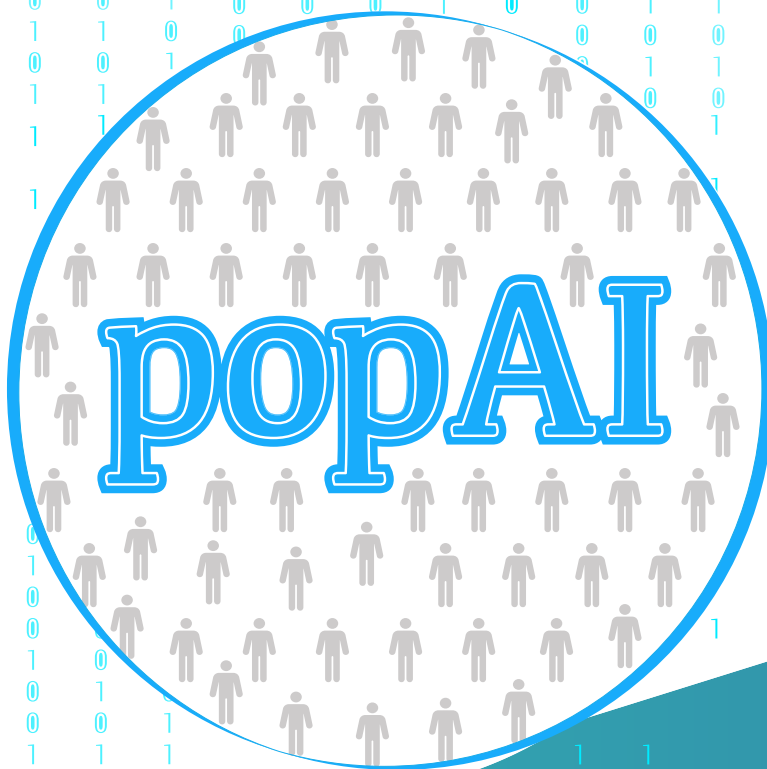
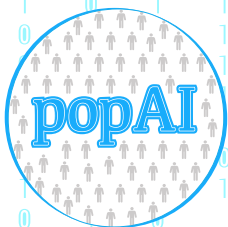


# Policy Brief No 2



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

September 2023



# 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)



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












# POLICY RECOMMENDATIONS OVERVIEW

POLICY RECOMMENDATIONS		TYPE OF POLICY RECOMMENDATION <sup>1</sup>		Target Audience	High-level Theme/ Aim of the Recommendation
		Reactive	Proactive		
Ethical Level, Societal Level, Organisational Level, Regulatory Level	1. EU to provide a <b>legal framework for continuous AI training and educational programmes</b> under the AI Literacy notion for LEAs and civil society			EC DG Home, EC, EU Member States, Ministries, Municipalities	AI literacy, Preserve privacy, Human rights, Non-discrimination, Societal Well-being
Regulatory Level	2. EU to establish a <b>common, harmonized, European AI regulation for LEAs</b> , that will govern the entire process from the design to the implementation and final use of AI systems by Law Enforcement authorities.			European Commission, European Parliament	Enhance transparency and fairness, Trustworthy AI, Lawfulness
Organisational Level, Ethical Level, Societal Level  "PRIOR TO USE PHASE"	3. Develop clear <b>guidelines and standards for the collection, storage, restriction, and use of sensitive data, such as biometric data or other data, by LEAs</b>			EC DG Home, DG Just	Avoid risk of discriminatory use of data
	4. Carrying out <b>impact assessments</b> even in cases when this is not obligatory by law – "voluntary AI Impact Assessments"			EU and MS legislative bodies	Respect for Fundamental Human Rights, Ethics, Democracy, Lawfulness
	5. Establishment and standardisation of a <b>holistic Impact Assessment procedure</b>			EU and MS legislative bodies	Respect for Fundamental Human Rights, Ethics, Democracy, Lawfulness
	6. Establishment of <b>lawfulness, transparency, and accountability protocols for LEAs</b>			EU legislative bodies, EU Member States	Lawfulness, Transparency, Accountability and Auditability
Organisational Level, Ethical Level, Societal Level  "USE PHASE"	7. EU to support the development of <b>guidelines designed especially for the use of AI systems by LEAs</b> .			European Parliament	Minimise risks of abuse or misuse, Transparency
	8. Formulating a <b>general ethical framework for the use of AI tools</b> , considering that the AI Regulation can only regulate the basic legal framework for the use of AI			EU Parliament, Member States, Universities, police academies	Preserve privacy, Fundamental Human Rights, Transparency in using the AI tools
	9. EU to ensure that the <b>use of AI tools by police officers</b> must be subject to <b>multi-level control</b>			Member States, Ministries, Police Agencies	Transparency in using AI tools, Accountability, Ethical use
Organisational Level, Ethical Level  "POST USE PHASE"	10. EU to establish a procedure for the <b>evaluation of AI tools used by LEAs</b> , from the ethical point of view			European Parliament	Ensure Fairness, Transparency, Accountability, Ethical use
	11. EU Member States to support the <b>continuous monitoring of AI systems</b> in use, taking into account the perspective of the civil society.			EU Member States	Enhance transparency, Preserve Privacy and Human Rights, Ethical use
	12. Establish a <b>European AI Systems Registry</b> that will hold basic information about each AI System used by each LEA/per country and its records will be accessible to all EU citizens.			European Commission, EU Member States	Enhance Transparency, Ensure Fairness, Ethical use, Trustworthy AI

<sup>1</sup> Reactive policy recommendations focus on the current state of affairs and proactive focus on the future state of affairs (short-term future).



POLICY RECOMMENDATIONS		TYPE OF POLICY RECOMMENDATION <sup>1</sup>		Target Audience	High-level Theme/ Aim of the Recommendation
		Reactive	Proactive		
Research	13. EU-funding investment for research and development in order to explore the use of AI systems in LEAs			European Commission	Ensure development of ethical and trustworthy AI systems for LEAs
Ethical Level, Societal Level, Inclusion Level	14. Institutionalisation of <b>multidisciplinary collaboration</b>			EU and MS legislative bodies, EU and MS Ministries	Diversity, Non-discrimination and fairness, Societal Well-being, Inclusion
Inclusion Level, Gender Diversity Level	15. Establish <b>Inclusive AI Development Standards</b>			European Commission	Non-discrimination & fairness, Societal Well-being, Respect for Fundamental Human Rights, Ethics, Democracy & Rule of Law, Trustworthy AI
	16 <b>Inclusion of the Civil Society</b>			EU & Member States' legislative bodies Parliaments, Municipalities, Civil Society Organisations	Social inclusion, diversity, non-discrimination, and fairness
Ethical Level, Societal Level, Legal/ Regulatory Level	17. EU to <b>empower people to lodge a complaint and seek redress</b> , when their rights have been violated by the use of an AI system for Law Enforcement			EC DG Home	Ensure non-discrimination principle is respected by LEAs, Societal well-being,

## 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.



## *What AI can offer to the Law Enforcement domain?*

Artificial Intelligence (AI) can provide significant support to numerous Law Enforcement operations. AI technologies and systems, like automated processing techniques to assist crime prevention are widely used by Law Enforcement Agencies (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?*

There is a need to balance security and fundamental rights when implementing AI technologies in the context of Law Enforcement. Such a balanced approach necessitates efficient actions and regulatory frameworks to build trust in AI, mitigate concerns and risks for the civil society and other relevant stakeholders, and ensure that AI systems uphold EU fundamental rights and values. This approach should prioritize human-centric and trustworthy AI while maximizing its societal benefits, especially in the Law Enforcement domain. How can this be achieved? popAI proposes a multidisciplinary and inclusive process, incorporating technical, organizational, ethical, legal, cultural, and diversity perspectives so as to allow the creation of ethical, transparent, inclusive, and accountable AI systems that gain the trust of 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 – Level: E, S, O, R



Level: Ethical, Societal, Organisational & Regulatory | AI System Life-cycle phase: N/A

EU to provide a legal framework for continuous AI training and educational programmes under the AI Literacy notion for LEAs and civil society.

