

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

D3.1: Map of AI in policing innovation ecosystem and stakeholders

Grant Agreement ID	101022001	Acronym	pop AI
Project Title	A European Positive Sum Approach towards AI tools in support of Law Enforcement and safeguarding privacy and fundamental rights		
Start Date	01/10/2021	Duration	24 Months
Project URL	www.pop-ai.eu		
Contractual due date	31/03/2022	Actual submission date	31/03/2022
Nature	R = Document, report	Dissemination Level	PU = Public
Authors	Pinelopi Troullinou, Eliza Jordan, Tim Jacquemard (TRI)		
Contributors	Kush Wadhwa, Vangjel Gjorgjiev, Zuzanna Warso (TRI)		
Reviewers	Francesca Trevisan (ERI), Dimitris Kyriazanos, Xenia Ziouvelou, Giorgos K. Thanos, Andreas Ikonopoulos (NCSR)		



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

Executive Summary

Law Enforcement Agencies (LEAs) have been increasingly relying upon innovative technologies and especially Artificial Intelligence (AI) to support their operations. Despite its potential, AI has become a heavy controversial topic resulting from cases of misuse and secrecy around the use of AI undermining the public trust in AI. To enhance trust in AI tools used by LEAs, it is fundamental to identify and understand who – and about what – is shaping the concerns and potential of AI in security as well as their interactions. This results in mapping an inclusive ecosystem around AI in civil security enabling to break the silos and build trustworthy, ethical, and socially acceptable AI tools in support of law enforcement. This deliverable contributes to this objective.

The report consists of four main sections. The first section (Section 2) introduces the main topics to be discussed in the deliverable, outlining the definitions and approaches on which the report is based. Despite AI being widely developed and discussed over the past decade, there is no consensus on its definition. The **broad and inclusive approach to AI** including any technology that is based on the digital processing of information to produce an outcome is presented. An **ecosystem approach** is adopted for this task to map the controversies in the use of AI by LEAs and identify the stakeholders involved. Therefore, pop AI's ecosystem approach aligns with the EU position on human-centric AI aimed at involving an array of stakeholders rather than solely innovators and technologists.

Section 3 **maps and discusses the controversies emerging from the use of AI technologies in the civil security domain** in the European Union. It provides an overview of AI technologies used and in development for the law enforcement purposes. Specific controversial cases are illustrated to explore the potentials and concerns emerged as well as the involved stakeholders. To this end, the mapping was structured around six broad security domains: **crime prevention; crime investigation; migration, asylum, and border control; administration of justice; cyber operations for law enforcement; and LEAs' training.**

Section 4 outlines the **institutional frameworks** that inform stakeholder interactions regarding the concerns discussed in the previous section such as gender and racial bias, violation of fundamental rights and lack of transparency and accountability in the design and employment of AI. Institutional frameworks are charted, including regulations, directives, reports and plans in the EU which are applicable to the use of AI by LEAs. Moreover, AI **national strategies** as well as **policy documents** and reports are presented to understand the discussions that governments and policy makers are having regarding AI in the security domain.

Section 5 draws together the **AI in civil security ecosystem** consisting of diverse categories of stakeholders; those involved in the research and development of AI technology and tools, as well as those who react to the use of AI, spread awareness and push for relevant policies.

The final section of this deliverable provides a conclusion, along with a summary of the content, linking the current findings to subsequent deliverables in pop AI.

Table of Contents

1	Introduction	5
1.1	Purpose and Scope	5
1.2	Approach for Work Package and Relation to other Work Packages and Deliverables	5
1.3	Structure of the Deliverable	6
2	Civil Security and AI ecosystem	7
2.1	Defining AI in civil security	7
2.2	Preliminary insights in controversies	8
2.3	Ecosystem approach	9
3	Civil Security and AI Controversy Mapping	10
3.1	Crime prevention	10
3.1.1.1	Predictive policing tools	11
3.1.1.2	Predictive policing controversial cases	11
3.2	Crime Investigation	14
3.2.1	Crime investigation AI driven tools	14
3.2.2	AI in Crime investigation controversial cases	14
3.3	Migration, asylum, and border control	16
3.3.1	Migration, asylum, and border management AI driven tools	16
3.3.2	Controversial cases of AI use in migration, asylum, and border management	17
3.4	Administration of Justice	18
3.4.1	AI tools in the context of administration of justice	18
3.4.2	Controversial cases on the use of AI in justice administration	18
3.5	Cyber operations for law enforcement	20
3.5.1	Cyberoperations for law enforcement controversies	20
3.6	Training	21
4	Institutional Frameworks chart	23
5	Stakeholders in the domain of AI in civil security	28
6	Conclusions	32
7	References	33
8	Annexes	41
8.1	Annex A. Reports and documents reviewing and critically engaging on the topic of AI in LEAs	41
8.2	Annex B. EU-funded projects relating to AI in the security domain	51
8.3	Annex C. Stakeholders by category	60

List of Figures

Figure 1 Stakeholders in the domain of AI in civil security.....28
 Figure 2 Stakeholder participation in EU-funded projects in the AI and security domain.....29
 Figure 3 Distribution of stakeholders involved in EU-funded projects on AI in the security domain .30

List of Tables

Table 1 Institutional frameworks chart23
 Table 2 National AI strategies in European countries25

List of Terms & Abbreviations

Abbreviation	Definition
AI	Artificial Intelligence
LEA	Law Enforcement Authority
MEP	Member of Parliament
AIA	Artificial Intelligence Act
GDPR	General Data Protection Regulation
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
BWC	Body-worn cameras
ABC	Automated border control
CSAM	Child Sexual Abuse Material

1 Introduction

pop AI is a 24-month Coordination and Support Action (CSA) project funded by Horizon 2020 undertaken by a consortium of 13 partners from 8 European countries. The core vision of the project is to boost trust in AI by increasing awareness and current social engagement, consolidating distinct spheres of knowledge, and delivering a unified European view and recommendations. To do so in an effective and inclusive manner, it is crucial to identify the key players that design and employ the innovative technologies and shape the discourses around it in the European context.

1.1 Purpose and Scope

This deliverable (D3.1) entitled *Map of AI in policing innovation ecosystem and stakeholders* explores the controversy ecosystem of AI development and use in the security domain. The aim is to identify the stakeholders involved ensuring the inclusion of diverse approaches in research as well as dissemination and communication activities of the project. The identification of the stakeholders emerges from a series of activities reported in the deliverable; the mapping of the ecosystem emerging from controversial cases of AI use and resulting campaigns; the charting of institutional frameworks addressing such controversies; and the tracking of EU funded research on AI for use in security domain.

The mapping conducted in the deliverable is not an exhaustive one but serves to identify who *is* and *should* be involved in the discussions, initiatives, and communications around AI in the security domain, supporting the creation of trustworthy, ethical, and socially acceptable AI tools in support of law enforcement.

The deliverable's outcomes align with and contribute to the overall objective of the project in creating a European AI hub for the Law Enforcement.

1.2 Approach for Work Package and Relation to other Work Packages and Deliverables

The deliverable is the outcome of Task 3.1 *Map the controversy ecosystems of AI tools in the security domain* setting the basis for the rest of the tasks in WP3 *Empirical Knowledge Collection and Management Framework*. More specifically the controversial cases and the stakeholders identified in this report will support the following tasks:

- Task 3.2 Understanding citizen discourses around AI and security controversies
- Task 3.3 Crowdsourcing stakeholder attitudes and pro-active solution ideations
- Task 3.4 Engaging LEAs and relevant experts through policy labs
- Task 3.5 Multi-Disciplinary Foresight scenarios
- Task 3.6 Engaging New Citizens through student photo and caption competition.

Furthermore, the chart of institutional frameworks including regulations, directives, reports, and plans in the EU which are applicable to the use of AI by LEAs will feed into the work undertaken in WP2, Task 2.2 *Legal framework and casework taxonomy: emerging trends and scenarios*. The insights of the controversies briefly discussed in this deliverable will be further examined in Task 2.3 *The controversies and risks that have shaped innovation and will shape AI in the next 20 years* while they will feed into WP4 The pandect of recommendations for the ethical use of AI for LEAs.

The list of stakeholders compiled in the context of this report will be utilised for the activities in WP5 *Dissemination, Communications and Sustainable Community Engagement*.

1.3 Structure of the Deliverable

The remainder of this deliverable is organised as follows:

Section 2 introduces the main topics discussed in the deliverable, outlining the definitions and approaches on which the report is based.

Section 3 maps and discusses controversial cases of AI in the security domain in the European Union allowing to identify involved stakeholders.

Section 4 outlines the institutional frameworks that inform stakeholder interactions regarding the use of AI in the security. Moreover, AI national strategies as well as policy documents and reports are charted.

Section 5 draws together the AI in civil security ecosystem consisting of stakeholders who design, develop, test, shape, the use and regulate AI technologies.

The final section of this deliverable provides a conclusion, along with a summary of the content, linking the current findings to subsequent deliverables in pop AI.

2 Civil Security and AI ecosystem

There is an increasing reliance on the use of innovative technologies and specifically Artificial Intelligence (AI) to respond to existing and emerging societal issues. AI promises to support the prediction, investigation, and combat of crime promoting citizen and border protection, safety, and security. In this context, European Union has been evolved into a dominant defence technological power (Csernatori, 2021). To this end, European Union invests over €270 million in artificial intelligence and security research over the next 2-5 years (European Commission, 2021). However, the developments and applications of AI driven technologies especially employed in security domain and specifically, by law enforcement agencies (LEAs) in the context of the pop AI project, raise great controversies.

This section operates as a preface to the report, introducing the main topics and providing the definitions and approaches. Firstly, it provides an overview of AI in the security domain explaining briefly what AI is and how the use of AI in this context has been used and envisioned. A preliminary discussion on the controversies around AI in the security domain follows. The section concludes by providing the approach to the ecosystem analysis so to justify the method adopted in the task T3.1 “Map the controversy ecosystems of AI tools in the security domain” the findings of which are presented here.

2.1 Defining AI in civil security

Artificial Intelligence is a term that is extensively used by the public and in public debates. However, there is a plethora of definitions attributing to AI diverse characteristics and emphasising on distinct applications, technologies, and methods. The European Commission’s Joint Research Centre (JRC) published a report (Samoili et al.,2020) in the context of AI Watch establishing an operational definition of AI that collected all definitions from 1995 to 2019 while providing a taxonomy and representative keywords. The starting definition for the report had been that from the HLEG’s below.

“Artificial intelligence (AI) refers to systems designed by humans that, given a complex goal, act in the physical or digital world by perceiving their environment, interpreting the collected structured or unstructured data, reasoning on the knowledge derived from this data and deciding the best action(s) to take (according to pre-defined parameters) to achieve the given goal. AI systems can also be designed to learn to adapt their behaviour by analysing how the environment is affected by their previous actions.

As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems).”

(EC HLEG, 2019, p. 6)

The report analysing the different definitions concluded that they all share specific common features as follows:

- Perception of the environment, including the consideration of the real-world complexity
- Information processing: collecting and interpreting inputs (in form of data)

D3.1: Map of AI in policing innovation ecosystem and stakeholders

- Decision making (including reasoning and learning): taking actions, performance of tasks (including adaptation, reaction to changes in the environment) with certain level of autonomy
- Achievement of specific goals: this is considered as the ultimate reason of AI systems

A clear and commonly agreed definition of AI is not a technicality. It proves to be crucial in related debates especially on a policy making level. This is the case with the forthcoming Artificial Intelligence regulation (AIA) that aims to set unified rules for the development, operationalisation, and application of AI in all member states of the European Union. This regulation will have a great impact on all levels of the Union from economic to legal, societal, and ethical. To this end, there is a heavy debate on the definition of AI so not to allow the exclusion of any systems from the protection of the regulation (Bryson, 2022).

For this reason, in this report we adopted a broad and inclusive approach to AI to map the ecosystem of AI tools in the security domain including **any technology that is based on the digital processing of information to produce an outcome**¹.

The Artificial Intelligence Act aims to address the potential risks emerging from AI systems' application categorising them in four levels of risk: unacceptable risk, high risk, limited risk, and minimal risk². The list of high-risk AI systems included in AIA Annex III, refers specifically to *law enforcement* area of application as well as *migration, asylum and border control management*, and *administration of justice* and democratic processes which will be discussed in this report (Section 3). Having defined our approach to AI, an introduction to related controversies will follow in the next section.

2.2 Preliminary insights in controversies

AI technologies have been used widely in the recent years from search engines to recommendations and virtual assistants. AI systems are increasingly developed for and employed by the security domain promising effective and efficient support to the law enforcement authorities (LEAs) which is the focus of the report. Yet, AI technologies raise great concerns especially when used by state authorities as democratic values are in stake in the fear of an Orwellian state, where the government is to control every aspect of people's lives. Publicity over the extensive use of personal data in the name of security such as Snowden's revelations but also China's Social Credit system have increased public awareness and sensitivity over privacy. Indeed, it has been argued that the media coverage of Snowden's revelation raised the salience over issues of internet privacy bringing privacy advocates at the forefront of policy-making process and therefore affecting the GDPR processes (Rossi, 2018).

To address the increasing concerns around the violation of human rights and privacy which are at the core of European values, AIA has categorised specific AI technology as prohibited. Specifically, in the security domain, it prohibits "real-time remote biometric identification systems used in publicly accessible spaces for the purpose of law enforcement with some limited exceptions (Art. 5, para. 1.)".

¹ A functionality taxonomy of AI will be documented in the public report D2.1 to be submitted in April 2022.

² <https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence>

D3.1: Map of AI in policing innovation ecosystem and stakeholders

Indeed, there are objections from civil organisations asking the extension of the specific article to include all actors, instead just law enforcement, as well as both ‘real-time’ and ‘post’ uses³.

This report, in Section 3, will map such controversies emerging from the use of AI technologies in the security domain and more specifically in law enforcement, migration, asylum, and border control management, as well as administration and justice listed as high-risk areas in the AIA. The mapping is not by any means exhaustive but serves to identify who *is* and *should* be involved in the discussions, initiatives, and communications around AI in the security domain, to ensure an inclusive understanding of concerns and potentials and to build trustworthy, ethical, and socially acceptable AI tools in support of law enforcement. The mapping of the controversies will support in understanding the relevant ecosystem of AI in civil security. The ecosystem approach followed is presented in the next section.

2.3 Ecosystem approach

As mentioned above, this report provides a mapping of the AI in security domain ecosystem with a specific focus on the law enforcement. To proceed, it is important to clarify the project’s approach on the ecosystem. Traditionally, an innovation ecosystem refers to the financial and industrial factors. More recently, it has been an observed re-focus on the societal facets of innovation (Jackson, 2011). Starting with the mapping of the controversies in the security domain, the report aims to shed light on the potentials of, as well as the concerns that emerge from the development and use of AI in the specific area of application. This will enable to identify the stakeholders involved in shaping, employing, promoting, and challenging the technology and how they interact.

Exploring the interactions on specific controversies, allows to map the stakeholders from an ethically driven and socially sustainable perspective identifying their position in the dynamic ecosystem and breaking the silos between the diverse nodes. This will be beneficial for the successful design, development and delivery of the project’s activities ensuring the inclusion of diverse backgrounds and experiences as well as of the more silent nodes of the ecosystem.

The pop AI’s approach on ecosystem is in line with the EU position on human-centric AI that requires the identification and inclusion of stakeholders beyond innovators and technologists. Furthermore, such an approach allows for effective engagement in co-creation processes that will result in the development of a structural ecosystem that will become the European AI hub for the Law Enforcement.

To this end, Section 3 will map and discuss the controversies in the security domain illustrating the AI technologies used, and in cases technologies under development that face challenges, and the stakeholders involved.

³ An EU Artificial Intelligence Act for Fundamental Rights A Civil Society Statement, 30/11/2021 <https://www.accessnow.org/cms/assets/uploads/2021/11/joint-statement-EU-AIA.pdf>

3 Civil Security and AI Controversy Mapping

In the light of the European regulation, AIA, to set the harmonized rules on Artificial Intelligence, there has been an ongoing deliberation on the ranking of AI tech based on potential risk and the areas of application. This includes discussions on what the implications of high-risk technologies might be, and how ethical concerns and legal issues emerged are to be addressed. As discussed in section 2.2, AIA prohibits the use of specific technologies by the LEAs, namely the real-time remote biometric identification systems in publicly accessible spaces. The draft provides some exceptions which is considered controversial. Indeed, privacy advocates and civil organisations are pushing for clear boundaries regarding prohibited technologies and areas of applications so not to allow diverse interpretations putting in risk fundamental human rights. Such initiatives come, amongst others, from European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) (Joint Opinion 5/2021), the collective statement of 38 civil society organizations⁴ and the European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters.

The security domain is a very crucial area of AI application raising serious risks to fundamental human rights. This section maps the controversial AI-powered technologies used, or developed to be used, by LEAs in European Union. The mapping around the controversial AI systems facilitates the identifications of both the related potentials and concerns, and the involved stakeholders. To allow a structured mapping, the civil security domain is structured around six broad contexts: crime prevention, crime investigation, cyber operations, migration, asylum, and border control, LEAs' training, and administration of justice.

3.1 Crime prevention

The use of technological innovation in policing has been a longstanding process involving diverse actors, heavily driven by the industry in the so-called “surveillance-industrial complex” (Hayes, 2012). Predictive policing is defined as “the use of analytical techniques by law enforcement to make statistical predictions about potential criminal activity” (Brayne et al., 2015, pp. 1). AI promises to support crime prevention based on the algorithmic identification of patterns, hence providing an opportunity to better predict, anticipate and prevent crime (Rolland, 2021).

There is a well-established body of literature examining the societal and ethical implications emerging from the development and application of AI use in policing and crime prevention (see for example surveillance studies, critical security studies). On the other hand, research on the perspective of practitioners identifies three main issues: “lack of financial and political support, issues in public-private partnerships, and public acceptability” while also highlighting a lack of clear guidelines and procedures (Laufs and Borrion, 2021).

In crime prevention domain, predictive analytics, and risk profiling, as well as CCTV surveillance systems and social network analysis (especially in the US, Gonzalez Fuster, 2020) are broadly used⁵.

⁴ Available at <https://www.accessnow.org/cms/assets/uploads/2021/11/joint-statement-EU-AIA.pdf>

⁵ A more detailed taxonomy of AI technologies will be provided in D2.1 “Functionality taxonomy and emerging practices and trends” to be submitted in April 2022.

3.1.1.1 Predictive policing tools

There is a distinction between two types of predictive policing: predictive mapping and predictive identification (Van Brakel, 2016, p. 120). Predictive mapping refers to the prediction of the time (when) and location (where) a crime might occur. In the case of predictive identification, the analysis refers to “predicting potential offenders, offenders’ identities, criminal behaviour, and potential victims of crime” (Van Brakel 2016, p. 120) as well as people who are likely to be victims of crimes (Brayne et al., 2015).

The AI algorithms used in predictive policing process large volumes of historical data to determine people and places at risk (Rolland, 2021). Newer applications can combine data from different sources such as abstracted data from mobile phones, demographic data, and hotspot methods (Van Brakel, 2016, p. 120). A range of AI tools have also been developed to predict the locations of high impact crime. The AI algorithms use police data, in conjunction at times with other data such as demographic, infrastructural and/or socio-economic data, to predict where crime is most likely to occur (Jansen, 2018).

