, ethical, and value-based AI application for LEA use. Specifically, the foresight scenarios presented in this report will feed into the Roadmap of AI in Law Enforcement 2040.

To this end, an iterative and collaborative approach was adopted encouraging and enabling the participation of diverse stakeholders in the development of the scenarios. popAI's foresight methodology informed and is informed by the research activities in work package 3 (WP3) which are designed to explore and understand stakeholders' stances regarding the AI application in the civil security domain.

Policy Labs (T3.4) have been designed following the foresight scenarios approach. LEAs are invited to provide case studies of LEAs use of AI, existing or futuristic, and discuss with external stakeholders the opportunities and risks emerging as well as mitigation actions. The findings of three Policy Labs, organised by the Greek, German, and Slovak LEA partners as well as the controversies identified in Task 3.1, and the computational methods employed in Tasks 3.2 and Task 3.3 exploring the stakeholders' views regarding the use of AI by LEAs informed the design of the foresight scenarios providing focal issues and drivers. Furthermore, a dedicated workshop for foresight scenario development was organised consisting of popAI partners and external participants and representing diverse stakeholders' groups. The analysis of all the aforementioned activities and the current AI Act version resulted in the main focal issues, the key drivers, and factors that shaped the foresight scenarios reported in this deliverable.

The richness of the foresight scenarios constitutes their utilisation and analysis significant for the development of the popAI roadmaps and specifically the Roadmap of AI in Law Enforcement 2040. According to the Foresight method followed here, the next stage is turning the scenarios into a strategy which is the aim of the Task 5.5. At this step, the five scenarios presented above will be analysed based on their implications regarding the development of responsible, ethical, and value-based AI use for LEAs purposes.

The next phase requires the participation of representatives of all identified stakeholder groups in Task 3.1 namely, LEAs and police academies, researchers from social studies and humanities, policy makers, government and public bodies, technologists/data scientists, civil society organisations, national and local authorities, as well as industry. popAI's Stakeholder Advisory Board provides already a very diverse background to support this stage. In this phase, the popAI team will organise virtual and hybrid workshops to assess the scenarios presented here. The scenarios will be carefully analysed based on the opportunities and threats that each one poses for the European values and the societal security. The aim is to identify which opportunities and threats are common to all, or nearly all, the scenarios so to base the strategic thinking on those ones. Following, the organizational, technological, and regulatory preparedness will be discussed so to explore the core competencies and the respective gaps. The analysis of the discussions will result in developing a portfolio of

strategic priorities that in combination with the WP4 recommendations will result in a future-focused roadmap and AI Act consultation.

7 References

Bertuzzi, L., 2023. AI Act: EU Parliament's crunch time on high-risk categorisation, prohibited practices (EURACTIV). [Online] Available at: https://www.euractiv.com/section/artificial-intelligence/news/ai-act-eu-parliaments-crunch-time-on-high-risk-categorisation-prohibited-practices/ [Accessed 4 April 2023].

Council, 2022. Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence and amending certain Union legislative acts - General approach (6 December 2022), Brussels: Interinstitutional File: 2021/0106(COD).

d'Aquin, M., Troullinou, P., O'Connor, N.E., Cullen, A., Faller, G. and Holden, L., 2018, December. Towards an" ethics by design" methodology for AI research projects. In Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society (pp. 54-59).

Ellis, T.S. and Griffith, D., 2000. The evaluation of IT ethical scenarios using a multidimensional scale. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *32*(1), pp.75-85.

EP & Council, 2021. Proposal for a Regulation of the European Parliament and of the Council laying down hamronised rules on artificial intelligence and amending certain Union legislative acts, Brussels: COM(2021) 206 final.

European Commission. (n.d.). *Strategic foresight*. European Commission. Retrieved March 21, 2023, from https://commission.europa.eu/strategy-and-policy/strategic-planning/strategic-foresight_en

European Foresight Platform. (n.d.). *Scenario method*. European Foresight Platform. Retrieved March 21, 2023, from http://foresight-platform.eu/community/forlearn/how-to-do-foresight/methods/scenario/

Jasanoff, S., 2012. *Science and public reason*. Routledge.

Randazzo, V., 2014. Article 346 and the qualified application of EU law to defence, s.l.: Brief Issue.

Kahn, H., & Wiener, A. J. (1967). The use of scenarios. *The Year 2000 A Framework for Speculation on the Next Thirty-Three Years*, 262-264.

Killeen, M., 2023. German Constitutional Court strikes down predictive algorithms for policing (EURACTIV). [Online] Available at: https://www.euractiv.com/section/artificial-intelligence/news/german-constitutional-court-strikes-down-predictive-algorithms-for-policing/ [Accessed 4 April 2023].

Ramirez, R., Mukherjee, M., Vezzoli, S. and Kramer, A.M., 2015. Scenarios as a scholarly methodology to produce “interesting research”. *Futures*, *71*, pp.70-87.

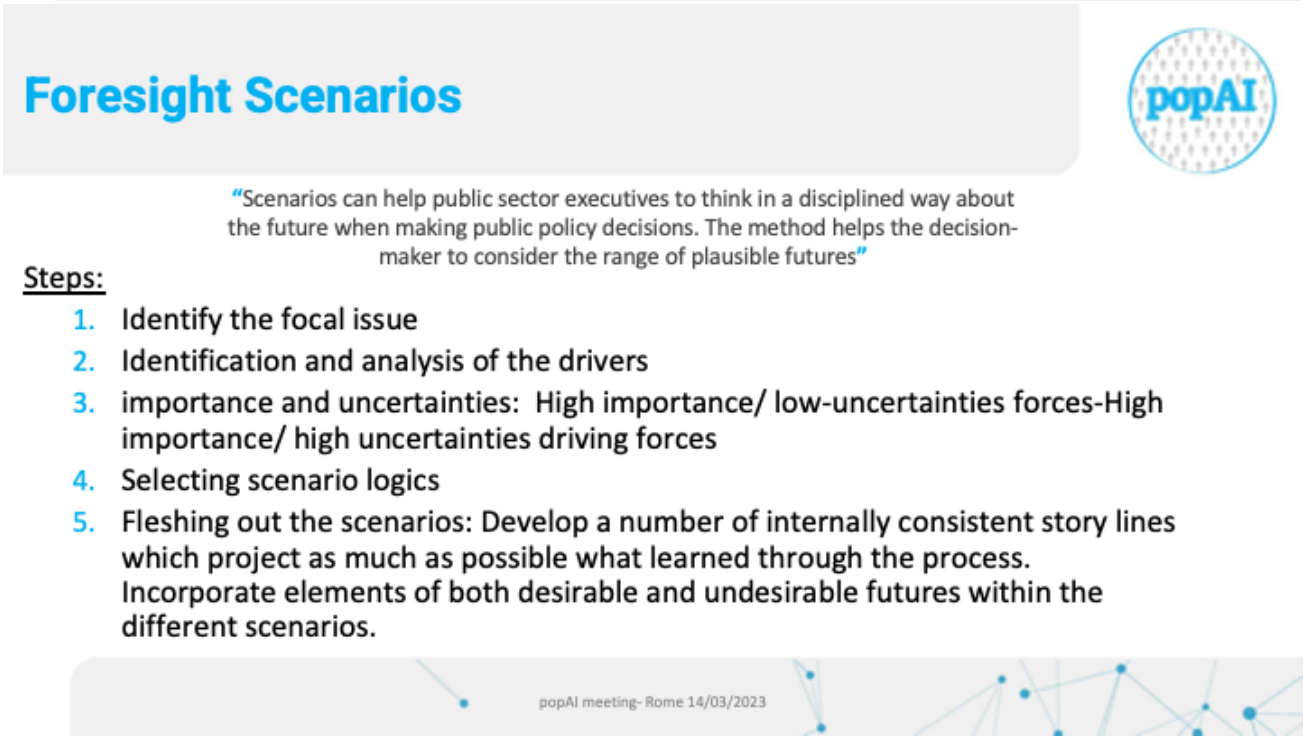
Troullinou, P. and d’Aquin, M., 2018. Using futuristic scenarios for an interdisciplinary discussion on the feasibility and implications of technology. Black Mirror and Critical Media Theory, p.69.