Aligned with the European Union's (EU) efforts to foster a responsible and trustworthy development and use of AI, it is important that emphasis is placed on the establishment of a comprehensive legal framework for the continuous AI training and educational programs for LEA and for the civil society. Falling under the broader concept of AI Literacy<sup>2</sup>, such a framework, would further highlight the importance of empowering Law Enforcement professionals and citizens, with the necessary knowledge, skills and competencies to make informed decisions and ensure the responsible and ethical use of AI systems.

**AI Literacy for LEAs:** As AI technologies are becoming increasingly integrated into Law Enforcement practices, from predictive policing to cybersecurity, it is important to ensure that LEAs can effectively and ethically leverage these AI systems, aligned with the European ethical and legal standards. In order for this to be achieved, AI literacy should be strengthened:

- (a) Across all levels of LEAs:** Law Enforcement officers, across all levels, should be adequately qualified, continuously educated with general and applied AI knowledge, providing best practices and highlighting the importance of high personal integrity standards and organizational culture. Towards this aim a structured and agile and life-long learning educational approach is essential; emphasizing the principles of transparency, accountability, fairness and non-discrimination while providing evolving best practices. Such an approach will strengthen the European responsible AI governance targets, by ensuring that LEAs are adequately empowered with a high level of AI skills and competencies to responsibly and effectively address the complexities associated with AI technologies in their pursuit of safety, justice, and security.
- (b) For LEA as AI system users:** the use of **AI systems by LEAs** should be accompanied by prior and regular comprehensive education and training to ensure that the users and, most importantly, the natural persons to whom the operation of an AI system is assigned to, understand how the system functions, as well as what their role and their ethical and legal obligations are and to guarantee that they are skilled enough to use it correctly, safely and responsibly in conformity with the regulatory framework.  
As such, police officers working with AI tools must be qualified, continuously educated and trained adopting a holistic training approach (multi-perspective approach with technical, ethical, legal, societal aspects, etc). In addition, the importance of individual values and virtues, linked with high personal integrity (as a synopsis of personal ethical standards) should be nurtured and acknowledged.
- (c) For LEAs as deployers of AI systems:** The **deployers of AI systems for Law Enforcement**, must have the necessary knowledge and (regular) training on what to ask for (i.e., the requirements given the legal and ethical considerations, etc) and what to expect by the **providers** as well as the capability to monitor the operation of such systems efficiently and regularly on the basis of the instructions of use.
- (d) For Students in Higher Education Institutions for LEAs:** In accordance with the notion of **AI Literacy**, as prescribed in the AI Act Proposal, it is **recommended** that the Member States add courses on “ethical and lawful AI” to the educational curriculums of Institutions of Higher Education such as **Universities** or equivalents that award degrees in Law or Humanities and Computer Science disciplines. Furthermore, the above courses should also constitute part of the **national educational programmes of LEAs** during their studies at the police academies as well as part of their life-long learning and regular training in the context of their duties. AI education and AI training can be provided through the organisation of relevant seminars and courses by the LEAs for the LEAs to ensure that the staff will be educated, well-trained and skilled, and, consequently, capable of using AI systems and dealing with AI-related issues. Further on, the participation of LEAs in EU-funded research and innovation projects that aim to the design and development of AI systems will help LEAs familiarise themselves with AI-enabled technologies and tools, define the user requirements and the system requirements of such technologies, test them through training sessions and pilot demonstrations and, finally, evaluate them prior to their deployment.

<sup>2</sup> The notion of AI Literacy represents EU's commitment to promoting a deep understanding of AI principles, ethics, and risks.





**Table: Indicative training programme parameters for LEA**

TYPES	TRAINING FREQUENCY	EDUCATORS/TRAINERS
Combination of: <ul style="list-style-type: none"><li>Ethical and legal education and training,</li><li>Technical education and training</li></ul>	<ul style="list-style-type: none"><li>Before the deployment of an AI technology or tool for the users/affected people to be well informed and prepared and for all required actions and measures to be taken timely.</li><li>Regularly (before and after the deployment of an AI system).</li></ul>	<ul style="list-style-type: none"><li>Ethics and legal advisors along with policymakers</li><li>Society representatives</li><li>Technology developers</li><li>Representatives of Law Enforcement agencies</li></ul>

**AI Literacy for Citizens:** In order to foster a democratic control of AI systems, the Commission, the Member States as well as providers and users of AI systems for Law Enforcement in particular (as well as at a general level), in cooperation with all relevant stakeholders, should promote the development of a sufficient level of AI literacy, awareness raising and information communication, towards all members of society. Towards this aim, **citizens'** awareness and AI related knowledge should be enhanced. This can be achieved via the development of relevant courses as part of: the national general education provided by the EU Member States (i.e., Schools), life-long learning programmes focusing on AI (i.e., "Elements of AI" in Finland, etc) and as part of the citizen education programs to inform citizen of their rights in the AI era, in an effective ways, as well as increase their knowledge on the ethical and legal concerns especially of AI in Law Enforcement. In addition, government awareness-raising campaigns should be established so as to inform citizens accordingly, as well as dedicated webpages and TV campaigns in an inclusive approach.

## Recommendation 2- Level: R



**Level: Regulatory | AI System Life-cycle phase: N/A**

EU to establish a common, harmonized, European AI regulation for LEAs, that will govern the entire process from the design to the implementation and final use of AI systems by Law Enforcement authorities.

The pervasive use of Artificial Intelligence in Law Enforcement, necessitates that a unified European AI regulatory framework for Law Enforcement Authorities (LEAs) is established. The regulation of AI for LEAs, and the harmonisation of the AI regulatory framework at the EU level, is important in order to avoid fragmentation, diverse AI adoption levels, and different levels of minimum protection for citizens at national level. Indeed, the Proposal for a Regulation at the EU level (AI Act), especially considering its direct effect in the national legal orders of the EU Member States, is considered as a necessary initiative towards this goal.

The harmonisation of the legal framework regarding the use of AI by LEAs at the EU level shall be compliant with the EU Charter on Fundamental Rights and Freedoms and among others, the right to privacy and data protection, and the respective obligations stemming from the data protection legislation. In addition, the AI legal framework shall be in line with the technological developments.