The outputs of computer science-oriented techniques and methods is argued to help law enforcement authorities to efficiently allocate their resources to prevent criminal behaviour (Meijer and Wessels, 2019). In the US, predictive policing is being commonly used by various LEAs, yet in Europe no country has revealed their intention to implement a predictive policing programme on a national level (McCarthy, 2019). However, at a local level, several local police forces in Europe in the Netherlands, Denmark, Italy, Switzerland, Belgium, and the UK have been trialling and deploying predictive policing (Watney, 2019).

3.1.1.2 Predictive policing controversial cases

Predictive identification raises great controversy over the societal and ethical concerns emerging from the design of algorithms, the methods of data collection, the impacts of false, inaccurate outcomes, the overreliance, the lack of training, and policy guidelines among others. In cases, the legal basis on which such technologies and systems are used are also criticized. Poor choices on the design of the algorithm as well as data restrictions can lead to inaccurate risk assessments and predictions.

This is the case of [ProKid 12 – SI](#), a system assessing the risk of future criminality of children and young people implemented by Dutch police that raised serious concerns due to the inaccurate assessments (Fair Trials, 2021). ProKid 12 – SI has also been heavily criticized for abuse of a series of rights such as “the rights of the child, the right to non-discrimination based on a number of protected characteristics, the presumption of innocence and data protection rights”⁶. Rights of the child are guaranteed in the UN Convention on the Rights of the Child⁷ whereas the remaining rights in the European Convention on Human Rights, and the Universal Declaration of Human Rights. It is important to note that EU member states are party to all of them.

⁶ EDRI’s briefing on Use cases: Impermissible AI and fundamental rights breaches examining ProKid 12 – SI amongst other cases. <https://edri.org/wp-content/uploads/2021/06/Case-studies-Impermissible-AI-biometrics-September-2020.pdf>

⁷ <https://www.unicef.org/child-rights-convention>

D3.1: Map of AI in policing innovation ecosystem and stakeholders

Similarly, [Amsterdam police's Top 600 criminals list](#), whose risk modelling and profiling system have been criticized for discrimination based on ethnic and socio-economic backgrounds. NPO, the Dutch public broadcaster, reported in May 2020 that over a third of the Top 600 boys are of Moroccan descent (Fair Trials, 2021).

In the first pop AI webinar, where the preliminary findings of this report were presented (March 2022, virtual), one of the stakeholders (researcher) made a very interesting point on the approach to AI tools in crime prediction:

Predictive tools are marketed as predicting future actions, when they are really a risk assessment based on historical data. (Participant 1)

The historical data used by the algorithm to provide predictive models might also be biased based on past discriminatory policy decisions. Racialised policing in the past can lead in unbalanced and inaccurate datasets regarding ethnic minorities which then can be used to model a predictive tool a priori biased towards specific racial characteristics. This biased algorithm then can have discriminatory impact not only to a person but also at a community level affecting location data too, especially when minority groups cluster in a similar location. Some individuals or neighbourhoods could be overpoliced, amplifying stereotypes, discrimination, and prejudice (Heaven, 2021).

Other controversial cases of this type of predictive policing systems include, but are not limited to, [Gladaxe system](#) (Denmark), [KeyCrime](#) (Italy), [Precobs](#), [Dyrias](#) and [ROS](#) (Switzerland), [Gangs Violence Matrix](#) (UK), [Crime Anticipation System](#) (Netherlands), [Video surveillance and the prediction of 'abnormal behaviour'](#) (Italy), [Offender Group Reconviction Scale](#) (UK), [iPolice](#) (Belgium), [National Data Analytics Solution](#) (UK), [Origins Software](#) (UK)⁸

A report published by Amnesty International in 2020 examined the use of predictive policing in the Netherlands, being one of the countries at the forefront of predictive policing in practice. The NGO identifies fundamental human rights violations during the pilot phases of predictive policing projects calling on law enforcement to stop all relevant projects until legislative safeguards are enforced (Amnesty International, 2020).

The Gangs Violence Matrix (UK) is presented below in more details to illustrate the technology used by LEAs to support the fight of a civil security issue, the concerns regarding the technology and the response by the LEA. This is to bring a vivid example that can guide the discussions on what is missing to develop and deliver a trustworthy and trusted AI application in LEAs' domain.

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

Since 2012, the Metropolitan Police (UK) has been using the Gangs Violence Matrix (GVM) to identify and risk-assess individuals across London involved in gang violence and identify those at risk of victimisation. The GVM creates a scoring system based on evidence of individuals committing violence and weapon offences, police intelligence about weapon access, or their involvement (or risk of involvement) in gang violence.

The scores obtained rank individuals, both adults and minors, as Red, Amber or Green reflecting the level of risk (for victims) or harm (for offenders) they present. The Metropolitan Police allows

⁸ See EDRI's briefing

more effective prioritisation and thus allocation of resources. (Metropolitan Police, 2022; Gonzalez Fuster, 2020).

Mayor's Office for Policing and Crime review highlighted that 38% of those on the list posed little or no risk, resulting in the removal of over a thousand young black men from the GVM (MOPAC, 2018; BBC News, 2021). An investigation by the Information Commissioner's Office found GVM data to be inaccurate while the system to breach numerous and serious data protection laws (ICO, 2018; Jones, 2018). Amnesty International as well as UK-based NGO, Liberty highlighted the lack of transparency in the design of the system emphasising the discrimination against people of colour, particularly Black men and boys. Furthermore, risks on data sharing with other services (schools, job centres, immigration enforcement, etc) have been stressed (Amnesty International, 2018; Liberty, 2022).

Despite these claims, the Metropolitan Police asserts that the use and operation of GVM is compliant with the Human Rights Act and is monitored to assure its compliance (Metropolitan Police, 2022).

Gangs Violence Matrix has been employed by the Metropolitan Police to fight gang violence. It is a risk-assessment tool that ranks the potential offenders as well as potential victims based on historical data and police intelligence for which there are allegations to consider social media activity⁹. Its potential is the effective prioritization and subsequently the allocation of resources based on the scoring. However, the lists produced proved inaccurate, collecting information on individuals never involved in violent crime, and biased ranking disproportionately black men. At the same time, even being victims of crime have been placed in the matrix being associated with the likelihood to be involved in serious crime. Civil society organisations such as EDRI, Amnesty International, and Liberty as well as national authorities, ICO, and local authorities, Mayor's Office for Policing and Crime, have raised serious concerns providing analyses of the issues above. The response by the Metropolitan Police though has been general providing no evidence that the concerns have been considered. The micro-ecosystem is clearly illustrated here as well as the lack of an effective regulation framework and clear processes for transparent design and implementation of AI use in civil security domain. The lack of transparent results and lack of accountability thus suggest that police cannot be held solely accountable for potential harmful actions (Rolland, 2021). This raises the question of who is to be held accountable for inaccurate predictions that can result in discriminatory actions on behalf of the police.

In March 2022, Fair Trials, European Digital Rights and 41 other civil society organisations joined forces and called on the EU to prohibit predictive and profiling AI systems in law enforcement and criminal justice. The organisations stress that fundamental harms are being caused by predictive, profiling and risk assessment AI systems in the EU including discrimination, surveillance, and over-policing; infringement of the right to liberty, the right to fair trial and the presumption of innocence; and lack of transparency, accountability and right to an effective remedy (Fair Trials, 2022).

⁹ For more information see the report by the Amnesty International <https://www.amnesty.org.uk/london-trident-gangs-matrix-metropolitan-police>

3.2 Crime Investigation

Technological innovations have been significantly supported the investigation of a crime from evidence-gathering tasks to analysis of information and clues, validation or disproval of theories and allegations, and finally to arrest a suspect. Here, we focus on AI technology that is related to the investigation of potential suspects.

3.2.1 Crime investigation AI driven tools

Similarly to crime prevention, Surveillance-Orientated Security Technologies (SOSTs) meaning, “technologies which collect information about the general population to monitor the activities of potential suspects and to prevent criminal acts from occurring” (Degli Esposti and Santiago-Gomez, 2015, p. 437) are broadly used. In the case of crime investigation, image, video, text, and sound from technological means such as CCTV cameras, drones, and body-worn cameras as well as personal digital devices such as mobile phones and computers can be used. Interactions with the suspect’s network can be analysed. Not only historical data but also real-time data coming from relevant identification systems such as automated license plate readers, automatic facial recognition systems, and voice identification systems can also be collected and analysed.

This intrusive surveillance raises great concerns as in the name of security abuse of fundamental rights are at stake and there is a well-grounded body of literature warning for the creation of a surveillance society exploring and theorizing the use of AI technologies in the name of security (see for example Beydoun 2021, Newell 2020, Norris and Armstrong 2020, Van Brakel and De Hert 2011, Wood et al., 2006).

3.2.2 AI in Crime investigation controversial cases

There has been a long history of technological developments being used in crime investigation as is the case of the use of photography for the purposes of crime control almost since the existence of the camera itself (Norris and Armstrong 2020, p. 77). Similarly, “since the late 1980s, over 1 million closed circuit television (CCTV) cameras” had been installed in the UK (Goold 2004, p.1-2). Subsequently, there have since been great debates over the securitisation of the society by the extensive use of technological developments and the emerging concerns mainly regarding abuse of privacy and discrimination (see for example, Norris and Armstrong 2020; 2017, Norris, McCahill and Wood 2004). The new capabilities CCTV cameras are equipped with, such as facial recognition, intensify relevant concerns especially regarding the use of ‘smart cameras’ in public spaces by the law enforcement agencies. Facial recognition is a system that generates high risks as will be illustrated in the case of Clearview AI, an American facial recognition company, presented below. The local police in Sweden was fined after unlawful use of the already legally controversial software system while it seems that other LEAs in the EU make use of it too.

Case study: Clearview AI in Sweden

Clearview was exposed in the media for devising a facial recognition app that was considered to pose great risk on privacy. Clearview AI is a facial recognition platform that contains more than 3 billion images from the public internet - Facebook, Twitter, Instagram, LinkedIn. With this application, one can take a picture of a person, upload it to the platform, and see all the public photos of that person.

In Sweden, the Authority for Privacy Protection concluded that the police had used Clearview AI on numerous occasions and in cases without prior authorisation. Using Clearview AI, the Swedish police unlawfully processed biometric data for facial recognition and failed to conduct a data protection impact assessment. Having infringed the Criminal Data Act, the police were fined. The Authority for Privacy Protection has also ordered the police to conduct further training for employees to avoid future breaches of data protection rules and regulations (European Data Protection Board, 2021).

In February 2022, the Italian SA fined the company, Clearview AI, €20 million having found several infringements of fundamental principles of GDPR. Among others, the company had unlawfully processed data, such as biometric and geolocation information¹⁰.

The case of Clearview AI has illustrated the risks emerging from such technologies but even more so the need for harmonised standards and binding regulations with regards to the use (or ban) of such invasive and harmful AI technologies especially for vulnerable categories of people. Furthermore, it is alarming that LEAs made use of such a controversial system with no explicit and formal permission. It is also evident from the case study that it is not clear to LEAs how the results are generated by AI technologies and prior training is not always provided.

EU-funded projects developing such technologies have raised respective 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 2009-2014¹¹. The project developed technological solutions and tools to automatically detect threat. 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, 2011).

Cameras have not only integrated further capabilities, but they have also been designed to be mobile. Small cameras, called **body-worn cameras** (BWC), have been increasingly implemented by law enforcement officers to record interactions between them and community members; national introduction of BWC in 2021 by all police departments in France (Thompson, 2020), the Netherlands (Politie, 2020) and Finland (Poliisi, 2021). The implementation of this technology came as a response to the public’s mistrust to police officers resulting from “consistent media portrayals of tense confrontations between police officers and citizen” (Wright and Headley 2020, p.1). However, the use of BWC has raised serious concerns mainly due to lack of transparency. For instance, transport company in Stockholm was fined following assessment by the Swedish Authority for Privacy Protection finding privacy shortcomings (European Data Protection Board, 2021). Similarly, in Ireland, the Garda Siochana Digital Recording Bill was released in 2021 stating that Gardai will wear a highly

¹⁰ EDPB, Facial recognition: Italian SA fines Clearview AI EUR 20 million, 10 February 2022
https://edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en

¹¹ <https://cordis.europa.eu/project/id/218086/reporting>

visible camera and before any recording they need to signal and justify their decision. Storage will not allow any editing or alteration to the footage to preserve its integrity (Gallagher, 2021).

In October 2021, Members of European Parliament (MEP) favoured banning AI mass surveillance (European Parliament 2021). MEPs point to the risk of algorithmic bias and discrimination in AI applications, making a disproportionate number of mistakes identifying ethnic minority groups, LGBTI people, elderly, and women. Therefore, to respect privacy and human dignity, MEPs ask for a permanent ban on automated recognition of individuals in public spaces. EU MEPs emphasise that human supervision and strong legal powers are needed to prevent discrimination by AI in law enforcement and border control. Moreover, MEPs ask for AI algorithms to be transparent, traceable, and sufficiently documented. The EU MEPs have also called for the ban on the use of private facial recognition databases, behavioural policing, and citizen rating (European Parliament, 2021; Calvi, 2021).

3.3 Migration, asylum, and border control

Currently, there is an increasing movement of people in and out of Europe, with these figures expected to continue to rise in coming years (CSS, 2019). Over 1.1 billion and 410 million passengers travelled by air (Eurostat, 2018a) and maritime ship (Eurostat, 2018b) respectively in the EU in 2018. Additionally, the ongoing migrant crisis has placed further challenges on external border control and management into the EU due to the high number of migrants and refugees reaching the EU's land, air, and sea borders (Frontex, 2021). Furthermore, it is expected that the EU external border control will be faced with future challenges related to greater levels of displacement due to climate change and trends related to human trafficking and cross-border crime (Frontex, 2021).

Considering the current and potential challenges at borders, EU countries are resorting to AI technologies with the aim of enhancing the effectiveness of border control and mitigating security risks related to cross-border terrorism and serious crime (Dumbrava, 2021). AI technologies have been implemented in cross-border law enforcement operations for border control and migration management to perform tasks such as identity checks, border security and control, analysis of data from visa and asylum applicants (Chui et al., 2018).

AI at EU borders is aimed to increase LEAs' *"capacity to detect fraud and abuses, better and timely access to relevant information for taking decisions, and enhanced protection of vulnerable people"* (Dumbrava, 2021, pp. II). However, the use of technologies in a domain that has also to protect vulnerable groups of population raise great concerns and controversies.

3.3.1 Migration, asylum, and border management AI driven tools

The European Parliamentary Research Service (2021) analysis classified AI applications in the context of EU border security and management in four main types: biometric identification (automated fingerprint and facial recognition); emotion detection; algorithmic risk-assessment; and AI tools for migration monitoring, analysis, and forecasting (Dumbrava, 2021). Border control management have been implementing innovation technologies in the name of security especially following terrorist attacks (Gregoriou and Troullinou, 2012). Automated border control (ABC) systems, or e-Gates, at airports are a common example of how facial recognition technology is used for border management (del Rio et al., 2016; CSS, 2019). As of 2019, ABC e-Gates were in operation at over 50 airports in 16 EU Member States and in Norway and Switzerland (IATA, 2019).

3.3.2 Controversial cases of AI use in migration, asylum, and border management

Academics and experts have suggested that the use of ABC systems at border crossing points has led to the multiplication of mistrust at European borders, increasing mistrust in the ‘manual’ work and competencies of border guards viewing them as unreliable or error-prone (Noori, 2021). Data protection advocates have also expressed their mistrust in ABC e-Gates highlighting that it often is not clear which biometric and biographical data is stored and processed in this technology (Clavell, 2017).

CCTV cameras can also be equipped with facial recognition technology and used in the context of border management. Live stream videos from CCTV cameras capture facial images and these are then compared against facial images from persons included in a watch list (Dumbrava, 2021).

European airports aim to enable the entire journey from check-in to boarding with people solely using their face as a form of identification (International Airport Review, 2021). Although some trials have stated they are collecting and processing information in accordance with GDPR regulations (International Airport Review, 2021), other trials have failed to report on storage processes (Murph, 2019).

Case study: Brussels Airport

In 2017, the Brussels Airport began piloting a new facial recognition system with four cameras installed in the airport. With the camera footage, the software created biometric templates of individuals which were then compared to a “blacklist” of individuals who are suspected of a crime (Peeters, 2020). Testing of the system was stopped in March 2017 due to a very high error rate, resulting in a large number of false positives (Automating Society, 2020).

The Belgian Supervisory Body for Police Information were not informed of the installation of the facial recognition cameras and consequently no Data Protection Impact Assessment was conducted as required. Two years after the termination of testing, in 2019, the Supervisory Body found that the system was still partially active, actively collecting and storing biometric data from passengers at Brussels Airport (although not comparing the biometric data against a “black list”) (Automating Society, 2020). The Supervisory Body discovered that a database was created with the data of the faces of hundreds of thousands of travellers temporarily stored failing the current Belgian law (Vanrenterghem & Heymans, 2019).

Although the use of real-time intelligent systems is permitted under the Belgian Police Act, the Supervisory Body argues on the purpose of data processing during the testing phase. Moreover, the Act does not specify the circumstances and conditions for the use of “intelligent systems” (Peeters, 2020). The Supervisory Body enforced a temporary ban on the pilot project as Belgian federal police did not comply with data protection and police information law (COC, 2020).

The case study above regarding the misuse of facial recognition technology in Brussels Airport notes concerns about the accuracy and data protection of the facial recognition system used. Currently, there is no legal regulation that permits Belgian law enforcement agencies to employ facial recognition technology (Galindo, 2019).

D3.1: Map of AI in policing innovation ecosystem and stakeholders

Moreover, the ReclaimYourFace campaign, a movement led by European civil society organisations, emphasised their worries about using facial recognition technologies in this domain. Campaigners argue that the algorithms are strongly unbalanced and discriminatory, placing people's fundamental rights in question (EDRi, 2021).

Civil society organizations and privacy advocates raise concerns over implementation with no prior official permission. In this line, even though, currently, emotion detection systems are not deployed at EU borders, EU-funded projects and initiatives developing such technologies raise great concerns.

Such is the case of the three-year EU funded H2020 project, iBorderCtrl, developing detection of deception based on facial recognition technology being trialled at the borders Hungary, Greece, and Latvia (Ahmed & Tondo, 2021) raising strong opposition; joint activists' initiatives (iBorderCtrl.no, 2022), legal actions (lawsuit by the MEP Patrick Breyer, Greens/EFA) and EP's concerns over financing such research projects (EP resolution on 6th October 2021). In December 2021, the EU Court of Justice ruled the EU research agency to publish the ethical and legal evaluation of technologies for "automated deception detection" or automated "risk assessment" (Hersey, 2021).

The types of AI application listed above raise great risks with specific technologies such as emotion detection being very controversial and recommended to be prohibited under the AIA (EDPB- EDPS, 2021).

3.4 Administration of Justice

An area of application that is gaining ground is the administration of justice. Even though administration of justice is related more to the court system than police activities, it relates to risks of overreliance to algorithms that might lack of transparency built as "black-box" and might result in biased outcomes. In the U.S., courts across states use Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) raising great debates as a recidivism risk assessment tool with racial bias. This is a decision support system to assist courts with predicting recidivism risk. In contrast to the US, AI use by LEAs in Europe is still relatively in its developmental stage (Oswald et al, 2018). AI based systems in the administration of justice domain are used in support of the judicial authority "in researching and interpreting facts and the law and in applying the law to a concrete set of facts" and are explicitly referred as high-risk in the Artificial Intelligence Act.

