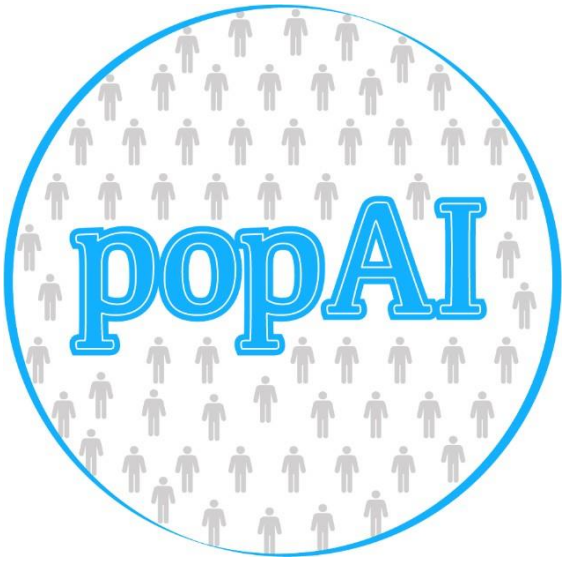


A European Positive Sum Approach towards AI tools in support of Law Enforcement and safeguarding privacy and fundamental rights

D3.3: Citizen produced priorities and recommendations for addressing AI in the security domain

Grant Agreement ID	101022001	**Acronym**	popAI
Project Title	A European Positive Sum Approach towards AI tools in support of Law Enforcement and safeguarding privacy and fundamental rights		
Start Date	01/10/2021	**Duration**	24 Months
Project URL	https://www.pop-ai.eu		
Document date	27/04/2023		
Nature	R = Document, report	**Dissemination Level**	PU = Public
Author	Simeon Stoyanov (ECAS)		
Contributors	Francesca Trevisan (Eticas), Pinelopi Troullinou (TRI), Claire Morot-Sir (ECAS), Anthoula Bania (Hellenic Police), Aikaterini Lefkaditi, Anastasios Drosou (CERTH/ITI), Dimitris Kyriazanos (NCSRD)		
Reviewers	Francesca Trevisan (Eticas), Andreas Ikonomopoulos, Dimitris Kyriazanos (NCSRD)		

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

Executive Summary

This deliverable presents the work and results of three different methods of engaging and understanding citizens in the context of AI systems used in the security domain – ethical social listening, social sending (social media listening) and crowdsourcing.

Based on previous research under the popAI project, the three activities focused on five categories of AI– Biometric identification, AI systems used to prevent crime (predictive policing), AI systems used in cyberoperations, Police hacking and Decision-making tools. The categories are broken downin subcategories that aim to source data relating to different aspects, such as possible invasion of privacy, oversight, legitimacy and others.

The findings of all three methods shows that public discourse on all covered topics is predominantly neutral, with fewer opinions being negative or positive. Negative discourse is larger in volume than the positive one. A social listening dashboard shows us that some topics, such as biometric identification, are constantly in the public eye, while others have recently started getting more attention.

The information presented in this document clearly identifies the biggest concerns that people have as discrimination, privacy and legitimacy. Nevertheless, there is wide-spread understanding and acceptance of the positive sides of AI in the security domain, therefore the conclusion is that it is possible to establish an overall positive attitude towards such systems (or, at least, minimise the negative reactions) with proper measures.

Overall, citizens want to see a combination of technological and transparency measures in place, so that LEA work using AI is subject extensive control and reporting.

Table of Contents

1 Introduction 5
1.1 Purpose 5
1.2 Work Methodology 5
1.3 Methodology and Structure of the Deliverable 7
2 Social listening 9
2.1 Methodology and Scope 9
2.2 Findings 13
2.2.1 Biometric Identifiers 14
2.2.2 Predictive Policing 18
2.2.3 Police Hacking 22
2.2.4 Decision making in the justice system 25
2.3 General findings across topics and subtopics 28
3 Crowdsourcing activity 29
3.1 Methodology 29
3.2 Results analysis 30
3.2.1 Phase 1 – Problem mapping 30
3.2.2 Phase 2 – Idea generation 34
3.2.3 Phase 3 – Idea selection 35
3.3 Phase 3 results discussion 39
4 Passive Social Listening though Location-Based Searches 42
4.1 Methodology of Social Sensing 42
4.1.1 Data collection from social media 42
4.1.2 Machine Learning approaches used to extract information 43
4.2 Results of Social Sensing 44
4.2.1 Sentiment analysis on European tweets 44
4.2.2 Dividing the dataset into 4 European Regions 45
4.2.3 Results of Sentiment Analysis on 4 European Regions 46
4.3 Conclusions 48
5 Citizen-produced recommendations. Next steps. 49
5.1 Biometric identification and Privacy 49
5.2 Police Hacking and Legitimacy 50
5.3 Predictive policing and discrimination 51
5.4 Next steps – connection to upcoming tasks 51
References 52
Annexes 53

Annex 1 “Social Listening keywords” 53
Annex 2 “Social listening – number of results by topics and sentiment” 66
Annex 3 “Crowdsourcing Phase 1 questions” 71
Exploring citizens' main concerns and attitudes with regard to the use of Artificial Intelligence by Law Enforcement Authorities (LEAs). 71

List of Figures

Figure 1 - D3.3 Validation Methodology overview 7
Figure 2 - Topics, Subtopics, Substrands chart 11
Figure 3 - Social listening results by topic 14
Figure 4 - Biometric Identifiers - subtopics distribution 14
Figure 5- Biometric Identifiers, sentiment distribution 15
Figure 6 - Biometric Identifiers, Efficiency, Reliability, Accuracy, sentiment distribution 16
Figure 7 –Biometric Identifiers, Legitimacy, sentiment distribution 17
Figure 8 – Biometric Identifiers, Discrimination, sentiment distribution 17
Figure 9 - Predictive Policing, subtopic distribution 19
Figure 10 - Predictive Policing, sentiment distribution 19
Figure 11 - Predictive policing, discourse volume and sentiment trends 20
Figure 12 - Predictive Policing, Discrimination, sentiment distribution 21
Figure 13 Predictive Policing, Efficiency, Reliability, Accuracy, sentiment distribution 21
Figure 14 – Police Hacking, subtopic distribution 22
Figure 15 - Police Hacking, Legitimacy, sentiment distribution 23
Figure 16 - Police hacking, trends over time 24
Figure 17 - Decision Making in the Justice System, distribution by subtopic 26
Figure 18 - Decision Making in the Justice System, Discrimination, sentiment distribution 26
Figure 19 - Decision making in the Justice System - trends over time 27
Figure 20 - Biometric Identification, distribution of votes 31
Figure 21 - Predictive Policing, distribution of votes 32
Figure 22 - Cyber Operations, distribution of votes 33
Figure 23 - Police Hacking, distribution of votes 33
Figure 24 - Decision-Making in the Justice System, distribution of votes 34
Figure 25 - Topic-Subtopic parings, Phase 2 35
Figure 26 - Proposed ideas, Phase 3 38
Figure 27 - First pairing, idea ranking 39
Figure 28 - Second pairing, idea ranking 39
Figure 29 - Third pairing, idea ranking 40
Figure 30 - Pie chart showing the results of Sentiment Analysis of 18,150 tweets from Europe 45
Figure 31 - Bar plot of number of tweets based on location, divided in 4 European Regions 46
Figure 32 - Results of Sentiment Analysis on every European region 47

1 Introduction

The work reported in the present deliverable contributes directly to the core mission of the popAI project, namely **to enhance confidence in AI by promoting understanding and active participation by society, unifying diverse areas of expertise, and presenting a cohesive European perspective along with policy recommendations**. The methodology employed under this task, as detailed below, combines multiple approaches to gain an insight into how artificial intelligence in the security domain is perceived – which are the topics that people feel most strongly about, whether it is positive or negative and, most importantly, what citizens think should be done to improve AI and increase trust in such tools. At the same time, the work component that directly engaged citizens also contributed to increase public understanding of the complex topic.