Such a regulatory framework can set standards for the design, implementation, and use of AI systems, ensuring their legal, ethical, non-discriminatory, and accountability perspectives. Safeguarding this way the European values, civil liberties and fundamental rights while maximizing the potential benefits of AI in policing. Thus, the European Commission and European Parliament must examine the particularities of each state-member and then establish a regulation of AI for LEAs that will govern the entire life-cycle of an AI system from the design, development, deployment and use, that can meet the needs of different members as a total. In order for this to be achieved, scientists with multi-disciplinary expertise should be actively involved (e.g., scientists specializing in technical, legal, and ethical aspects of AI systems, among others), as well as relevant civil society representatives from social organisations dealing with issues of personal data protection and human rights.

Additionally, **guidelines in the form of “Recommendations”** which shall be consistent with the EU legal order, are suggested to be adopted at the EU level, to provide for clarifications or templates to be used by the Member State providers, users and affected by AI systems communities. This will, proactively, ensure consistency and transparency across member states, safeguarding against potential abuses and discrimination, while at the same promoting innovation and accountability and reinforcing citizens’ trust in Law Enforcement agencies.

## Recommendation 3 - Level: O, E, S



**Level: Organisational, Ethical, Societal | AI System Life-cycle phase: Prior to use**

EU to develop clear guidelines and standards for the collection, storage, restriction, and use of sensitive data, such as biometric data or other data, by LEAs.

The rapid technological advancements in AI systems, is interlinked with the growing concerns over individual privacy, liberty and preservation of Human Rights and European Values. In this era, it is imperative for the EU to take proactive actions in order to protect the rights and liberties of its citizens and empowering this way the foundations of a united Europe, laid upon the core values and principles, which bind countries and peoples together: respect for human dignity, freedom, democracy, equality, the rule of law and fundamental rights, including those of minorities (Lisbon Treaty – Art. 2)<sup>3</sup>. An important area that demands immediate attention is linked with the collection, storage, restriction, and use of sensitive data, particularly biometric data, by LEAs.

The advancements of biometric technology<sup>4</sup> have revolutionized the field of Law Enforcement, providing unique applications that empower Law Enforcement officers to detect and stop criminal activity. However, at the same time the collection, storage, restriction, and use of sensitive data such as biometric data by LEAs raises significant ethical, privacy, and security concerns<sup>5</sup>.

Despite the very nature of biometric data, to be directly linked to an individual, to date, there are no particular, legal provisions in the world specific to biometric data protection<sup>6</sup>. The collection and use of biometric data is generally regulated within the framework of personal data protection and privacy laws in a broad sense. As such, biometric data, as a special category of sensitive personal data resulting from a specific technical processing related to the physical, physiological, or behavioral characteristics of a natural person, is subject to some fundamental rules of General Data Protection Regulation (GDPR) including users’ consent and the “right to be forgotten”.

<sup>3</sup> The European Union is founded on the following values (as laid out in Article 2 of the Lisbon Treaty and the EU Charter of Fundamental Rights): **Human dignity:** Human dignity is inviolable. It must be respected, protected and constitutes the real basis of fundamental rights. **Freedom:** Freedom of movement gives citizens the right to move and reside freely within the Union. Individual freedoms such as respect for private life, freedom of thought, religion, assembly, expression and information are protected by the EU Charter of Fundamental Rights. **Democracy:** The functioning of the EU is founded on representative democracy. A European citizen automatically enjoys political rights. Every adult EU citizen has the right to stand as a candidate and to vote in elections to the European Parliament. EU citizens have the right to stand as a candidate and to vote in their country of residence, or in their country of origin. **Equality:** Equality is about equal rights for all citizens before the law. The principle of equality between women and men underpins all European policies and is the basis for European integration. It applies in all areas. The principle of equal pay for equal work became part of the Treaty of Rome in 1957. **Rule of law:** The EU is based on the rule of law. Everything the EU does is founded on treaties, voluntarily and democratically agreed by its EU countries. Law and justice are upheld by an independent judiciary. The EU countries gave final jurisdiction to the European Court of Justice - its judgments have to be respected by all. **Human rights:** Human rights are protected by the EU Charter of Fundamental Rights. These cover the right to be free from discrimination on the basis of sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation, the right to the protection of your personal data, and the right to get access to justice. (Source: European Commission).

<sup>4</sup> Biometric technologies (like facial recognition systems) usually refer to all processes used to recognize, authenticate and identify persons based on physical and/or behavioral characteristics (i.e., facial images, fingerprints, iris scan etc).

<sup>5</sup> The use of biometric techniques “raise a number of ethical issues, as an individual cannot easily change biometric features, and as these techniques tend to intrude into the human body and ultimately the human self” (Wendehorst and Duller, 2021).

<sup>6</sup> Furthermore, “legal norms that regulate the use of biometric techniques can be found on an international, EU and national level; more specifically, fundamental rights and data protection law set limits for the use of biometric techniques. Legislation on border security on the other hand, contains explicit authorisations for using biometric technology in specific situations.” (Wendehorst and Duller, 2021).





However, in order to keep up with the evolving aspects of biometric technologies and biometric data, it is necessary to develop a clear set of guidelines and standards to govern the handling of biometric data by LEAs; ensuring this way that they are used responsibly and in accordance with the rule of law across EU region. In addition, necessary safeguards should also be introduced, in order for example to prevent data breaches and unintentional sharing of biometric data templates, while also ensuring that the technical robustness of any biometric identification system must be guaranteed at any time (Wendehorst and Duller, 2021, Jain et al., 2005)<sup>7</sup>.

## Recommendation 4 – Level: O, E, S



**Level: Organisational, Ethical, Societal | AI System Life-cycle phase: Prior to use**

Carrying out impact assessments even in cases when this is not obligatory by law – “voluntary AI impact assessments”.

A crucial and often overlooked practice in the area of AI is related to impact assessments. AI impact assessments (AI-IAs)<sup>8</sup> constitute a way of identifying potential risks and negative impacts associated with an AI system either before its deployment (ex-ante AI-IAs), after (ex-post AI-IAs) and/or on a continuous basis, by being embedded in organisational processes and structures, regularly reviewed and updated, in order to safeguard AI’s benefits and avoid its downsides for individuals and society at large. As such AI-IAs will play a crucial role in future AI governance (Stahl et al., 2023).

These assessments encompass a wide range of considerations, including ethical concerns, human rights considerations, biases, privacy implications, and societal impacts and enable AI developers, researchers, and policy makers among others to better understand and reflect on AI technologies. Existing research in the area indicates that AI-IAs should be “revisited and revised at each new phase of AI lifecycle (Council of Europe 2019), when significant changes are introduced (Brey 2022, p. 1), e.g., changes to data collection, storage, analysis or sharing processes (UK Governmental Digital Service 2020) and before the production of the system.... and renewed at a set time, every couple of years (AI Now Institute 2018a)” (Stahl et al., 2023, p: 12812)<sup>9</sup>.

The latest Amendments to the AI Act Proposal, necessities that a **fundamental human rights impact assessment** is conducted for high-risk AI systems by the providers prior to the design and development stage as well as by the LEAs prior to putting such systems into use. However, **voluntary impact assessments** even in the absence of relevant legal mandates is strongly advised, and in cases where it is not obligatory by law (namely for the rest of AI systems which fall under the AIA scope), so as to ensure the responsible and ethical deployment of artificial intelligence across different phases of its life-cycle (ex-ante, ex-post and ongoing).