3.4.1 AI tools in the context of administration of justice

AI and automated decision-making (ADM) systems are already used by European LEAs and criminal justice authorities supporting the sentencing and probation decisions assessing people's "alleged 'risk' of criminality or re-offending in the future" (Fair Trials, 2021, p.4). Lawyers and courts are using AI powered law-tech, which is software for legal services, to assist them with different types of tasks: locating information; supporting legal processes; and assisting them with decision making (Oireachtas Library & Research Services, 2021). The interpretation of the law, as well as the decision-making process are based on algorithmic analysis that can generate great concerns as already seen in the above sections based on the technical limitations and design choices, the processes of application, and the training regarding the use of these technologies.

3.4.2 Controversial cases on the use of AI in justice administration

The use of AI technologies in support of the justice administration has been limited in Europe with UK leading the way. One of the first uses of AI by LEAs to administer justice in the UK was Durham

D3.1: Map of AI in policing innovation ecosystem and stakeholders

Constabulary's Harm Assessment Risk Tool (HART) in 2017 presented below to show the controversies raised and the stakeholders involved to shape the future of AI application in a trusted framework.

Case study: Harm Assessment Risk Tool (HART)

Harm Assessment Risk Tool (HART) is an algorithmic tool aimed to improve data intelligence to support decision-making process on whether a prosecuted person should be detained, released, or should be allowed to follow an alternative programme for dealing with an offence outside of court prosecution (Oswald et al, 2018). HART's recommendations then are significant both for suspect and the police, as well as for public safety (Cambridge University, 2018). The tool has been developed by statistical experts based at the University of Cambridge in collaboration with Durham Constabulary (Oswald et al, 2018). The tool assesses the risk of reoffending within the following two years and indicates if the risk for an individual is low (no offence within the next 2 years), medium (non-serious offence within the next 2 years) or high (serious offence within the next 2 years) (Burges, 2018; FOI request). HART contains the histories of 104,000 people who have been in custody in Durham over five years and follows up two years after the custody decision (University of Cambridge, 2018).

The HART model does not make automated decisions about detention but ultimately custody officers are responsible. Although not completely transparent, under conditions the outcome of the algorithm can be deconstructed making it not a complete black box (Babuta, Oswald & Rinik, 2018). The database may be expanded with information from other sources than then Durham police force, such as the national database of the UK police (Burges 2018). Currently, it appears to use only data from the Durham Constabulary according to the involved researcher in a Council of Europe committee hearing (Council of Europe, 2020). As a result, their predictions cannot fully be explained. Across all indicators, the difference in accuracy between the Hart model and custody officers proved minor (HART was accurate 53.8% while custody officers' accuracy was 52.2%) (Durham Police, 2022).

HART gained significant media attention regarding the potential of HART to reflect existing biases and discriminate against people with disadvantaged socio-economic backgrounds (see for example, BBC 2018, Burges 2018, Nilson 2019, Statt 2017). Civil liberty organisations stressed the racial and socio-economic bias issues emerging from the use of postcode dataset from data broker Experian which included reference to racial categories such as Asian heritage (Big Brother Watch, 2018; Liberty, 2019; Fair Trails, 2021). Acknowledging these issues, HART removed postcode as a predictor value due to the risk of amplifying existing inequality (Oswald et al, 2018). Another perceived potential for bias is the system skewing towards false positives considering a low-risk score for a high offender worse than a high-risk score for a low offender (Lyll, 2021). Additionally, lack of transparency has also been raised (Fair Trails, 2021). Finally, efficacy is a concern of which the police say they will monitor and subsequently abandon the technology if it does not prove helpful (Nilson, 2019).

The case of HART proves once more the importance of decision making in the design of the algorithm as well as the limitations of predictive analytics based on historical data that can lead in new or

D3.1: Map of AI in policing innovation ecosystem and stakeholders

amplify existing societal biases. Even though the algorithm has been readjusted excluding indicators that could result in biased outcomes, the reasons behind these choices are not clear. There is no official statement that the modification on the algorithms followed the privacy advocates' such as Big Brother Watch, responding to ethical, societal, and legal requirements. Even though Oswald et al., (2018) refers to bias as a reason for scrapping postcode, the head of criminal justice at Durham Constabulary argued in media coverage by Financial Times, on a decision based on financial factors (Nilson, 2019).

In Catalonia, the RisCanvi algorithm¹² support the decision on whether inmates are paroled based on a re-offense risk assessment. Even though the final decision is made by professionals of the justice system, yet in the great majority of the cases the evaluation of the professionals align with the algorithm's one which is criticised for lack of transparency.

3.5 Cyber operations for law enforcement

LEAs are called to fight crime not only in a physical world, but also on a digital environment where communications between the criminals might take place, as well as crimes can be conducted. The use of computer science methods such as social network analysis are increasingly used to support LEAs to detect and predict criminal activities. However, the use of such technologies is still limited as it is a high-risk area of application that also demands expertise and appropriate training.

3.5.1 Cyberoperations for law enforcement controversies

One area where AI driven technologies are used is the detection and takedown of online Child Sexual Abuse Material (CSAM) (INHOME, 2020). Private companies, such as Google, use AI in addition to people to detect CSAM in their networks. Law enforcement agencies receive a rapidly growing number of reports on online child sexual abuse material. Yet, there are strong oppositions due to privacy and surveillance concerns in relation to access to personal data or private databases (NATO, 2022).

Case study: CSAM detection by The AviaTor Project

The AviaTor project, which stands for Augmented Visual Intelligence and Targeted Online Research is funded by the EU Internal Security Fund. AviaTor is developing automation and intelligence to support the processing, assessment, and prioritisation of CSAM by LEAs. It is also developing a service of automatic crawling of online sources for complementing information for investigations in compliance with the national legal requirements¹³. The National Police in Netherlands has been using the first version of AviaTor tool since December 2021 and the project is currently in its second iteration (INHOPE, 2021).

There are challenges associated with AI to identify CSAM, which include (1) the quality of CSAM data; and (2) the lack of standardised classifications for content (INHOPE, 2020) while there are also legal obstacles in collecting CSAM reports from different countries. Furthermore, NGOs have

¹² <https://algorithmwatch.org/en/riscanvi/>

¹³ <https://www.inhope.org/EN/aviator?locale=en>

accused abuse of the system and targeting artists, such as cartoonists, and marginalised communities by sharing innocent and legal reports as CSAM (Bukovska, Finan & Malcolm, 2020).

The AviaTor case showed that using AI systems in cyberoperations might prove effective in combating crime but at the same time raise both technical and legal concerns where they can have great impact to innocent citizens that are in no way involved in criminal activities. Therefore, AI driven cyberoperations are highly controversial especially when used by private entities. For example, Apple rolled back on its AI CSAM detection technology in 2021 after backlash from privacy experts, NGOs, and academics (Whittaker, 2021).

Since unauthorised access to personal information is a great threat, companies protect their consumer technology and data with tools such as encryption. This means that LEAs have difficulties accessing large amounts of information necessary for computational analysis (Ilbiz & Kaunert, 2021)¹⁴. Specifically in cyberoperations to combat sociotechnical threats such as disinformation, experts assert that filtering disinformation and misinformation through AI may conflict with values such as freedom of speech, media pluralism, privacy, surveillance, transparency etc, especially when an AI decides what counts as mis/disinformation or legal/illegal (STOA, 2019).

3.6 Training

In recent years, conventional LEA training has started to be complemented with technology-enabled learning such as the relatively new virtual reality (VR), with numerous technology companies developing and selling VR simulators to law enforcement agencies for training purposes (Houser, 2021). It is an interesting area of application to include in this mapping due to growing use of the technology and the potential risks to privacy and biases in training.

The use of VR for police training may pose multiple benefits such the creation of a limitless array of scenarios, in addition to the possibility of creating scenarios difficult to create in real-life due to financial constraints or ethical reasons (involving children, dogs and bombs which cannot be re-created in real-life) (VR & Police Network, 2022).

Police forces in the UK (Dormehl, 2018; Derbyshire Constabulary, 2020) have trialled using VR to training officers on tasks such as using tasers. Since 2013, a police academy in Poland has trained officers using a simulator recreating police activities in crisis situations helping shape police officers' skills and abilities (Kamiński et al., 2020). EU-funded project SHOTPROS (Grant No. 833672) is currently being conducted aiming to develop a virtual-reality enhanced training for European police to improve decision making and action capabilities under stress and high-risk situations (SHOTPROS, 2021).

The PLUS (Police Training Using Simulations) project conducted by Bournemouth University in collaboration with the Dorset Police force aims to create a gamified training application for police training aiming to prepare police officers for real-life situations (Bournemouth University, 2022). The H2020 EU-funded project LAW-GAME (Grant No. 101021714) brings together experts and LEAs to

¹⁴ See also the recent campaign against encrypted private messaging apps <https://www.bbc.com/news/technology-60072191>

D3.1: Map of AI in policing innovation ecosystem and stakeholders

design and develop a training system based on serious games, virtual reality, and artificial intelligence (LAW-GAME, 2021; SIMAVI, 2021).

Analysis of training using AI assisted technologies highlights numerous threats from the use of VR in police training: conditioning towards weapon use; adverse effects of habituation; health risks (including cybersickness); illegal outside access and misuse of private data (Giessing 2021).

Section 3 provided numerous controversial cases of AI based technologies in civil security domain and specifically in the areas of crime prevention; crime investigation; migration, asylum, and border control; administration of justice; cyber operations for law enforcement; and LEAs' training. The potential risks of the cases were discussed, especially the violation of fundamental rights such as discrimination based on potential gender and racial bias of the algorithms, as well as the lack of transparency and accountability, and appropriate training. Through this discussion the involved stakeholders were identified illustrating an important part of the AI in civil security ecosystem. Section 4 will chart the institutional frameworks that inform stakeholder interactions regarding the use of AI in the security domain contributing to the further mapping of the ecosystem.

4 Institutional Frameworks chart

The previous section (Section 3) mapped the controversy ecosystem of the AI use in the context of LEAs, identifying diverse stakeholders involved. This section charts the institutional frameworks – laws that are in force (or planned to come into force) and policy documents - that inform stakeholder interactions regarding the use of AI in the security domain. The institutional frameworks chart contributes to the ecosystem mapping identifying the policies around the use of AI in civil security domain. Furthermore, it feeds into the work undertaken in Task 2.2 *Legal framework and casework taxonomy: emerging trends and scenarios*.

AI has rapidly evolved in the past two decades and with that its incorporation into LEAs. However, the regulatory framework for AI at international level is still very limited. In 2021, the EU became the first region in the world to establish a proposal for regulation on AI, with the European Parliament and European Council jointly issuing the “Proposal for a Regulation laying down harmonized rules in the field of artificial intelligence (Artificial Intelligence Act) and amending certain legislative acts of the Union” (European Parliament, 2021). It is a strategic decision for the EU to create regulations to unify legislation on the use of AI and address issues and controversies emerging from the field of AI.

Table 1 below lists institutional frameworks, including regulations, directives, reports and plans in the EU which are applicable to the use of AI by LEAs.

Table 1 Institutional frameworks chart

Policy framework	Year	Type	Objective
Proposed AI Regulation ¹⁵	2021	Proposal for a regulation	Rules to ensure that AI systems used in EU are safe, transparent, ethical, impartial and under human control Prohibits real-time biometric identification – however exception for law enforcement purposes ¹⁶
General Data Protection Regulation ¹⁷	2018	Regulation	Data and privacy security law in the European Union and European Economic Area
Law Enforcement Directive ¹⁸	2018	Directive	Parallel to GDPR - Processing of personal data by data controllers for law enforcement purposes
Passenger Name Record Directive ¹⁹	2018	Directive	Regulates use of passenger name data in the EU for the prevention, detection, investigation and prosecution of terrorist offences and serious crimes

¹⁵ Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts COM/2021/206 <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206>

¹⁶ Art.5(1)(d)(iii), (2), (3), and (4), Proposed AI Regulation

¹⁷ <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

¹⁸ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680>

¹⁹ <https://eur-lex.europa.eu/eli/dir/2016/681/oj>

D3.1: Map of AI in policing innovation ecosystem and stakeholders

EU Declaration on Cooperation on Artificial Intelligence ²⁰	2018	Declaration	Participating Member States agree to cooperate on boosting the EU's AI and its uptake, addressing socio-economic challenges and ensuring an adequate legal and ethical framework
Communication on Artificial Intelligence ²¹	2018	Report	Lays out EU's approach to AI
Coordinated Plan on Artificial Intelligence ²²	2018	Plan	Proposes joint actions for closer and more efficient cooperation between Member States, Norway, Switzerland and the Commission
Coordinated Plan on Artificial Intelligence 2021 Review ²³	2021	Plan	Review of Coordinated Plan on AI proposed in 2018
The European Convention on Human Rights (ECHR)	1953	Convention	International treaty to protect human rights and freedoms of people in countries that belong to the Council of Europe
The European Charter of Fundamental Rights	2000	Charter	Brings together the fundamental rights of those living in the EU
Schengen Agreement	1995	Treaty	Treaty which led to the creation of Europe's Schengen Area, in which internal border checks have largely been abolished
Schengen Borders Code (Regulation 2016/399)	2016	Regulation	Rules governing the movement of persons across borders.
Regulation 2017/458	2017	Regulation	Amends regulation 2016/399 with regard to the reinforcement of checks against relevant databases at external borders
Regulation 2017/225	2017	Regulation	Use of Entry/Exit System
Regulation 2019/817	2019	Regulation	Establish framework for interoperability between EU information systems in the field of borders and visa

The processing of personal data for research normally takes place under the general data protection legal regime (i.e., the GDPR). In parallel, processing of personal data by LEAs takes place under the regime created by the national implementation of the Law Enforcement Directive (LED). This, therefore, poses a question as to which data protection regime should apply to the processing of personal data where LEAs engage in research. Research is stated in some national laws as a public function of LEAs (e.g., in Romania), but other jurisdictions go further and provide for research as a specific law enforcement activity (e.g. Ireland). Where the national law implementing the LED provides for research activities, it can be lawful to process personal data for the purpose of research under the LED legal regime. However, the research ethics framework is much more akin to the GDPR

²⁰<https://ec.europa.eu/jrc/communities/en/node/1286/document/eu-declaration-cooperation-artificial-intelligence#:~:text=Declaration%20signed%20at%20Digital%20Day%20on%2010th%20April%202018.&text=This%20Declaration%20builds%20on%20the,of%20a%20Digital%20Single%20Market.>

²¹ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN>

²² https://knowledge4policy.ec.europa.eu/publication/coordinated-plan-artificial-intelligence-com2018-795-final_en

²³ <https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review>

D3.1: Map of AI in policing innovation ecosystem and stakeholders

regime, such as the provision of data-subject rights, for example. As such, it is generally recommended that LEA research takes place under the GDPR regime.²⁴

In addition to the institutional frameworks mentioned above, the majority of countries across Europe have outlined AI national strategies. By June 2021, 20 EU Member States and Norway had adopted national AI strategies and 7 Member States were in the final drafting phase and ready to publish their strategy in the following months (Van Roy et al., 2021). Table 2 shows the national strategies adopted by each country (AI Watch, 2021; OECD.AI, 2021; Knowledge for Policy, 2021).

Table 2 National AI strategies in European countries

National AI strategies	Year	Country	Objective
Concept for the Development of AI in Bulgaria until 2030	2020	Bulgaria	Focus effort on the development and implementation of AI systems.
National AI strategy: Key action for promoting the integration and development of AI in Cyprus	2020	Cyprus	To maximise investments through partnerships, to nurture talent, skills, and life-long learning and to develop ethical and trustworthy AI
National AI Strategy for the Czech Republic	2019	Czech Republic	Active involvement of the Czech Republic in the EU Initiative on AI.
National Strategy for AI	2019	Denmark	Sets forth 24 key initiatives, including several directly related to the public sector
National AI Strategy	2019	Estonia	Advance the take-up of AI in private and public sector, to increase the relevant skills and research and development base as well as develop the legal environment.
Finland's age of artificial intelligence	2017	Finland	Highlights possibilities and strengths and weaknesses in AI and provides a range of policy actions and recommendations for Finland to thrive in the age of AI
National Strategy on AI	2018	France	Propel France among the champions of AI, with the following priorities: research, human skills, and ethical issues
Artificial Intelligence Strategy	2018	Germany	Sets out framework for a holistic policy on the future development and application of AI
National AI strategy	2020	Hungary	Support and boost all relevant sections of the AI value chain
National AI strategy on developing AI solutions	2020	Latvia	Promote uptake and growth of AI in the whole economy

²⁴ A more detailed elaboration on this point will be available in Leanne Cochrane, Joshua Hughes, Krzysztof Garstka, David Barnard-Wills, Stergios Aidinlis, Agata Gurzawska, Richa Kumar, "Between the GDPR and the LED: demystifying data protection issues in security research" (forthcoming).

D3.1: Map of AI in policing innovation ecosystem and stakeholders

Lithuanian AI strategy: a vision for the future	2019	Lithuania	Modernise and expand the current AI ecosystem in Lithuania and ensure that the nation is ready for a future with AI
AI: a strategic vision for Luxembourg	2019	Luxembourg	Support the development of a human-centric AI based on an efficient and sustainable data-driven ecosystem
National AI strategy	2019	Malta	Gain a strategic competitive advantage in the global economy in the field of AI
Strategic Action Plan for AI	2019	Netherlands	Initiate concrete measures to achieve intended acceleration and national profiling.
National Strategy for AI	2020	Norway	Outline the policy actions that AI can bring for individuals, business and industry, and for the public sector
Policy for the development of AI in Poland from 2020	2020	Poland	Focus on actions on society, education, science, business, public affairs and international relations under the strategic mission of protecting human dignity of people and supporting condition of fair competition in global rivalry
AI Portugal 2030 – National Strategy for AI	2019	Portugal	Foster a collective process mobilising citizens at large and key stakeholders towards building-up a knowledge intensive labour-market with a strong community of forefront companies producing and exporting AI technologies supported by research and innovation communities involved in excellent high-level research
Action plan for the digital transformation of Slovakia for 2019-2022	2019	Slovakia	Concrete steps to build a sustainable, human-centric, and trustworthy AI ecosystem
National Programme on AI	2021	Slovenia	Establish support to research and deployment of AI. Strengthen technological and industrial capabilities. Provide an appropriate ethical and legal framework.
National strategy on AI	2020	Spain	Generate an environment of trust regarding the development of an inclusive and sustainable AI, placing citizens at its heart
National approach for AI	2018	Sweden	Points out general direction for AI in Sweden in order to create a basis for future policy actions and priorities.

Moreover, a chart of policy documents and reports that underline the implications of AI and suggest recommendations of how AI can be used in different areas can be found in Annex A. Task 2.2 *Legal casework taxonomy: emerging trends and scenarios*, will explore the legal framework taxonomy of AI in the security domain more deeply and highlight the gaps that exist in current legal frameworks.



D3.1: Map of AI in policing innovation ecosystem and stakeholders

Section 5 will provide the stakeholders emerged from the controversy ecosystem mapping as well as the charting of initiatives and institutional frameworks that inform their interactions. Stakeholders identified through additional activities such as tracking relevant EU projects and initiatives as well as campaigns highlighting risks regarding the use of AI in security domain are also included.

