Recommendations towards a safe use of AI tools in the security domain

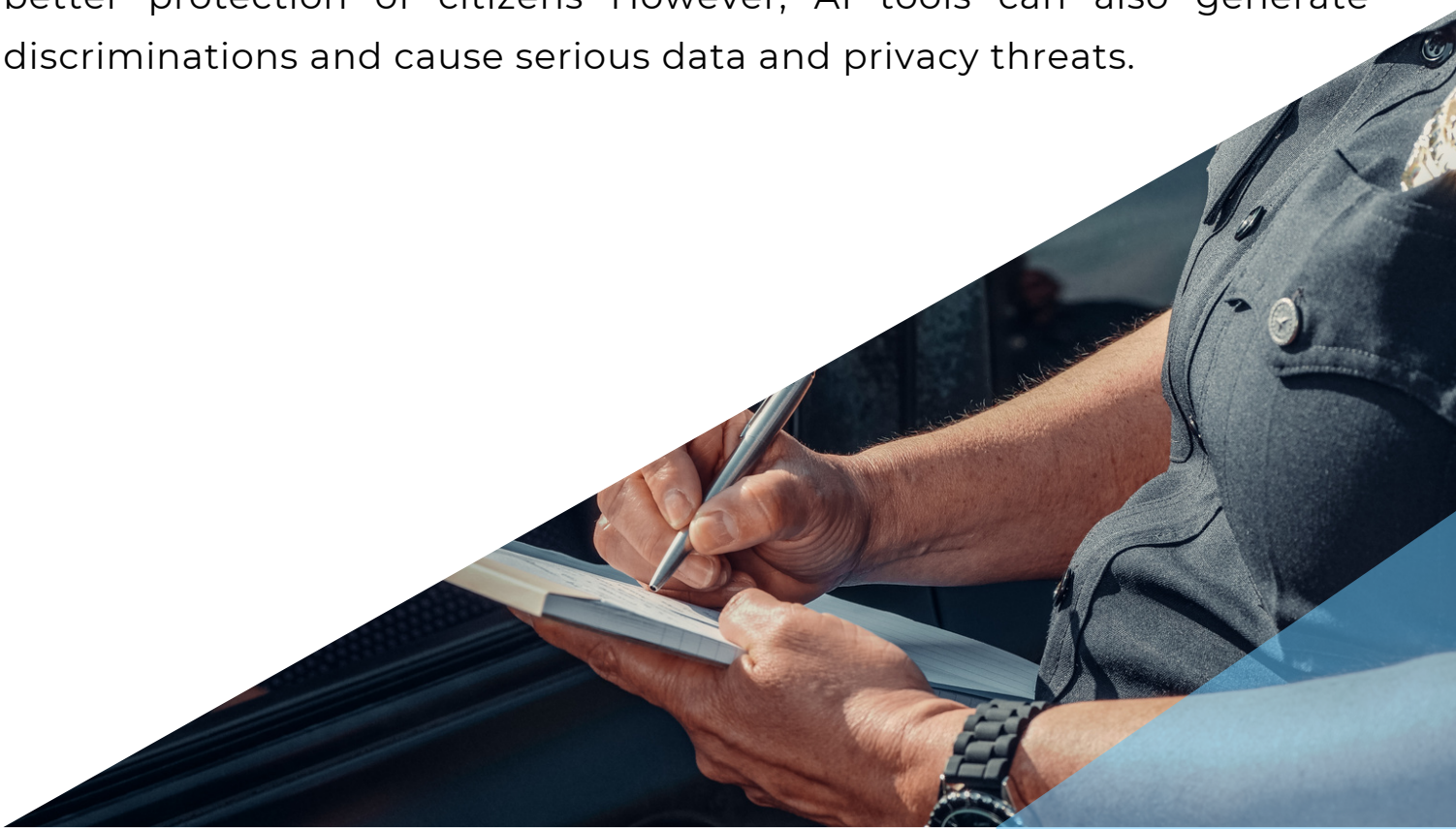
January 2024

What is popAI?

popAI is a 2-year Horizon project, gathering 13 organisations from 8 European Member States with the aim to foster trust in the use of AI (artificial intelligence) by law enforcement authorities (police).

What type of AI tools are used in the security domain?