Troullinou, P., Tiddi, I., and d’Aquin, M. (2017), Proceedings of the Re-coding Black Mirror 2017 Workshop co-located with 16th International Semantic Web Conference (ISWC 2017), CEUR-WS proceedings, http://ceur-ws.org/Vol-1939/

Wright, D., Stahl, B., & Hatzakis, T. (2020). Policy scenarios as an instrument for policymakers. *Technological Forecasting and Social Change*, *154*, 119972.

8 ANNEX

Workshop Interactive Presentation



Foresight Scenarios

Surveillance is Coming Home

Arriving back from a holiday in Florida in 2016, the Jones family face a rather different border. Both Britain's and the USA's immigration and border control services, along with those of all EU countries and other G10 industrialised countries, are outsourced to the same transnational private consortium, BorderGuard25. Continued fears of illegal immigration and government rhetoric about the 'War on Terror' led these governments to implement a 'smart border' scheme. Passport control is now a series of cameras and scanners taking images of face, iris and fingers, which are compared with those on the standardised biometric passports, or in Britain's case, the ID card, introduced across the G10 countries and the EU26. The data on the built-in RFID chip now includes all citizenship, immigration, visa and criminal justice data, along with health information, and is compared instantaneously with both national and international databases, as well as a whole raft of data-mined information on consumer transactions that BorderGuard gets from specialist companies27. For most of the family the transition is swift, but for grandmother Geeta there are problems. Pakistan has not yet signed up to the full version of the smart borders scheme and Geeta has never bought a biometric passport. She consequently has to wait in line for several hours and is subjected to various extra searches and questions. Despite her British ID, mother Yasmin's obviously 'Asian' features also mean that her movement through the border triggers alerts and extra questions. Then, at customs, everyone is subjected to a full-body scan, a virtual strip search...

A Report on the Surveillance Society For the Information Commissioner,
by the Surveillance Studies Network Public Discussion Document September 2006

popAI meeting- Rome 14/03/2023

Predictive policing

"the use of analytical techniques by law enforcement to make statistical predictions about potential criminal activity"

(Brayne et al., 2015, pp. 1)

Expectations:

- support crime prevention providing an opportunity to better predict, anticipate and prevent crime

Risks:

- Historical data might be biased based on past discriminatory policy decisions; unbalanced and inaccurate datasets regarding ethnic minorities, discriminatory impact not only to a person but also at a community level affecting location data too, especially when minority groups cluster in a similar location. Some individuals or neighbourhoods could be overpoliced, amplifying stereotypes, discrimination, and prejudice

popAI meeting- Rome 14/03/2023

Predictive policing; Case study: Gangs Violence Matrix – Metropolitan Police (UK)

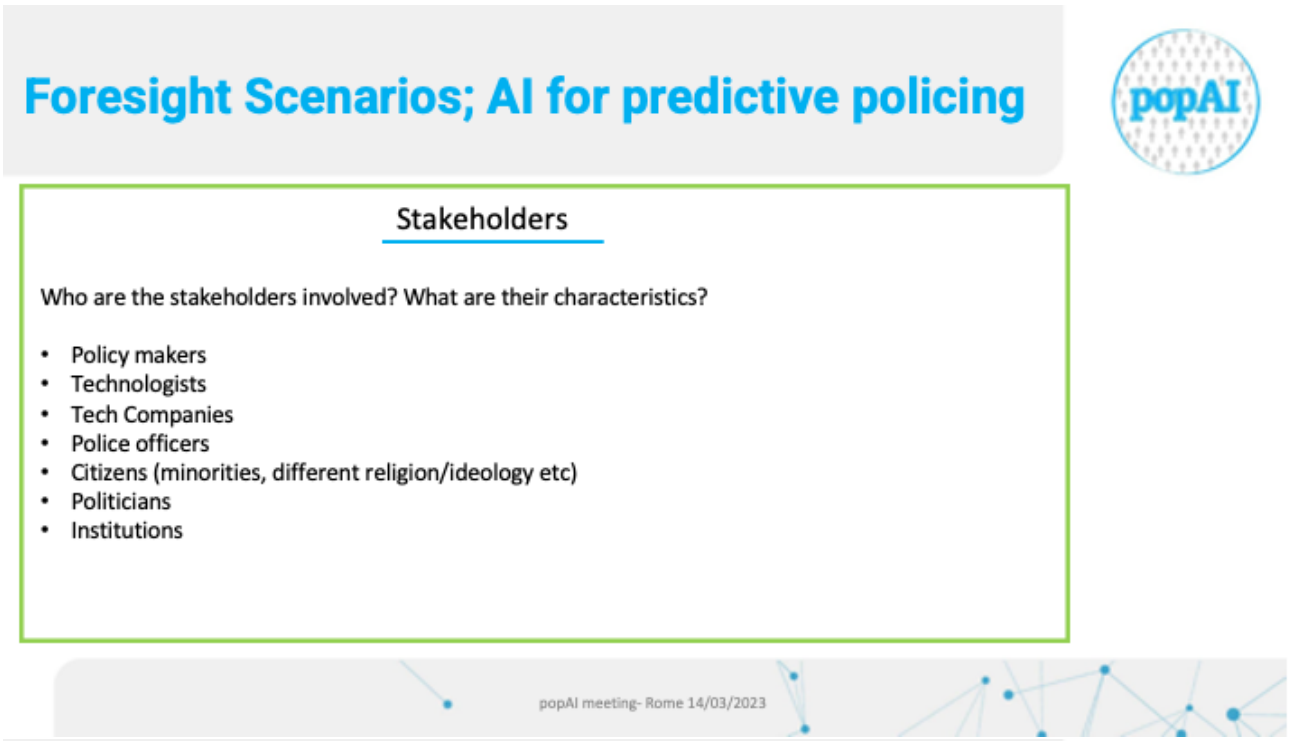
- Since 2012, the Metropolitan Police (UK) has been using the Gangs Violence Matrix (GVM) to identify and risk-assess individuals across London involved in gang violence and identify those at risk of victimisation. The GVM creates a scoring system based on evidence of individuals committing violence and weapon offences, police intelligence about weapon access, or their involvement (or risk of involvement) in gang violence.
- The scores obtained rank individuals, both adults and minors, as Red, Amber or Green reflecting the level of risk (for victims) or harm (for offenders) they present. The Metropolitan Police allows more effective prioritisation and thus allocation of resources. (Metropolitan Police, 2022; Gonzalez Fuster, 2020).
- Mayor's Office for Policing and Crime review highlighted that 38% of those on the list posed little or no risk, resulting in the removal of over a thousand young black men from the GVM (MOPAC, 2018; BBC News, 2021). An investigation by the Information Commissioner's Office found GVM data to be inaccurate while the system to breach numerous and serious data protection laws (ICO, 2018; Jones, 2018). Amnesty International as well as UK-based NGO, Liberty highlighted the lack of transparency in the design of the system emphasising the discrimination against people of colour, particularly Black men and boys. Furthermore, risks on data sharing with other services (schools, job centres, immigration enforcement, etc) have been stressed (Amnesty International, 2018; Liberty, 2022).
- Despite these claims, the Metropolitan Police asserts that the use and operation of GVM is compliant with the Human Rights Act and is monitored to assure its compliance (Metropolitan Police, 2022).