5 Stakeholders in the domain of AI in civil security

The controversy ecosystem mapping as well as the exploration of initiatives and institutional frameworks that inform their interactions resulted in the identification of stakeholders involved in the domain of AI and security such as local authorities, civil organisations, and ICT and software companies. Furthermore, we identified research projects and initiatives funded by the EU developing AI technologies to be used in the security domain and/or recommendations of their employment and application whose partners are key stakeholders in the domain. Through our research and discussions with project partners, several categories of stakeholders emerged; those involved in the research and development of AI technology and tools, as well as those who react to the use of AI, spread awareness 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 (Figure 1) that co-shape the development and use of AI in the security domain. The mapping of diverse stakeholders is indeed very crucial for the pop AI project aiming to create a structural ecosystem which will be the basis for a European AI hub for the Law Enforcement.

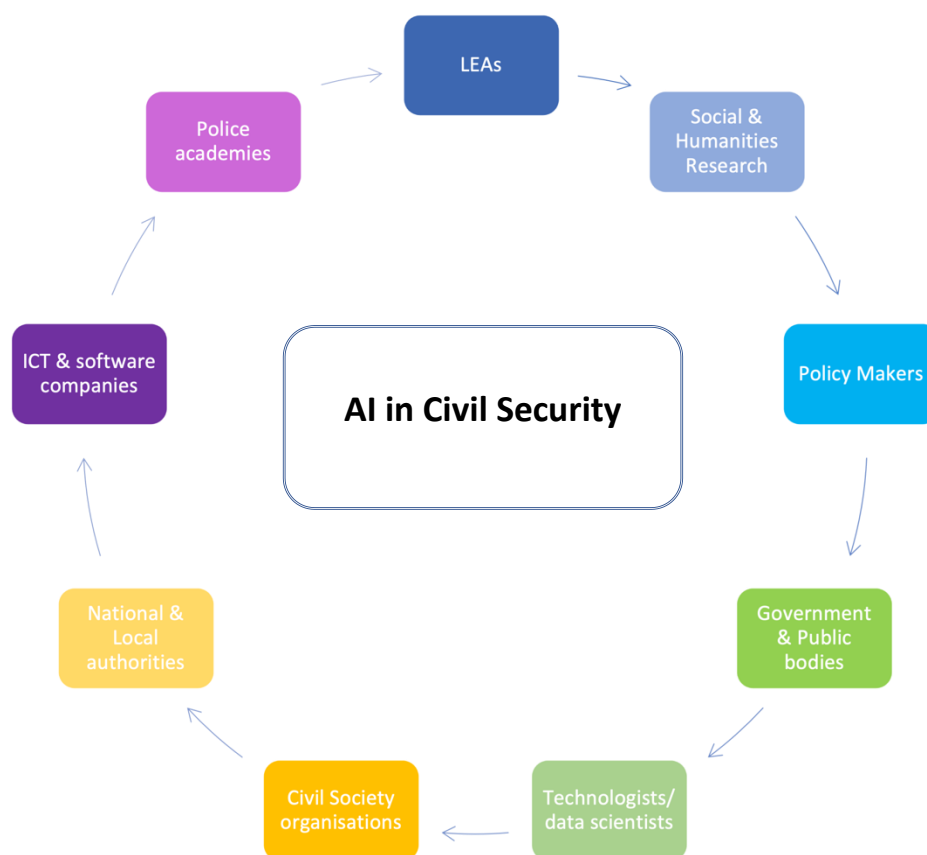


Figure 1 Stakeholders in the domain of AI in civil security

To identify the stakeholders participating in the research and development of AI for LEAs, we collated a list of EU-funded projects, from the European Commission’s CORDIS webpage (<https://cordis.europa.eu/>), and their project partners, specifying the type of stakeholder of each project partner and the countries they were from. Moreover, throughout the research we conducted

D3.1: Map of AI in policing innovation ecosystem and stakeholders

to map the controversy ecosystems of AI tools in the security domain, we identified further relevant EU-funded projects which were incorporated into the list. A table with the EU-funded projects identified, along with their aim and which technologies they use, can be found in Annex B.

From the EU-funded project partners identified, overarching categories of stakeholders were apparent, and were classified as follows:

- ⇒ Research organisations
- ⇒ Universities
- ⇒ ICT and software companies
- ⇒ Law enforcement agencies
- ⇒ Police academies
- ⇒ Government and public bodies
- ⇒ National and local authorities
- ⇒ Not-for-profit and advocacy organisations
- ⇒ Audit and consultancy organisations
- ⇒ Suppliers and end users
- ⇒ Project specific partners

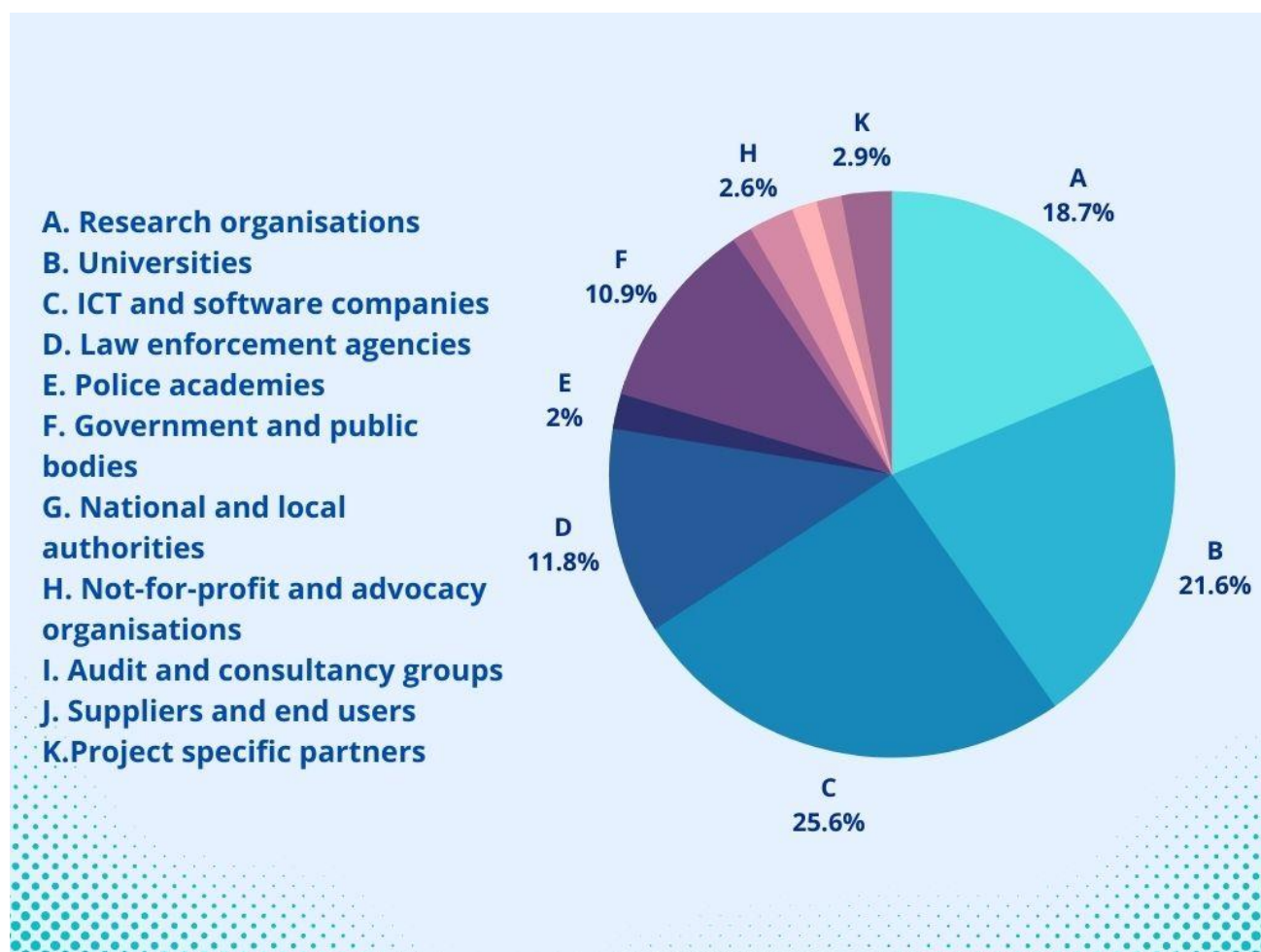


Figure 2 Stakeholder participation in EU-funded projects in the AI and security domain

D3.1: Map of AI in policing innovation ecosystem and stakeholders

A total of 348 different stakeholders were collated from the EU-funded projects identified. As displayed in Figure 1, the majority of stakeholders were ICT and software companies, followed by universities and research organisations. For a detailed list of stakeholders in each category as defined above, see Annex C.

Project partners were geographically mapped to visualise which countries are predominately involved in EU-funded projects assessing and developing AI tools in the field of law enforcement. Moreover, the geographical mapping also allows us to observe which countries are underrepresented in researching AI in the security domain.

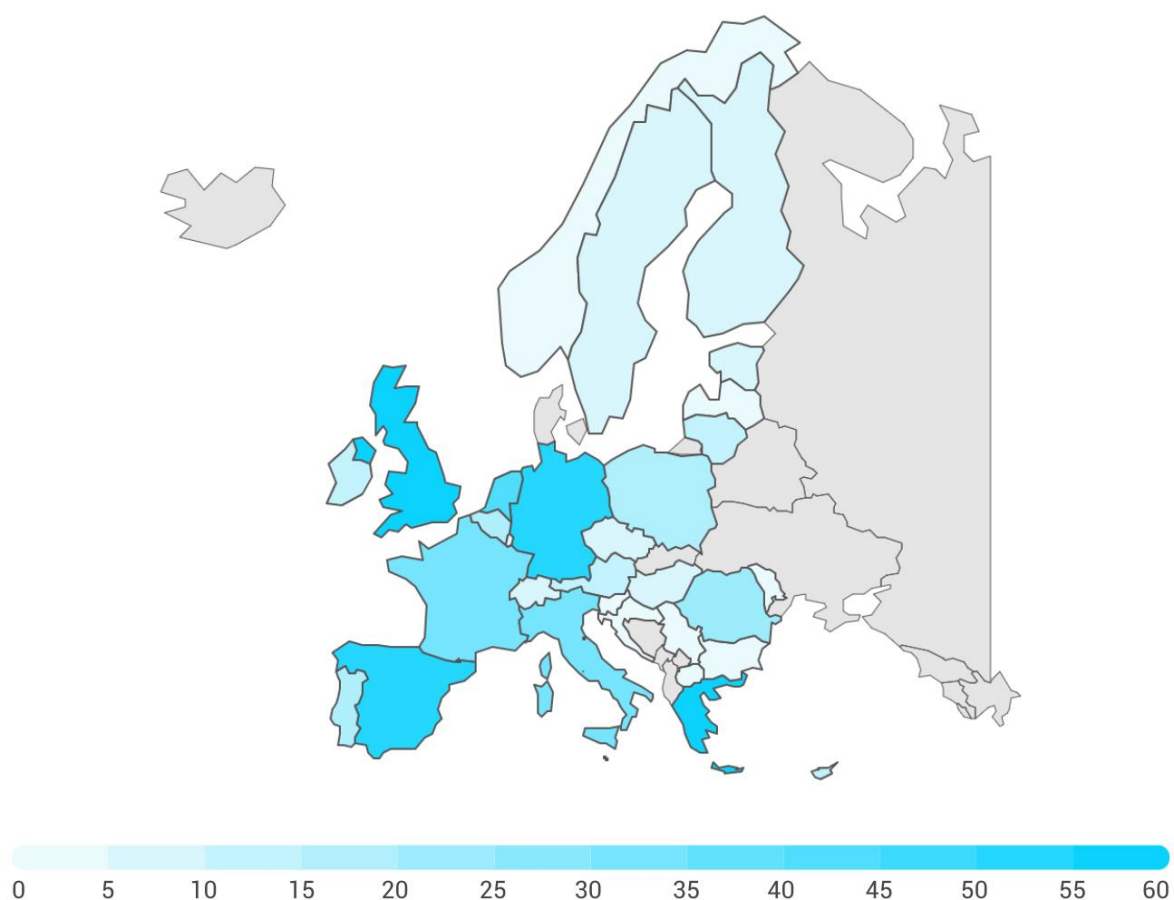


Figure 3 Distribution of stakeholders involved in EU-funded projects on AI in the security domain

As represented in Figure 2, the stakeholders involved in EU-funded project in the field of AI in the security domain are mainly from Greece, the United Kingdom, Spain, Germany, and the Netherlands. Stakeholders from various European countries (Albania, Andorra, Armenia, Azerbaijan, Belarus, Bosnia and Herzegovina, Denmark, Georgia, Iceland, Kosovo, Liechtenstein, Monaco, Montenegro, Russia, San Marino, Slovakia, Ukraine, Vatican City) have not been involved to date in such EU-funded projects. Moreover, some stakeholders from non-European countries have participated in the projects we identified (Israel, China, Brazil), however these have not been included in Figure 2 for completeness.

D3.1: Map of AI in policing innovation ecosystem and stakeholders

As it emerges from the above, it is important to find ways to consult with civil society organisations in the early stages of the AI development due to their underrepresentation in the consortia. As seen in the controversies section, civil society organisations play a key role voicing the concerns and risks of vulnerable groups that can be most affected by the LEAs' use of AI as well as promoting awareness and shaping relevant policies.

Stakeholders reacting to and involved in discussions about potential risks of AI in the security domain also emerged from exploring relevant campaigns in Europe such as Reclaim Your Face (<https://reclaimyourface.eu/>) and iBorderCtrl.no (<https://iborderctrl.no/>). Stakeholders were also identified from statements and open letters which call on the EU to prohibit certain AI systems in law enforcement and criminal justice. Annex C includes a table listing all the civil society organisations identified from these research activities²⁵.

The stakeholders identified in the current deliverable will inform further activities in WP3, along with activities undertaken as part of Work Package 4 *The pandect of recommendations for ethical use of AI for LEAs* and Work Package 5 *Dissemination, Communications and Sustainable Community Engagement*.

²⁵ A list including the names and email addresses of the stakeholders identified will be shared strictly with the consortium partners for research purposes of pop AI due to GDPR restrictions on sharing personal data.

6 Conclusions

Over the past decades, law enforcement agencies have been increasingly relying on AI based technologies to support their operations raising concerns regarding violation of fundamental rights that can impact people both on a personal as well as on a societal level especially vulnerable groups of the society. Therefore, it is crucial to reflect on the concerns, fears and risks surrounding the use of AI and to address these issues from a technical, organizational, and legal perspective. This process will result in the development of ethical, transparent, and accountable systems by design that will gain the trust both of the LEAs and the public.

To do so, it is necessary to identify the stakeholders involved in the process of the design, development, employment as well the policies regarding the employment of AI, and the groups affected by its use so to ensure an inclusive process that considers all diverse experiences, needs, concerns and potentials. This report adopted an ecosystem approach to map the controversies in AI tools in the security domain to understand the issues and potentials discussed. The ecosystem approach allowed us to gain a holistic overview and map stakeholders from an ethically driven and socially sustainable perspective.

The mapping of AI controversies was evolved around six broad civil security domains: crime prevention; crime investigation; migration, asylum, and border control; administration of justice; cyber operations for law enforcement; and LEAs' training. The mapping highlighted controversies regarding privacy issues, gender and racial discrimination, lack of transparency and accountability both in the design of the technologies as well as in the policies and procedures of their employment, and violation of human rights.

Following, institutional frameworks that inform stakeholder interactions regarding the controversies around the use of AI in the security domain were charted. The charting included regulations, directives, reports and plans in the EU which are applicable to the use of AI by LEAs, highlighting current and upcoming efforts to manage AI in the security domain.

Drawing together the stakeholders identified through the controversy mapping (section 3) and the insights emerging from charting the institutional frameworks (section 4), the stakeholders involved in the ecosystem of AI in the civil security domain were identified. The stakeholders' categories were completed by identifying the partners of EU funded projects and initiatives around the area of AI and security. Assessing the stakeholders involved in EU-funded projects in AI and security, we were able to identify the categories of stakeholders that have the greatest as well as the least participation in these projects and the countries in which they are based. In doing so, we noted that there are voices that need to be included during the making process of AI technologies such as civil society organisations to provide insights on potential risks especially impacting more vulnerable groups who are generally more silent and not heard such as ethnic minorities, LGBTI people, elderly people, and women.

The current report maps the ecosystem of AI in the security domain to support the further research, dissemination and communication activities contributing to the overall objective of the project to create a European AI hub for the Law Enforcement, breaking the silos between the distinct nodes.

7 References

- AccessNow (2021). *An EU Artificial Intelligence Act for Fundamental Rights. A Civil Society Statement*. Available at: <https://www.accessnow.org/cms/assets/uploads/2021/11/joint-statement-EU-AIA.pdf>
- AI Watch (2021). *National strategies on Artificial Intelligence: A European perspective, 2021 edition*. Available at: <https://publications.jrc.ec.europa.eu/repository/handle/JRC122684>
- Akhgar, B., Redhead, A., Davey, S. & Saunders, J. (2019). Introduction: Serious Games for Law Enforcement Agencies. In: Akhgar, Babak, (ed.) *Serious Games for Enhancing Law Enforcement Agencies – From Virtual Reality to Augmented Reality*. Security Informatics and Law Enforcement. Springer, pp. 1-11.
- Algorithmic Watch (2020). *Automating Society Report 2020*. Available at: <https://automatingsociety.algorithmwatch.org/wp-content/uploads/2020/12/Automating-Society-Report-2020.pdf>
- Amnesty International (2020). *Netherlands: We sense trouble: Automated discrimination and mass surveillance in predictive policing in the Netherlands*. Available at: <https://www.amnesty.org/en/documents/eur35/2971/2020/en/> (Accessed: 12 February 2022)
- AXON (2021). *Axon Launches New Virtual Reality Simulator Training for Today's Public Safety Challenges*. Available at: <https://www.axon.com/news/about/vr-simulator-training>
- Babuta, A., Oswald, M. & Rinik, C. (2018). Machine Learning Algorithms and Police Decision-Making: Legal, Ethical and Regulatory Challenges. RUSI Whitehall Report 3-18. Available at: https://static.rusi.org/201809_whr_3-18_machine_learning_algorithms.pdf.pdf (Accessed: 10 March 2022).
- BBC News (2018). Durham police criticised over 'crude' profiling. *BBC News*, 9 April. Available at: <https://www.bbc.com/news/technology-43428266> (Accessed: 21 February 2022).
- BBC News (2021). Met Police gangs matrix at lowest levels in seven years. *BBC News*, 3 February. Available at: <https://www.bbc.com/news/uk-england-london-55918556> (Accessed: 1 February 2022).
- Beydoun, K.A., (2021). The New State of Surveillance: Societies of Subjugation. *79 Washington & Lee*, pp. 1-49.
- Bournemouth University (2022). PLUS Project: Serious games for police training. Available at: <https://www.bournemouth.ac.uk/research/projects/plus-project-serious-games-police-training>
- Brayne, S., Rosenblat, A. & Boyd, D. (2015). Predictive Policing. *Data & Civil Rights: A New Era of Policing and Justice*. Available at: https://www.datacivilrights.org/pubs/2015-1027/Predictive_Policing.pdf (Accessed: 8 March 2022).
- Bryson J. (2022). *Europe Is in Danger of Using the Wrong Definition of AI*. Available at: https://www.wired.com/story/artificial-intelligence-regulation-european-union/?fbclid=IwAR3e8Wa31aq8_qjJfRsvLIW0LcT_Ehf6fgxVqxQJc2FHG1GafsX3d8BMuQ