Biometric identifiers, police hacking, predictive policing tools, video surveillance, drones, cyber operations... Policing activities rely more and more on AI tools to gain efficiency in their operation and ensure a better protection of citizens However, AI tools can also generate discriminations and cause serious data and privacy threats.



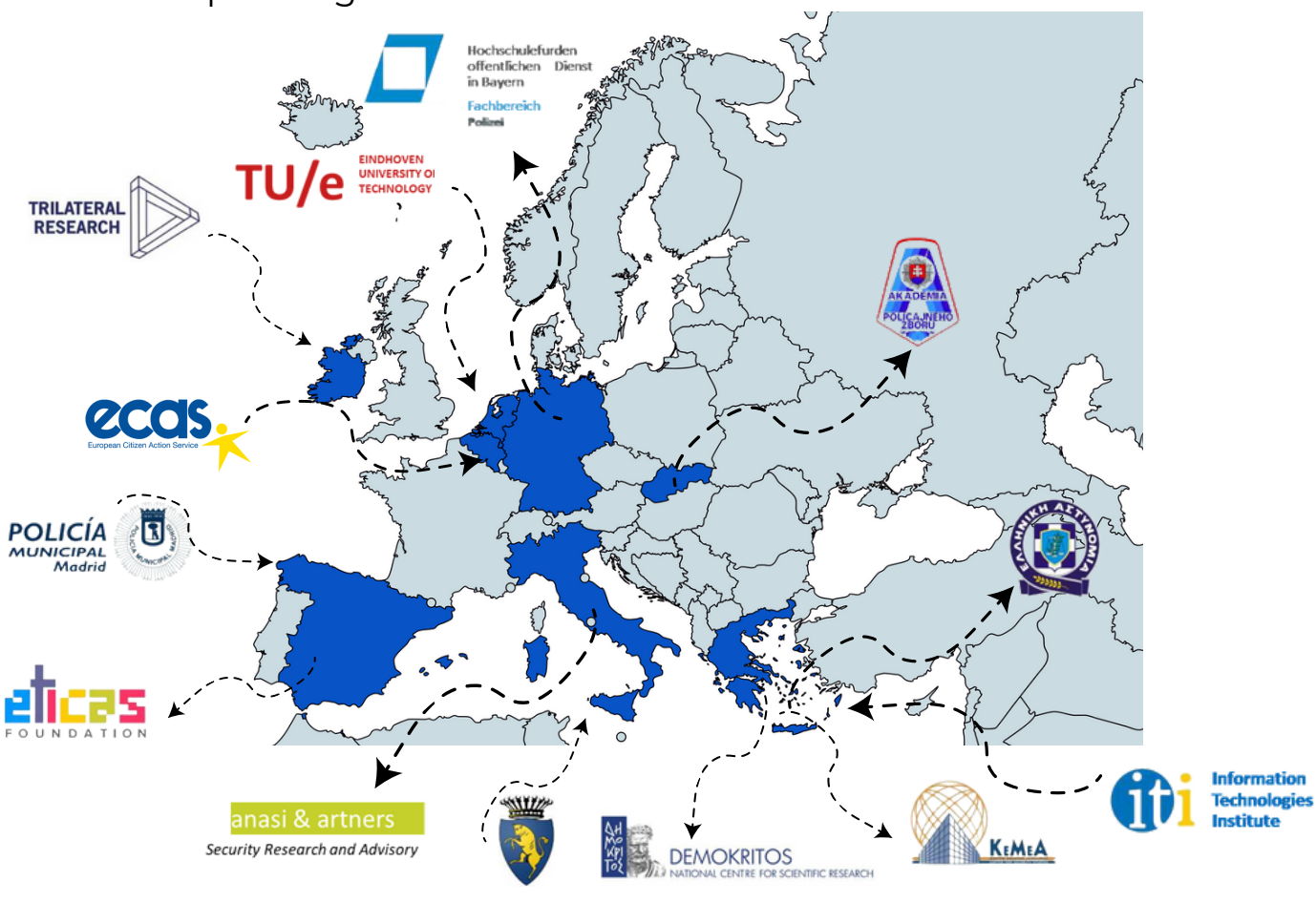
How was ECAS involved?