1.1 Purpose

The purpose of the activities covered in this document is to understand citizen's attitudes towards AI in the security domain by combining passive and active engagement tools. Inclusion of the public in the discussions of complex topics is challenging, but provides a platform for less knowledgeable and underrepresented groups to participate in forming and informing policy-decisions and identifyfurther research opportunities. The open access of tools such as the crowdsourcing platform is a chance for people of different backgrounds to take part in a common, cross-border effort, and goes beyond engaging the usual stakeholders such as tech providers, researchers, law enforcement, human rights defenders and others.

Apart from this, actively engaging citizens, communicating the opportunity for them to participate and sharing the results at the end of an activity serves to build at least a basic understanding of the topic. This understanding goes both ways – citizen's priorities and recommendations may provide policy makers with information about certain policies and measures that are already in place, but are not well-known to the public or are performing poorly.

At the same time, making public participation possible does not automatically mean that a lot of people will want to engage. The topic of AI in the security domain is not extremely popular and forming an opinion on its aspects requires strong interest, technical knowledge or both. Furthermore, crowdsourced opinions under popAI will form policy recommendations but will not necessarily be turned into actual policy. Therefore, the passive understanding of the public discourse is required to validate and strengthen the findings of the crowdsourcing activity. For the purposes of popAI, this passive understanding is supplied by employing social listening.

1.2 Work Methodology

The deliverable builds on top of the work done the in following tasks:

- Task 2.2 Legal framework and casework taxonomy: emerging trends and scenarios
- Task 2.3 The controversies and risks that have shaped innovation and will shape AI in the next 20 years

- Task 3.1 Map the controversy ecosystems of AI tools in the security domain

The deliverable will contribute to following tasks:

- Task 3.5 Multi-Disciplinary Foresight scenarios
- Task 4.1 Recommendations for and from policymakers and LEAs
- Task 4.2 Recommendations for and from the Civil Society
- Task 4.3 Recommendations for and from Technology Developers

To construct a framework of topics and subtopics for AI tools used by law enforcement ***Task 2.2, Task 2.3*** and ***Task 3.1*** provided underlying foundation. More specifically, **Task 3.1** explored controversies in five key areas, which were taken as the basis for forming the five topics explored inthe social listening and crowdsourcing discussed below. Building on this, **Tasks 2.2** and **2.3** further explore *why* certain use-cases were controversial and were used to build the subtopics (i.e., possibleconcerns) that were explored for all topics.

The results from the tasks listed above and the constructed framework were discussed with the law enforcement authority project partners for additional validation. The LEAs also worked with the ECAS team with regard to the crowdsourcing phases as follows:

- Before Phase 1, to provide short explanatory paragraphs for citizens for each of the five topics;
- After Phase 1, to cross-reference crowdsourcing and social listening results and determine the topics and subtopics that will be put forward for citizen ideation in Phase 2;
- After Phase 2, to sort, summarise and fine-tune the citizen proposals that will be put forward for citizen selection in phase 3.

All of the above is presented schematically in Figure 1

In terms of accessibility, all partners contributed to the translation of the platform and questionnaires in the languages covered by the project, namely Italian, Slovak, Greek, Spanish, German, and Dutch.

The crowdsourcing activity was subject to close scrutiny by the project Ethics Board in the following key points:

- **Use of financial incentives to recruit human participants:** it was decided that no incentives should be provided to increase the number of participants;
- **Platform login functionality:** it was decided that users will be allowed to answer or vote anonymously during all phases;
- **Data Privacy disclaimer:** an additional data privacy disclaimer was placed on the platform to provide citizens with a brief overview of how users' data will be used and the contact of ECAS' GDPR officer was provided.

Furthermore, T3.1 also provided an extensive mapping of relevant stakeholders to be contacted in the crowdsourcing activity in cooperation with ***WP5 Dissemination, Communications and Sustainable Community Engagement.***

Finally, the work under this deliverable will feed into ***Task 3.5*** by providing insight into the positive and negative public reception of AI tools in law enforcement and will serve to inform ***WP4*** with citizen-produced recommendations for different stakeholders such as citizens, civil society, policy-makers and law enforcement authorities.

Deliverable Number	Title	Input from:	Output to:	Validation Methodology			
				Theoretical	Empirical		
				Literature review or Scientific Validation	Experts	LEAs	Civil Society
D3.3	Citizen produced priorities and recommendations for addressing AI in the security domain	T3.1, T2.2, T2.3	T4.1, T4.2, T4.3	Crowdsourcing methodology based on: Lironi, E., May 2016, POTENTIAL AND CHALLENGES OF E-PARTICIPATION IN THE EUROPEAN UNION, *Policy Department for Citizens' Rights and Constitutional Affairs*, Aitamurto T., Landemore H., 2015 Five Design Principles for Crowdsourced Policymaking: Assessing the Case of Crowdsourced Off-Road Traffic Law in Finland, *Journal Social Media for Organizations, Vol. 2, Issue 1,*	ERI, TRI, internal ECAS discussions; Discussions during Policy Labs 1, 2 and 3 were taken into account for each crowdsourcing phase;	Meetings and discussions with HP, HfoD, PLTO on constructing the framework of the topics and subtopics, and before each of the three crowdsourcing phases;	meetings with Ethics Board, consultations with ECAS GDPR expert

Figure 1 - D3.3 Validation Methodology overview

1.3 Methodology and Structure of the Deliverable

The rest of the Deliverable is structured as follows:

Sections 2 presents the ethical social listening activity carried out by ECAS. It outlines the methodology explains the tools and algorithms used and presents a quantitative and qualitative analysis of the final set of results.

While social listening carried out by ECAS was initially planned as part of Deliverable 3.2, two factors justify its inclusion in the present document. Firstly, the number of respondents to the crowdsourcing platform is at the lower end of the performance indicator, therefore it further justification of the results and process is needed through a larger dataset. Secondly, this activity it shares the exact structure of the crowdsourcing activity with its topics and subtopics.

Section 3 presents the crowdsourcing activity along the three phases which took place on ECAS' crowdsourcing platform. It presents a detailed review of the data gathered from each phase. Section 3 also discusses the solutions ranked by citizens as most desirable to solve some perceived problems on the topic of AI in the security domain.

Section 4 presents an additional social media listening activity (social sensing) carried out by CERTH that complements the rest of the work and introduces a dimension of regionality to the results.