These voluntary AI-IAs can empower the reflection and understanding of the broader implications of AI systems, initially at an early phase (ex-ante followed by ex-post). This will in turn, enable developers to refine their technologies in order to better meet the expectations of users and minimize unintended consequences and harms. As such voluntary impact assessments can lead to responsible technology-driven innovation that is aligned with societal values and needs; conveying trustworthiness.

Therefore, it is suggested that, without affecting the obligation of providers/deployers of high-risk AI systems to conduct an Impact Assessment, the EU legislator should also **provide a recommendation/guideline for the voluntary conduct of Impact Assessments** regarding the rest of AI systems used by LEAs falling into the AIA scope, enabling them to address potential issues before they escalate, safeguarding both individuals and society at large.

<sup>7</sup> Wendehorst, C., and Duller, Y. (2021). Biometric Recognition and Behavioural Detection Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces. EPRS: European Parliamentary Research Service. Belgium. Jain, A. K., Ross, A., & Uludag, U. (2005, September). Biometric template security: Challenges and solutions. In 2005 13th European signal processing conference (pp. 1-4). IEEE.

<sup>8</sup> AI impact assessment can build on and incorporate numerous existing impact assessments, including: (1) Data protection impact assessment, (2) Algorithmic impact assessment, (3) Human rights impact assessment, (4) Socio-economic impact assessment, (5) Environmental impact assessment, (6) Ethics impact assessment, (7) Responsible innovation assessment. Existing AI impact assessments developments exist, for example in the IEEE 7010-2020 standard on Recommended Practice for Assessing the Impact of Autonomous and Intelligent Systems on Human Well-Being or the Dutch ECP AI Impact Assessment. (Source: [SHERPA project](#)).

<sup>9</sup> Stahl, B. C., Antoniou, J., Bhalla, N., Brooks, L., Jansen, P., Lindqvist, B., ... & Wright, D. (2023). A systematic review of artificial intelligence impact assessments. Artificial Intelligence Review, 1-33. LINK

## Recommendation 5 – Level: O, E, S



**Level: Organisational, Ethical, Societal | AI System Life-cycle phase: Prior to use**

Establishment and standardisation of a holistic Impact Assessment procedure

AI impact assessments (AI-IAs) are essential tools that should be used in order to evaluate the potential effects of artificial intelligence technologies on various aspects of society, economy, and individuals. Aligned with the latest Amendments to the AI Act Proposal, it is necessary that a **fundamental human rights impact assessment is conducted for high-risk AI systems** by the providers prior to the design and development stage as well as by the LEAs prior to putting such systems into use. In addition to this, for compliance with the applicable data protection legislation, where applicable, a **data protection impact assessment** must be conducted and, in order to ensure that the affected persons are informed and heard, the fundamental rights impact assessment should be accompanied by an ethical and social impact assessment.

Therefore, it is suggested that the EU legislator establishes an obligation for the conducting of a **holistic Impact Assessment procedure for high-risk AI systems, and a recommendation for the rest of AI systems falling into the AIA scope**, considering fundamental human rights, the rule of law and democracy, ethical and social implications. To this end, it is recommended that the EU legislator, provides for a regulatory framework including the obligation or recommendation (respectively, as above) of carrying out a thorough and all-inclusive impact assessment for AI systems used by LEAs, accompanied by a standard impact assessment template.

The impact assessment template could be part of the **AIA ANNEX, or incorporated into “Recommendations”**<sup>10</sup>, guidelines or communicated via other appropriate means. It is highly recommended that such template draws inspiration from the methodologies: **HRIA** (Human Rights Impact Assessment), **HUDERIA**<sup>11</sup> (Human Rights, Democracy, and Rule of Law Impact Assessment), **AFRIA**<sup>12</sup> (ALIGNER EU Project Fundamental Rights Impact Assessment), **DPIA**<sup>13</sup> (Data Protection Impact Assessment), **HRESIA**<sup>14</sup> (Human Rights, Ethical and Social Impact Assessment) and **ESIA**<sup>15</sup> (Ethical, Social Impact Assessment). Finally, it is essential to report herein that the impact assessments (or at least a summary) shall be made publicly available, where appropriate, as well as multidisciplinary and inclusive, to engage citizens in policymaking.

<sup>10</sup> EUR-Lex, Official Website of the EU, Glossary of summaries, Recommendations, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LE-GISSUM:recommendations>

<sup>11</sup> Ad Hoc Committee on Artificial Intelligence (CAHAI), Policy and Development Group (CAHAI-PDG), Human Rights, Democracy, and the Rule of Law Assurance Framework (HUDERAF) for AI systems, Executive Summary, 8 October 2021, available at <https://rm.coe.int/cahai-pdg-2021-09-huderaf-executive-summary/1680a416de>

<sup>12</sup> ALIGNER Project <https://aligner-h2020.eu/fundamental-rights-impact-assessment-fria/>

<sup>13</sup> Article 27 GDPR (EU General Data Protection Regulation)– DPIA (Data Protection Impact Assessment) - DPIAs assess how AI and machine learning technologies handle personal data (i.e., understanding how the AI system collects that data and use it, in order to subsequently implement the right measures to protect individual rights, spot the security and compliance gaps, and address them).

<sup>14</sup> The HRESIA methodology takes into account a variety of different societal issues, which do not necessarily concern fundamental rights and freedoms, for example interoperability and openness (Mantelero, 2018).

<sup>15</sup> Mantelero A., (2018), ‘AI and Big Data: A blueprint for a human rights, social and ethical impact assessment’, available at <https://www.sciencedirect.com/science/article/pii/S0267364918302012>



## Recommendation 6 – Level: O, E, S

Level: Organisational, Ethical, Societal | AI System Life-cycle phase: Prior to use

Establishment of lawfulness, transparency, and accountability protocols for LEAs

Among other concerns raised by citizens, is the need for transparency about them being subject to the use of an AI-system, the provision of information to them for their data processing by LEAs and the establishment of a procedure to object to unjust decisions were raised.

It is a **demand** that the citizens are informed timely, appropriately and (if possible) automatically about their exposure to AI-systems used by LEAs and the processing of their data by LEAs and that they can exercise their respective rights through established and accessible them procedures, considering their specific conditions and particularities.

A broader field of application of Article 52 of the latest Amendment to the AI Act Proposal is suggested, in the sense that the persons affected by Law Enforcement AI shall be informed that they are subject to an AI system, its purpose, the humans responsible for making the decision, the decision-making process, the adherence to the ALTAI principles (Assessment List of Trustworthy AI<sup>16</sup>) and about their rights (including their right to object, redress and the right to seek explanation). In addition, the enforcement of the data subjects' right to be informed about and request access to: (indicatively) the types of data processed, the data origins, the data controller, the purposes and types of data processing, the legal basis for processing, the retention period and exercise their data protection rights could be accomplished through this mechanism/procedure. The mechanism or procedure to inform the exposed to an AI system person and data subject, about (indicatively and as a minimum) the above, is proposed to be conducted timely and automatically, if possible.

