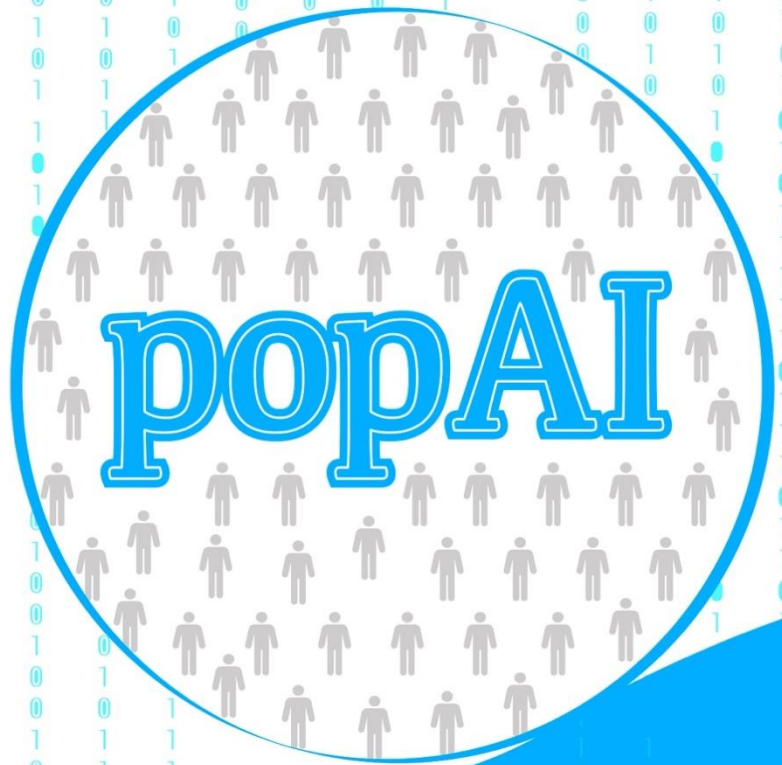
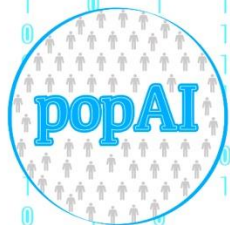


Policy Brief



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





popAI project

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

The 3 main work pillars of the project

- 1** Analysis of theoretical legal, ethical, social framework related to the use of AI tools in the security domain
- 2** Empirical Research on the AI tools in the security domain, raising awareness, societal acceptance and ethics
- 3** Final recommendations/best practices/white book, coordination and networking activities with Stakeholders across Europe, with other sibling projects to spread the research results identified during the project and to assess and generalise the research results with them. In addition, a set of carefully curated policy briefs will be provided aiming to bring human-centric, socially driven, ethical and secure-by-design AI for the security domain at the core of the most important policy debates in Europe.

The popAI partnership

Project Coordinator:
Dr. Dimitris Kyriazanos
National Centre for Scientific Research "Demokritos" (Greece)















Hochschule für den
öffentlichen Dienst
in Bayern
Fachbereich
Polizei



LOCAL POLICE OF TURIN

POLICY RECOMMENDATIONS OVERVIEW

Policy Recommendations		Type of Policy Recommendation ²		Target Audience	High-level Theme/ Aim of the Recommendation
		Reactive	Proactive		
Ethical Level, Organisational Level	1. EU to support the development of frameworks for the evaluation of AI tools ensuring their ethical, fair, and transparent adoption by public sector			EC DG Home, EU Parliament	Ensure fairness, transparency
Societal Level	2. EU Member States to develop meaningful dialogue with civil society organisations to strengthen citizens' confidence in the use of AI tools in support of the law enforcement authorities			Member States Parliaments, Ministries, Civil Society Organisations and Initiatives	Enhancing transparency, social inclusion, awareness creation
Regulatory Level	3. EU to adopt a European regulation to enhance transparency in the planning, implementation, and use of AI systems with the participation of civil society organisations			European Commission (EC), EU Parliament, Member States Parliaments	Enhancing transparency, inclusion
Organisational Level, Societal Level	4. EU Member States to implement procedures for continuous monitoring of AI systems , with the active participation of civil society organisations, for appropriate employment and use			Member States Parliaments, Ministries	Enhancing transparency, Preserve privacy and human rights, social inclusion
	5. EU to support the development and employment of clear guidelines and procedures for the use of AI systems by LEAs			EU Parliament, Member States Parliaments, Ministries	Minimise risks of abuse and/or misuse, enhance transparency,
Ethical Level, Societal Level	6. EC and EU Member States to ensure that AI systems are inclusive, fair, equitable and non-discriminatory .			EC, EU Parliament, Member States Parliaments, Ministries	Preserve privacy and human rights, fairness, equality, inclusion, non-discrimination
Gender Diversity Level	7. EU to support and invest in the development of guidelines for gender sensitive policing in the AI era.			EC DG Home	To address gender diversity, social inclusion
Research Level (EU-funded research)	8. EU to establish ethics committees that review proposals in the security domain based on potential ethical and societal issues.			European Commission	Ensure development of ethical outputs
	9. EU to promote inclusive participation (stakeholders and countries) regarding EU projects in the security domain			European Commission	Promote inclusivity