D3.1: Map of AI in policing innovation ecosystem and stakeholders

- Burges, M. (2018). UK police are using AI to inform custodial decisions – but it could be discriminating against the poor. *Wired*, 1 March. Available at: <https://www.wired.co.uk/article/police-ai-uk-durham-hart-checkpoint-algorithm-edit> (Accessed: 11 March 2022).
- Clavell, G. G. (2017). Protect rights at automated borders. *Nature*, 543(7643), pp.34–36. doi:10.1038/543034a.
- Coull, N. et al. (2017). On the use of serious games technology to facilitate large-scale training in cybercrime response.
Available at: <https://bulletin.cepol.europa.eu/index.php/bulletin/article/view/274>
- Council of Europe (2020). *Justice by algorithm – the role of artificial intelligence in policing and criminal justice systems*. Parliamentary Assembly.
Available at: <https://assembly.coe.int/LifeRay/JUR/Pdf/DocsAndDecs/2020/AS-JUR-2020-22-EN.pdf>
- Damjanovic, L., Pinkham, A. E., Clarke, P., & Phillips, J. (2014). Enhanced threat detection in experienced riot police officers: Cognitive evidence from the face-in-the-crowd effect. *Quarterly Journal of Experimental Psychology*, 67(5), 1004–1018. doi:10.1080/17470218.2013.839724 PMID:24152089
- Degli Esposti, S. & Santiago-Gomez, E. (2015). Acceptable surveillance-orientated security technologies: Insights from the SurPRISE Project. *Surveillance & Society*, 13(3/4), pp.437-454.
- del Rio, J. S., Moctezuma, D., Conde, C., de Diego, I. M., & Cabello, E. (2016). Automated border control e-gates and facial recognition systems. *computers & security*, 62, 49-72.
- Derbyshire Constabulary (2020). *Derbyshire police trialling cutting edge virtual reality training tool*. Available at: <https://www.derbyshire.police.uk/news/derbyshire/news/news/forcewide/2020/august/derbyshire-police-trialling-cutting-edge-virtual-reality-training-tool/>
- Dorheml, L. (2018). Welsh police force is first in U.K to use virtual reality to train its officers. *Digital Trends*, February 26. Available at: <https://www.digitaltrends.com/cool-tech/uk-police-virtual-reality-training/> (Accessed: 21 March 2022).
- Dumbrava, C. (2021). Artificial intelligence at EU borders: Overview of applications and key issues. *European Parliament*.
Available at: [https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/690706/EPRS_IDA\(2021\)690706_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/690706/EPRS_IDA(2021)690706_EN.pdf)
- Durham Police (2022). AI can predict reoffending, university study finds. Available at: <https://durham.police.uk/News/News-Articles/2022/January/AI-can-predict-reoffending-university-study-finds.aspx> (Accessed: 10 March 2022).
- Euractiv (2011). MEPs question ‘Big Brother’ urban observation project. Euractiv, 25 February. Available from: <https://www.euractiv.com/section/justice-home-affairs/news/meps-question-big-brother-urban-observation-project/> (Accessed: 13 February 2022).
- EDPB (2022). *Facial recognition: Italian SA fines Clearview AI EUR 20 million*. Available at: https://edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en

D3.1: Map of AI in policing innovation ecosystem and stakeholders

- EDPB-EDPS (2021). *Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. Available at: https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf
- EDRI (2021). *Use cases: Impermissible AI and fundamental rights breaches*. Available at: <https://edri.org/wp-content/uploads/2021/06/Case-studies-Impermissible-AI-biometrics-September-2020.pdf>
- EDRI (2021). *Chilling use of face recognition at Italian borders shows why we must ban biometric mass surveillance*. Available at: <https://edri.org/our-work/face-recognition-italian-borders-ban-biometric-mass-surveillance/>
- European Commission (2022). *A European approach to artificial intelligence*. Available at: <https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence>
- European Data Protection Board (2021). *Unlawful use of body cams in Stockholm’s public transport*. *European Data Protection Board*, June 21. Available at: https://edpb.europa.eu/news/national-news/2021/unlawful-use-body-cams-stockholms-public-transport_en
- Eurostat (2018a). *Record number of air passengers carried at more than 1.1 billion in 2018*. Available at: <https://ec.europa.eu/eurostat/documents/2995521/10265946/7-06122019-AP-EN.PDF/8f2c9d16-c1c4-0e1f-7a66-47ce411faef7> (Accessed on: 3 March 2022).
- Eurostat (2018b). *Passengers embarked and disembarked in all ports*. Available at: https://ec.europa.eu/eurostat/cache/digpub/eumove/vis/eumove_03_04_01/index.html?lang=en (Accessed on: 3 March 2022).
- Fair Trials (2021). *Automating Injustice: The use of artificial intelligence & automated decision-making systems in criminal justice in Europe*. Available at: https://www.fairtrials.org/app/uploads/2021/11/Automating_Injustice.pdf (Accessed: 22 February 2022).
- Fair Trials (2022). *AI Act: EU must ban predictive AI systems in policing and criminal justice*. Available at: [https://www.fairtrials.org/articles/news/ai-act-eu-must-ban-predictive-ai-systems-in-policing-and-criminal-justice/#:~:text=Share%20by%20Email,%20AI,%20Act%3A%20EU%20must%20ban%20predictive%20AI,in%20policing%20and%20criminal%20justice&text=Today%2C%20Fair%20Trials%2C%20European%20Digital,Artificial%20Intelligence%20Act%20\(AIA\)](https://www.fairtrials.org/articles/news/ai-act-eu-must-ban-predictive-ai-systems-in-policing-and-criminal-justice/#:~:text=Share%20by%20Email,%20AI,%20Act%3A%20EU%20must%20ban%20predictive%20AI,in%20policing%20and%20criminal%20justice&text=Today%2C%20Fair%20Trials%2C%20European%20Digital,Artificial%20Intelligence%20Act%20(AIA)) (Accessed: 25 February 2022).
- Frontex (2021). *How AI can support the European Border and Coast Guard*. RAND Europe. Available at: <https://www.rand.org/randeurope/research/projects/european-border-coast-guard-artificial-intelligence.html>
- Frontex (2021b). *Frontex Entry Exit System Pilot Project*. Available at: <https://frontex.europa.eu/media-centre/news/news-release/frontex-entry-exit-system-pilot-project-6FimQn>
- Galindo, G. (2019). ‘No legal basis’ for facial recognition cameras at Brussels Airport. *The Brussels Times*, 10 July. Available at: <https://www.brusselstimes.com/brussels-2/60362/no-legal-basis->

D3.1: Map of AI in policing innovation ecosystem and stakeholders

[for-facial-recognition-cameras-identity-brussels-airport-intelligent-cameras](#) (Accessed: 20 February 2022).

Gallagher, C. (2021, April 26). Garda body cameras likely to be used only in potential confrontations. *The Irish Times*.

<https://www.irishtimes.com/news/crime-and-law/garda-body-cameras-likely-to-be-used-only-in-potential-confrontations-1.4547228>

Giessing, L. (2021). The potential of virtual reality for police training under stress: a SWOT analysis. In *Interventions, Training, and Technologies for Improved Police Well-Being and Performance* (pp. 102-124). IGI Global

Goold, B.J., 2004. *CCTV and policing: Public area surveillance and police practices in Britain*. Oxford University Press on Demand.

Gonzalez Fuster, G. (2020). *Artificial Intelligence and Law Enforcement: Impact on Fundamental Human Rights*. Brussels: European Parliament. Available at: [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU\(2020\)6562_95_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU(2020)6562_95_EN.pdf) (Accessed: 1 March 2022).

Gregoriou, C. & Troullinou, P. (2012). Scanning Bodies, Stripping Rights? How Do UK Media Discourses Portray Airport Security Measures?, In Gregoriou, C. (eds), *Constructing Crime*, London: Palgrave Macmillan, pp. 19-33.

Hayes, B. (2012). 'The surveillance-industrial complex', in Ball, K., Haggerty, K. D., & Lyon, D. *Routledge handbook of surveillance studies*, Abingdon: Routledge Handbooks Online, pp.167-175

Heaven, W. D. (2021). Predictive policing is still racist—whatever data it uses. *MIT Technology Review*, February 5. Available at: <https://www.technologyreview.com/2021/02/05/1017560/predictive-policing-racist-algorithmic-bias-data-crime-predpol/> (Accessed: 19 March 2022).

Hersey, F. (2021). Partial success in transparency lawsuit into EU's AI lie detector research. *Biometric Update*. Available at: <https://www.biometricupdate.com/202112/partial-success-in-transparency-lawsuit-into-eus-ai-lie-detector-research>

High-level Expert Group on Artificial Intelligence (2019). A Definition of AI: Main capabilities and disciplines. Available at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=56341

Houser, K. (2021). Controversial police killings are being recreated in VR. *Freethink*, 5 May. Available at: <https://www.freethink.com/social-change/vr-police-training> (Accessed: 20 February 2022).

IATA (2019). *Automated border control implementation*. Available at: <https://web.archive.org/web/20190527155531/https://www.iata.org/whatwedo/passenger/Pages/automated-bordercontrol-maps.aspx>

iBorderCtrl.no (2022). Fighting iBorderCtrl. Available at: <https://iborderctrl.no/act>

ICO (2018). *Supervisory Powers of the Information Commissioner Enforcement Notice*. Available at: <https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/about-us/gangs-violence-matrix/ico-enforcement-notice.pdf>

Ilbiz, E. & Kaunert, C. (2021). *EU, Turkey and Counter-terrorism: Fighting the PKK and ISIS*. Cheltenham: Routledge.

D3.1: Map of AI in policing innovation ecosystem and stakeholders

- INHOPE (2020). *Artificial Intelligence in the fight against online CSAM*. Brussels: European Commission. Available at: <https://www.inhope.org/media/pages/articles/inhope-ai-focus-group-highlights/3270139400-1591781903/inhope-safer-internet-day-ai-focus-group-report-highlights.pdf>
- International Airport Review (2021). *Facial recognition pilot programme launched at Barcelona-El Prat Airport*. Available at: <https://www.internationalairportreview.com/news/172772/facial-recognition-pilot-programme-launched-at-barcelona-el-prat-airport/>
- Jackson, D. J. (2011). What is an innovation ecosystem. *National Science Foundation*, 1(2), pp.1-11.
- Jansen, F. (2018). Data Driven Policing in the Context of Europe. Data Justice Lab. Available at: <https://datajusticeproject.net/wp-content/uploads/sites/30/2019/05/Report-Data-Driven-Policing-EU.pdf> (Accessed: 1 March 2022).
- Jones, C. (2018). ICO says Metropolitan Police breached data protection laws with Gangs Matrix. IPro, 23 November. Available at: <https://www.itpro.co.uk/data-processing/32432/ico-says-metropolitan-police-breached-data-protection-laws-with-gangs-matrix> (Accessed: 4 March 2022).
- Kamiński, J., Jurczak, J. & Jakubczyk, R. (2020). Simulator of Police Actions in Crisis Situations as an Application of an Intelligent Decision Support System in the Process of Improving Polish Police Actions. *Internal Security*, pp.137-145
- Knowledge for policy (2021). Monitor the development, uptake and impact of Artificial Intelligence for Europe. Available at: https://knowledge4policy.ec.europa.eu/ai-watch/national-strategies-artificial-intelligence_en
- Lamb, H. (2020). Good cop, good cop: Can VR help to make policing kinder? IET, 8 January. Available at: <https://eandt.theiet.org/content/articles/2020/01/good-cop-good-cop-can-vr-make-policing-kinder/> (Accessed: 5 March 2022).
- Laufs, J. and Borrion, 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
- LAW-GAME (2021). Available at: <https://lawgame-project.eu/>
- Liberty (2022). *Liberty challenges MET Police's discriminatory gangs matrix*. Available at: <https://www.libertyhumanrights.org.uk/issue/liberty-challenges-met-polices-discriminatory-gangs-matrix/>
- Meijer, A. & Wessels, M. (2019). Predictive Policing: Review of Benefits and Drawbacks, *International Journal of Public Administration*, 42(12), 1031-1039. <https://doi.org/10.1080/01900692.2019.1575664>
- Meta (2020). *Here's how we're using AI to help detect misinformation*. Available at: <https://ai.facebook.com/blog/heres-how-were-using-ai-to-help-detect-misinformation/> (Accessed: 21 March 2022).
- Metropolitan Police (2022). *Gangs violence matrix*. Available at: <https://www.met.police.uk/police-forces/metropolitan-police/areas/about-us/about-the-met/gangs-violence-matrix/> (Accessed on: 7 March 2022).

D3.1: Map of AI in policing innovation ecosystem and stakeholders

- MOPAC (2018). *Review of the Metropolitan Police Service Gangs Matrix*. Available at: https://www.london.gov.uk/sites/default/files/gangs_matrix_review_-_final.pdf
- Murph, D. (2019). One of Europe's Busiest Airports Is Testing Facial Recognition Boarding. *The Points Guy*, 18 February. Available at: <https://thepointsguy.com/news/amsterdam-schiphol-test-trial-facial-recognition-boarding/>
- NATO (2022). The role of AI in the battle against disinformation. Riga: NATO StratCom COE. Available at: <https://stratcomcoe.org/pdfjs/?file=/publications/download/The-Role-of-AI-DIGITAL.pdf?zoom=page-fit> (Accessed: 10 March 2022).
- Newell, B.C. (2020). *Police on Camera: Surveillance, Privacy, and Accountability*. Routledge
- Nilson, P. (2019). UK police test if computer can predict criminal behaviour. *Financial Times*, 6 February. Available at: <https://www.ft.com/content/9559efbe-2958-11e9-a5ab-ff8ef2b976c7>
- Nolan, S. (2021) How Singapore is using simulations and robots for police training. *GovInsider Asia*, 6 December. Available at: <https://govinsider.asia/digital-gov/how-singapore-is-using-simulations-and-robots-for-police-training-anthony-ng-singapore-police-force/>
- Noori, S. (2021). Suspicious Infrastructures: Automating Border Control and the Multiplication of Mistrust through Biometric E-Gates. *Geopolitics*, pp. 1-24. Available at: <https://www.tandfonline.com/doi/full/10.1080/14650045.2021.1952183>
- Norris, C. & Armstrong, G. (2017). CCTV and the social structuring of surveillance. In *Surveillance, Crime and Social Control* (pp. 81-102). Routledge.
- Norris, C. & Armstrong, G. (2020). *The maximum surveillance society: The rise of CCTV*. Routledge.
- Norris, C., McCahill, M. & Wood, D. (2004). The growth of CCTV: a global perspective on the international diffusion of video surveillance in publicly accessible space. *Surveillance & Society*, 2(2/3).
- Peeters, B. (2020). Facial recognition at Brussels Airport: face down in the mud. *KU Leuven Centre for IT & IP Law*. Available at: <https://www.law.kuleuven.be/citip/blog/facial-recognition-at-brussels-airport-face-down-in-the-mud/>
- Pew Research Center (2016). *Number of Refugees to Europe Surges to Record 1.3 Million in 2015*. Available at: <https://www.pewresearch.org/global/2016/08/02/number-of-refugees-to-europe-surges-to-record-1-3-million-in-2015/> (Accessed: 28 February 2022).
- Poliisi (2021). *Body-worn police cameras introduced this spring in all Finland*. Available at: <https://poliisi.fi/en/-/body-worn-police-cameras-introduced-this-spring-in-all-finland>
- Politie (2020). *New bodycams fully operational in summer 2021*. Available at: <https://www.politie.nl/nieuws/2020/oktober/27/nieuwe-bodycams-in-zomer-2021-volledig-operationeel.html>
- OECD.AI (2021), powered by EC/OECD (2021), Database of national AI policies. Available at: <https://oecd.ai>
- Oireachtas Library & Research Service (2021). *L&RS Spotlight: Algorithms, Big Data and Artificial Intelligence in the Irish Legal Services Market*
- Oswald, M., Grace, J., Urwin, S. & Barnes, G. C. (2018). Algorithmic risk assessment policing models: Lessons from the Durham HART model and 'Experimental' proportionality, *Information & Communications Technology Law*, 27(2), pp.223-250.

D3.1: Map of AI in policing innovation ecosystem and stakeholders

- Rolland, A. (2021). Ethics, Artificial Intelligence and Predictive Policing. The Security Distillery, July 23. Available at: <https://thesecuritydistillery.org/all-articles/ethics-artificial-intelligence-and-predictive-policing#:~:text=AI%20algorithms%20are%20used%20in,as%20risk%20or%20threat%20assessment> (Accessed: 3 March 2022).
- Rossi, A. (2018). How the Snowden revelations saved the EU general data protection regulation. *The International Spectator*, 53(4), pp.95-111.
- Samoili, S., López Cobo, M., Gómez, E., De Prato, G., Martínez-Plumed, F., & Delipetrev, B. (2020). *Defining Artificial Intelligence. Towards an operational definition and taxonomy of artificial intelligence*. Luxembourg: Publications Office of the European Union. doi:10.2760/382730, JRC118163.
- SIMAVI (2022). *LAW-GAME – elevating experiential training for police officer through gamification technologies*. Available at: <https://www.simavi.ro/en/node/101>
- Statt, N. (2017). UK police will start using AI to decide whether suspects should be kept in custody. *The Verge*, 10 May. Available at: <https://www.theverge.com/2017/5/10/15614980/uk-durham-police-ai-risk-assessment-policing> (Accessed on: 10 March 2022).
- SHOTPROS (2022). The SHOTPROS project. Available at: <https://shotpros.eu/the-shotpros-project/>
- STOA (2019). Regulating disinformation with artificial intelligence. European Parliament. Available at: [https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624279/EPRS_STU\(2019\)624279_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624279/EPRS_STU(2019)624279_EN.pdf) (Accessed: 1 March 2022).
- Thompson, H. (2020). All police in France will wear body cameras by July 2021. *The Connexion*, 15 September. Available at: <https://www.connexionfrance.com/article/French-news/All-police-in-France-will-wear-body-cameras-by-July-2021-says-Gerald-Darmanin-minister-interior> (Accessed: 1 March 2022).
- Ulnicane, I. (...) et al. (2021). Framing governance for a contested emerging technology: insights from AI policy. *Policy and Society*, 40(2), pp.158-177.
- University of Cambridge (2018). *Helping police make custody decisions using artificial intelligence*. Available at: <https://www.cam.ac.uk/research/features/helping-police-make-custody-decisions-using-artificial-intelligence>
- Van Brakel, R. and De Hert, P. (2011). Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies. *Technol. Led Policing*, 20, pp.165-192.
- Van Brakel, R. (2016). 'Pre-emptive big data surveillance and its (dis) empowering consequences: The case of predictive policing', in van de Sloot, B., Broeders, D. & Schrijvers E., *Exploring the Boundaries of Big Data*, Amsterdam: University Press, pp.117-141.
- Vanreenterghem, A. & Heymans, P. (2019). Police are no longer allowed to use automatic facial recognition at the airport. *VRT*, 20 September. Available at: <https://www.vrt.be/vrtnws/nl/2019/09/20/politie-mag-geen-automatische-gezichtsherkenning-gebruiken-op-de-app/> (Accessed: 1 February 2022).
- VR & Police Network (2022). Topics about VR & Police. Available at: <https://vrandpolice.eu/topic/> (Accessed: 19 March 2022).
- Watney, M. M. (2019). 'Law Enforcement Use of Artificial Intelligence for Domestic Security: Challenges and Risks', in Griffiths, P. & Kabir M., *ECIAIR 2019 European Conference on the Impact of Artificial Intelligence and Robotics*, Oxford: EM-Normandie Business School.