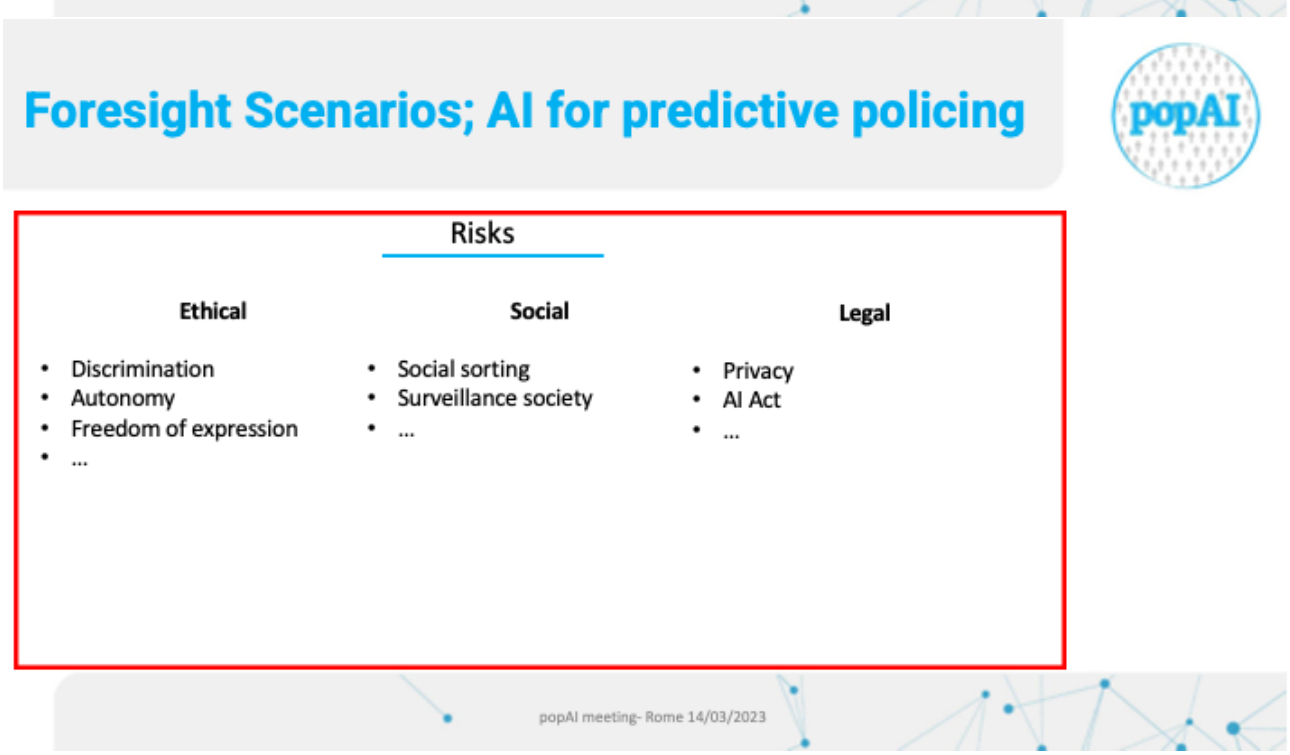
Foresight Scenarios; AI for predictive policing

Technology

What technology is to be used for accomplishing the expectations?

- Predictive analytics
- Risk profiling
- ...


Foresight Scenarios; AI for predictive policing
popAI
Stakeholders
Who are the stakeholders involved? What are their characteristics?
• Policy makers
• Technologists
• Tech Companies
• Police officers
• Citizens (minorities, different religion/ideology etc)
• Politicians
• Institutions
popAI meeting- Rome 14/03/2023


Foresight Scenarios; AI for predictive policing
popAI
Risks
Ethical
• Discrimination
• Autonomy
• Freedom of expression
• ...
Social
• Social sorting
• Surveillance society
• ...
Legal
• Privacy
• AI Act
• ...
popAI meeting- Rome 14/03/2023

Foresight Scenarios; AI for predictive policing

Title:

popAI meeting- Rome 14/03/2023

Crime Investigation

"Similarly to crime prevention, Surveillance-Orientated Security Technologies (SOSTs) meaning, "technologies which collect information about the general population to monitor the activities of potential suspects and to prevent criminal acts from occurring" are broadly used.

(Degli Esposti and Santiago-Gomez, 2015, p. 437)

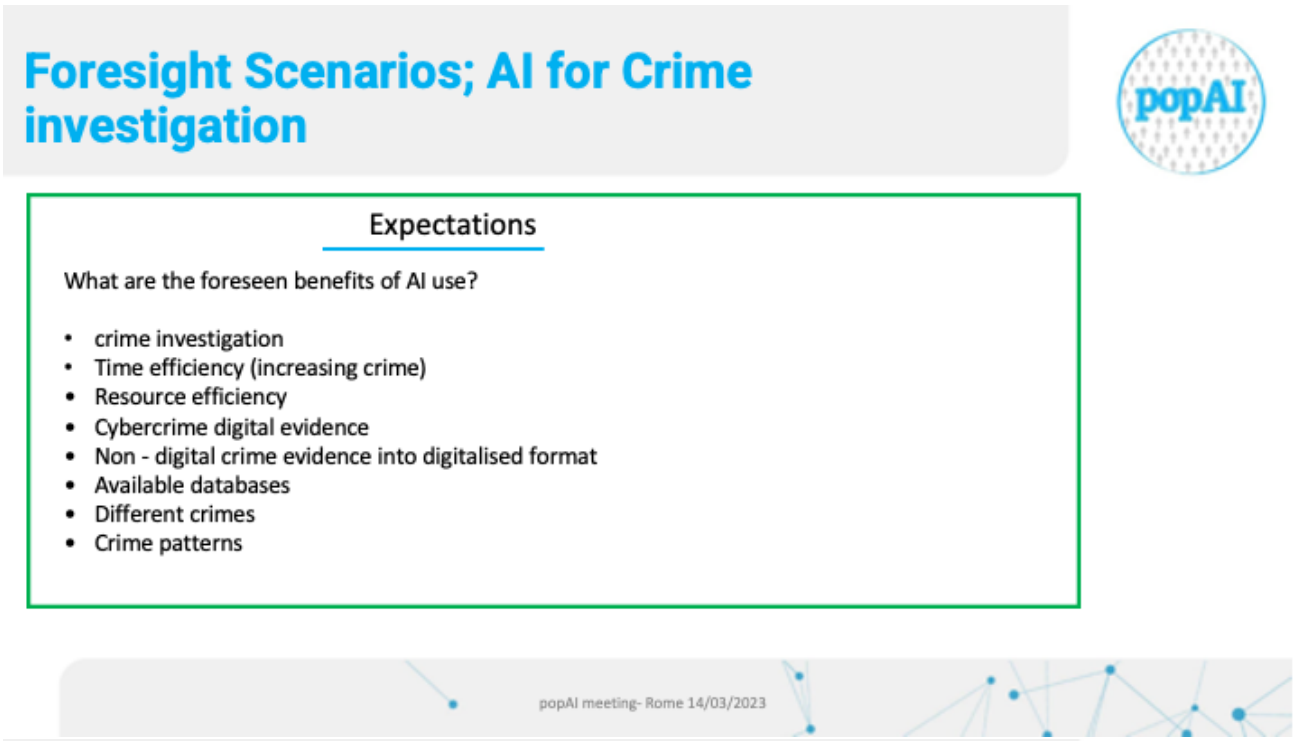
Expectations:

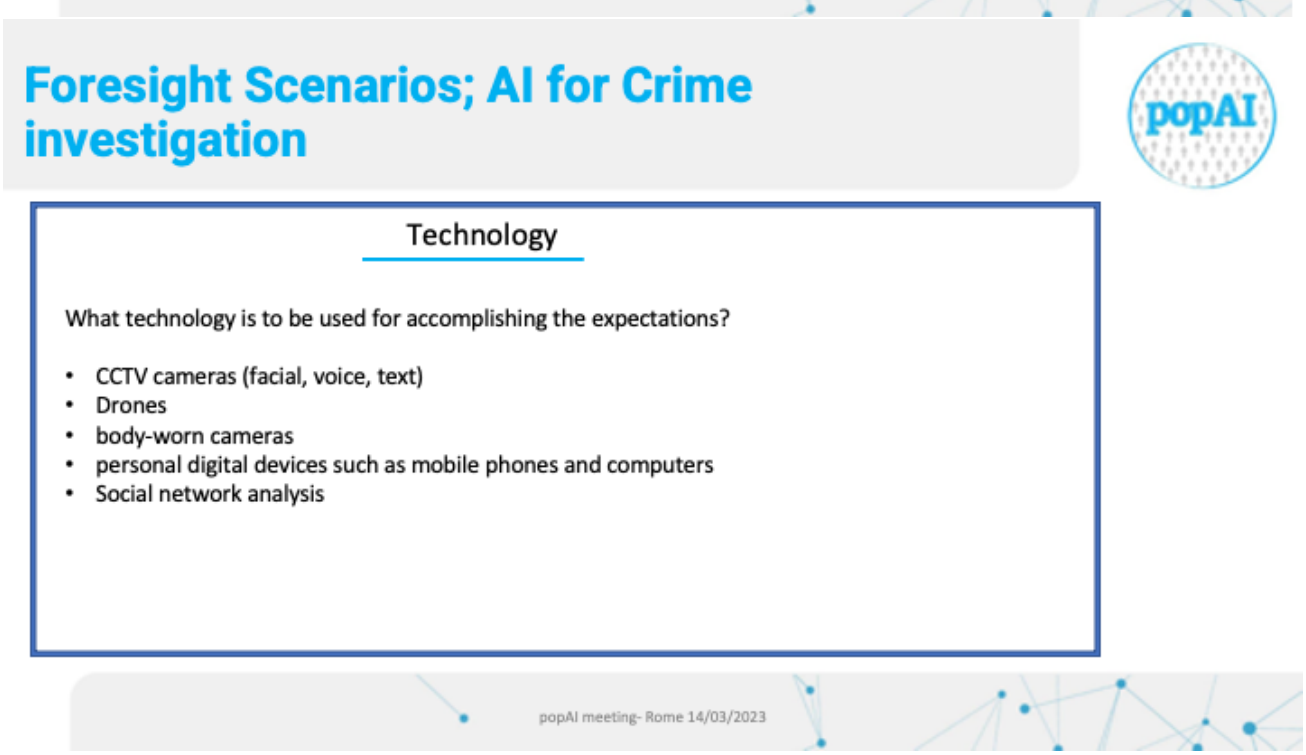
- Not only historical data but also real-time data coming from relevant identification systems such as automated license plate readers, automatic facial recognition systems, and voice identification systems can also be collected and analysed to enhance .