Our organisation, the European Citizen Action Service, has participated in the following activities of the popAI project:

-a social listening exercise, screening the internet to understand citizens' discourses around the use of AI in policing;

-a crowdsourcing activity where citizens' opinions were gathered as well as their solutions to develop AI tools in an efficient yet ethical manner;

- workshops in the form of Policy Labs where law enforcement authorities, NGOs, policy-makers and academics reflected together on the use of AI in the security domain. Each Policy lab session started with the presentation of a concrete case study on artificial intelligence tools used in policing.



What are the recommendations provided by the participants?

Throughout the activities described above, participants have elaborated recommendations targeting specifically law enforcement authorities, developers, policy makers and citizens themselves, as listed below per categories.

Recommendations for LEAs are aiming at supporting LEA staff towards an ethical and efficient use of new AI tools helping them performing operational tasks in the security domain.

The following solutions arise from popAI activities engaging various stakeholders:

- As it should not be assumed that end-users of AI tools in the security domain possess basic understanding of technology, it is crucial that LEA staff receive proper training on the use of AI, determining clear legal and ethical limitations;
- LEAs should be trained as well on data protection and privacy laws, on how to protect human rights and how to comply with the principles of non-discrimination;
- A psychological evaluation should be foreseen for all LEA officers who use AI systems;
- Training should occur before AI tools are ready to be in use, but also anytime they are updated. Support should be provided to identify potential biases and correct errors which might lead to discrimination;

- With regards to the trainers, their expertise, professionalism and ethical conduct should be given very careful consideration, under the “train the trainers” notion;
- Strict rules should limit access to personal data to a reduced number of trained LEAs;
- On the use of hacking as an investigate technique, it was recommended that clear guidelines are provided for police hacking operations, including the types of crimes that can be investigated and the circumstances under which hacking can be used.

Recommendations for policymakers attempt to provide solutions for future legal developments on the scope, purpose and limitations on the use of AI in the security domain

- The current data processing legal framework should be supplemented with clearer guidelines on storage, restriction and use of biometric data by LEAs, including duration of data retention and number of individuals with access to the data;
- Lawfulness, transparency and accountability (binding) protocols for LEAs should be put in place;
- Rules regarding data retention must be better harmonised at the EU level to ensure a robust and streamlined legal framework across Member States;
- AI systems that categorise individuals based on biometric data into groups based on ethnic origin, gender, sexual orientation or any other forms of discrimination must be fully prohibited;

- It is crucial to create independent oversight/intermediary bodies, who review the use of biometric identification and monitor the use of predictive policing algorithms to avoid discriminatory use of AI;
- Legislation should be updated and make it compulsory for LEAs to report on the data they use, and make sure that data reports are available.