D3.1: Map of AI in policing innovation ecosystem and stakeholders

- Whittaker, Z. (2021). Apple delays plans to roll out CSAM detection in iOS 15 after privacy backlash. Tech Crunch, 3 September. Available at: <https://techcrunch.com/2021/09/03/apple-csam-detection-delayed/>
- Winter, C. (2019). German police storing bodycam footage on Amazon cloud. *DW*, 2 March. Available at: <https://www.dw.com/en/german-police-storing-bodycam-footage-on-amazon-cloud/a-47751028> (Accessed: 8 March 2022).
- Wood, D.M., Ball, K., Lyon, D., Norris, C. & Raab, C. (2006). A report on the surveillance society. Surveillance Studies Network, UK, pp.1-98.
- Wright, J.E. & Headley, A.M. (2020). Can technology work for policing? Citizen perceptions of police-body worn cameras. *The American Review of Public Administration*, 51(1), pp.17-27.

8 Annexes

8.1 Annex A. Reports and documents reviewing and critically engaging on the topic of AI in LEAs

Adapted from Ulnicane et al. (2020)

Name	Year	Author	Type of document	What it is	Concern addressed
APPG AI Findings ²⁶	2017	Big Innovation Centre/All-Party Parliamentary Group on AI	Policy Report	Recommends the appointment of a Minister for AI in the Cabinet Office Role of minister should be based on 6 policy areas: data, infrastructure, skills, innovation & entrepreneurship, trade, and accountability	Privacy Explainability Accountability
Algorithms and artificial intelligence: report on the ethical issues ²⁷	2017	CNIL	Policy Report	Outlines founding principles of loyalty and continued attention and vigilance. Suggests policy recommendations and highlights major ethical concerns in AI	Discrimination, profiling, threat to rights
Artificial Intelligence, Robotics, Privacy and Data Protection ²⁸	2016	EDPS	Policy Report	Presents topics within AI and robots and question for reflecting and discussion on data protection and privacy of these technologies	Data protection, privacy
Artificial Intelligence A European Perspective ²⁹	2018	European Commission	Policy Report	Outlines the history of AI and the use of AI in the EU, USA and China. Summarises diverse perspectives concerning AI	

²⁶ https://www.biginnovationcentre.com/wp-content/uploads/2019/07/BIC_APPG-AI-2017-FINDINGS_6.12.2017.pdf

²⁷ <https://www.cnil.fr/en/algorithms-and-artificial-intelligence-cnils-report-ethical-issues>

²⁸ https://edps.europa.eu/sites/default/files/publication/16-10-19_marrakesh_ai_paper_en.pdf

²⁹ <https://publications.jrc.ec.europa.eu/repository/handle/JRC113826#:~:text=We%20are%20only%20at%20the,opportunities%20to%20improve%20our%20lives.>



D3.1: Map of AI in policing innovation ecosystem and stakeholders

Artificial Intelligence – The consequences of AI on the (digital) single market, production, consumption, employment and society ³⁰	2017	European Economic and Social Committee	Opinion	Series of conclusions and recommendations	Ethics, privacy, safety, transparency, accountability, equality
Statement on AI, Robotics and ‘Autonomous’ Systems ³¹	2018	European Group on Ethics in Science and New Technologies	Policy statement	Call for common, internationally recognised ethical and legal framework for the design, use and governance of AI, robotics and autonomous systems	
European Civil Law Rules in Robotics ³²	2016	European Parliament	Report for JURI Committee	Evaluation and analysis from ethical and legal perspective of a number of future European civil law rules in robotics	
Report with recommendations on the Commission on Civil Law Rules on Robotics ³³	2017	European Parliament	Report	Series of recommendations concerning the Civil Law Rules on Robotics	
Understanding Artificial Intelligence ³⁴	2018	European Parliament	Policy Brief	Discussion of AI, limitations and issues with AI and new frameworks for the development of AI	Data privacy, inequality, autonomous decision making, impact on job market

³⁰<https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/artificial-intelligence-consequences-artificial-intelligence-digital-single-market-production-consumption-employment-and>

³¹ <https://op.europa.eu/en/publication-detail/-/publication/dfebe62e-4ce9-11e8-be1d-01aa75ed71a1>

³² [https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU\(2016\)571379_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU(2016)571379_EN.pdf)

³³ https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_EN.html

³⁴ [https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI\(2018\)614654](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2018)614654)



D3.1: Map of AI in policing innovation ecosystem and stakeholders

The Malicious Use of AI: Forecasting, Prevention and Mitigation ³⁵	2018	Future of Humanity Institute et al.	Policy brief	Surveys potential security threats from the malicious use of AI technologies, and proposes ways to prevent and mitigate these threat with a series of recommendations	
AI: opportunities and implications for the future of decision making ³⁶	2016	Government Office for Science	Policy brief	Use of AI for innovation and productivity by government and the effects it poses on labour market, and new challenges posed by AI	
Growing the AI industry in the UK ³⁷	2017		Independent report	Series of recommendations to assist the growth of AI in the UK	
AI Sector Deal ³⁸	2019	HM Government	Policy report	£1 billion package of support from the UK government and industry to boost the UK's global position as a leader in developing AI and related technologies	
Robotics and artificial intelligence ³⁹	2016	House of Commons	Policy report	General overview on the use and implementation of AI and robotics	
AI in the UK: ready, willing and able? ⁴⁰	2018	House of Lords	Policy report	Overview of AI, how it is designed and developed, mitigating risks of AI and a summary of conclusions and recommendations	
Ethically aligned design. A vision for prioritising human well-being with	2017	IEEE	Policy report	Advance public discussion about how we can establish ethical and social implementations for intelligent and autonomous systems and technologies and facilitate the	

³⁵ <https://arxiv.org/pdf/1802.07228.pdf>

³⁶ https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/566075/gs-16-19-artificial-intelligence-ai-report.pdf

³⁷ <https://www.gov.uk/government/publications/growing-the-artificial-intelligence-industry-in-the-uk>

³⁸ <https://www.gov.uk/government/publications/artificial-intelligence-sector-deal/ai-sector-deal>

³⁹ <https://publications.parliament.uk/pa/cm201617/cmselect/cmsctech/145/14502.htm>

⁴⁰ <https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf>



D3.1: Map of AI in policing innovation ecosystem and stakeholders

autonomous and intelligent systems ⁴¹				emergence of national and global policies that align with these principles	
AI: Calling on Policy Makers to Take a Leading Role in Setting a Long-Term AI Strategy ⁴²	2017	IEEE European Policy Initiative	Policy report	Series of recommendations to target EU institutions, the member states' governments, and the involved agencies	
Big data, artificial intelligence, machine learning and data protection ⁴³	2017	Information Commissioner's Office	Policy report	Data protection implications of the AI, big data and machine learning and compliance tools	
AI for Good Global Summit Report 2017 ⁴⁴	2017	International Telecommunications Union	Global summit report	Platform for government official, UN agencies, NGO's, industry leaders and AI experts to discuss the ethical, technical, societal and policy issues related to AI	
Managing automation: Employment, inequality, and ethics in the digital age ⁴⁵	2017	Institute for Public Policy Research	Discussion Paper	Argues that public policy should seek to accelerate automation to reap the productivity benefits, while building new institutions to ensure the dividends of technological changes are broadly shared	

⁴¹ https://standards.ieee.org/wp-content/uploads/import/documents/other/ead_v2.pdf

⁴² <http://globalpolicy.ieee.org/wp-content/uploads/2017/10/IEEE17021.pdf>

⁴³ <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>

⁴⁴ <https://www.itu.int/en/ITU-T/AI/Pages/201706-default.aspx>

⁴⁵ <https://www.ippr.org/publications/managing-automation>



D3.1: Map of AI in policing innovation ecosystem and stakeholders

Finland's Age of Artificial Intelligence ⁴⁶	2017	Ministry of Economic Affairs and Employment	Policy report	Highlights Finland's possibilities in the global market along with its strengths and weaknesses in AI. Provides a range of policy actions and recommendations	
A Law on Robotics and Artificial Intelligence in the EU? ⁴⁷	2017	European Trade Union Institute ETUI	Foresight Brief	Strategic thinking about the future challenges of a law on robotics and AI in the EU	Visibility, accountability, liability
Human Rights in the Robot Age: Challenges arising from the use of robotics, AI and VR/AR ⁴⁸	2017	Rathenau Institute	Report	Analysis of the challenges resulting from the use of AI, robotics, AR/VR and series of recommendations for the Parliamentary Assembly of the Council of Europe	
APPG AI Findings ⁴⁹	2017	Big Innovation Centre/All-Party Parliamentary Group on AI	Policy Report	Recommends the appointment of a Minister for AI in the Cabinet Office Role of minister should be based on 6 policy areas: data, infrastructure, skills, innovation & entrepreneurship, trade, and accountability	Privacy Explainability Accountability
Algorithms and artificial intelligence: report on the ethical issues ⁵⁰	2017	CNIL	Policy Report	Outlines founding principles of loyalty and continued attention and vigilance. Suggests policy recommendations and highlights major ethical concerns in AI	Discrimination, profiling, threat to rights

46 https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160391/TEMrap_47_2017_verkkojulkaisu.pdf?sequence=1&isAllowed=y

47 https://www.etui.org/sites/default/files/Foresight_Brief_02_EN.pdf

48 <https://www.rathenau.nl/en/digitale-samenleving/human-rights-robot-age>

49 https://www.biginnovationcentre.com/wp-content/uploads/2019/07/BIC_APPG-AI-2017-FINDINGS_6.12.2017.pdf

50 <https://www.cnil.fr/en/algorithms-and-artificial-intelligence-cnils-report-ethical-issues>



D3.1: Map of AI in policing innovation ecosystem and stakeholders

Artificial Intelligence, Robotics, Privacy and Data Protection ⁵¹	2016	EDPS	Policy Report	Presents topics within AI and robots and question for reflecting and discussion on data protection and privacy of these technologies	Data protection, privacy
Artificial Intelligence A European Perspective ⁵²	2018	European Commission		Outlines the history of AI and the use of AI in the EU, USA and China. Summarises diverse perspectives concerning AI	
Artificial Intelligence – The consequences of AI on the (digital) single market, production, consumption, employment and society ⁵³	2017	European Economic and Social Committee	Opinion	Series of conclusions and recommendations	Ethics, privacy, safety, transparency, accountability, equality
Statement on AI, Robotics and ‘Autonomous’ Systems ⁵⁴	2018	European Group on Ethics in Science and New Technologies	Policy statement	Call for common, internationally recognised ethical and legal framework for the design, use and governance of AI, robotics and autonomous systems	
European Civil Law Rules in Robotics ⁵⁵	2016	European Parliament	Report for JURI Committee	Evaluation and analysis from ethical and legal perspective of a number of future European civil law rules in robotics	

51 https://edps.europa.eu/sites/default/files/publication/16-10-19_marrakesh_ai_paper_en.pdf

52 <https://publications.jrc.ec.europa.eu/repository/handle/JRC113826#:~:text=We%20are%20only%20at%20the,opportunities%20to%20improve%20our%20lives.>

53 <https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/artificial-intelligence-consequences-artificial-intelligence-digital-single-market-production-consumption-employment-and>

54 <https://op.europa.eu/en/publication-detail/-/publication/dfbe62e-4ce9-11e8-be1d-01aa75ed71a1>

55 [https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU\(2016\)571379_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU(2016)571379_EN.pdf)



D3.1: Map of AI in policing innovation ecosystem and stakeholders

Report with recommendations on the Commission on Civil Law Rules on Robotics ⁵⁶	2017	European Parliament	Report	Series of recommendations concerning the Civil Law Rules on Robotics	
Understanding Artificial Intelligence ⁵⁷	2018	European Parliament	Policy Brief	Discussion of AI, limitations and issues with AI and new frameworks for the development of AI	Data privacy, inequality, autonomous decision making, impact on job market
The Malicious Use of AI: Forecasting, Prevention and Mitigation ⁵⁸	2018	Future of Humanity Institute et al.	Policy brief	Surveys potential security threats from the malicious use of AI technologies, and proposes ways to prevent and mitigate these threat with a series of recommendations	
AI: opportunities and implications for the future of decision making ⁵⁹	2016	Government Office for Science	Policy brief	Use of AI for innovation and productivity by government and the effects it poses on labour market, and new challenges posed by AI	
Growing the AI industry in the UK ⁶⁰	2017		Independent report	Series of recommendations to assist the growth of AI in the UK	
AI Sector Deal ⁶¹	2019	HM Government	Policy report	£1 billion package of support from the UK government and industry to boost the UK's global position as a leader in developing AI and related technologies	

56 https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_EN.html

57 [https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI\(2018\)614654](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2018)614654)

58 <https://arxiv.org/pdf/1802.07228.pdf>

59 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/566075/gs-16-19-artificial-intelligence-ai-report.pdf

60 <https://www.gov.uk/government/publications/growing-the-artificial-intelligence-industry-in-the-uk>

61 <https://www.gov.uk/government/publications/artificial-intelligence-sector-deal/ai-sector-deal>



D3.1: Map of AI in policing innovation ecosystem and stakeholders

Robotics and artificial intelligence ⁶²	2016	House of Commons	Policy report	General overview on the use and implementation of AI and robotics	
AI in the UK: ready, willing and able? ⁶³	2018	House of Lords	Policy report	Overview of AI, how it is designed and developed, mitigating risks of AI and a summary of conclusions and recommendations	
Ethically aligned design. A vision for prioritising human well-being with autonomous and intelligent systems ⁶⁴	2017	IEEE	Policy report	Advance public discussion about how we can establish ethical and social implementations for intelligent and autonomous systems and technologies and facilitate the emergence of national and global policies that align with these principles	
AI: Calling on Policy Makers to Take a Leading Role in Setting a Long-Term AI Strategy ⁶⁵	2017	IEEE European Policy Initiative	Policy report	Series of recommendations to target EU institutions, the member states' governments, and the involved agencies	
Big data, artificial intelligence, machine learning and data protection ⁶⁶	2017	Information Commissioner's Office	Policy report	Data protection implications of the AI, big data and machine learning and compliance tools	

62 <https://publications.parliament.uk/pa/cm201617/cmselect/cmsctech/145/14502.htm>

63 <https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf>

64 https://standards.ieee.org/wp-content/uploads/import/documents/other/ead_v2.pdf

65 <http://globalpolicy.ieee.org/wp-content/uploads/2017/10/IEEE17021.pdf>

66 <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>



D3.1: Map of AI in policing innovation ecosystem and stakeholders

AI for Good Global Summit Report 2017 ⁶⁷	2017	International Telecommunications Union	Global summit report	Platform for government official, UN agencies, NGO's, industry leaders and AI experts to discuss the ethical, technical, societal and policy issues related to AI	
Managing automation: Employment, inequality, and ethics in the digital age ⁶⁸	2017	Institute for Public Policy Research	Discussion Paper	Argues that public policy should seek to accelerate automation to reap the productivity benefits, while building new institutions to ensure the dividends of technological changes are broadly shared	
Finland's Age of Artificial Intelligence ⁶⁹	2017	Ministry of Economic Affairs and Employment	Policy report	Highlights Finland's possibilities in the global market along with its strengths and weaknesses in AI. Provides a range of policy actions and recommendations	
A Law on Robotics and Artificial Intelligence in the EU? ⁷⁰	2017	European Trade Union Institute ETUI	Foresight Brief	Strategic thinking about the future challenges of a law on robotics and AI in the EU	Visibility, accountability, liability
Human Rights in the Robot Age: Challenges arising from the use of robotics, AI and VR/AR ⁷¹	2017	Rathenau Institute	Report	Analysis of the challenges resulting from the use of AI, robotics, AR/VR and series of recommendations for the Parliamentary Assembly of the Council of Europe	
Top 10 Principles for ethical artificial	2017	UNI Global Union	Report	Outline of top principles for ethical AI	Transparency, biases, fundamental freedoms and rights

67 <https://www.itu.int/en/ITU-T/AI/Pages/201706-default.aspx>

68 <https://www.ippr.org/publications/managing-automation>

69 https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160391/TEMrap_47_2017_verkkojulkaisu.pdf?sequence=1&isAllowed=y

70 https://www.etui.org/sites/default/files/Foresight_Brief_02_EN.pdf

71 <https://www.rathenau.nl/en/digitale-samenleving/human-rights-robot-age>



D3.1: Map of AI in policing innovation ecosystem and stakeholders





intelligence, The future world of work ⁷²					
For a Meaningful Artificial Intelligence: Towards a French and European Strategy ⁷³	2018	Cedric Villani	Policy report	Overview of creating a meaningful AI across France and Europe	
Artificial Intelligence in Swedish business and society – summary ⁷⁴	2018	Vinnova	Policy report	Identify and analyse opportunities in the use of AI within business and public services in Sweden, development of Sweden's use of AI and AI skills in business and public services	

72 http://www.thefutureworldofwork.org/media/35420/uni_ethical_ai.pdf




73 https://www.aiforhumanity.fr/pdfs/MissionVillani_Report_ENG-VF.pdf

74 <https://www.vinnova.se/en/publikationer/artificial-intelligence-in-swedish-business-and-society/>

8.2 Annex B. EU-funded projects relating to AI in the security domain

Project	Project ID	Dates	Area	Technologies	Aim
	833635	2019-2022	Crime prevention/ Crime investigation	<ul style="list-style-type: none"> • Speech processing • Natural language processing • Video and geographical meta-data processing • Network analysis 	Facilitate the identification of criminals
	883297	2020-2023	Crime prevention/ Crime investigation	<ul style="list-style-type: none"> • Internet of Things • DARLENE cloud • Wearable Augmented Reality glasses 	Improve situational awareness when responding to criminal and terrorist activities
	720417	2017-2018	Crime prevention/ Crime investigation	<ul style="list-style-type: none"> • Situational awareness framework • Advanced content-based search • Search expansion tools 	Analyse video footage from heterogeneous surveillance video archives and efficiently identify and extract relevant information
	786629	2018-2021	Crime prevention/ Crime investigation	<ul style="list-style-type: none"> • Advanced correlation engine • Sophisticated representational model • Evidence collection platform 	Revolutionize the capacity of LEAs to deal with extreme volumes and diversity of data in order to accomplish highly- efficient crime

D3.1: Map of AI in policing innovation ecosystem and stakeholders






				<ul style="list-style-type: none"> • Threat prediction engine by semantic reasoning • Augmented intelligence tools 	prevention and investigation.
	833276	2019-2023	Crime prevention/ Crime investigation	<ul style="list-style-type: none"> • Big data analytics • Cognitive machine learning • Blockchain approaches • Knowledge discovery techniques 	Improve digital and forensic capabilities, and reduce the complexity and cost of cross-border collaboration
	883293	2020-2023	Crime prevention/ Crime investigation	<ul style="list-style-type: none"> • Extended reality technologies • Automated systems • Immersive AR/VR 	Equip investigators with cutting-edge tools to acquire, process, visualise and act upon enormous quantities of data with automated systems and instinctive interfaces and controls.
	83315	2019-2021	Crime prevention/ Crime investigation	<ul style="list-style-type: none"> • Visual intelligence modules • Data mining modules • Semantic fusion representation and fusion modules • Detection modules for cybercrime activities • Trends detection 	Provide LEAs with advanced, almost-real-time, analytical support for multiple Big Data streams. Build self-knowledge graphs. Organise use cases.