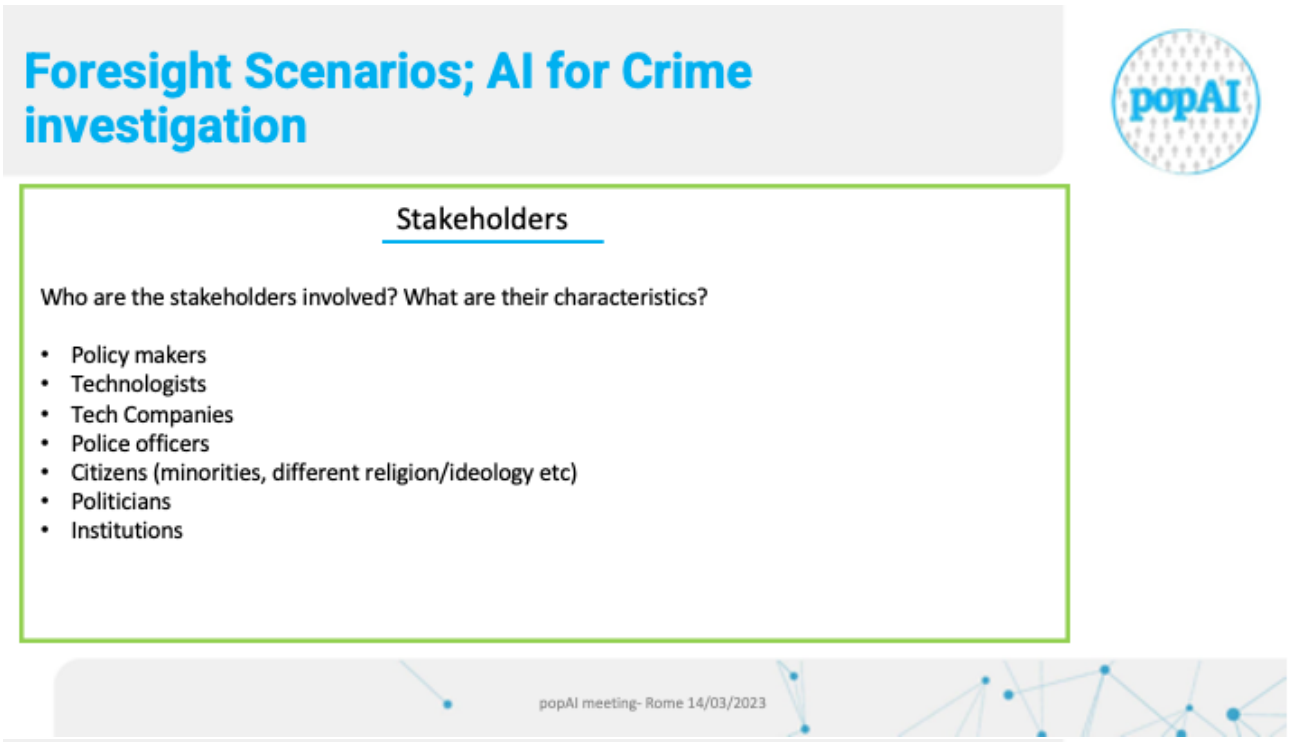
Risks:

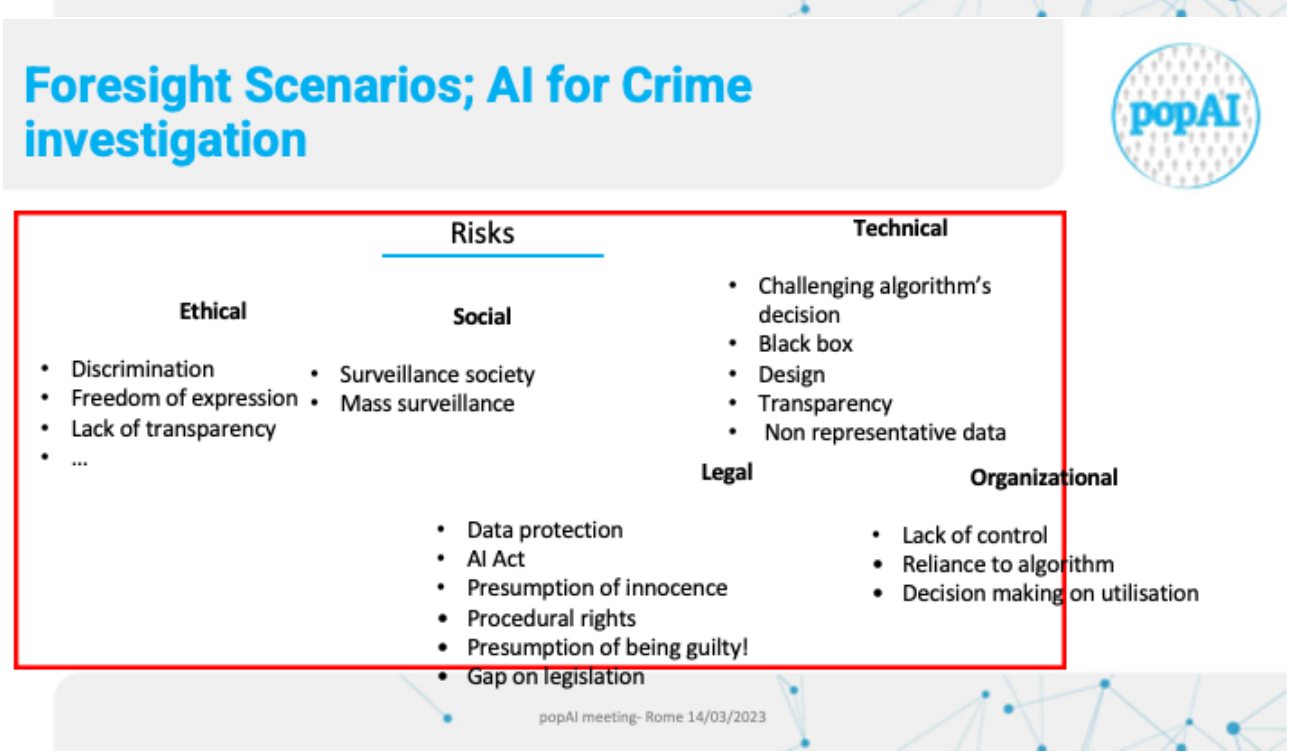
- abuse of fundamental rights are at stake; creation of a surveillance society

popAI meeting- Rome 14/03/2023


Foresight Scenarios; AI for Crime investigation
popAI
Expectations
What are the foreseen benefits of AI use?
• crime investigation
• Time efficiency (increasing crime)
• Resource efficiency
• Cybercrime digital evidence
• Non - digital crime evidence into digitalised format
• Available databases
• Different crimes
• Crime patterns
popAI meeting- Rome 14/03/2023