Aim of this Policy Brief

To provide initial policy recommendations for **fostering trust in AI for the security domain** drawing upon the early findings of the **popAI project**. The project consolidates **distinct spheres of knowledge** (theoretical & empirical knowledge by academics & non-academics), in order to offer a unified European view across LEAs, and specialised knowledge outputs (recommendations, roadmaps, etc), while creating an ecosystem that will form the structural basis for **a sustainable and inclusive European AI hub for Law Enforcement**.

² Reactive policy recommendations focus on the current state of affairs and proactive focus on the future state of affairs (short-term future).

What AI can offer to the Law Enforcement domain?

Artificial Intelligence (AI) can offer support for Law Enforcement operations. AI technologies and systems, like automated processing techniques to assist crime prevention are widely used by Law Enforcement Authorities (LEAs). AI in the security field promise to **offer significant opportunities and benefits** ranging from enhanced efficiency and provision of situational awareness and context at a higher level of accuracy related to criminal activity and public safety, as well as extended capabilities to tackle new types of digital and physical attacks and fraudulent cases, which contribute to higher levels of citizen protection and safety.

Which are the issues raised and controversies?

Recent developments and AI applications (e.g., Clearview AI case which offered to 2200 LEAs an AI facial analytics application and a dataset of 3 billion Web-accessible citizen photos) have drawn **significant concerns** in terms of their compatibility with EU fundamental rights, values, and freedoms. The lack of clarity, transparency, and a concrete regulatory framework, raises concerns and potential risks of AI systems that are used in security domain as for example, in critical situations with clear power imbalances, such as border control, which may lead to abuses as well as reproduction and amplification of existing biases and inequalities.

How can we foster trust in AI for the security domain?

How can we minimise the trade-offs between the pursuit of security and the respect for fundamental rights, values and freedoms and the risk to destroy our democracy on the grounds of defending it? It is important for the endorsement of AI technologies in the field of Law Enforcement to be accompanied by efficient actions and regulatory frameworks to foster trust in AI, address the concerns, and risks and to guarantee that AI systems do not compromise, during their design, development or deployment and use, EU fundamental rights and freedoms. These actions and regulatory frameworks should promote a human-centric and trustworthy approach to AI based on fundamental rights that manages risks while taking full advantage of the benefits AI can bring for the whole of society including the law enforcement domain. Towards this aim a multidisciplinary and inclusive process should be adopted that encompasses technical, organizational, ethical, legal, cultural, and diversity perspectives that are future-proof, involving all members of our society. This process will result in the development of ethical, transparent, inclusive and accountable systems by design that will gain the trust both of the LEAs and the public.

Which policy approach has been utilized for the proposed policy recommendations?

popAI brings together different types of stakeholders, ranging from the industry to the single individual. This approach aims to guarantee that all voices and perspectives are taken into consideration, as we recognise that this topic - and in particular ethics and legal aspects - could have significant impact and raise diverse concerns depending on the societal sectors under consideration. As such, popAI follows a multi-perspective approach in order to provide effective policy recommendations and ensure their future-proofing. This novel approach combines both (a) **bottom-up** (citizen and stakeholder driven) and **top-down** recommendations (research and partners) that focus on (b) a **reactive** (focusing on the current state of affairs) and a **proactive approach** (focusing on the future state of affairs and an “anticipatory policy action”) aiming to prevent potential problems and concerns from occurring in the near future. Although, proactive policies are more challenging due to the fact that it is more difficult to commit resources (money, time, effort, etc.) to a problem that has not yet occurred, we believe that the emphasis on such policies will at minimum create awareness for future potential problems in the area of AI in the law enforcement across policy makers and relevant stakeholders while also impacting positively a change in the culture of policy making for law enforcement that is more “anticipatory” in nature.