Moreover, and in accordance with the accountability principle, the development and establishment of an easy-to-follow, yet well-defined procedure towards enabling the review of information, provision of feedback and the objection against unjust decisions by the citizens, for example through a centralised online platform, **is** considered of paramount importance. Finally, a **“feedback mechanism”** is recommended to be implemented, in order to receive input on how to improve the system directly from those potentially affected by it.



## Recommendation 7 – Level: O, E, S

Level: Organisational, Ethical, Societal | AI System Life-cycle phase: Use

EU to support the development of guidelines designed especially for the use of AI systems by LEAs.

As AI has and will continue to play a pivotal role in the Law Enforcement domain, it is important that we harness AI's benefits, while safeguarding fundamental rights and European values. Towards this aim, it is recommended that the European Union (EU) develops clear guidelines and protocols, tailored to the needs of the security domain. For example, it could support the creation of a special group with a multi-stakeholder approach (experts from Law Enforcement agencies, AI researchers, legal experts, relevant EU institutions etc) that can establish these guidelines based on fairness and respect of individual rights. So, the risk of abuse or misuse can be minimised and transparency can be enhanced.

Aiming to address this pressing concern, the EU could consider the establishment of a specialized working group, that will be comprised by a diverse set of stakeholders and scientific disciplines, and relevant EU institutions, adopting a multi-stakeholder approach. This group should include experts from Law Enforcement agencies, AI researchers, legal experts, technology experts, ethics, and social scientists as well as Law Enforcement officers across Europe and civil society representatives among others. Such a collaborative working group can create a solid basis for ensuring a comprehensive and balanced perspective when formulating clear and practical guidelines for the use of AI in policing.

<sup>16</sup> The seven principles of the ALTAI are: 1. Human agency and oversight, 2. Technical robustness and safety, 3. Privacy and data governance, 4. Transparency, 5. Diversity, non-discrimination, and fairness, 6. Societal and environmental well-being, 7. Accountability (EC, ALTAI, <https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment>)



These guidelines should prioritise fairness, accountability, transparency and the protection of human rights, fostering responsible deployment of AI systems by Law Enforcement officers, and at the same time fostering citizens trust in AI for the policing context. Such guidelines could thus, enable EU and Member States to mitigate the risks of AI misuse and abuse. Finally, it is important that these guidelines and protocols are frequently updates and are aligned with the legal, ethical guidelines and best practices in AI systems deployment in policing.

## Recommendation 8– Level: O, E, S



**Level: Organisational, Ethical, Societal | AI System Life-cycle phase: Use**

Formulating a general ethical framework for the use of AI tools, considering that the AI Regulation can only regulate the basic legal framework for the use of AI.

The emergence of AI has introduced transformative capabilities with the potential to reshape the Law Enforcement domain among others. While the regulatory bodies around the world are striving to keep up with the pace of AI development, it is becoming increasingly clear that a more comprehensive and holistic approach is needed. This makes the need for formulating a general ethical framework for the use of AI tools in Law Enforcement, even more evident. More specifically, taking into account that the AI Act (and/or any other regulation on the level of European Union law-making authorities) can only regulate the basic legal framework for the use of AI, it is necessary to formulate a **general ethical framework for the use of AI tools in Law Enforcement**.

As the AI Regulation establishes the important rules and guidelines, addressing issues such as safety, accountability, transparency, and data protection, it is important to acknowledge that the pace of AI innovation often outpaces our ability to adapt and respond swiftly to emerging ethical concerns and unanticipated consequences. As a result, it is important that regulations are integrated with context-specific ethical frameworks as in the case of AI for Law Enforcement, so that we can sufficiently address the full spectrum of ethical dilemmas posed by current and future AI systems. Such an ethical framework will complement the legal framework by encompassing a broad spectrum of ethical considerations for the use of AI tools for policing, that will (go beyond legality) provide the **“operational context”** within which responsible AI deployment and use in Law Enforcement can occur.

Furthermore, the Members States’ national laws have their specificities and therefore some aspects of the use of AI tools for Law Enforcement may differ. These aspects are, among others, the way in which the use of AI tools will be used and controlled (not only) with the Law Enforcement context. Consequently, an **“ethical framework for AI in Law Enforcement”** will specify among others, how the users of AI systems in LEAs (especially police officers) who will be the ones using them, on a daily basis, will collect the necessary information, how they will be selected and how these individuals (in particular police officers) will be educated and trained an on-going basis (with technical and ethical training courses). This means that these ethics rules should be developed with an anticipatory and multifaced perspective so that they create “supranational” and “timeless” rules that would create standards for the way in which information will be obtained through AI tools as well as for controlling for what reasons and to what extent this information will be obtained.



## Recommendation 9 – Level: O, E, S



Level: Organisational, Ethical, Societal | AI System Life-cycle phase: Use

EU to ensure that the use of AI tools by police officers must be subject to multi-level control.

AI has emerged as a powerful tool for effectively supporting Law Enforcement Agencies in their mission to maintain public safety. However, in order to harness the full potential of AI for policing it is important that we adequately address the numerous associated concerns and prevent the negative impacts. Towards this aim, we should ensure as society, that the use of AI tools by police officers must be subject to multi-level control and on-going supervision, in order to safeguard fundamental human rights and freedoms and at the same time prevent potential unintended negative consequences and abuses.

Aligned with the European values, legal and ethical principles, is the need to show a strong commitment to upholding human rights and privacy, manifested via multi-level controls of AI systems used in the policing context, among others. Such regular controls could involve a number of key aspects including, for example, the (indicative list):

- **Legal alignment:** ensure legal alignment at all times
- **Ethical alignment:** Developing ethical guidelines for preventing bias, discrimination, and other ethical concerns associated with AI systems used in the policing context. These ethical principles should be frequently monitored
- **Data Protection alignment:** Protecting personal data, and aligning with relevant EU regulation for the collection, storage, and use of data, by AI systems in Law Enforcement.
- **Transparency alignment:** Acknowledging the importance of transparency for building public trust, Law Enforcement Agencies should be required to disclose information about their AI systems, including their purpose, functionality, and potential impact on communities. Internal transparency controls should be implemented early on (and on an on-going basis) to ensure that the transparency obligations are met.
- **Accountability alignment:** Accountability controls are essential and should be implemented on a regular basis, so as to ensure that Individuals responsible for AI system decisions are identifiable, and that adequate mechanisms are set to hold them accountable for any misconduct.
- **Training alignment:** A crucial aspect for the responsible use of AI tools in policing is the ongoing AI training for Law Enforcement officers, across all levels. Such AI training, should include technical, operational training on AI tools including ethics training to promote the ethical use and responsible use of AI deployment in an operational context. These trainings should constantly evolve and include EU best practices.
- **Public Engagement:** Public trust in AI for Law Enforcement will be fostered via inclusivity and public participation. As such these multi-level controls should involve civil society and civil society representatives, NGOs, experts, and the public (see Recommendation No.11).