Foresight Scenarios; AI for Crime investigation
popAI
Technology
What technology is to be used for accomplishing the expectations?
• CCTV cameras (facial, voice, text)
• Drones
• body-worn cameras
• personal digital devices such as mobile phones and computers
• Social network analysis
popAI meeting- Rome 14/03/2023


Foresight Scenarios; AI for Crime investigation
popAI
Stakeholders
Who are the stakeholders involved? What are their characteristics?
• Policy makers
• Technologists
• Tech Companies
• Police officers
• Citizens (minorities, different religion/ideology etc)
• Politicians
• Institutions
popAI meeting- Rome 14/03/2023


Foresight Scenarios; AI for Crime investigation
popAI
Risks
Ethical
• Discrimination
• Freedom of expression
• Lack of transparency
• ...
Social
• Surveillance society
• Mass surveillance
Technical
• Challenging algorithm's decision
• Black box
• Design
• Transparency
• Non representative data
Legal
• Data protection
• AI Act
• Presumption of innocence
• Procedural rights
• Presumption of being guilty!
• Gap on legislation
Organizational
• Lack of control
• Reliance to algorithm
• Decision making on utilisation
popAI meeting- Rome 14/03/2023

Foresight Scenarios; AI for Crime investigation

Title:

victim : RIOT police to secure scene, technical police to collect evidence, investigation team,cameras, scanners, real time comparison with databases; crime investigators use evidence and interviews environment, AI possible investigation patterns suggesting best practices in similar situations in other countries.

Scenario organization focus; protagonist LEA to collect data, body-worn cameras,
Companies conflict of interest with companies so inclomplete data for LEAs
Through movements, calls,
Interrogation through the autonomous system interrogation
Internet facial recognition, video, CCTV cameras automatic investigation basedon historical data commited,
Identifying patterns,

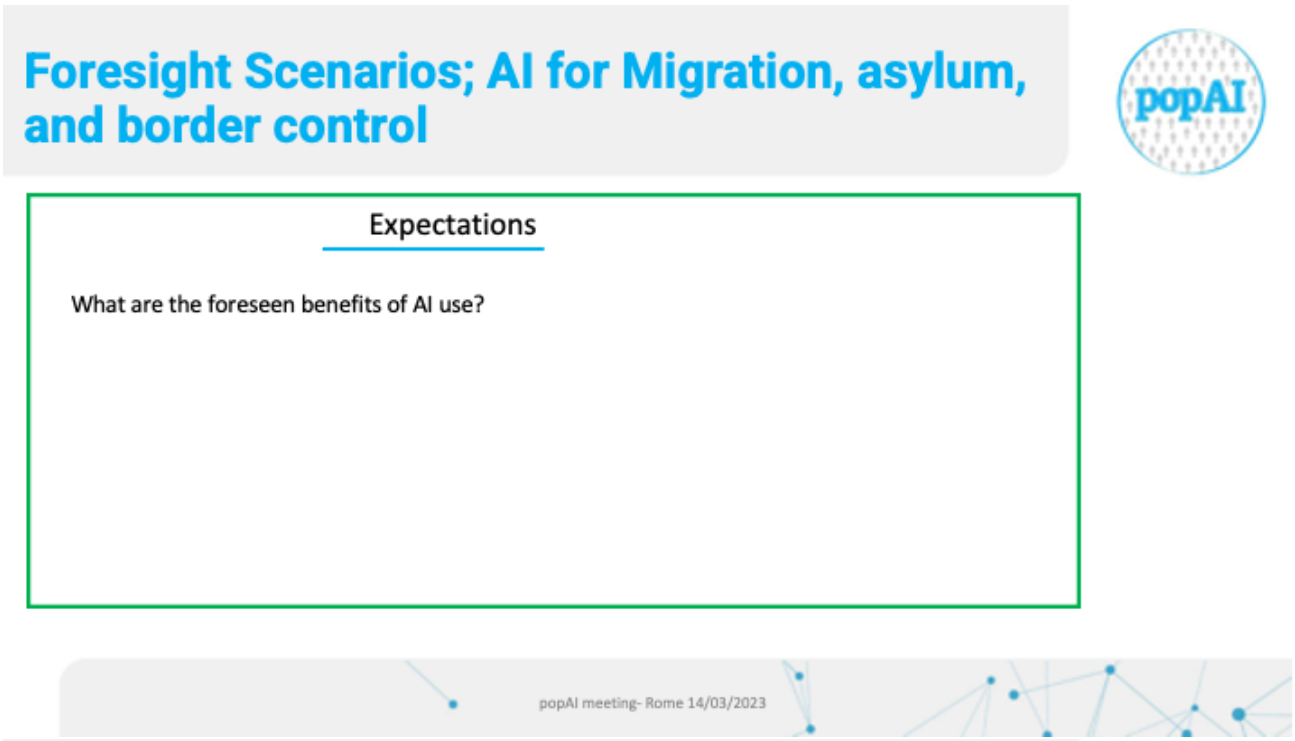
Systems flags suspect and assigns ranking ofpotential suspects