POLICY RECOMMENDATIONS



Recommendation 1: Ethical Level, Organisational Level

EU to support the development of frameworks for the evaluation of AI tools ensuring their ethical, fair, and transparent adoption by public sector

The public sector, like other facets of society, is subject to efficiency standards, which can justify the adoption of Artificial Intelligence (AI) tools. The public sector, however, varies from private businesses in terms of its legal standing and particular social function, which carries with it certain requirements for responsibility, transparency, and equity. Given its special role, the public sector deserves a wider approach to impact assessment for the adoption of AI tools. In literature, several frameworks^{3 4 5} are available including ways of assessing AI tools and methods which provide indicators for risks that a company might face when adopting an AI tool, while also include mitigation actions and best practices that could be followed. Each of these frameworks includes different guidelines, assessment criteria and mitigation recommendations concerning the adoption of AI. However, most of them are focused on the private sector, leading thus to a lack of assessment frameworks as well as clear implementation procedures that will include guidelines, recommendations, and mitigation indicators for the adoption of AI tools in the public sector.

This policy recommendation aims, *proactively*, at the **development of frameworks** that will be able to support the **analysis and evaluation of the AI tools used by public administrations, in order to ensure transparency, equity, and accountability**. Extensive research shall be applied both on the development of such frameworks, and also in the development of the corresponding interdisciplinary assessment measures/metrics. Within this scope, the adoption of an AI tool can be assessed by a set of interdisciplinary metrics, developed in an inclusive manner, including the system scope, its performance, usability, data used for its training and evaluation including ethical processing, and impact on human rights among others. At this point, it should be mentioned that the corresponding framework is recommended to include specific guidelines on bias mitigation among others, allowing thus the further assessment of AI models in this scope.

External Independent Multidisciplinary Committees (AI Observatory Body) consisting of interdisciplinary committees and stakeholders with ethical, legal, technical, organisational and practical capabilities could assess the system's compliance with legal and ethical rules and regulations. This could act as a form of **external certification** of the system's accountability, and certification of ethical, and secure-by-design AI tools in the Law Enforcement domain. In addition, **certifications of system accountability** through specific processes and frameworks, including algorithm audits and the extent to which systems use "democratic" data in addition to "robust" algorithms would be of value.



Recommendation 2: Societal Level

EU Member States to develop meaningful dialogues with civil society organisations to strengthen citizens' confidence in the use of AI tools in support of the law enforcement authorities.

Civil society organisations are often not included in consultations regarding the employment of AI by national enforcement authorities. Therefore, they express their concerns on emerging risks through announcements and legal actions. This gap is creating tensions that are constantly widening and damage the trust between the involved parties, namely the citizens and the state.

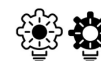
To repair the trust issues, civil society organizations should be involved in open dialogues with public bodies and law enforcement authorities regarding the employment of AI systems. The results of such activities would

³ High-Level Expert Group (HLEG) - Assessment List for Trustworthy Artificial Intelligence (ALTAI). Available at [LINK](#).

⁴ World Economic Forum (WEF) AI Governance framework. Available at [LINK](#).

⁵ NOREA Guiding Principles Trustworthy AI investigation. Available at [LINK](#).

enable European member states to integrate the European Regulation into their law, tailoring it to the culture and the specificities that govern their societies. Civil society organisations should be actively involved in the process of designing and implementing AI systems, as well as in the monitoring of the existing ones. They should also determine the best way to operate these systems to ensure human rights and generate acceptance across citizens.



Recommendation 3: Regulatory Level

EU to adopt a European regulation to enhance transparency in the planning, implementation, and use of the systems that apply AI with the participation of civil society organisations

Civil society and civil society organisations question the proper usage of AI systems and, above all, whether these systems can guarantee human rights, such as respect for privacy and family life, protection of personal data, prohibition of discrimination (racial, religious, etc.), avoidance of prejudices etc. especially when these systems are challenged or endangered by actions of public or private organisations.