Section 5 concludes the deliverable by systematizing the information into citizen-produced recommendations that address the most common concerns regarding AI in the security domain and explains how these results will inform other tasks within the project.

Annexes at the end include all raw data such as keywords used for social listening and the results thereof, the questionnaires in the crowdsourcing activity and any information produced by the citizens.

2 Social listening

2.1 Methodology and Scope

Social listening is a term most frequently used in marketing to denote a process through which one can identify what is being said about a certain brand, product, service or topic. Agencies and companies used it to acquire competitor intelligence, see how the public perceives their new product and follow the latest industry trends. When it comes to social listening in the social sciences sphere, the instrument serves a similar purpose - to let researchers know how societal trends about a certain topic progress over time.

The database that ECAS uses in order to conduct the social listening exercise is called CommonCrawl - an open web repository for the last 7 years, containing 3.1 billion pages, where each month's worth of data totals more than 300 terabytes. To extract meaning from the CommonCrawl dataset, ECAS employs a subcontractor with technical expertise to employ an algorithm to search through the crawl for strings of keywords that identify topics of interest to the popAI project. The activity is also referred to as "ethical social listening" to differentiate it from "social media listening/monitoring" because results are completely anonymous and no data is gathered on the individuals expressing the opinions.

The limitations of this instrument are several. Firstly, the data extracted cannot be definitely attributed to a certain geographical location, therefore it cannot be definitely said if the sentiment expressed is indicative for the population of a country or continent. Still, this limitation is insignificant, as internet users (in most cases) have access to data from all over the world and it forms their opinion regardless of the origin of a post, text or news article. The second limitation is that, while CommonCrawl provides access to a vast amount of data, it still does not cover the whole internet. For example, the Google search index (which, it must be pointed out, itself does not cover 100% of the internet) is about hundreds of times bigger than CommonCrawl. Thirdly, it is impossible for one to conceive of all possible words that people can use to discuss a certain topic or subtopic or expression of approval/disapproval. This limitation is addressed by employing a sentiment analysis algorithm with a high degree of accuracy for recognizing positive, negative or neutral point of view of the message.

In the context of social listening, neutrality is defined either (i) in the absence of sentiment-catching keywords which are labelled either as bearing positive or negative sentiment or (ii) through a total scoring function where the sum of positive and negative sentiment keywords (and respective scoring) on a certain topic are closing towards an average value of zero.

Scope

Within the crowdsourcing platform there are 5 major topics of possible AI implementation in LEAs - Biometric Identification, Predictive Policing, Cyber Operations, Police Hacking Operations, Decision making in the justice systems - and each of these is divided into subtopics of possible concern to citizens. The subtopics are universal across each topic and are as follows - Respect to human rights, Human oversight, Accuracy, Reliability, Respect to privacy, Legitimate access to people's data, Transparency, Prejudice and discrimination, Benefit to society, Sustainability, Accountability.

For the purposes of the social listening some of these were grouped together as they could be used

interchangeably in online conversations while discussing the single feature/theme, resulting in the following set of subtopics under each major topic - (1) privacy, (2) efficiency, reliability, accuracy, (3) legitimacy, (4) transparency, accountability, (5) discrimination. Each of these subtopics is then further divided in two sub strands - positive and negative. For a visual overview, please see Figure 1 - "Topics, Subtopics, Substrands chart" below. In the positive sub strand we include keywords that would show a favourable disposition on the part of the communicator. An example of this would be the combination of the keyword "privacy" with keywords such as "acknowledge", "promote", "respect", "safeguard", "by design", "upholding". In the negative sub strands, the keywords paired with "privacy" are "disrupt", "impedes'', "does not acknowledge", "not sensitive", "harm", "abuse", "restrict". Apart from the keywords - the ones that we want to see included in the results- we also include a section of exclusions that we don't want to be present in the results. As an example, in the positive sub strand of "Legitimacy" we exclude "no legitimacy" and "low legitimacy". For the full set of keywords used to define our search, please see Annex 1 "Social listening keywords".

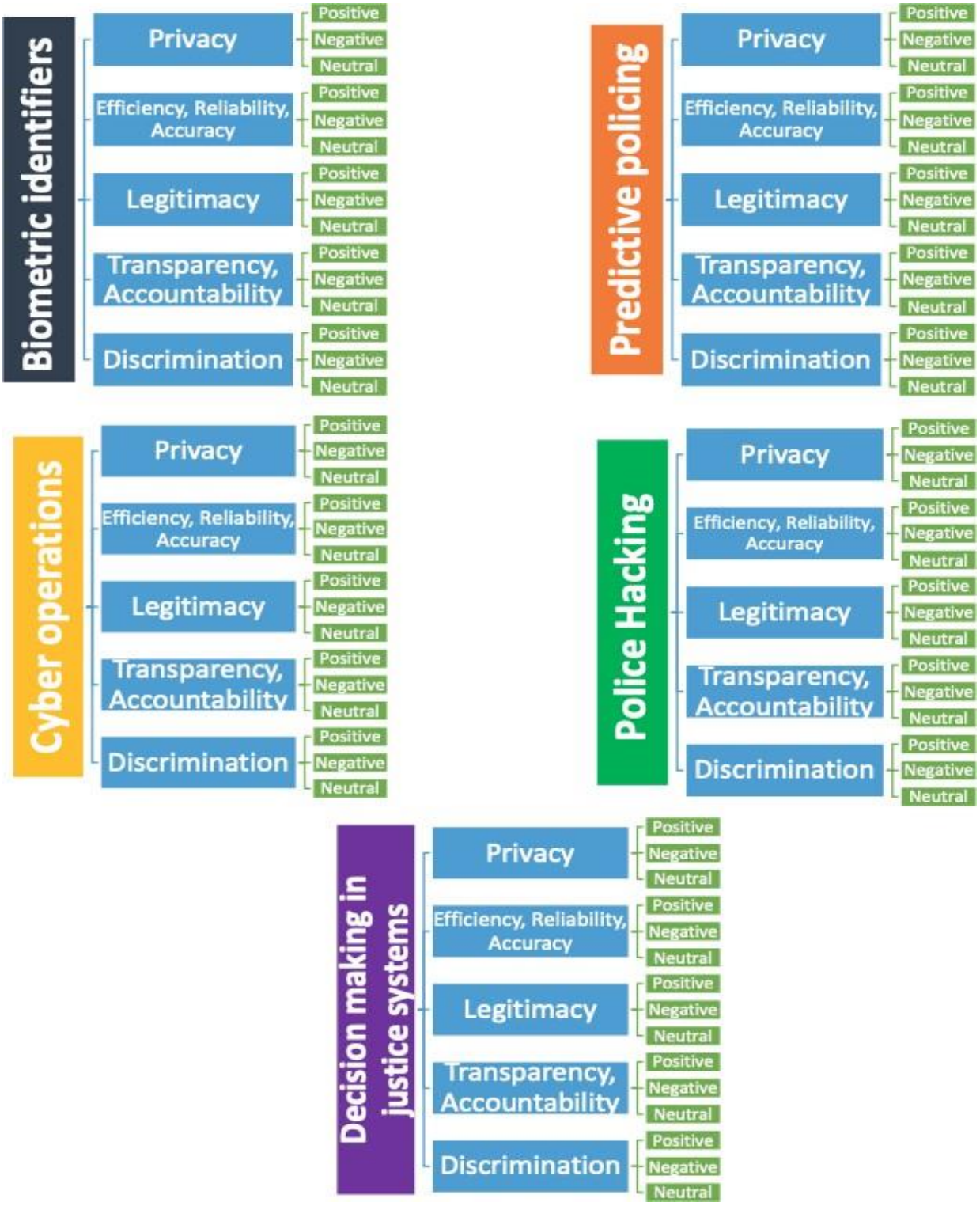


Figure 2 - Topics, Subtopics, Substrands chart

By gathering data in such a way, the methodology will provide us with both quantitative and qualitative insight into the public's perception of law enforcement operations or functions that rely on or can include AI algorithms, purportedly in order to increase their efficiency, accuracy, speed, etc. On the quantitative side, the results will show us which topics identified by the popAI consortium