**Implementing multi-level controls:** It is important that external independent oversight bodies/committees are established. These bodies should be responsible for conducting these multi-level controls and approving the deployment and use of AI tools in policing. Regular control audits and impact assessments of AI systems used by police should be set, so as to ensure that they adhere to legal and ethical principles. Furthermore, it is important that these multi-level controls are conducted on a regular basis (continuous monitoring – see Recommendation No. 11 of this report), in order to adequately address the emerging concerns raised by the use of AI in Law Enforcement, providing this way a robust multi-level control mechanism.

## Recommendation 10 – Level: O, E



**Level: Organisational, Ethical | AI System Life-cycle phase: Post Use**

EU to establish a procedure for the evaluation of AI tools used by LEAs, from an ethical point of view.

Acknowledging the importance of complementing the legal framework with an ethical perspective that will empower Law Enforcement, to swiftly respond to emerging ethical concerns and unanticipated consequences of the AI systems that are used for policing. Fostering this way trust around the legal and ethical use of AI tools by European LEAs. For this to be realised, it is important that EU establishes a comprehensive procedure for the evaluation of AI tools used by LEAs in the EU from an ethical perspective. Ethical considerations in the use of AI system in policing, constitute an important parameter for safeguarding fundamental rights, preserving public trust, and ensuring accountable governance of AI systems at all times.

As such, complementing popAI's Policy Recommendation No. 8 – focusing on the development on an ethical framework for AI in policing - there is a need for the European Union to establish and support a common procedure (across all Member States) for the evaluation of AI tools used by European Law Enforcement Agencies. Such a procedure should involve regular ethical audits and impact assessments of AI systems in use, so that their effectiveness and potential social consequences are evaluated. For example, EU Member States could compel Law Enforcement Agencies to conduct regular impact assessments on their predictive policing algorithms. In case that bias is identified, agencies would have to take corrective actions to face this issue and improve the algorithms used.

## Recommendation 11 – Level: O, E



**Level: Organisational, Ethical | AI System Life-cycle phase: Post Use**

EU Member States to support the continuous monitoring of AI systems in use, taking into account the perspective of the civil society.

Once an AI system is adopted by a LEA and put in use, its continuous monitoring must be taken into account. Aligned with the need for multi-level control of AI systems used in Law Enforcement within the EU and its Member States (presented in Recommendation No.9), it is important to ensure the continuous monitoring of these systems, while taking into account the perspective of the civil society. European Union and EU Member States play a critical role in promoting and safeguarding the legal as well as ethical use of AI technologies in policing. This can be ensured, among others, via the continuous multi-level monitoring of AI systems for LEAs, ensuring the ethical AI practices in policing and their on-going alignment with our European values, freedoms, and fundamental rights.

These continuous, multi-level monitoring practices can be broadened up, by integrating the perspective of the civil society and civil society representatives that play a pivotal role in safeguarding democratic principles, protecting individual rights, and promoting transparency. Therefore, only via ongoing and proactive monitoring processes of AI systems that include civil society representatives we can enhance the identification of potential biases and misuses, while also assessing the societal, ethical and human rights impact of these technologies and their potential unintended consequences for minorities and/or under-represented communities.

However, for this to be realised EU and EU Member States should invest in creating and cultivating a culture of responsible AI use adopting an inclusive perspective, that integrates among others the civil society's standpoint in the design as well as in the monitoring processes of AI systems. In this way, it can be ensured that AI technologies align with the expectations of EU citizens and civic insights will be integrated; insights that are crucial for the formulation of inclusive AI systems and policies.





## Recommendation 12 – Level: O, E

**Level: Organisational, Ethical | AI System Life-cycle phase: Post Use**

Establish a European AI Systems Registry that will hold basic information about each AI System used by each LEA/per country and its records will be accessible to all EU citizens.

Citizens' concerns about the use of AI systems by LEAs, combined with the real ethical and legal risks of their use, make it necessary for all stakeholders to know what is actually there and what is "at risk". As such it is highly recommended that EU establishes a pan-European AI Systems Registry that will hold basic information about each AI system used by each LEA at a country level and its records will be accessible to all EU citizens.

As such the creation of this registry at European level will oblige each LEA in each country to provide a concrete record on a compulsory basis, with specific information regarding each AI system that is used currently or it is planned to be use in the near future. The information that will be provided could include for example: a brief description of the AI system use, the technology it uses (with a general description), when it was designed/implemented, its data sources, when it was deployed, if and when and by whom it has undergone GDPR compliance checks, Impact Assessments (AI-IAs), etc. Access to all or part of this information may be available to all citizens or only to interested parties after request. In this way, transparency will be enhanced, control will be strengthened, and a uniform approach to the legal and ethical use of AI in LEAs will be achieved. Since transparency is a cornerstone of trust, such a European AI Systems Registry for LEAs would ensure citizens trust in AI and at the same time it would ensure the responsible AI use, and promotion of collaboration among agencies within Europe.

## Recommendation 13 – Level: R



**Level: Research | AI System Life-cycle phase: N/A**

EU-funding investment for research and development in order to explore the use of AI systems in LEAs.

In order to explore the use of AI systems in Law Enforcement and understand their operationalisation, impacts and societal implications it is important that we invest adequate financial resources in AI research and development activities for this domain (in addition to others) as well as deployment and testing via the establishment of regulatory sandboxes for AI in this sector. This funding will further support cutting-edge, multi-disciplinary and cross-disciplinary research and innovation in AI for Law Enforcement and ensure the establishment of regulatory sandboxes enabling us to balance between innovation and accountability.

Although AI technologies, such as facial recognition and predictive policing algorithms, have the potential to revolutionise Law Enforcement, their deployment may give rise to significant risks, bias, privacy and human rights infringements, lack of transparency, among others. Thus, it is important to create controlled environments for testing these technologies, exploring their usage for Law Enforcement and evaluating them under higher levels of scrutiny so as to ensure that the ethical, legal and human rights standards are met successfully.

Thus, providing dedicated financial resources for research and innovation activities will, reflect from the one side the recognition that AI has the potential to revolutionize the Law Enforcement practices, but it requires sustained investment to fully realize its potential in a responsible and sustainable way. While on the other side it will signal the European commitment to fostering trust in AI via collaboration and co-creation between academia, industry, LEAs and government entities as well as civil society; aligning this way with the European human-centric, trustworthy AI approach. As such increased EU funding investment in research and development will not only fuel economic growth but also underscores Europe's commitment to responsible AI development, ensuring that the benefits of AI are realized while minimizing potential risks for the Law Enforcement domain.

## Recommendation 14 – Level: E, S, I



Level: Ethical, Societal, Inclusion | AI System Life-cycle phase: N/A

Institutionalisation of multidisciplinary collaboration.