To strengthen citizens' trust regarding the use of AI systems in the security domain, a legal harmonization at a national and European level should be pursued, anchored in the European values and fundamental rights. To this process, the active involvement of civil society organizations is crucial. This regulatory framework will ensure the transparent and trustworthy design, development, and implementation of AI system safeguarding the rights and freedoms of the citizens. Harmonised rules regarding AI technologies and applications emphasising on a clear legal framework on protection/restricted use of biometric data and copyright issues should be established.



Recommendation 4: Organisational Level, Societal Level

EU Member States to implement procedures for continuous monitoring of AI systems with the active participation of civil society organisations to adapt them appropriately and improve the results of their use.

EU should support the continuous, inclusive, and multidisciplinary monitoring of AI systems across their life-cycle. In particular, EU Member States should invite the civil society organisations and create **joint working groups**, which will check, per organisation of the Member State, the individual AI systems they use in order to highlight potential issues from such usage (*a posteriori monitoring and assessment*). These joint working groups should also be consulted when designing and developing new AI systems and technologies that will be applied in the future (*a priori monitoring and assessment*).

The purpose is to improve and adapt them appropriately to ensure that they protect citizens' rights. This will support the use of existing systems by individual Member States, as well as the development of new ones that will cover the current needs. In this way, it is estimated that the interaction of the Member States with the civil society organisations should be continuous, at regular intervals and the dialogue and control by the civil society organisations should be strengthened in all stages of the operation of an AI system (design, implementation, maintenance, upgrade).



Recommendation 5: Organisational Level

EU to support the development and employment of clear guidelines and procedures for the use of AI systems by LEAs

This recommendation (reactively) aims at the development and employment of clear **guidelines and procedures for the adoption and use of AI systems by LEAs**. Research on the perspective of practitioners regarding the use of AI in policing and crime prevention, highlights the lack of clear guidelines and procedures regarding the use of AI tools while financial and political support are also not sufficient⁶.

Therefore, there is a high risk of abuse and/or misuse of the tools leading on stigmatization and potential violence of privacy and human rights. As such it is important that EU and Member States support the development of clear guidelines and procedures for the adoption and use of AI system in the security domain.



Recommendation 6: Societal & Ethical Level

EC and EU Member States to ensure that AI systems are inclusive, fair, equitable and non-discriminatory.

EC and EU Member States should take necessary actions to ensure, inclusive design and diversity in AI systems and technologies as well as fairness, equality and non-discrimination in the design and use of these systems. In order for this to be achieved, special attention should be given to ensure inclusive dialogue with diverse stakeholder segments and civil society (race, ethnicity, age, gender diverse groups) at all stages of AI design, development and use. To this end, EC and EU Member States need to promote and ensure citizens' awareness regarding the existence and implementation of an AI system and enable objection to potential unjust decisions.

Open discussions between Member States and civil society organisations can support transparency at every stage to minimize the risks of discrimination. In addition, this should also be taken into consideration during systems procurement, where for example the technical specifications must be accepted by **civil society organizations and agencies** while during the system implementation phase, monitoring and assessment by **representatives of social and other bodies** should be foreseen.



Recommendation 7: Gender Diversity Level

EU to support and invest in the development of guidelines for gender sensitive policing in the AI era.

This recommendation is a *proactive one* and aims at the development of the corresponding guidelines for the promotion of gender sensitive and gender-responsive policing^{7 8} especially in the era of AI. In 2010, the Women Police Officers Network (WPON)⁹ was established with the support of Southeast Europe Police Chiefs Association. Its scope was to place gender sensitive policing at the top of the agenda of police reform and to serve as a platform for knowledge and experience change across police services, needs and priorities of policewomen. This network has so far achieved gender sensitive policing with an emphasis on recruitment, selection, and professional development of women in police services. However, apart from this initiative, it is

⁶ Laufs, J. and Borrión, H. (2021). Technological innovation in policing and crime prevention: Practitioner perspectives from London. *International Journal of Police Science & Management*, pp. 1-20. DOI: 10.1177/14613557211064053

⁷ Women, U. N. (2021). Handbook on gender-responsive police services for women and girls subject to violence.