are generating the most public discourse, that is to say, for example, if citizens discuss more the biometric identification capabilities of police forces rather than algorithms being used to set bail in the court system. Moreover, it will provide us with an overview of the specific subtopics that generate the majority of the interest, for example the relationship between biometric identification and privacy or between biometric identification and discrimination. This two-layered approach is going to provide us with a multitude of comparison possibilities. On the qualitative side, we'll get an insight into the sentiment used for all examples given above - positive, negative or neutral. To achieve this goal, we employ two tools already discussed above. Firstly, we try to 'manually' define the sentiment through the keywords used. On top of that, because this approach can produce both false positives and false negatives, we run all results through a sentiment analysis tool - a roBERTa-base model trained on 58 million tweets - that scores the positive, negative and neutral sentiment of each result. The interpretation of the results from the model is showed as a numerical value ranging from -1 (most negative) to +1 (most positive), including decimal numbers in between.

The structure outlined above will also provide with an understanding of if people react differently when their opinion is being actively sourced as with the crowdsourcing platform, as opposed to the sentiment found in conversations, blogs, articles, scientific papers, news and others around the internet.

Expectations

Pertaining to the quantitative results of the social listening exercise, we expect to see that the majority of the data relates to the following major topics - Biometric Identifiers, Predictive Policing and Police Hacking. All three of these topics have seen serious coverage in the media due to controversies that emerged such as "ClearView" that gained a lot of attention. As for the subtopics, we expect that the most results will come from "Privacy", "Discrimination" and "Transparency, Accountability" because these are the areas that were in the centre of the aforementioned controversies and are closest to the citizens. On the other hand, the "Legitimacy" subtopic is more of concern to human rights advocates, defenders,and lawyers and the debate around "Efficiency, Reliability, Accuracy" is a highly-specialised one where scientists and researchers are mostly engaged in.

Process

The information outlined in the "Scope" section of the deliverable is the end result of three test searches on CommonCrawl and refinements that the research team undertook in order to accommodate the multitude of goals, topics and constraints of the exercise. Each test search encompasses a month worth of data on CommonCrawl, namely January 2020.

Initially, the team set out to conduct the sentiment analysis based on the keywords only. The first test run clearly showed that there was a high number of false positives and false negatives. That is to say, there were results in the "positive" substrand that technically included a combination of the keywords but the text sentiment was negative and vice versa. This led to the necessity to include a third "neutral" substrand for each subtopic, where no sentiment-catching keywords are used. At the end of the research, a sentiment analysis algorithm was employed that would be fed with all hits from all substrands for a topic-subtopic combination (positive, negative and neutral) and score each

one on negativity, positivity and neutrality, so as to have the broadest possible dataset. Because we're averaging the sentiment score for each subtopic, and removing duplicates, this is not going to influence the results.

In the process of running the test results, the keywords came up in results that did not constitute a comprehensive text, but represented a string of words, most probably used in websites for Search Engine Optimisation, caches or other system files that were public on the internet. Furthermore, some results could not be understood without further context that was not part of the text sourced. For this, the team had to employ a simple algorithm to sort through the data and determine if a certain result was, in fact, a useful 'signal' or 'noise' that had to be removed. To teach the algorithm to recognise the meaningful results, after each of the three test runs the team manually went through 250 results for each topic, subtopic and substrand, totalling approximately 18 000 hits per test. In total, more than 50 000 results were categorised as relevant or not and were fed into the algorithm until it succeeded in categorising correctly automatically.

The research ran into two major setbacks which led to postponing of result reporting and including the data in the present deliverable. Firstly, the manual review and training of the algorithm to sort relevant and irrelevant results had to be revised, as different team members categorised the same result in subsequent test runs one time as relevant and another as irrelevant, due to different interpretations or simply by mistake. While not fatal for the overall process, this problem meant that some hits in the final set of results would be erroneously included or excluded, therefore not providing the cleanest dataset possible. Secondly, at the time of conducting the final search on the CommonCrawl, the database was overloaded by a large volume of users' requests, meaning the extraction was considerably slower although the servers would have otherwise been able to mine close to their full capacity.

2.2 Findings

The final dataset that was extracted from the CommonCrawl database amounted to 301 766 results. The hits are unique, except in outlier cases where the text of the result mentions more than one topic or subtopic. The reviews of the three test results and random samplings of the final dataset showed that the amount of such repetitions is extremely low. These were distributed among topics rather unevenly, as the pie-chart shows:

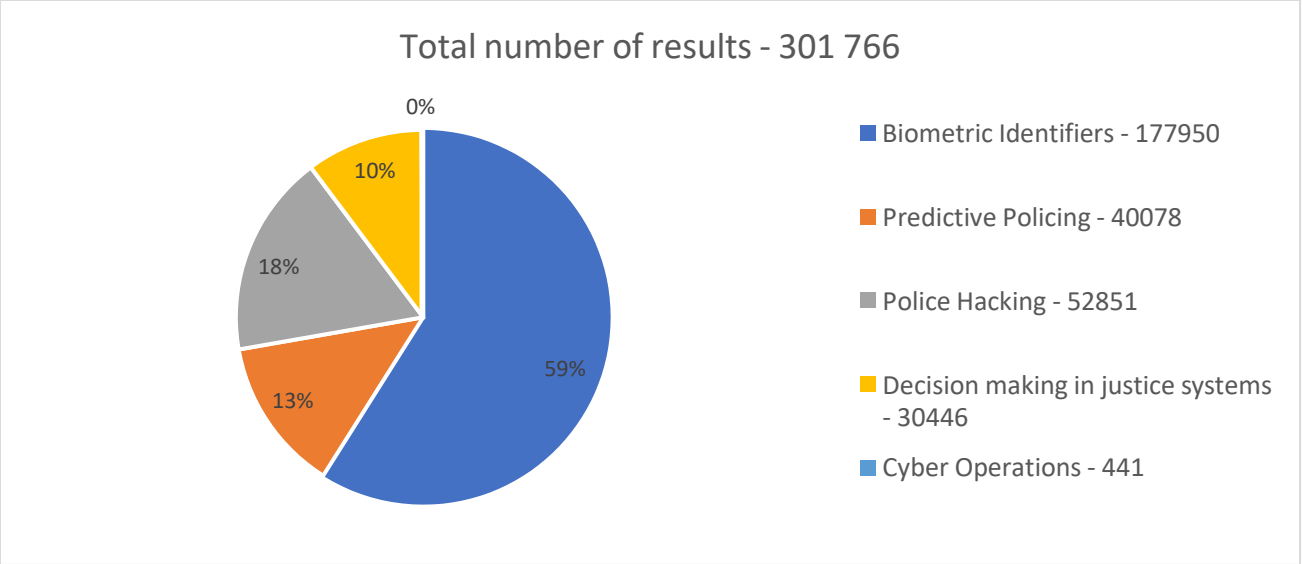


Figure 3 - Social listening results by topic

The topic "Biometric Identifiers" produced almost 60% of the total volume of results, followed by "Police Hacking", "Predictive Policing" and "Decision Making in the Justice System". "Cyber Operations" sourced only 441 results, or less than 1% of all data, which makes it statistically insignificant, therefore this topic is excluded from further analysis.