In order to understand new disruptive technologies, their operational dynamics, associated benefits, risks, their broader societal, and environmental implications and at the same time to attain the ethical and secure design, development and deployment of trustworthy AI, it is imperative that we invest in the active participation of diverse stakeholder segments including citizens. Building upon the principle of human oversight, one that resembles a “human-over-the-loop” approach, it is important that a **robust collaboration framework** that promotes joint efforts between diverse stakeholder segments and fosters multi and inter-disciplinary scientific collaboration. Such a collaborative framework should actively involve LEAs, ethics and legal experts, policymakers, technology developers and civil society representatives (including end users and affected persons from vulnerable groups among others), who should remain actively involved throughout the entire lifecycle of the AI system – from its design and development phases through testing, validation, implementation, and monitoring and ongoing enhancements. Such a formalised system of multidisciplinary and cross-actor collaborations, both at the EU and national levels, is important in order to ensure the responsible and ethical advancement of AI technology as well as its interconnection with other technologies. Not only recognising but also addressing the need for a holistic and inclusive approach to AI development for Law Enforcement, one that integrates a diverse range of perspectives and expertise; is critical to address the multifaceted challenges posed by AI. Therefore, the institutionalisation of multidisciplinary collaboration at the EU and national level between legal and ethics experts, developers of AI tools, end-users, and the affected persons (including vulnerable groups) is highly recommended. Therefore by institutionalising multidisciplinary collaboration in the area of AI for Law Enforcement (and beyond), is needed in order to pave the way for the co-creation of AI solutions that not only adhere to ethical standards but also genuinely serve the needs and values of our society in a responsible and sustainable way.

## Recommendation 15 – Level: I, GD



Level: Inclusion, Gender Diversity | AI System Life-cycle phase: N/A

Establish Inclusive AI Development Standards.

Promoting inclusion and gender diversity in AI for Law Enforcement is not only a matter of ethical responsibility but also it is a critical parameter for establishing trust and ensuring the equitable and effective use of AI technologies. Towards this aim, it is important for EU to establish inclusive AI development standards and frameworks for Law Enforcement in Europe. Such frameworks must adopt comprehensive and inclusive AI development standards that will guide Law Enforcement agencies across Europe as to how they can achieve these inclusion and diversity goals while harnessing the full potential of AI for public safety.

Some of the key principles that should underpin such standards and frameworks could entail for example:

- (a) **a requirement for diverse teams:** ensuring this way that AI development teams in Law Enforcement agencies should include members from diverse backgrounds, including gender, ethnicity, and expertise in ethics and bias mitigation;
- (b) **transparency and accountability requirement:** AI systems used in Law Enforcement should be transparent both in their operation but also in their decision-making processes. Thus, it is important to ensure that Law Enforcement agencies will provide transparent documentation of AI development processes, data sources, algorithms used and model explanations; accompanied by clear roles and responsibilities and redress mechanisms, among others;
- (c) **a requirement for “bias and fairness audits”:** ensuring that LEAs implement regular audits to identify and resolve bias and fairness issues in AI algorithms developed and used in Law Enforcement. Such audits should be conducted by independent, third-party organisations.

The establishment of inclusive AI development standards for AI in LEAs will, therefore, contribute to fair, transparent, and accountable AI systems that benefit society.

popAI’s “inclusion and diversity checklist for AI in Law Enforcement” (see next page) aims to contribute to a more inclusive and diverse in AI for Law Enforcement, by providing a short and holistic checklist for LEAs. This checklist is based on the popAI inclusion framework that integrates diverse perspectives (technical, societal, individual) and has derived from bottom-up research that integrates all stakeholder segments including civil society.

# popAI Inclusion & Diversity Checklist for AI in Law Enforcement

- 1 Define your Inclusion & Diversity goals:** It is important to define what inclusion and diversity mean to your organization, and for your AI system. Such a process could entail identifying the relevant stakeholders, and underrepresented groups, and those that are more likely to suffer the consequences of AI system risks. It is important that this process is done in a transparent manner. (For example, LEAs could publish these goals online or create a written internal policy, so as to showcase both internally to officers or publicly to external audience, what inclusion and diversity means, and strengthen their accountability, since these goals will state the official position with which officers will need to comply with and respect.)
- 2 Create Diverse Teams:** The AI development teams should be diverse and inclusive, to ensure that your AI system is designed with inclusivity and diverse set of perspectives taken into consideration from the beginning.
- 3 Training and Awareness:** Provide ongoing training and awareness-raising activities to all stakeholders involved in the design, development, and use of the AI systems in Law Enforcement; empowering them to understand the importance of diversity and inclusion and fairness, ensuring this way that these principles are reflected in the system. These activities should be part of the broader training activities for AI in Law Enforcement.
- 4 Acquire User Feedback:** Ensure collaboration and structured feedback process form a diverse range of stakeholders, throughout the development process of an AI system (i.e., especially from underrepresented groups, individuals from impacted communities, etc.). This process will ensure that the envisioned AI system reflects the needs and perspectives of a diverse range of users, making it inclusive and equitable. For example, incorporating their feedback into the model's design and testing the model with users from different backgrounds.
- 5 Define the problem and goals:** Define the problem that the AI system is intended to solve and define the goals of the project, considering the potential impact on different communities and stakeholders.
- 6 Inclusive and diverse data:** Ensure that the training data that will be used to build the AI model is diverse and representative of the population it will be serving. This includes ensuring that the data includes examples from a range of backgrounds, experiences, and perspectives, including those historically underrepresented.
- 7 Check for Bias:** Run bias tests on your AI system for any potential sources of bias and ensure mitigation actions. Bias can arise from data collection, model design, or the use of proxies. Therefore, it is important to evaluate how the data is collected, labeled, and preprocessed, whether any potential biases in the system's decision-making process exist, as well as considering the potential for algorithmic bias during training and testing. With this regard, it will be crucial to provide for confidential channels that LEOs could use to report such biases.
- 8 Ongoing Monitoring & Continuous improvement:** Set and conduct ongoing monitoring practices that will enable you to evaluate and improve the AI system's performance and use in the field, taking into consideration aspects related to inclusion and diversity, biases, fairness, unintended consequences and impacts of your system on different groups of people, and take the necessary corrective action. Throughout this process ensure that you are open to feedback from different stakeholders including civil society and external consultation from experts, if and when needed.

## Recommendation 16 – Level:



Level: Inclusion, Gender Diversity | AI System Life-cycle phase: N/A

Inclusion of the Civil Society.

Trustworthy AI means that the AI systems are designed, developed and used in a way that makes them understood, accepted and valued by the users and the affected persons. At the same time, it is equally necessary that the affected persons obtain information about the purposes, the risks and the impact of AI-based technologies and tools on the society and the environment and have the right to give their feedback. This is essential, especially, in the case of Law Enforcement, since the LEAs actions that involve certain uses of AI systems are characterised by a significant degree of power imbalance and may lead to surveillance, arrest or deprivation of a natural person's liberty as well as other adverse impacts on fundamental rights guaranteed in the Charter.

It is critical that: sufficient information about the AI systems planned to be used or already being used in Law Enforcement, transparent information about the datasets used and the way in which the AI outcomes are produced, is provided to the affected persons to enhance public understanding and trust and to ensure that their rights are not violated. It is also suggested that a feedback mechanism is established in order to collect input on how to improve the system directly from those potentially affected thereby<sup>17</sup>.

### Recommended Practices (indicative list):

- The **organisation of events** (physical, online and hybrid) to inform citizens about AI technologies, in an inclusive manner taking into consideration the diverse level of digital skills that civil society members have,
- **Visits and talks at schools and universities**, across regional areas of Member States
- **Drafting of protocols and code of conduct** governing the use of AI tools in Law Enforcement and making them publicly available,
- The creation of **educational videos and campaigns**, including serious game,
- The establishment of **communication channels, public registers and feedback mechanisms**,
- Conducting of **ethical and social impact assessments** prior to the development/ deployment of AI systems by LEAs and collect valuable feedback about the citizens' expectations, concerns, fears and objections and to actively involve the affected persons in the evaluation and validation of the AI systems used in Law Enforcement,
- The establishment of **multidisciplinary and diverse teams in the deployer's entity** that also communicate with civil society representatives through communication channels and feedback mechanisms.