⁸ Bonkat-Jonathan, L., & Ejalonibu, G. L. (2021). A Review of Some Discriminatory Laws against Women and the Need for Legislative-Gender Responsive Actions in Nigeria.

⁹ Kekić, D., Đukanović, D., & Tomić, M. Women Police Officers Network (WPON).

important in today's developed society to promote and develop appropriate actions and guidelines on the equality of all people in society to ensure no group is disadvantaged over another in its treatment by the police.

This policy recommendation aims at the development of the corresponding guidelines, from the EU and the relevant EU-funded projects, to raise awareness on the position of women in police services and the development and implementation of sustainable solutions for the improvement of recruitment and retention of women personnel and their active involvement in the design and development of AI systems for security purposes. In addition, and in order to achieve gender-responsive policing, these guidelines should focus on the empowerment of gender equality in law enforcements with an emphasis on the needs of all parts of the community (women and girls, men and boys including minority or marginalised groups), and facilitate the inclusive design and development of the corresponding AI systems to ensure that no group is mistreated by the police. Furthermore, these guidelines shall be based on the outcomes of the WPON Southeast Europe in order to find absence of data leads to ineffective policies, the gaps as well as the legal framework that exists around the subject, and to include the appropriate information so that gender sensitive policing can be enhanced.



Recommendation 8: EU-funded Research Level

EU to establish ethics committees that review proposals in the security domain based on potential ethical and societal issues.

EU-funded projects developing AI driven technologies for the security domain have often raised concerns. This is the case with the European FP7 project entitled “Intelligent information system supporting observation, searching and detection for security of citizens in urban environment” (INDECT) which ran from 2009-2014¹⁰. The project developed technological solutions and tools to automatically detect threats. Amongst these technologies, they developed video and audio analytics of camera footage. The secrecy of the project and the potential impact on civil liberties and fundamental rights sparked concerns among Members of European Parliament calling on the European Commission to clarify the purpose of the INDECT project (Euractiv, 2011¹¹).

As such this policy recommendation aims at the establishment of specialised interdisciplinary Ethics Committees that will review the proposals in the security domain, so as to prevent potentially serious ethical, societal, and legal issues as well as abuse of human rights. Aligned with Recommendation No.1 these Committees will have ethical, legal, technical, organisational, and practical capabilities so as to assess the system’s compliance with legal and ethical rules and regulations. This could act as a form of **internal EU certification for EU-funded projects** in relation to the system’s accountability and the ethical, inclusive and secure-by-design AI systems in the course of EU-funded research and development.



Recommendation 9: EU-funded Research Level

Inclusive participation (stakeholder and country level) in the EU-funded projects in the security domain.

Research conducted in the context of project (Task 3.1) identified the stakeholder groups involved in the research, development, use, and implementation of AI technology and tools, as well as those who promote awareness regarding emerging risks, and push for relevant policies. These different categories of stakeholders should not be seen as “rivals” but rather as key components of a unified ecosystem that co-shape the development and use of AI in the security domain. The identified stakeholders are namely, LEAs, social and humanities research, policy makers, government and public bodies, technologists/ data scientists, civil society

¹⁰ [INDECT \(Intelligent Information System Supporting Observation, Searching and Detection for Security of Citizens in Urban Environment\), Cordis Project Page.](#)

¹¹ Euractiv (2011), “MEPs question ‘Big Brother’ urban observation project”.

organizations, national and local authorities, ICT and software companies, and police academies. Mapping the EU funded projects in the security domain, 348 different stakeholders were collated with the majority of stakeholders being ICT and software companies, followed by universities and research organisations. It is recommended that the EC, explores ways (i.e., call requirements, specifications) for **EU-funded projects to include civil society organisations** in the early stages of the AI design and development as they are underrepresented in the project consortia, while their voices are very important to preserve privacy and human rights.

Likewise, project partners were geographically mapped. The analysis indicated that various European countries such as Albania, Denmark, and Ukraine have been underrepresented to date in EU-funded projects in the security domain. Involvement of partners from unrepresented Member States would enable the inclusion of potentially cultural and geographic differences in regards to the needs and acceptance of AI systems. Thus, it is recommended that the EC, explores ways (i.e., call requirements, specifications) for **EU-funded projects to include underrepresented Member States** in the AI design and development.