Following subsections will discuss the most significant findings across the four remaining topics, while the rest of the data is structured in Annex 2 "Social listening – number of results by topics and sentiment" in Section 6 of this document and/or on the publicly-available online dashboard. Emphasis is placed on identifying negative discourses, as the social listening activity aims to feed into and support Phase 1 (problem mapping) of the crowdsourcing discussed in Section 4.

2.2.1 Biometric Identifiers

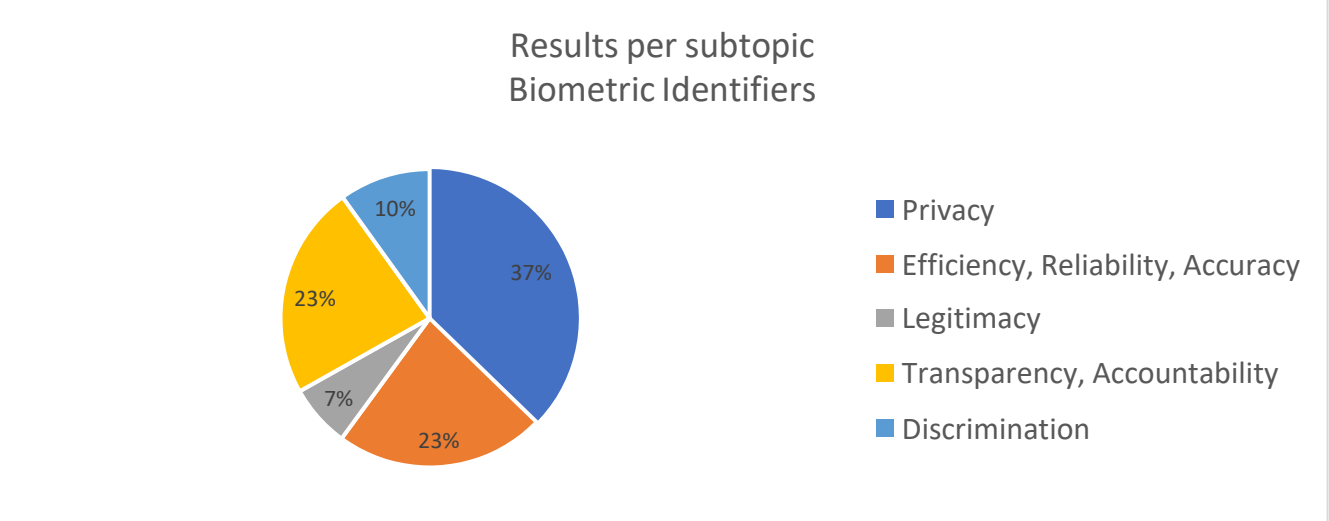


Figure 4 - Biometric Identifiers - subtopics distribution

In the framework of most discussed topic, Biometric Identifiers (Figure 4), the subtopic that produced the most results were “Privacy” with more than 66 000 results, followed by “Efficiency, Reliability, Accuracy” and “Transparency, Accountability” with approximately 41 000 each.

The overall sentiment distribution across all subtopics is shown in numerical terms (Figure 5) below.

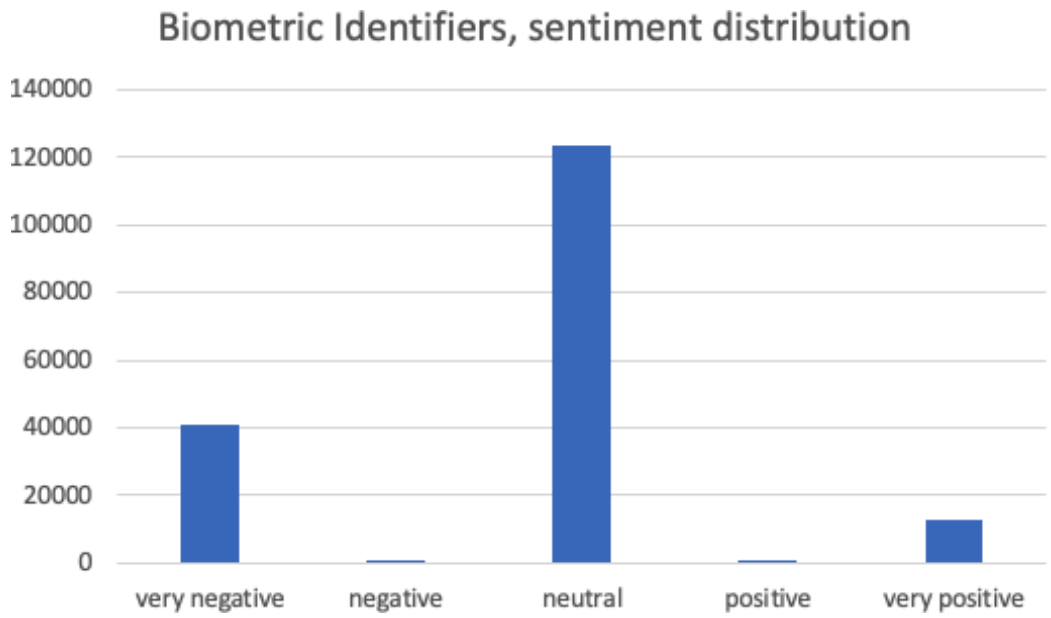


Figure 5- Biometric Identifiers, sentiment distribution

The average sentiment rating for the topic “Biometric Identifiers” is therefore also very close to the neutral middle value of 0, with a value of -0.11. In other terms, 23% of all results were of negative sentiment.

These values are driven mainly by the three largest subtopics, “Privacy”, “Efficiency, Reliability, Accuracy” and “Transparency, Accountability”, which have average sentiments of -0.079, -0.038 and -0.127. In the “Efficiency, Reliability, Accuracy” this balance is due to large numbers in both ends of the spectrum, as evidenced by Figure 6. The data shows that there is also widespread understanding of the public benefits of such tools, which may be due to the application of such systems in consumer electronics and therefore reliance on the part of individuals on their reliability.