## Recommendation 17 – Level: E, S, R



Level: Ethical, Societal, Regulatory/Legal | AI System Life-cycle phase: N/A

EU to empower people to lodge a complaint and seek redress, when their rights have been violated by the use of an AI system for Law Enforcement.

As AI technology becomes more integrated into various aspects of society including its use by for Law Enforcement purposes, there is growing recognition of the need for accountability and transparency in these AI systems. Relevant established and upcoming regulations and mechanisms exist for addressing concerns and complaints related to AI systems. For example, the GDPR plays a significant role in addressing concerns related to the use of personal data in AI systems and therefore citizens can lodge complaints with Data Protection Authorities, if they believe their data privacy rights have been violated. In addition, citizens Consumer Protection Agencies are responsible for handling complaints related to AI systems that may have led to unfair practices, or other issues.

<sup>17</sup> Ad Hoc Committee on Artificial Intelligence (CAHAI), Possible elements of a legal framework on artificial intelligence, based on the Council of Europe's standards on human rights, democracy and the rule of law, 3 December 2021, p.12



However, additional ways should be examined so that citizens can easily voice their complaints about AI systems irrespective of their digital skills level and their AI competencies. Furthermore, EU should enhance human rights protection in the upcoming regulation of AI and prohibit harmful and discriminatory surveillance and other abusive applications of AI, while at the same time provide effective remedies for people harmed by AI, aligned with the Human Rights Watch, 2023 statement<sup>18</sup>. Towards this aim civic society should be empowered to understand, when and how the use of AI systems in the general as well as in the context of Law Enforcement, can potentially harm and violate their fundamental rights so that they can complaint and seek redress.

## CONCLUSIONS

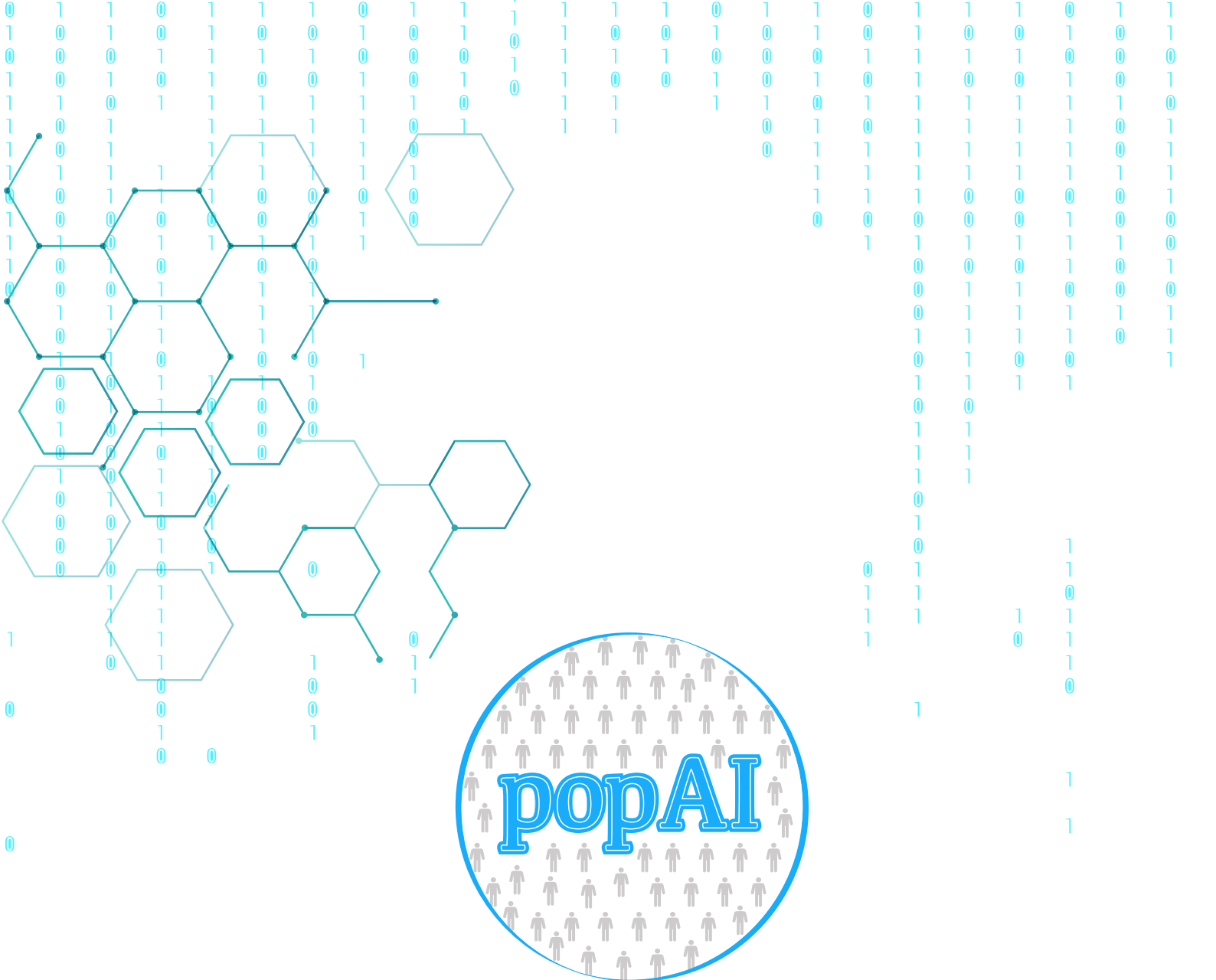
AI can provide significant support to numerous Law Enforcement operations. AI technologies and systems, like automated processing techniques to assist crime prevention are widely used by LEAs. AI in the security field promise to offer significant opportunities and benefits ranging from enhanced efficiency 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.

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.

Such a multidisciplinary approach should also be inclusive, creating this way a solid basis, not only for building but also maintaining trust in AI for LEAs. Such an approach necessitates the involvement of diverse stakeholders segments including civil society and NGOs, that must be actively engaged in AI discussions and participate in AI system design and development. Such an inclusive approach will ensure that the AI systems are just, ethical, and trustworthy for everyone, serving the public good and align with our European values and principles. Only by integrating civil society's voice can Law Enforcement balance between protecting the public from potential AI harms and promoting responsible, ethical, and secure AI-driven innovation.

---

<sup>18</sup> "EU Trilogues: The AI Act must protect people's rights - A civil society statement on fundamental rights in the EU Artificial Intelligence Act" (2023), [link](#).



# popAI project

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

## Acknowledgement

This work is part of the popAI deliverable D1.7 Policy Briefs - 2nd Year. The authors would like to express their appreciation to all popAI partners for their insightful comments.



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

© Edited by NCSR Demokritos, September 2023

 [pop-ai.eu](https://pop-ai.eu)

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

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