POLICY IMPLICATIONS

Recommendation 1: EU to support the development of frameworks for the evaluation of AI tools ensuring their ethical, fair, and transparent adoption by public sector

The first policy recommendation aims to increase transparency, accountability, and fairness via the development of frameworks for the evaluation of AI tools by the public sector. Through the development of frameworks for this scope, the public sector will be able to adopt AI tools with reduced risks and will be able to also evaluate their use more frequently. By allowing the end users to identify and be informed about the risks of using an AI tool or its output, is of great importance and will increase digitization in the public sector. However, the percentage of digital literacy in some countries is increased, therefore the public organisations that will aim to use such frameworks might need to organise **public education programs and campaigns**, that will enable the end users of the AI systems and technologies to understand the importance of using evaluated AI tools in public sector and educating them on using these tools. Similar training programs should also be designed for civil society to empower citizens to actively participate in the development of such AI frameworks (i.e., the example of Finland with the 'Elements of AI' massively open (free) online course¹²). Furthermore, to ensure consistency across EU countries, such programmes could be included within student exchange programmes such ERASMUS or similar. This would have a twofold benefit: i) reaching young people, who represent the future of our societies; and ii) facilitate harmonisation of literacy levels across countries.

Recommendation 2: EU Member States should develop meaningful dialogues with civil society organisations in order to strengthen citizens' confidence in the use of AI tools for law enforcement by the Law Enforcement Authorities.

At the beginning of implementation, delays in the design and implementation of AI systems are expected due to disagreement in viewpoints between representatives advocating their use for a specific purpose and representatives defending human rights. However, with a willingness to cooperate and constructive dialogue, it is expected that the controversies/disagreements between them will be alleviated. In the end, with everyone's agreement, the desired result should be achieved, which is the use of AI systems for the purpose

¹² Elements of AI (Finland), <https://www.elementsofai.com/>

of security in the everyday lives of citizens, which will be accepted by all (including representatives of civil society organisations).

Recommendation 3: EU to adopt a European regulation to enhance transparency in the planning, implementation and use of the systems that apply AI, with the participation of civil society organisations

It is expected that there will be delays in the issuance of the European regulation that will clearly reflect the procedures for the design, implementation, and control of AI systems, as it will have to be preceded by an extensive dialogue between all involved parties. Also, any requests made by each member state, based on the different requirements of its own civil society organisations, should be discussed. However, once it is completed, it is expected that there will be a clear general regulatory framework, commonly accepted by representatives of civil society organisations, which will govern the entire process and take into account - leave room for adaptation - the particularities of the Member States.

Recommendation 4: EU Member States should implement procedures for continuous monitoring of AI systems, with the active participation of civil society organisations, in order to adapt them appropriately and improve the results of their use.

It is expected that serious reservations will be raised during the process of continuous monitoring of existing AI systems and by representatives of civil society organisations, as the findings may violate human rights and be discriminatory (gender, religion, etc.). Also, it is expected to be established that Member States will raise objections regarding the procedures to be followed in the evaluation and monitoring of these systems. However, the involvement of civil society representatives in the verification process will enhance transparency, while at the same time the adaptation of AI systems with their observations will ensure that they are moving towards the goal of not violating human rights. Moreover, the systems will serve the purpose for which they were procured. Money and time should also be made available for the appropriate adaptation of the AI systems.

Recommendation 5: EU to support the development and employment of clear guidelines and procedures for the use of AI systems by LEAs

The development and employment of clear guidelines and procedures for the use of AI systems, necessitates not only investment in their development but also investment and support for the creation of a broader **culture of ethical and responsible use of AI systems within LEAs**. This will be facilitated via the creation of an AI culture within LEAs as well as the design and implementation of **AI training and education programs and campaigns** so as to empower the users of these systems to understand how these systems functions, their potential implications and controversies that they may raise. This process will also enable them to actively participate in the development and deployment of these AI systems in the future.

Recommendation 6: EC and EU Member States to ensure that AI systems are inclusive, fair, equitable and non-discriminatory.