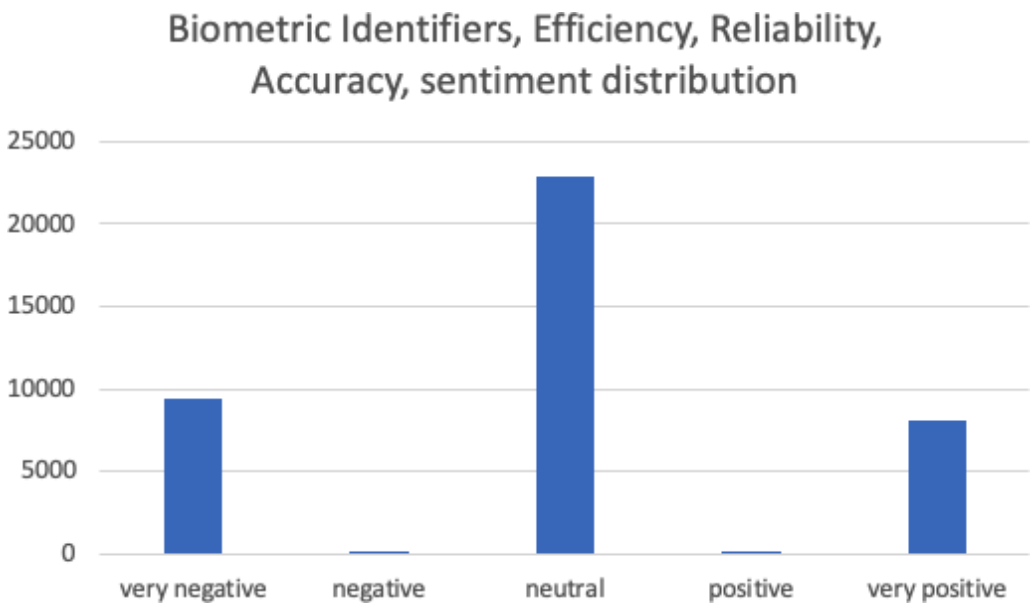


Figure 6 - Biometric Identifiers, Efficiency, Reliability, Accuracy, sentiment distribution

This is not the case for the other two subtopics of the group, where positive results are a minority of the total, but the large volume of discourse in the middle pushes the average sentiment towards neutrality.

The rest of the subtopics shown in Figures 7 and 8, “Legitimacy” and “Discrimination”, are considerably more negative with an average sentiment score of -0.223 and -0.274 respectively. In both cases, the number of negative hits - on the left of the middle column - is quite close (although lower) to the number of neutral ones – middle column.

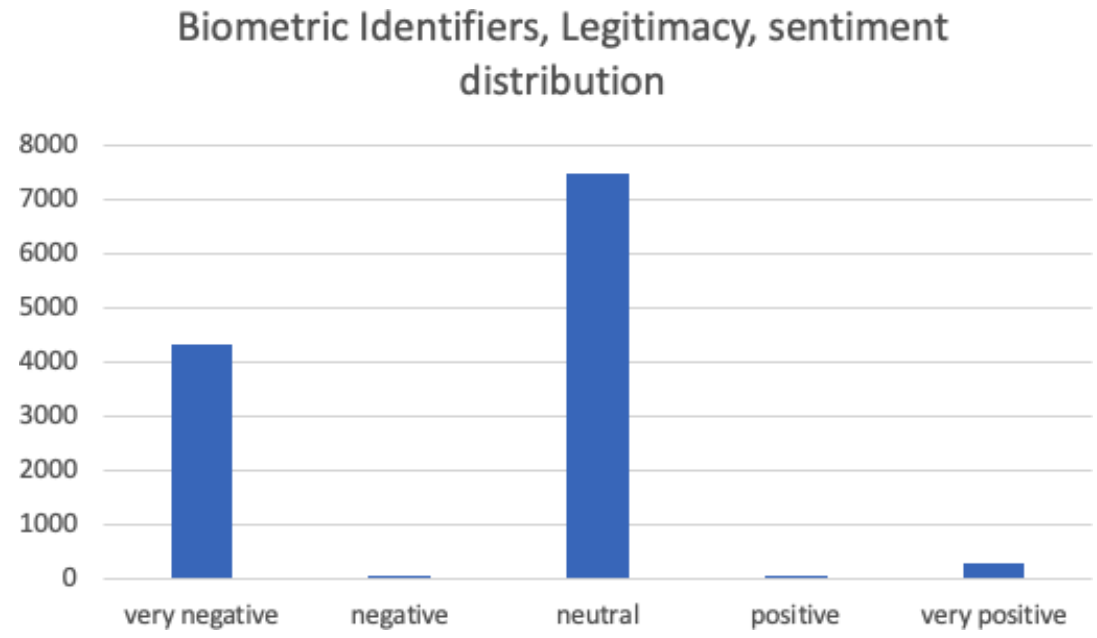


Figure 7 –Biometric Identifiers, Legitimacy, sentiment distribution

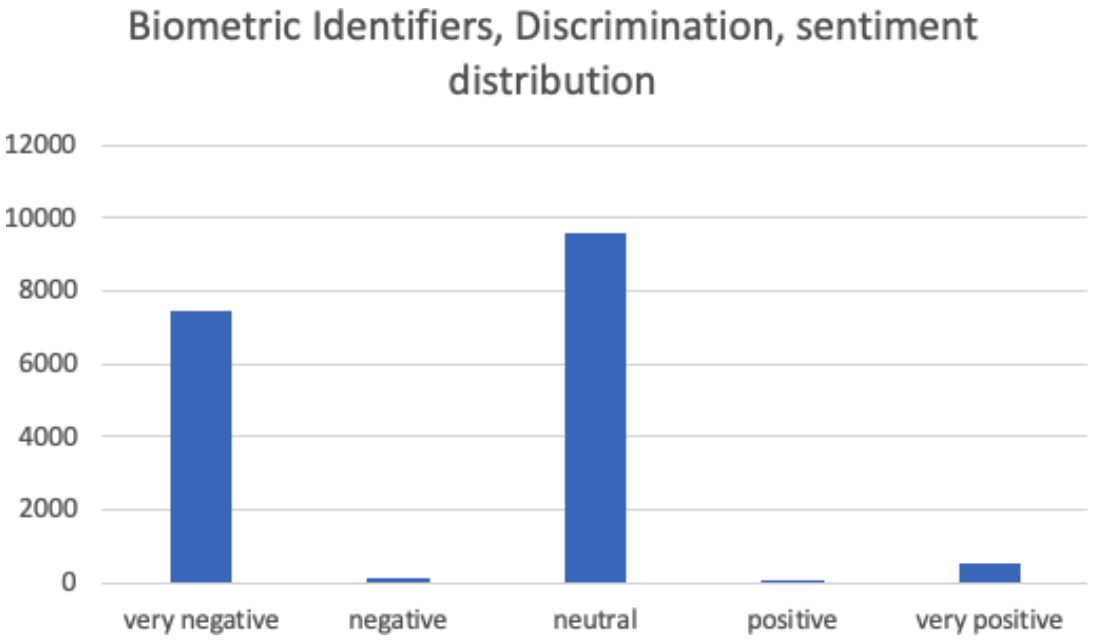


Figure 8 – Biometric Identifiers, Discrimination, sentiment distribution

Important takeaway

Citizens are mostly worried that Biometric Identification tools can be discriminatory and biased in their results. Surprisingly, the discourse surrounding privacy is not overly negative. This is still the most discussed issue and has the highest number of negative results in absolute terms. Nevertheless, the discrepancy in public discourse between the results of "privacy" and "legitimacy" must be discussed.