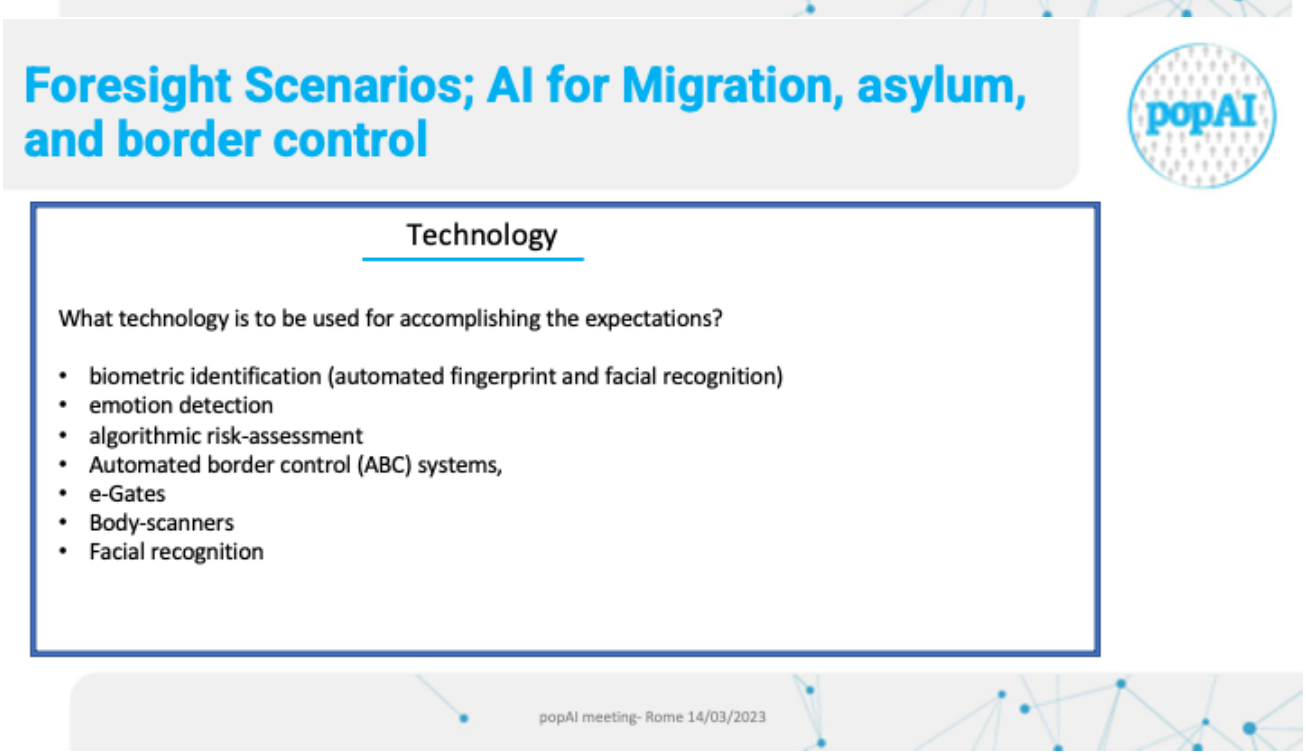
popAI meeting- Rome 14/03/2023

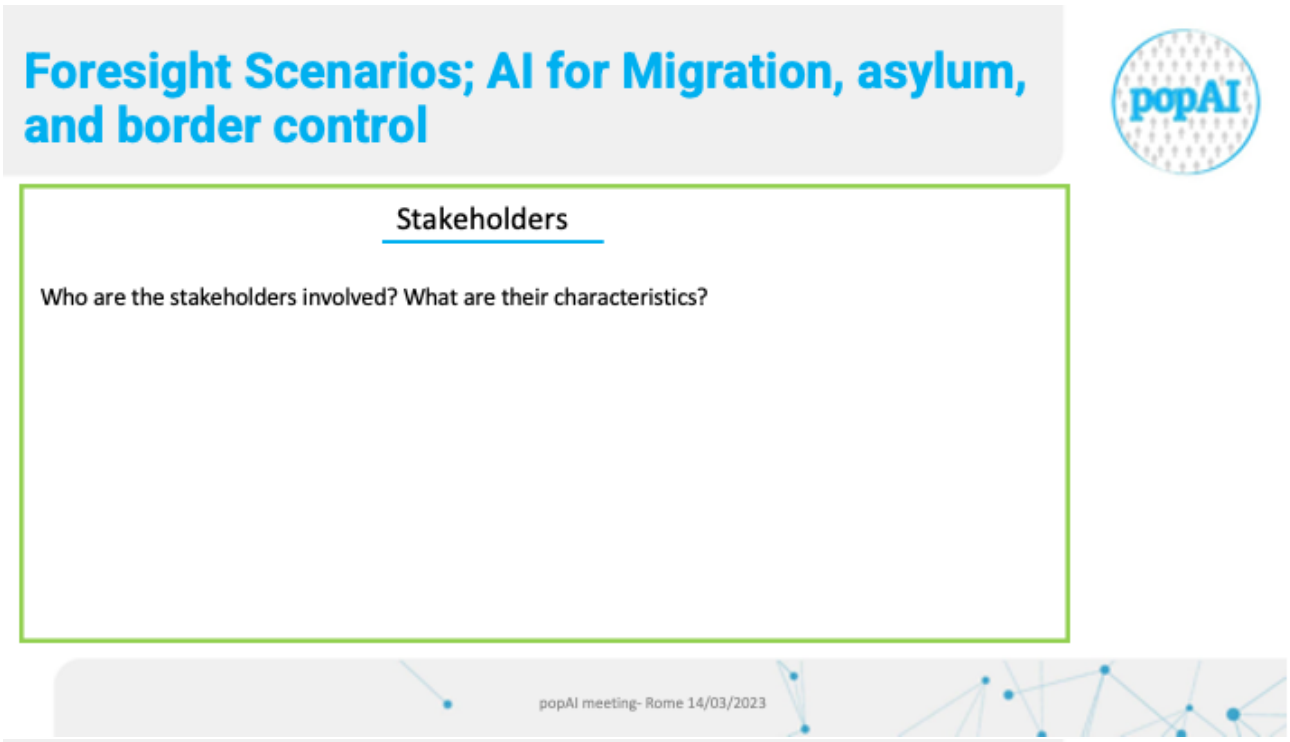
Migration, asylum, and border control; Case study: Brussels Airport

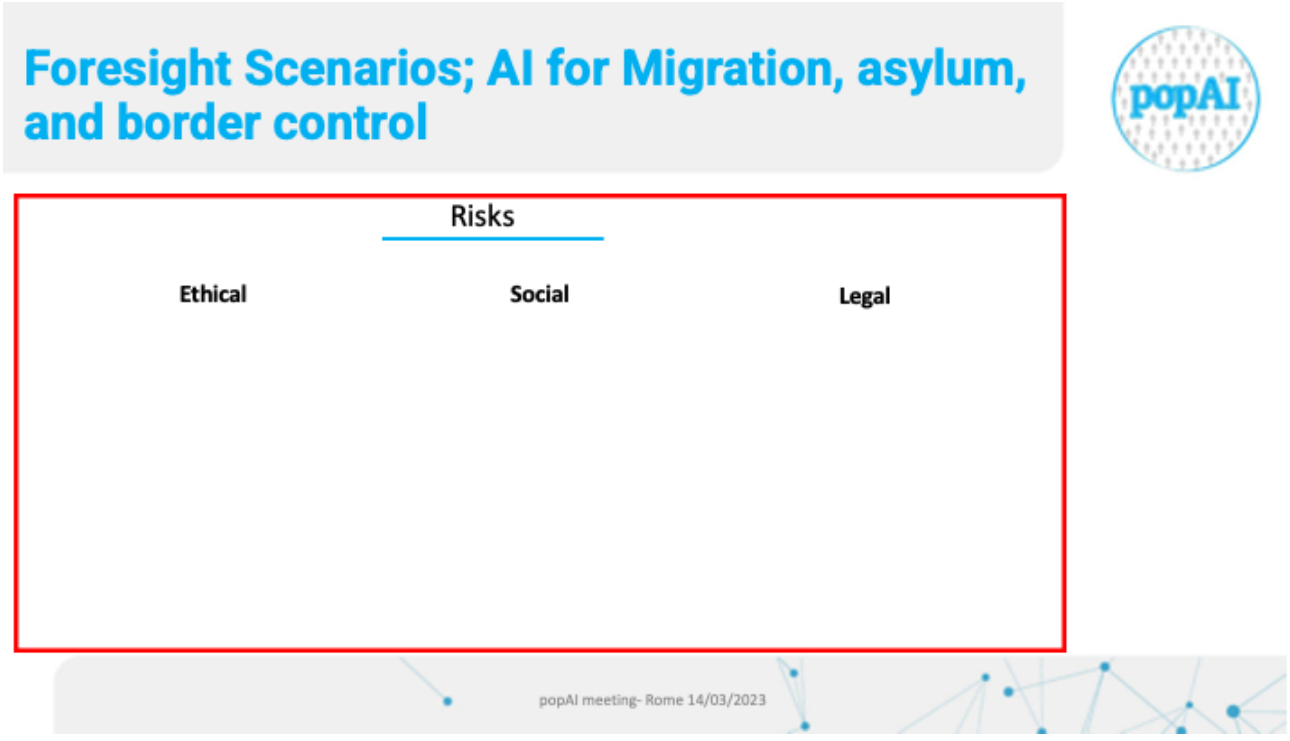
- In 2017, the Brussels Airport began piloting a new facial recognition system with four cameras installed in the airport. With the camera footage, the software created biometric templates of individuals which were then compared to a "blacklist" of individuals who are suspected of a crime (Peeters, 2020). Testing of the system was stopped in March 2017 due to a very high error rate, resulting in a large number of false positives (Automating Society, 2020).
- The Belgian Supervisory Body for Police Information were not informed of the installation of the facial recognition cameras and consequently no Data Protection Impact Assessment was conducted as required. Two years after the termination of testing, in 2019, the Supervisory Body found that the system was still partially active, actively collecting and storing biometric data from passengers at Brussels Airport (although not comparing the biometric data against a "black list") (Automating Society, 2020). The Supervisory Body discovered that a database was created with the data of the faces of hundreds of thousands of travellers temporarily stored failing the current Belgian law (Vanrenterghem & Heymans, 2019).
- Although the use of real-time intelligent systems is permitted under the Belgian Police Act, the Supervisory Body argues on the purpose of data processing during the testing phase. Moreover, the Act does not specify the circumstances and conditions for the use of "intelligent systems" (Peeters, 2020). The Supervisory Body enforced a temporary ban on the pilot project as Belgian federal police did not comply with data protection and police information law (COC, 2020).

popAI meeting- Rome 14/03/2023


Foresight Scenarios; AI for Migration, asylum, and border control
popAI
Expectations
What are the foreseen benefits of AI use?
popAI meeting- Rome 14/03/2023


Foresight Scenarios; AI for Migration, asylum, and border control
popAI
Technology
What technology is to be used for accomplishing the expectations?
• biometric identification (automated fingerprint and facial recognition)
• emotion detection
• algorithmic risk-assessment
• Automated border control (ABC) systems,
• e-Gates
• Body-scanners
• Facial recognition
popAI meeting- Rome 14/03/2023


Foresight Scenarios; AI for Migration, asylum, and border control
popAI
Stakeholders
Who are the stakeholders involved? What are their characteristics?
popAI meeting- Rome 14/03/2023


Foresight Scenarios; AI for Migration, asylum, and border control
popAI
Risks
Ethical
Social
Legal
popAI meeting- Rome 14/03/2023

Cyber operations for law enforcement

Use of computer science methods such as social network analysis are increasingly used to support LEAs to detect and predict criminal activities.