It is expected to be a time-consuming process with extensive dialogues with diverse stakeholders, but the outcome will lead to faster planning and implementation of trusted AI systems for the benefit of citizens. Special attention should be paid to the fact that the dialogue should include representatives from all

stakeholders, regardless of gender, age, nation, ethnicity, etc. across the AI lifecycle (design, development, deployment, use/re-purpose).

As mentioned before, it is important to empower the different stakeholder segments and create an AI culture. As such Europe and its Member States should invest in **public education programs and campaigns**, that will enable different stakeholder segments to understand the importance of AI technologies and systems, the risks that may be raised through their use in the security domain while also propose ways to actively participate so as to facilitate the creation of transparent, inclusive, equitable and ethical AI use in the public sector.

Recommendation 7: EU to support and invest in the development of guidelines for gender sensitive policing in the AI era.

This *proactive* recommendation proposes a similar network has already been established in Southeast Europe with reported results so far. The development of a set of guidelines to enhance gender sensitive policing aims to increase gender equality, inclusive design and development of AI systems for security purposes and the feel of security in communities. In addition, the existence of such guidelines will empower and promote gender sensitive policing not only of law enforcements but also of the public administrations in general, paving the way to safe and trustworthy communities, where all citizens will be considered as equal by the police and public administrations in general.

Recommendation 8: EU to establish ethics committees that review proposals in the security domain based on potential ethical and societal issues.

This proactive policy recommendation places emphasis on the establishment of a specialised interdisciplinary Ethics Committees that will be responsible for conducting an assessment of EU funded proposals and projects aiming to prevent potentially serious ethical, societal and human rights issues in the security domain. Although such an internal EU certification for EU-funded projects that would provide guidelines and recommendations and which will continue to review projects as they are implemented will be able to draw hands-on feedback from the security domain, so as to subsequently provide guidelines and broader recommendations for the domain. As an implication, it will be time consuming to set up such Committees as well as to design the appropriate internal assessment frameworks that will enable them to assess not only the accountability and transparency of the AI system but also the ethical, inclusive, human rights perspectives.

Recommendation 9: Inclusive participation (stakeholder and country level) in the EU-funded projects in the security domain.

This recommendation addresses both the current state of affairs (reactive) and future one (proactive). Facilitating the inclusive participation at a stakeholder and country level may create a number of implications that could impact the EU-funded projects. Although balancing a number of requirements could create potential problems for the applicants and their proposed ideas during the proposal application stage, these could continue during the project implementation stage as well. As such it is important to create the frameworks for the current and future calls, and explore alternative ways to ensure that EU-funded projects include civil society organisations and underrepresented Member States in the early stages of the AI design and development as they are underrepresented in the project consortia. As mentioned in previous recommendations, a key pre-requisite entails the creation of awareness as well as the provision of the necessary AI education and training programs for the different stakeholders segments across the different EU

Member States in order to ensure an effective and efficient collaboration of such consortia during the project implementation phase.

CONCLUSIONS

Over the past several years, Law Enforcement Agencies have been increasingly relying on AI based technologies to support their operations. However, these technologies have and continue to raise concerns regarding the violation of fundamental rights, freedoms and values, that can impact citizens, especially vulnerable groups, on a personal and on a societal level. It is important therefore, to reflect on the concerns, fears and risks surrounding the use of AI as well its design and development and to take actions that address these issues adopting a multidisciplinary approach that encompasses both technical, organizational, ethical, legal, cultural and diversity perspectives while ensuring that it is future-proof.

In addition, in order to build trust around AI and create an ecosystem where the voices of all the stakeholders are heard, it is important that civil society is actively included in the AI dialogue but also participates in the design and development of AI systems. Thus, integrating the voice of the civil society and co-creating inclusive AI systems that are more just, ethical and trustworthy for all and for the public good will facilitate a trustworthy AI development and deployment in law enforcement. This process will balance the tension between protecting the public from the potential harmful effects of AI technologies in the security domain, while encourage responsible, ethical and secure-by-design AI-driven innovation.



popAI project

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



popAI is funded by the Horizon 2020
Framework Programme of the European Union
for Research and Innovation. GA number: 101022001

1 October 2021 - 30 September 2023

 pop-ai.eu

 [@popaiproject](https://twitter.com/popaiproject)

 [/company/popai-project/](https://company/popai-project/)