On one hand, people may not be as concerned about their privacy in relation to biometric identification tools because they believe that these tools are necessary for law enforcement to do their job effectively. They may see biometric identification tools as necessary means to catch criminals and maintain public safety. In this sense, people may view the use of biometric identification tools by law enforcement as a trade-off between privacy and security, where security takes priority.

On the other hand, people may be very concerned with the overall legitimacy of biometrics used by police because they fear that the use of these tools may lead to abuses of power or violations of civil rights. They may worry that biometric identification tools could be used to target certain groups or individuals unfairly, or that the data collected by these tools could be misused for other purposes.

In this sense, people's concerns about the legitimacy of biometrics used by police may be more related to the fairness and transparency of the overall system, rather than the specific privacy implications of biometric identification tools.

2.2.2 Predictive Policing

Within the topic, the distribution subtopics contributing to the volume of hits is shown in Figure 9:

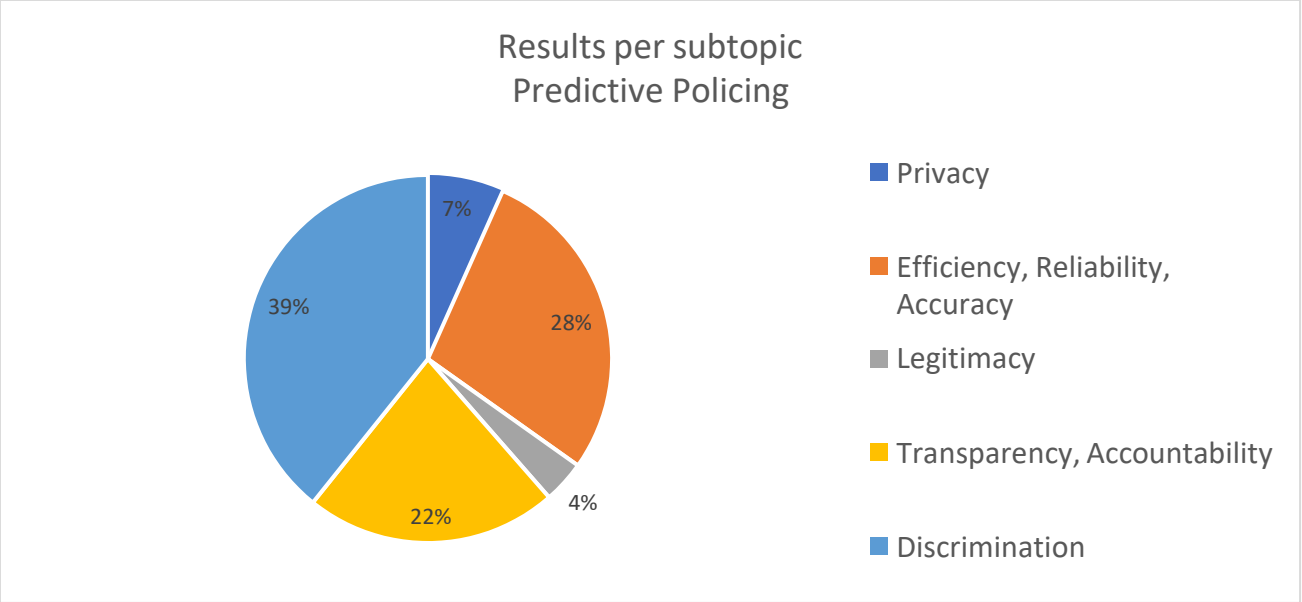


Figure 9 - Predictive Policing, subtopic distribution

The average sentiment score is -0.201, with 32% of all results being negative (Figure 10).

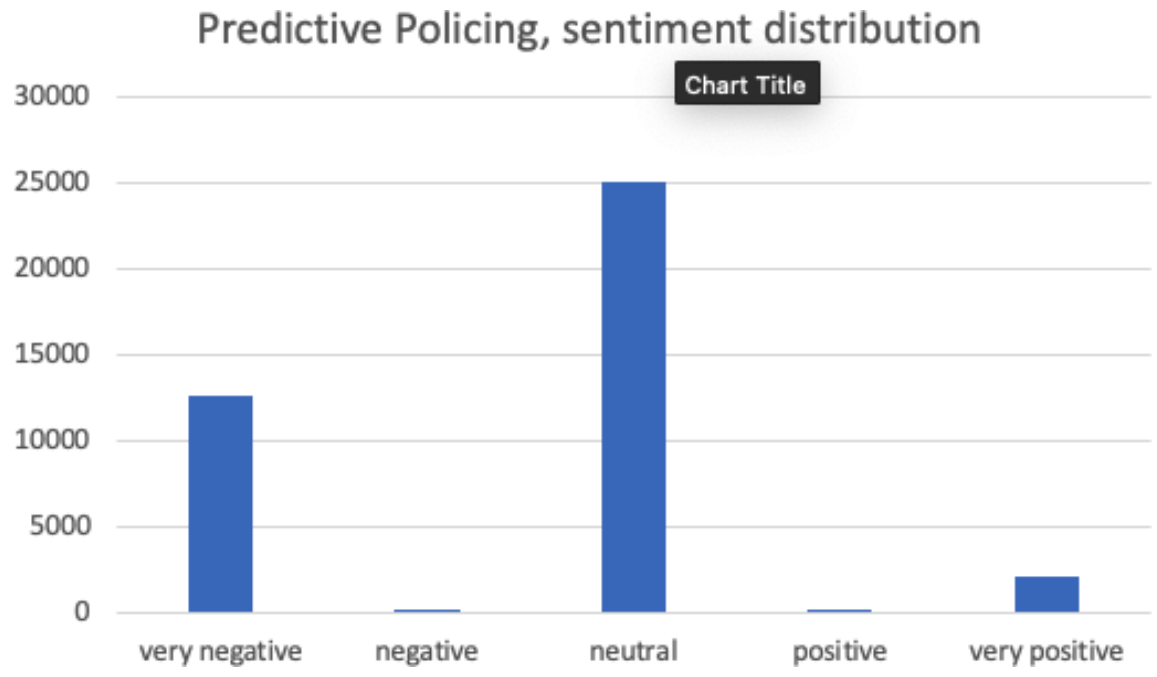


Figure 10 - Predictive Policing, sentiment distribution

The most interesting outcomes in the topic "Predictive Policing" are to be found when looking at the distribution of results over time, as well as the progression of discourse sentiment for the same period. This is visually represented in Figure 11 and also available on the digital dashboard.