Expectations:

- Support LEAs to fight crime on a digital environment where communications between the criminals might take place, as well as crimes can be conducted.
- AI tools can help LEAs process large amounts of data in a more efficient and productive way
- Automated processes can help protect the mental health of LEA officers from exposition to these materials and images
- They can produce of taxonomy of images based on the user profiles, so more effective, and spend less time
- Social network analysis can help identify behaviorial changes, specifically support user requirement tracking and certification development

Risks:

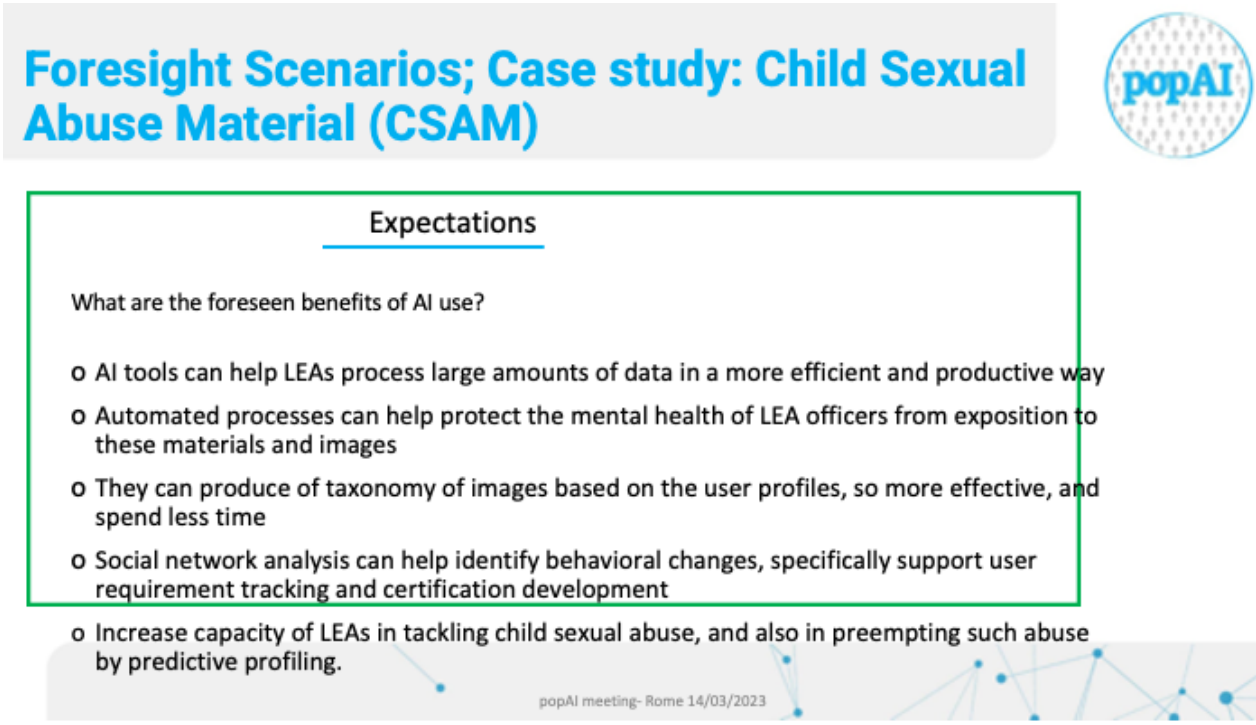
- Abuse of freedom of expression and privacy
- Legal: data governance issues associated with web crawling (largely unregulated), privacy protection, individual freedom
- Misuse of tools by police officers, if not properly trained, eg. misidentification of suspects, mass surveillance
- The limitations of specific technologies, eg. false positives for CSAM, how do we deal with this type of risk?
- Interesting parallels to be drawn with the use of AI in migration and asylum Formal consultation on EASO's social media monitoring reports (case 2018-1083)