D3.1: Map of AI in policing innovation ecosystem and stakeholders

				<ul style="list-style-type: none"> Situational awareness and HMI modules 	
	10101222004	2021-2024	<p>Crime prevention/ Crime investigation</p>	<ul style="list-style-type: none"> Neural machine translations Speech-to-text video transcriptions Automatic content categorisation Network filtering and visualisation 	Identify, track and document illicit financial flows
	740688	2017-2020	Cyber-operations	<ul style="list-style-type: none"> Natural language processing Social network analysis Complex event processing Semantic media analysis Artificial intelligence 	Collect, process, visualize and store online terrorist group data for LEAs to take coordinated action in real-time while preserving the privacy of citizens
	883596	2020-2023	Cyber-operations	<ul style="list-style-type: none"> AI and deep learning techniques applied to big data analytics Automated data mining Extensive content extraction Information extraction and fusion Machine learning AI, predictive and visual learning 	Focus on cybercrime and terrorism by approaching specific issues related to LEAs using pioneering machine learning and artificial intelligence methods

D3.1: Map of AI in policing innovation ecosystem and stakeholders




 CC-DRIVER	883543	2020-2023	Cyber-operations	<ul style="list-style-type: none"> • Analysis automation • Data mining • Awareness tools 	Focus on the human factors behind juvenile cyber-delinquency and adolescent hacking
	101021808	2021-2024	Cyber-operations	<ul style="list-style-type: none"> • Accountable metrics • Verifications tools • System framework 	Address challenges of black box AI and data management in cybersecurity
	883341	2020-2023	Cyber-operations	<ul style="list-style-type: none"> • Semi-automated content analysis and prioritisation • Federal learning infrastructure 	Equip European LEAs with advanced analytical and investigative capabilities to respond to the spread of online child sexual exploitation material
 TRUST aWARE	101021377	2021-2024	Cyber-operations	<ul style="list-style-type: none"> • User-friendly tools • Collective intelligence • Security/privacy-by-design in software engineering 	Provide actionable intelligence and tools, offering mechanisms that protect citizens' freedom, security, and privacy to improve trust in software
		2019-2021	Cyber-operations	<ul style="list-style-type: none"> • Porn detection • Sexual organs detection 	Creation of a forensic analysis tools to assist LEAs







D3.1: Map of AI in policing innovation ecosystem and stakeholders

				<ul style="list-style-type: none"> • Intelligent text-based classification • Face detection with age estimation • Intelligent video summarising 	in combating child exploitation
	787120	2018-2021	Migration, asylum, and border management	<ul style="list-style-type: none"> • Person tracking re-identification • Data fusion and risk assessment • RFID luggage tracking • Real-time behavioural analysis • Passenger mobile app • OCULUS control and command centre • Crowd simulation and visualisation • Control and simulation VR platform • Web intelligence analysis • Security personnel mobile app 	Introduce a dynamic risk-based integrated Border security management across all border modalities, thus overcoming the current rule-based approach.






D3.1: Map of AI in policing innovation ecosystem and stakeholders

	653879	2015-2018	Migration, asylum, and border management	<ul style="list-style-type: none"> • Intelligent remote image processing • Video surveillance • Biometrics • Open-source intelligence • Crowdsourcing • Behavioural analysis and cognitive algorithms • Passenger mobile applications • RFID luggage tracking 	Develop and demonstrate an innovative integrated and end-to-end airport security process for passengers
	833704	2019-2022	Migration, asylum, and border management	<ul style="list-style-type: none"> • Biometric technologies • Thermal and multispectral imaging • Computer vision algorithms • Advanced morphed face detection algorithms through Convolutional Neural Networks • Smartphone applications • Deep Neural Networks 	Develop a set of tools and systems to address emerging threats in document and identity verification
	700626	2016-2019	Migration, asylum, and border management	<ul style="list-style-type: none"> • Face matching tool • Risk based assessment tool • Automatic deception detection tool • Document authenticity tool 	Create border control system that detects deception based on facial recognition technology and the measurement of micro-expressions





D3.1: Map of AI in policing innovation ecosystem and stakeholders

				<ul style="list-style-type: none"> • Biometrics • Mobile app • Border control analytics tool 	
	740593	2017-2021	Migration, asylum, and border management	<ul style="list-style-type: none"> • Radar network • Robotics • Biometrics • Multimodal sensors 	Develop and demonstrate a fully functional autonomous border surveillance system with unmanned mobile robots
	833672	2019-2022	LEA training	<ul style="list-style-type: none"> • Virtual reality 	Improve performance of European police officers by developing VR enhanced training
	832735	2019-2022	Administration of justice	<ul style="list-style-type: none"> • Blockchain technology • Cloud and mobile forensics 	Digital evidence for juridical decisions
	832800	2019-2022	Administration of justice	<ul style="list-style-type: none"> • Mobile forensics 	Reviews current mobile forensics and assess requirements of LEAs
	101004949	2018-2020	AI, Ethics and Law		Bring moral values to the forefront in field of advanced digitisation

D3.1: Map of AI in policing innovation ecosystem and stakeholders

	741716	2017-2021	AI, Ethics and Law		Ethical issues in technology areas of human genomics, human enhancement, and human-machine interaction
	313062	2013-2014	AI, Ethics and Law		Analysis of good practice to take to account for the societal dimensions of security research
	101020574	2021-2024	AI, Ethics and Law		Unite European actors who have concerns about AI, law enforcement and policing to discuss how to enhance Europe's security
	101021797	2021-2025	AI, Ethics and Law		Increase awareness, adoption and long-term results of AI applications in European LEAs
	786993	2018-2021	AI, Ethics and Law	<ul style="list-style-type: none"> • Keyword based refined search • Keyword based automated search • Multi-purpose web crawler • Content Database System • Face extraction and matching 	Develop, test, train and evaluate a new privacy preserving intelligence analysis for resolving identities system prototype

D3.1: Map of AI in policing innovation ecosystem and stakeholders

				• Graph visualisation	
	241918	2010-2014	AI, Ethics and Law		Improve planning and executive of change initiatives in the police
	700281	2016-2018	AI, Ethics and Law		Community for sharing experiences in the use of social media for public security
	815356	2018-2020	AI, Ethics and Law		Establish an overarching concept where tools, technology, training, and field demonstrations will lead to situational awareness and improve direct responses to secure public places in a terrorist threat
	786641	2018-2021	AI, Ethics and Law		Analysis of how AI and big data analytics impact ethics and human rights

8.3 Annex C. Stakeholders by category

RESEARCH ORGANISATIONS	
Name of stakeholder	Country
AIT Austrian Institute of Technology GMBH	Austria
Software Competence Center Hagenberg	Austria
USECON – The Usability Consultants GmbH	Austria
Vienna Centre for Societal Security	Austria
Institute for Sociology of Law and Criminology	Austria
National Institute for Criminalistics and Criminology	Belgium
Defence Institute “Professor Tsvetan Lazarov”	Bulgaria
Additess Advanced Integrated Technology Solutions and Services Ltd	Cyprus
Stremble Ventures Ltd	Cyprus
European Organisation for Security	Europe
VTT - Technical Research Centre of Finland	Finland
Protection Avancee contre le Recel	France
Privanova SAS	France
Histoire et Sources des Mondes Antiques	France
French Alternative Energies and Atomic Energy Commission	France
Centre National de la Recherche Scientifique CNRS	France
Aegis IT Research GMBH	Germany
Cybercrime Research Institute GMBH	Germany
Fraunhofer Society	Germany
Fraunhofer Institute for Telecommunications	Germany
Fraunhofer Institute for High Frequency Physics and Radar Techniques	Germany
Fraunhofer Institute of Optronics, System Technologies and Image Exploitation	Germany
ZITIS - Central Office for Information Technology in the Security Sector	Germany
Hamburg-Consult Gesellschaft fur Verkehrsberatung	Germany
German Research Centre for Artificial Intelligence	Germany
KEMEA – Kentro Meleton Asfaleias	Greece
ICCS - Institute of Communications and Computer Systems	Greece
CERTH - The Centre for Research and Technology, Hellas	Greece
Foundation for Research and Technology	Greece
National Center for Scientific Research Demokritos	Greece
EKETA - Ethniko Kentro Erevnasd Kai Technologikis Anaptyxis	Greece
Athena Research & Innovation Center	Greece

D3.1: Map of AI in policing innovation ecosystem and stakeholders

Institute of Chemical Engineering Sciences	Greece
Maeven Seven Solutions Zartkoruen Mukodo Reszvenytarsasag	Hungary
United Technologies Research Centre Ireland	Ireland
Trilateral Research Ltd	Ireland
Interdisciplinary Center Herzliya	Israel
C.G. Smartech	Israel
Consiglio Nazionale delle Ricerche	Italy
ABI Lab Centro di ricerca e innovazione per la banca	Italy
NATO Science & Technology Organization (STO) Centre for Maritime Research & Experimentation	Italy
Fondazione Links - Leading Innovation & Knowledge for Society	Italy
Centro Europeo di Psicologia Investigazione e Criminologia	Italy
FORMIT	Italy
Baltic Institute of Advanced Technology	Lithuania
Lithuanian Cybercrime Centre of Excellence for Training, Research and Education	Lithuania
TNO – Netherlands Organisation for Applied Scientific Research	Netherlands
Industrial Research Institute for Automation and Measurements PIAP	Poland
SIRC SP ZOO	Poland
Polska Platforma Bezpieczeństwa Wewnętrznego	Poland
CTTC - Centre Tecnològic de Telecomunicacions de Catalunya	Spain
Fundacion Centro de Tecnologias de Interaccion Visual y Comunicaciones Vicomtech	Spain
Telefonica Investigacion y Desarrollo	Spain
Instituto Tecnológico de Informatica	Spain
INCIBE	Spain
IMDEA Networks Institute	Spain
EVERIS	Spain
Telefonica Investigacion y Desarrollo	Spain
Totalforsvarets Forskningsinstitut	Sweden
Fondation de l'Institut de Recherche IDIAP	Switzerland
Trilateral Research Ltd	UK
Information Catalyst for Enterprise	UK
CENTRIC - Centre of Excellence in Terrorism, Resilience, Intelligence & Organised Crime Research	UK
Innova Integra Limited	UK

D3.1: Map of AI in policing innovation ecosystem and stakeholders

UNIVERSITIES	
Stakeholder name	Country
Katholieke Universiteit Leuven	Belgium
University of Antwerp	Belgium
Vrije Universiteit Brussel	Belgium
Federal University of Rio de Janeiro	Brazil
Dalian University of Technology	China
University of Central Lancashire Cyprus	Cyprus
Vysoke Uceni Technicke v Brne	Czechia
University of Masaryk	Czechia
University of Tartu	Estonia
Leibniz Universitat Hannover	Germany
Universitat des Saarlandes	Germany
Centre for Security and Society	Germany
Embry-Riddle Europe	Germany
Ruprecht-Karls-Universität Heidelberg	Germany
Hochschule fur den Offentlichen Dienst in Bayern	Germany
University of Hannover	Germany
Technical University of Berlin	Germany
Hochschule Mittweida	Germany
Technische Universitat Berlin	Germany
National and Kapodistrian University of Athens	Greece
University of Athens	Greece
Ionian University	Greece
Eotvos Lorand Tudomanyegyetem	Hungary
University College Dublin	Ireland
Military University of Technology	Ireland
Universita Cattolica del Sacro Cuore	Italy
National Interuniversity Consortium for Telecommunications	Italy
University of Padova	Italy
University of Milan	Italy
Krygyz Technical University	Kyrgyzstan
SECAN Lab Research Group	Luxembourg

D3.1: Map of AI in policing innovation ecosystem and stakeholders

University of Malta	Malta
University of Groningen	Netherlands
Vrije Universiteit Amsterdam	Netherlands
University of Twente	Netherlands
Erasmus University Rotterdam	Netherlands
Utrecht University	Netherlands
Delft University of Technology	Netherlands
Maastricht University	Netherlands
Universiteit van Tilburg	Netherlands
University St Kliment Okridski Bitola	North Macedonia
Norwegian University of Sciences and Technology	Norway
National University of Ireland Maynooth	Poland
Military University of Technology	Poland
Universidade Nova de Lisboa	Portugal
TEKEVER	Portugal
Babes-Bolyai University	Romania
University of Cape Town	South Africa
Universitat Politecnica de Valencia	Spain
Universidad de Leon	Spain
Universidad Carlos III de Madrid	Spain
University of Granada	Spain
Universidad Politecnica de Madrid	Spain
Universidad Autonoma de Barcelona	Spain
Fundacion Esade	Spain
Linkopings Universitet	Sweden
Uppsala University	Sweden
University of Lausanne	Switzerland
IoT Lab	Switzerland
Queen Mary University of London	UK
Aston University	UK
City University of London	UK
Birmingham City University	UK
Sheffield Hallam University	UK
University of East London	UK
University of Reading	UK

D3.1: Map of AI in policing innovation ecosystem and stakeholders

Manchester Metropolitan University	UK
King's College London	UK
University of Stirling	UK
University of Durham	UK
University of Sheffield	UK
Coventry University	UK
London Metropolitan University	UK
The University of Warwick	UK
De Montfort University	UK

ICT AND SOFTWARE COMPANIES	
Stakeholder name	Country
Hensoldt Analytics GMBH	Austria
European Dynamics Belgium SA	Belgium
Inlecom Group	Belgium
V-ICT-OR	Belgium
MOTIVIAN Bulgaria	Bulgaria
IOTAM Internet of Things Applications and Multi Layer Development Ltd	Cyprus
eBOS Technologies Limited CY	Cyprus
Catalink Limited	Cyprus
Ianus Consulting Ltd	Cyprus
Phonexia SRO	Czechia
Lingea Sro	Czechia
F-SECURE OYJ	France
Capgemini Technology Services	France
ICTS	France
THALES	France
Microwave Characterization Center	France
HGH Systemes Infrarouges	France
Systems Factory	France
Montimage	France
RAYTRIX GmbH	Germany
VERIDOS GMBH	Germany

D3.1: Map of AI in policing innovation ecosystem and stakeholders

Institut fur musterbasierte Prognosetechik	Germany
NEC Laboratories Europe	Germany
Ellectronica GmbH	Germany
COPTING GmbH	Germany
Munich Innovation Labs GMBH	Germany
Infil	Greece
EXODUS S.A.	Greece
IMC Technologies	Greece
Space Hellas S.A.	Greece
Synelixis Solutions SA	Greece
Nydor Systimata Technologies Anonymos Etairia	Greece
SingularLogic	Greece
Biosec Group KFT	Hungary
Sindice Limited	Ireland
Intu-View LTD	Israel
Elbit Systems Ltd	Israel
EMZA	Israel
Youbiquo	Italy
Engineering Ingegneria Informatica SpA	Italy
Pluribus One SRL	Italy
Rina Consulting SpA	Italy
Zanasi & Partners	Italy
Innovation Engineering SRL	Italy
Neurosoft	Italy
Lutech Spa	Italy
Synthema Artificial Intelligence	Italy
Regula Baltija SIA	Latvia
Tilde Sia	Latvia
Proflow GMBH	Malta
RE-liON Group B.V.	Netherlands
Netherlands Forensic Institute	Netherlands
CFLW Cyber Strategies BV	Netherlands
Stichting Dutch Institute for Technology, Safety & Security	Netherlands
Web-IQ BV	Netherlands
Brainport Eindhoven	Netherlands

D3.1: Map of AI in policing innovation ecosystem and stakeholders

ITTI Sp ZOO	Poland
JAS Technologie SP	Poland
Voiceinteraction – Tecnologias de Processamento de Fala	Portugal
OceanScan - Marine Systems & Technology	Portugal
INOV	Portugal
Bitdefender SRL	Romania
SIMAVI – Software, Imagination & Vision S.R.L.	Romania
Maniflux	Serbia
Semantika	Slovenia
XLAB	Slovenia
Eurob Creative	Spain
Insikt Intelligence S.L.	Spain
Expert System Iberia SL	Spain
EVERIS Aeroespacial y Defensa SL	Spain
Acciona Construccion SA	Spain
ETRA Investigacion y Desarrollo	Spain
Vicomtech	Spain
Tree Technology SA	Spain
Everis Aerospace, Defense and Security	Spain
Robotnik Automation SLL	Spain
Advanced Model Solutions SA	Spain
Herta Security	Spain
Micro Systemation AB	Sweden
APSS Software & Services	Switzerland
OVD Kinegram AG	Switzerland
Swiss Center for Electronics and Microtechnology SA	Switzerland
Venaka Media	UK
ICTS UK	UK
CBRNE Ltd	UK
Cyberlense LTD	UK
A E Solutions Limited	UK

D3.1: Map of AI in policing innovation ecosystem and stakeholders

LAW ENFORCEMENT AGENCIES		
Stakeholder name	Level	Country
INTERPOL	International	France
EUROPOL	Europe	Netherlands
Belgian Federal Police	National	Belgium
Cyprus Police	National	Cyprus
Policejní Prezidium České Republiky	National	Czech Republic
Central Directorate of the Judicial Police	National	France
Bundespolizei	National	Germany
North Rhine-Westphalia Police Force (LAFP NRW)	State	
Polizeiprasidium München	Local	
Berlin Police		
Hellenic Police	National	Greece
Piraeus Port Authority	Local	
Hungarian National Police	National	Hungary
An Garda Síochána	National	Ireland
Latvian State Border Guard	National	Latvia
Lithuanian Police	National	Lithuania
State Border Guard Service		
Malta Police	National	Malta
Serviciul de Protecție și Pază de Stat	National	Moldova
The National Police of the Netherlands	National	Netherlands
Royal Netherlands Marechaussee		
Brussels Police		
Komenda Główna Policji	National	Poland
Border Guard of the Republic of Poland	State	
Provincial Police Headquarters in Poznań		
Komenda Wojewódzka Policji w Bydgoszczy	Local	
Policia Judiciária	National	Portugal

D3.1: Map of AI in policing innovation ecosystem and stakeholders

Policia Seguranca Publica	National	Romania
Guarda Nacional Republicana		
Politia Romana		
Serviciul de Protectie si Paza		
Inspectoratul General al Politiei Romane		
Guardia Civil	National	Spain
Cuerpo Nacional de Policia		
Policia Municipal de Sabadell		
Policia Local Valencia	Local	
Policia Local Malaga		
Swedish Police Authority	National	Sweden
Police Service of Northern Ireland	National	UK
Special Operations (SO15) Counter-Terrorist Command		
West Midlands Police and Crime Commissioner		

POLICE ACADEMIES	
Stakeholder name	Country
European University Cyprus	Cyprus
Estonian Academy of Security Sciences	Estonia
Ecole Nationale Superiere de la Police	France
University of Applied Sciences for Public Administration and Legal Affairs in Bavaria	Germany
Bradenburg State Police Academy and College	
LSOP	Netherlands
Higher Police School	Poland

GOVERNMENT AND PUBLIC BODIES		
Stakeholder name	Level	Country
European Forum for Urban Security	European	Europe
Austrian Standards International	National	Austria
Ministry of Interior		