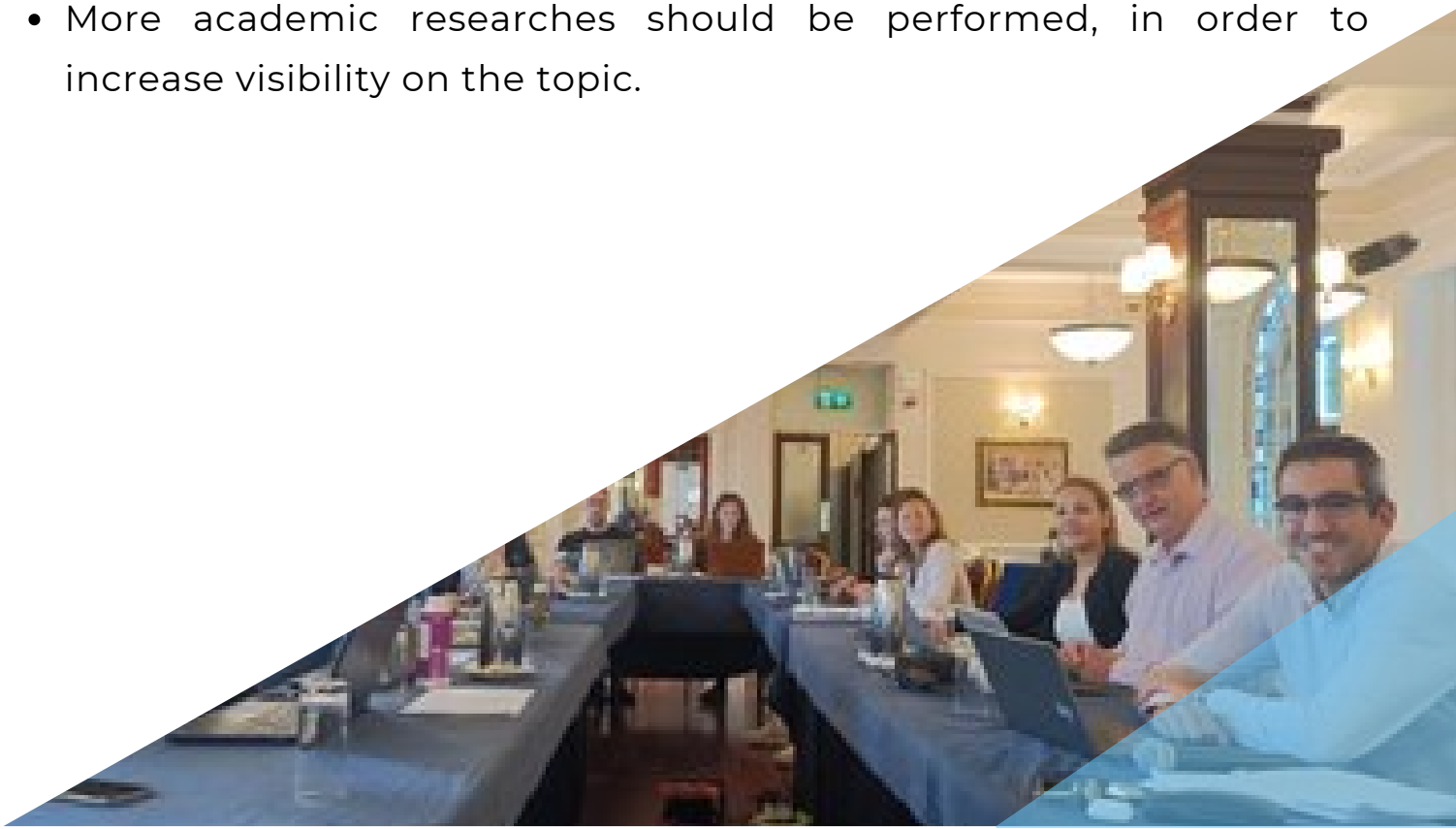
Recommendations for technology developers provide ideas for AI tools designers to ensure that ethical and non-discriminatory principles are respected throughout the development phase:

- Tools must support but not replace human beings : human intervention must always remain possible at any time;
- A principle of “non-discriminatory algorithms” should be implemented as from the early stage of development and constantly checked during the testing phase;
- Algorithms should be trained and constantly evaluated to ensure a total absence of discrimination and/or bias;
- Ethical tools should be elaborated as from the early design phase of AI tools developments;
- Algorithms should be trained on a diverse and representative dataset, which accurately reflects the population it is meant to serve, and this way avoids discriminatory results. This includes not only demographic data, but also data on crime patterns, socioeconomic factors, and other relevant variables.

Participants to the popAI activities gathered ideas and solutions to involve citizens in the development of AI tools and make sure that citizens are given the opportunity to share their thoughts on the decision-making process of a new legal framework on the use of AI in the security domain

Awareness-raising;

- It is crucial to bring citizens closer to the decision-making process on the use of AI in the security domain by fostering transparency and communication;
- Citizens should have access to definitions, requirements and guidelines on the use, scope and purpose of AI tools in policing activities;
- Informing citizens of the different steps of the design of AI tools in policing and involving them in the discussion would ensure more transparency;
- More academic researches should be performed, in order to increase visibility on the topic.



Recommendations for policymakers:

- Legislation should make it compulsory to inform citizens whenever their personal data is being used for policing activities (including reasons for collection and length of storage);
- New laws should introduce mechanisms allowing citizens to easily withdraw their consent and have personal data deleted.
- Whenever legislation around the use of AI by LEAs is amended/updated, citizens should be involved in the decision-making process;
- A central platform accepting citizens' reports of incidents associated with the potential violation of freedoms and rights should be created.

Contact Us

BeCentral Cantersteen 12, 1000, Brussels, Belgium

info@ecas.org

ecas.org

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