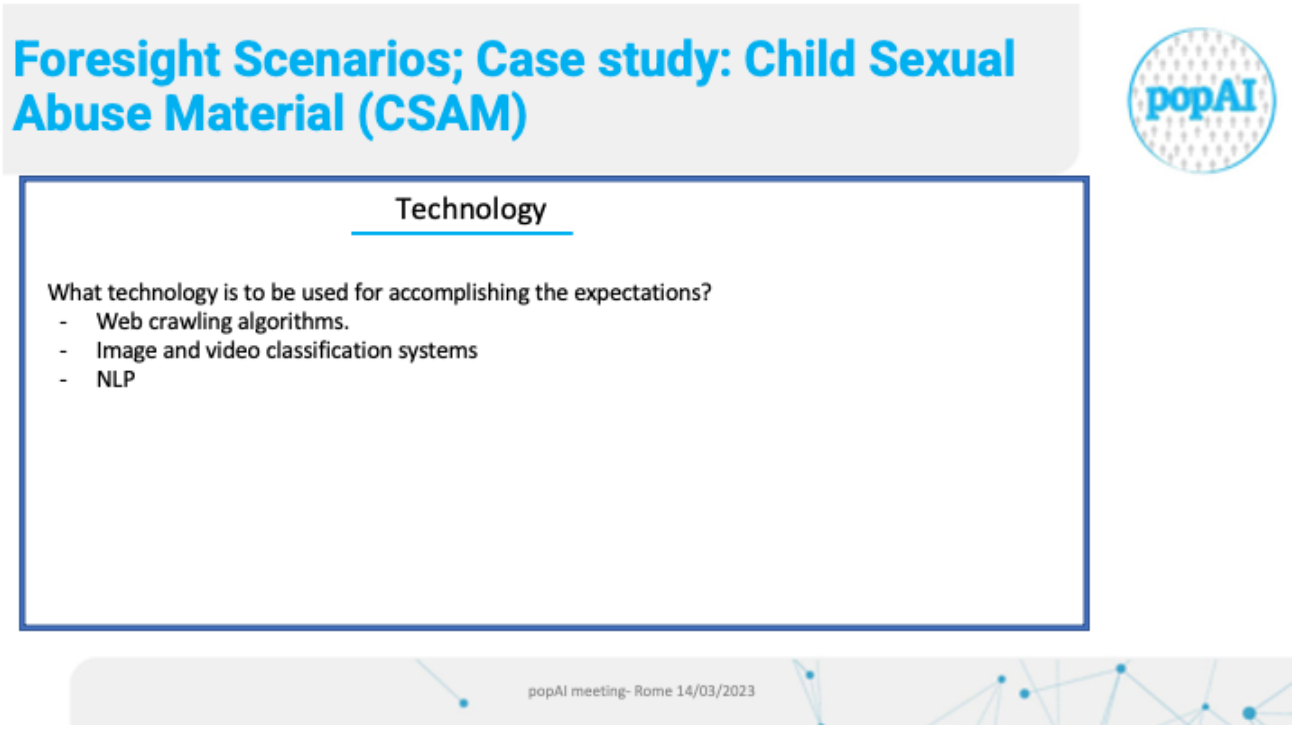
popAI meeting- Rome 14/03/2023

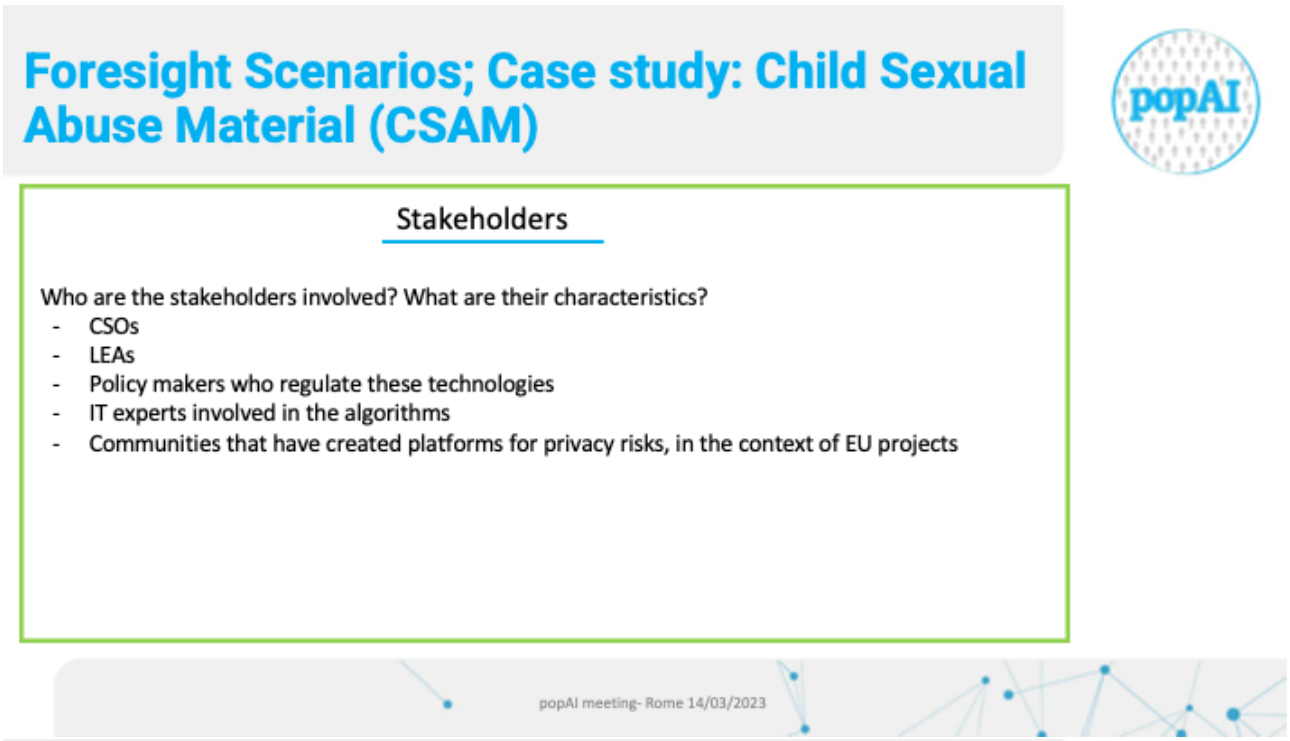
Cyber operations for law enforcement Case study: Child Sexual Abuse Material (CSAM)

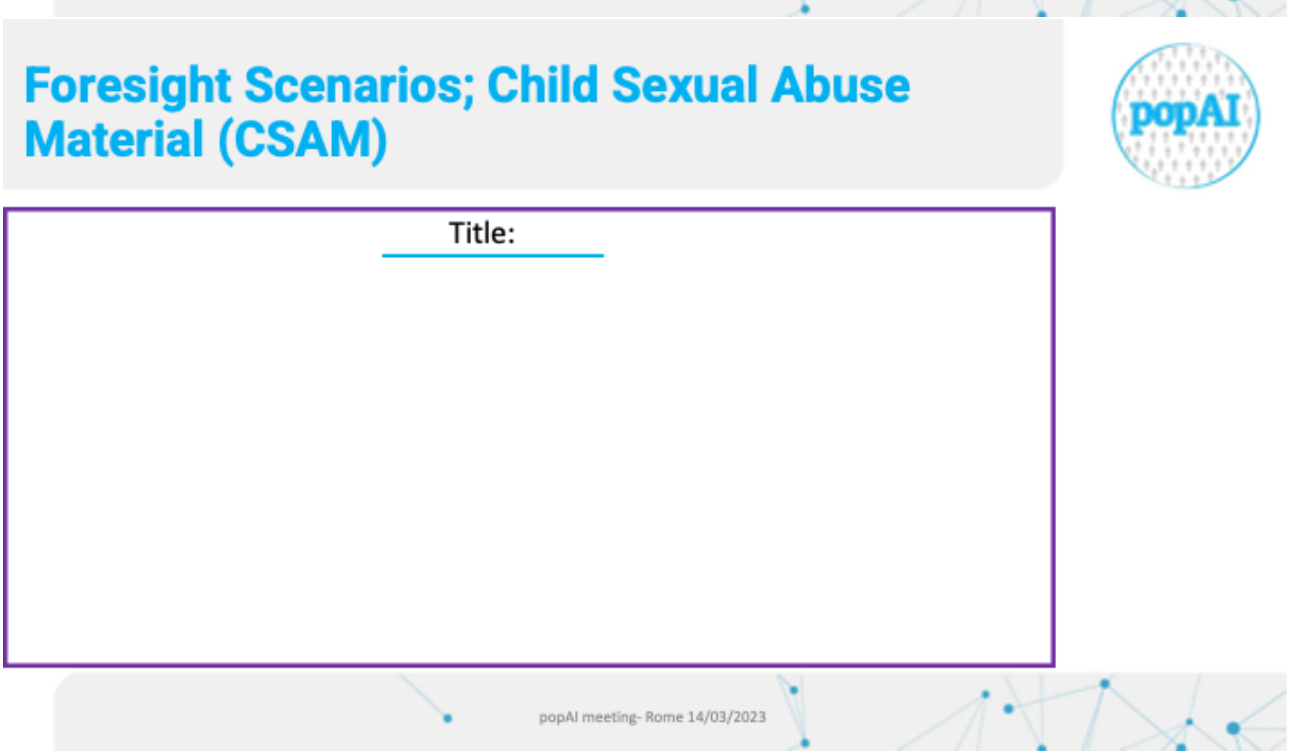
- The AviaTor project, which stands for Augmented Visual Intelligence and Targeted Online Research is funded by the EU Internal Security Fund. AviaTor is developing automation and intelligence to support the processing, assessment, and prioritisation of CSAM by LEAs. It is also developing a service of automatic crawling of online sources for complementing information for investigations in compliance with the national legal requirements. The National Police in Netherlands has been using the first version of AviaTor tool since December 20219 and the project is currently in its second iteration (INHOPE, 2021).
- There are challenges associated with AI to identify CSAM, which include (1) the quality of CSAM data; and (2) the lack of standardised classifications for content (INHOPE, 2020) while there are also legal obstacles in collecting CSAM reports from different countries. Furthermore, NGOs have accused abuse of the system and targeting artists, such as cartoonists, and marginalised communities by sharing innocent and legal reports as CSAM (Bukovska, Finan & Malcolm, 2020).

popAI meeting- Rome 14/03/2023


Foresight Scenarios; Case study: Child Sexual Abuse Material (CSAM)
popAI
Expectations
What are the foreseen benefits of AI use?
o AI tools can help LEAs process large amounts of data in a more efficient and productive way
o Automated processes can help protect the mental health of LEA officers from exposition to these materials and images
o They can produce of taxonomy of images based on the user profiles, so more effective, and spend less time
o Social network analysis can help identify behavioral changes, specifically support user requirement tracking and certification development
o Increase capacity of LEAs in tackling child sexual abuse, and also in preempting such abuse by predictive profiling.
popAI meeting- Rome 14/03/2023


Foresight Scenarios; Case study: Child Sexual Abuse Material (CSAM)
popAI
Technology
What technology is to be used for accomplishing the expectations?
- Web crawling algorithms.
- Image and video classification systems
- NLP
popAI meeting- Rome 14/03/2023


Foresight Scenarios; Case study: Child Sexual Abuse Material (CSAM)
popAI
Stakeholders
Who are the stakeholders involved? What are their characteristics?
- CSOs
- LEAs
- Policy makers who regulate these technologies
- IT experts involved in the algorithms
- Communities that have created platforms for privacy risks, in the context of EU projects
popAI meeting- Rome 14/03/2023


Foresight Scenarios; Child Sexual Abuse Material (CSAM)
popAI
Title:
popAI meeting- Rome 14/03/2023


Thank You!
popAI
DEMOKRITOS
NATIONAL CENTRE FOR SCIENTIFIC RESEARCH
TRILATERAL RESEARCH
eticas FOUNDATION
KEMEA
iti Information Technologies Institute
TU/e EINDHOVEN UNIVERSITY OF TECHNOLOGY
Zanasi & Partners
Security Research and Advisory
ecas
Hochschule für den öffentlichen Dienst in Bayern
Fachbereich Polizei
POLICÍA MUNICIPAL Madrid
popAI meeting- Rome 14/03/2023