D3.1: Map of AI in policing innovation ecosystem and stakeholders

Directorate General Crisis Centre of the Belgian Federal Public Service	National	Belgium
Institut National de Criminologie et de Criminologie		
Campus Vesta APB - Autonom Provinciebedrijf	State	
Ministry of Interior	National	Croatia
Police and Border Guard Board	National	Estonia
Tax and Customs Board		
National Bureau of Investigation	National	Finland
Ministry of Interior	National	France
ZITIS - Central Office for Information Technology in the Security Sphere	National	Germany
Bavarian Ministry of Interior, Sport, and Integration		
Independent Authority for Public Revenue	National	Greece
Ministry of Maritime Affairs and Insular Policy		
Hellenic Ministry of Defence		
Ministry of Public Security	National	Israel
Direzione Centrale Anticrimine della Polizia di Stato	National	Italy
Ministry of Interior		
North Tyrrhenian Sea Port System Authority		
Lithuanian Forensic Science Center	National	Lithuania
Financial Crime Investigation Service		
State Protection and Guard Service	National	Moldova
Ministry of Justice and Security	National	Netherlands
Immigration and Naturalization Service		
Norwegian Ministry of Justice and Public Safety	National	Norway
Ministry of Justice	National	Portugal

D3.1: Map of AI in policing innovation ecosystem and stakeholders

Ministry of Internal Affairs	National	Romania
Protection and Guard Service		
Ministry of Internal Affairs	National	Serbia
Ministry of Interior	National	Spain
Gobierno Vasco - Departamento Seguridad	State	
Ayuntamiento de Madrid	Local	
Ayuntamiento de Valencia		
Swedish Defence Research Agency	National	Sweden
UK Home Office	National	UK
DSTL - Defence Science and Technology Laboratory		
Police and Crime Commissioner for Thames Valley		

NATIONAL AND LOCAL AUTHORITIES		
Stakeholder name	Level	Country
Stad Antwerpen	State	Belgium
City of Larissa	City	Greece
City of Vilnius	City	Lithuania
City of Brasov	City	Romania

NOT-FOR-PROFIT AND ADVOCACY ORGANISATIONS	
Stakeholder name	Country
Michael Culture Association	Belgium
E-Seniors Association	France
Malta Information Technology Law Association	Malta
Stichting CUING Foundation	Netherlands
Portuguese Association of Victim Support	Portugal
Pravo I Internet Foundation	Romania
Fundacion Andaluza para el Desarrollo Aeroespacial	Spain
Fundacion Cibervoluntarios	

D3.1: Map of AI in policing innovation ecosystem and stakeholders

Tax Justice Network	UK
---------------------	----

AUDIT/CONSULTANCY ORGANISATIONS	
Stakeholder name	Country
CIN Consult Unternehmensberatungs GMBH	Austria
VLTN GCV	Belgium
Time.Lex	
PAWA	Poland
CBRNE Ltd	UK

SUPPLIERS AND END USERS	
Stakeholder name	Country
Airbus Defence and Space SAS	France
CS Group France	
TrainOSE	Greece
IDS Ingegneria dei Sistemi SPA	Italy
Luxembourg Findel Airport	Luxembourg

PROJECT SPECIFIC PARTNERS		
Stakeholder name	Expertise	Country
Systran SA	Translation	France
Privanova	Information security	
Strane Innovation	Sustainable development	
Fondazione Mondo Digitale	Private law body	Italy
Netherlands Forensic Institute		Netherlands
Royal Schipol Group		
InfoCons Association	Private Law Association	Romania
Australo	Marketing services for research	Spain
Finopz Ltd	Financial Operations	UK
Information Security Forum Ltd	Information security	

D3.1: Map of AI in policing innovation ecosystem and stakeholders

CIVIL SOCIETY STAKEHOLDERS				
Name	Type of stakeholder	Country	What they do	Website
Amnesty International	NGO	International	Human rights	https://www.amnesty.org/en/
Liberty	NGO	UK	Challenge injustice, defends freedom and campaigns to make sure everyone in the UK is treated fairly	https://www.libertyhumanrights.org.uk/
Fair Trials	NGO	UK	Global criminal justice watchdog, campaigning for fairness, equality and justice	https://www.fairtrials.org/
European Digital Rights	Advocacy group	Europe	Civil and human rights organisations across Europe	https://edri.org/
Access Now	NGO	International	Defend and extend the digital rights of users at risk around the world	https://www.accessnow.org/
AlgoRace	Entity	Spain	Analyse and propose suggestions to decrease discrimination and racial inequality in AI and automated decision systems	https://algorace.org/
AlgoRights	Collaborative network	Spain	Defend human rights in the field of AI	http://www.algorights.org/
AlgorithmWatch	Non-profit research and advocacy organisation	Europe	Watches, unpacks and analyses automated decision-making systems and their impact on society	https://algorithmwatch.org/en/
Algorithmic Justice League	Independent organisation active on algorithmic bias	US	Raise awareness and activism on the algorithmic bias threats to society	https://ajl.org/
Big Brother Watch	Non-profit civil liberties and privacy campaigning organisation	UK	Reclaim privacy and defend freedoms in relation to intelligent surveillance systems	https://bigbrotherwatch.org.uk/
Bits of Freedom	Digital rights foundation	Netherlands	Privacy and communications freedom in the digital age	https://www.bitsoffreedom.nl/
Bulgarian Helsinki Committee	NGO	Bulgaria	Protection and promotion of human rights in Bulgaria	https://www.bghelsinki.org/en/

D3.1: Map of AI in policing innovation ecosystem and stakeholders

Centre for European Constitutional Law – Themistokles and Dimitris Tsatsos Foundation	Non-profit research organisation	Greece	Aims to contribute to the promotion of democratic institutions and the welfare state under the rule of the law, the deepening of European integration and the strengthening of international cooperation with respect for the cultural identity of each state	https://www.cecl.gr/en/
Citizen D	NGO	Slovenia	Inclusive promotion of human and digital rights	https://www.drzavljand.si/en/
Civil Rights Defenders	International human rights organisation	Sweden	Defends people's civil and political rights	https://crd.org/
Controle Alt Delete	Independent organisation	Netherlands	Committed to fair and effective law enforcement and activism against ethnic profiling and disproportionate violence	https://controlealtdelete.nl/
Council of Bars and Law Societies of Europe (CCBE)	Non-profit association	Europe	Advance the views of European lawyers and defend legal principles upon which democracy and the rule of law are based	https://www.ccbe.eu/
De Moeder is de Sleutel	Self-help organisation	Netherlands	Parent group which allows parents to be heard and advice on how to offer support to their children	https://demoederisdesleutel.nl/
Digital Fems	Entity	Spain	Design projects that increase the presence of women in technological environments	https://www.digitalfems.org/
Electronic Frontier Norway	Non-profit digital rights organisation	Norway	Working for digital rights such as freedom of speech, privacy, freedom from surveillance, open standards, etc.	https://efn.no/
European Centre for Not-for-Profit Law (ECNL)	NGO	Netherlands	Aims to create legal and policy environments that enable individuals, movements and organisations to exercise and protect their civic freedoms	https://ecnl.org/
European Criminal Bar Association (ECBA)	Association of independent specialist defence lawyers	Europe	Promote fundamental rights of persons under criminal investigation, suspects, accused and convicted persons	https://www.ecba.org/content/

D3.1: Map of AI in policing innovation ecosystem and stakeholders

European Disability Forum (EDF)	NGO	Belgium	Defends the interests of persons with disabilities in Europe	https://www.edf-feph.org/
European Network Against Racism (ENAR)	NGO	Europe	Combats racism, racial discrimination and xenophobia	https://www.enar-eu.org/
European Sex Workers Alliance (ESWA)	Sex worker-led network	Europe	Ensure that voices of sex workers in the region are heard, listened to and respected and raise awareness about the social exclusion of sex workers	https://www.eswalliance.org/eswa_members
Equinox Initiative for Racial Justice	Coalition of racial and social justice leaders and organisations	Europe	Working to advance rights and justice for all people in Europe	https://www.equinox-eu.com/
Equipo de Implementación España Decenio Internacional Personas Afrodescendientes	Campaign group	Spain	Promotes social, economic, political and cultural rights of persons of African descent in Spain	https://africandescent.org/
Éticas Foundation	Non-profit organisation	Spain	Address challenges around data, society and responsible innovation	
Fundación Secretariado Gitano	NGO	Spain	Provides services for the deployment of the Roma community in Spain and Europe	https://www.gitanos.org/
Ghett'Up	Network of young actors of change	France	Create conditions for young people from working class neighbourhoods to develop, fulfill themselves and take their place in society	https://ghettup.fr/
Greek Helsinki Monitor	NGO	Greece	Monitors, publishes, lobbies and litigates on human and minority rights and anti-discrimination	https://greekhelsinki.wordpress.com/
Helsinki Foundation for Human Rights	Human rights organisation	Poland	Promote the development of a culture based on respect of freedom and human rights in Poland and abroad	https://www.hfhr.pl/
Homo Digitalis	Civil organisation	Greece	Protection of internet users in Greece	https://www.homodigitalis.gr/en
Human Rights Watch	NGO	International	Defend human rights	https://www.hrw.org/

D3.1: Map of AI in policing innovation ecosystem and stakeholders

International Committee of Jurists	NGO	International	Grupo of eminent jurists who work to develop national and international human rights standards through the law	https://www.icj.org/
Irish Council for Civil Liberties	NGO	Ireland	Support civil liberties and human rights of people in Ireland	iccl.ie
Iuridicum Remedium (IuRe)	NGO	Czech Republic	Promote human rights	https://www.iure.org/
Ligue des Droits Humains	NGO	Belgium	Observe, defend and promulgate human rights	https://www.liguedh.be/
Novact	NGO	Spain	Support non-violent movements in the promotion of peace, the defence of human rights and social transformation	https://novact.org/
Observatorio de Derechos Humanos y Empresas en la Mediterránea (ODHE)	Applied research organisation	Spain	Human rights of those in conflict in the Mediterrean	http://www.odhe.cat/es/
Open Society European Policy Institute	Advocacy group	Europe	Influence and inform decision-making on EU laws, policy, funding, and external action to maintain and promote open societies	https://www.opensocietyfoundations.org/
Panoptykon Foundation	NGO	Poland	Defend basic freedom and human rights against threat posed by the development of modern surveillance technologies	https://en.panoptykon.org/
PICUM	NGO	Europe	Promote social justice and respect for the human right of undocumented migrants	https://picum.org/
Refugee Law Lab	Research and advocacy group	Canada	Impact of new legal technologies on refugees, other displaced communities and people on the move	https://refugeelab.ca/
Rights International Spain	NGO	Spain	Defend civil rights and liberties	http://www.rightsinternationalspain.org/
Statewatch	Non-profit organisation	Europe	Monitors civil liberties and other issues in EU and encourages investigative reporting and research	https://www.statewatch.org/

D3.1: Map of AI in policing innovation ecosystem and stakeholders

ZARA – Zivilcourage und Anti-Rassismus-Arbeit	NGO	Austria	Promote civil courage and a racism-free society in Austria	https://www.zara.or.at/de
Frontex	European Border and Coast Guard Agency	Poland	Border control of the European Schengen Area	https://frontex.europa.eu/
European Parliamentary Research Service	Research department of European Parliament	Europe	Provide objective and authoritative analysis of policy issues relating to the EU	https://www.europarl.europa.eu/at-your-service/en/stay-informed/research-and-analysis
Article19	International human rights organisation	International	Defend and promote freedom of expression and freedom of information worldwide	https://www.article19.org/
Chaos Computer Club	Association of hackers	Germany	Provide information about technical and societal issues such as surveillance, privacy, freedom of information, data security, etc.	https://www.ccc.de/en
Defesa dos Direitos Digitais	Non-profit association	Portugal	Defend digital rights	https://direitosdigitais.pt/
Digital Courage	Privacy and digital rights organisation	Germany	Campaigns for civil and human rights, consumer protection, privacy, freedom of information and related issues	https://digitalcourage.de/en
epicenter.works	Civil organisation	Germany	Protects data and privacy	https://epicenter.works/
Hermes - Center for Transparency and Digital Human Rights	Civil rights organisation	Italy	Promotes the awareness of transparency, accountability, freedom of speech online and the protection of rights and personal freedoms in a connected world	https://www.hermescenter.org/
IPVM	Independent organisation in the field of video surveillance	US	Provide information and advocacy on ethical practices. Digital surveillance technology and human rights abuses	https://ipvm.com/
IT Political Association of Denmark	NGO	Denmark	Collect information on It and convey to politicians and society to get the best possible grounds for legislation	https://itpol.dk/
Ireland-Palestine Solidarity Campaign	NGO	Ireland	Argue that the Irish and Northern Irish police should not collaborate with the Israeli police in the EU-funded ROXANNE project due to the political situation in Palestine	https://www.ipsc.ie/action-item/stop-gardai-psni-collaboration-with-israels-ministry-of-death-torture-and-racism

D3.1: Map of AI in policing innovation ecosystem and stakeholders

La Quadrature du Net	Advocacy group	France	Promote digital rights and freedoms of its citizen	https://www.laquadrature.net/en/
Civil Liberties Union for Europe	Human rights watchdog organisation	Europe	Promote basic human rights and freedoms	https://www.liberties.eu/en
Metamorphosis	NGO	North Macedonia	Strengthens awareness and capacity of citizens and civil society so they can take on the best possible role as activists for democracy	https://metamorphosis.org.mk/
NetBlocks	Private business	Turkey	Focuses on digital rights, cybersecurity, and internet governance	https://netblocks.org/
Privacy International	NGO	UK	Defends and promotes the right to privacy across the world	https://privacyinternational.org/
SHARE foundation	Non-profit organisation	Serbia	Advance human rights and freedoms online and promote positive values of an open and decentralised internet	https://www.sharefoundation.info/en/
All Out	NGO	International	Political advocacy for human rights of LGBTQIA+ communities	https://allout.org/en
Aquilenet	Free internet platform	France	Defend the culture of a local internet that promotes sharing and is open and neutral	https://www.aquilenet.fr/
Associazione Luca Coscioni	NGO	Italy	Promote civil liberties and human rights	https://www.associazionelucacoscioni.it/
Ban Facial Recognition Europe	Petition	Europe	Campaigns for the permanent ban of Facial Recognition used for Identification and profiling in Europe.	https://ban-facial-recognition.eu/
Certi Diritti	Non-profit organisation	Italy	Promote and protect civil rights and equal rights of LGBTI people	https://www.certidiritti.org/
Italian Coalition for Civil Liberties and Rights	Network of civil society organisations	Italy	Protect and expand the rights and liberties of all through advocacy, public education and legal action	https://cild.eu/en/
Danes Je Nov Dan	NGO	Slovenia	Nurture critical thinking among society	https://danesjenovdan.si/
DataPanik	Advocacy group	Netherlands	Critical of surveillance and control, concerns over rights	https://www.datapanik.org/over-ons/

D3.1: Map of AI in policing innovation ecosystem and stakeholders

			and rights by increasing surveillance	
Digitale Freiheit	Independent organisation	Germany	Promotes data protection and criticises surveillance	https://digitale-freiheit.jetzt/
EFN - Elektronisk Forpost Norge	Electronic civil rights organisation	Norway	Fights for civil rights in a digital rights	https://efn.no/
European Digital Society	Association	Europe	Empower European citizens through a more ethical, inclusive and sustainable European digital ecosystem	https://europeandigitalsociety.org/
Eumans!	Citizens and activists	Europe	Advocate for socially and democratically sustainable EU policies	https://www.eumans.eu/
Fight for the Future	Non-profit advocacy group	US	Advocates for digital privacy	https://www.fightforthefuture.org/
FIFF	Forum	Germany	Computer scientists raises concerns about technology	https://www.fiff.de/
Germanwatch	NGO	Germany	Influence public policy on trade, the environment, and relations between countries in the industrialised north and underdeveloped south	https://www.germanwatch.org/en
German acm Chapter	Specialist society for computer science	Germany	Promote of networking and exchange of knowlegde between computer scientists	https://germany.acm.org/
Gong	NGO	Croatia	Promotion and protection of human rights	https://gong.hr/en/
Hellenic Association of Data Protection & Privacy	NGO	Greece	Communicate and promote ongoing issues of data protection, privacy and security	https://www.dataprotection.gr/
Hellenic League for Human Rights	Human rights organisation	Greece	Advocacy for human rights and freedoms	hlhr.gr/en/
Info.nodes	Advocacy group	Estonia	Supports journalists and activists to expose the truth and promote effective social changes	https://www.infonodes.org/#campagne
Kameras Stoppen	Initiative	Germany	Campaign against police video surveillance in Cologne	https://kameras-stoppen.org/
Digital Guerilla	Consultancy	UK	Ensure use of digital tehcnology improved through training, educaiton and support	https://digital-guerrilla.scot/

D3.1: Map of AI in policing innovation ecosystem and stakeholders

Ministry of Privacy	Privacy activist watchdog	Netherlands	Spread the word about the importance of privacy	https://ministryofprivacy.eu/
Privacy Network	Non-profit organisation	Italy	Promote privacy, data protection and digital rights of individuals	https://www.privacy-network.it/
Progetto Winston Smith	Informational and operational project	Italy	Promote privacy and security	https://www.winstonsmith.info/
Science for Democracy	Platform	Belgium	Promote the right to science as a structural component of liberal democracies	https://sciencefordemocracy.org/
Strali	NGO	Italy	Promotes the protection of rights in the judicial system	https://www.strali.org/
Stop Wapenhandel	Independent research and campaign organisation	Netherlands	Opposes arms trade and the arms industry	https://stopwapenhandel.org/
The Good Lobby	Non-profit association	Italy	Equalise access to power for a more plural, inclusive and democratic society	https://www.thegoodlobby.eu/about/
UNI - Global Union Europa	European services workers union	Europe	Gives workers a platform and voice	https://www.uni-europa.org/
unsurv	Website	Germany	Exposes offline surveillance and tracking	https://unsurv.org/
WASP-HS	Swedish National Research Programme	Sweden	Research challenging AI with investments on researching humanities	https://wasp-hs.org/
Xnet	Activists and experts	Spain	Propose advanced solutions in different areas related to digital rights and democracy	https://xnet-x.net/es/
JUSOS	Volunteer youth organisation of the Social Democratic Party	Germany	Campaign for diverse society issues and movements	https://jusos.de/
Belgian Supervisory Board for Police Information	Autonomous federal parliamentary body	Belgium	Monitor the management of police information and data controller for the police services	https://www.contrôleorgaan.be/en#
Piratenpartei Deutschland	Political Party	Germany	Shape digital revolution	https://www.piratenpartei.de/
Piratska Stranka	Political Party	Slovenia	Respect human rights, privacy and data protection, free internet, government and political transparency	https://piratskastranka.si/

D3.1: Map of AI in policing innovation ecosystem and stakeholders

The Greens/EFA in the European Parliament	Political Group of the European Parliament	Europe	Green and regionalist political parties	https://www.greens-efa.eu/en/
MEP Patrick Beyer	Member of Parliament	Germany	Greens/EFA	https://www.patrick-breyer.de/en/
MEP Marcel Kolaja	Member of Parliament	Czechia	Greens/EFA	https://www.kolaja.eu/en/
MEP Anne-Sophie Pelletier	Member of Parliament	France	The Left	https://left.eu/people/anne-sophie-pelletier/
MEP Kateřina Konečná	Member of Parliament	Czechia	The Left	https://left.eu/people/kateina-konechna/
MEP Sophia in 't Veld	Member of Parliament	Netherlands	Renew Europe	https://www.sophieintveld.eu/nl/sophie-in-t-veld
Margrethe Vestager	European Commission Vice President for Digital Police	Netherlands		https://ec.europa.eu/commission/commissioners/2019-2024/vestager_en
Rop Gonggrip	Hacker and activist	Netherlands		
Dr Vera Wilde	Expert on lie detection	US		

-----End of Document-----