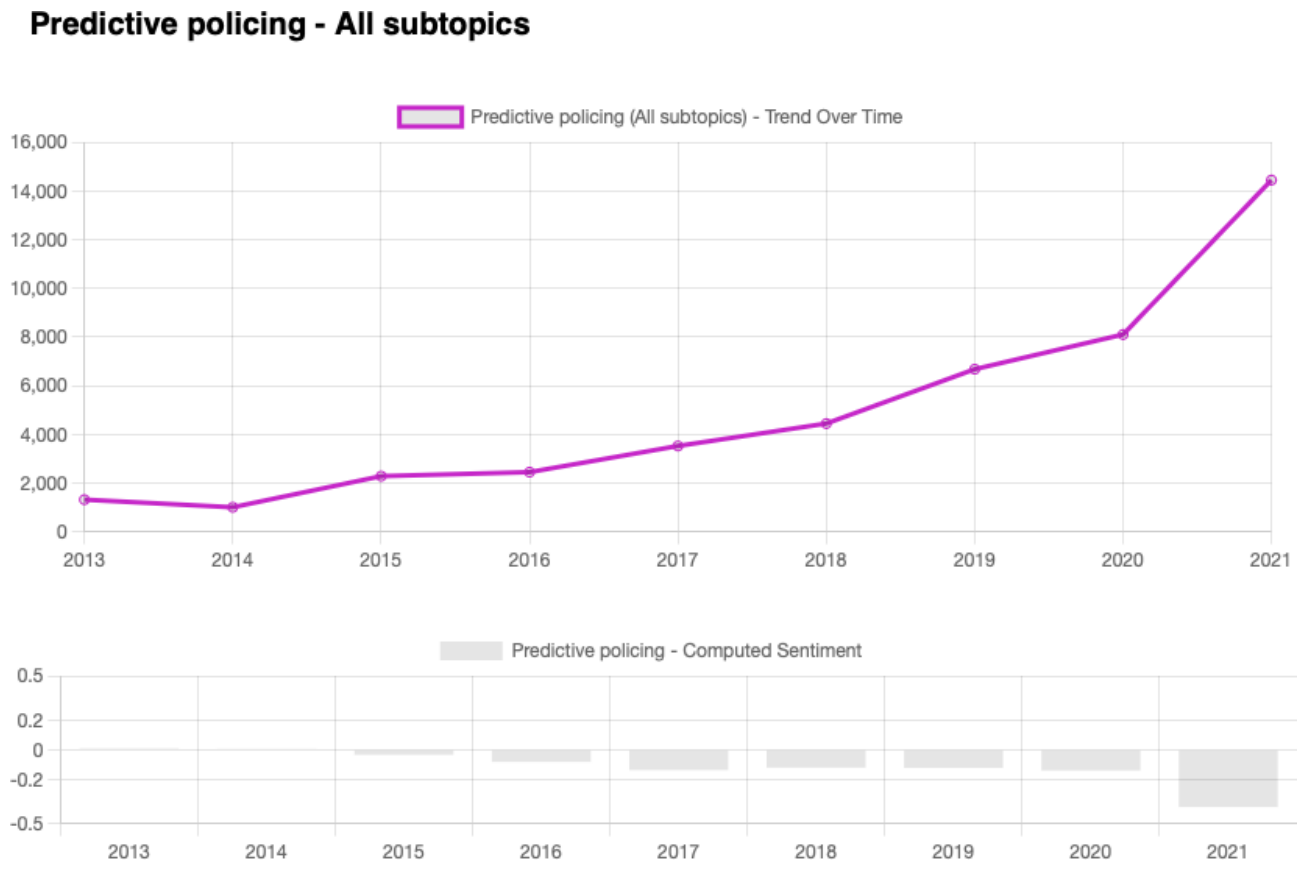


Figure 11 - Predictive policing, discourse volume and sentiment trends

There is a clearly defined upward trend, and at the same time the average attitudes are increasingly negative. Here, most subtopics tend to show an average sentiment close to the neutral value:

- Privacy – -0.11
- Efficiency, Reliability, Accuracy – -0.05
- Legitimacy – -0.169
- Transparency, Accountability – -0.08

The trends shown above and the negative average sentiment are therefore driven by a single subtopic, "Discrimination", which also constitutes the largest number of hits under the topic "Predictive policing", as shown in Figure 9. This is also one of the three topic-subtopic pairings in the social listening dataset where the number of negative results outweighs the sum of the positive and neutral ones, the other one again concerning the issue of discrimination. This pairing shows the same trends for increasing volume of public discourse, as well as deepening of negative attitudes – see digital dashboard, section Predictive policing - Discrimination.

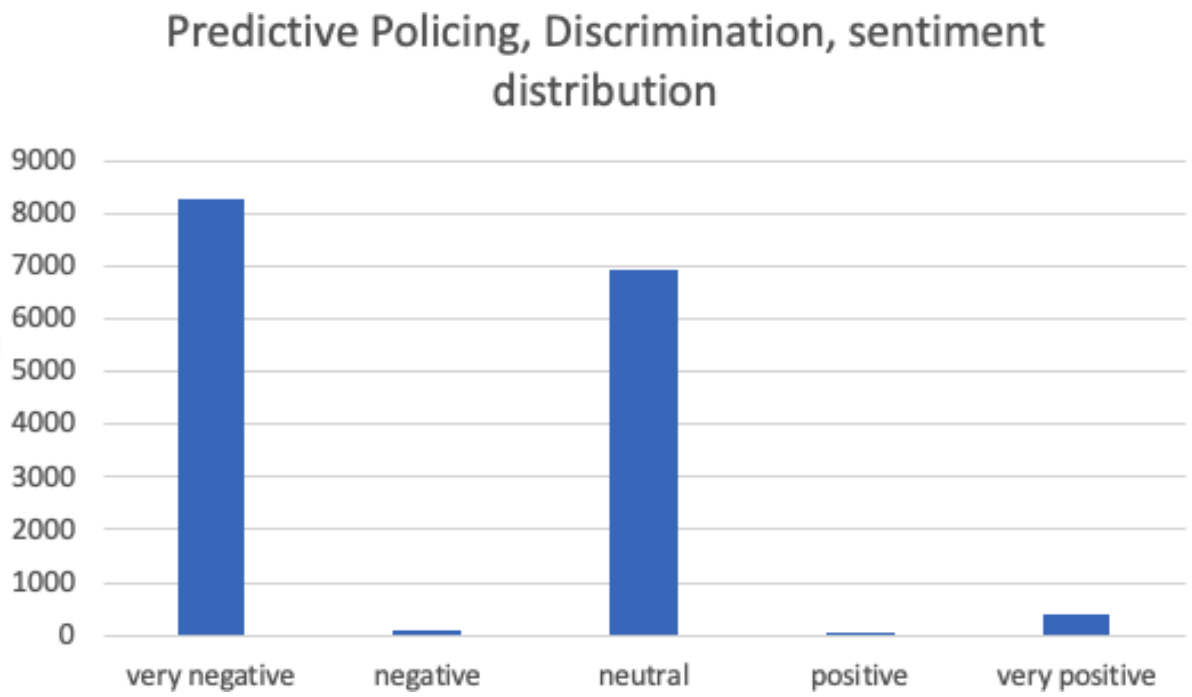


Figure 12 - Predictive Policing, Discrimination, sentiment distribution

Again, it is worth pointing out the finding (Figure 13) of a relative balance between positive and negative attitudes towards the aspects of efficiency, reliability and accuracy of predictive policing algorithms.

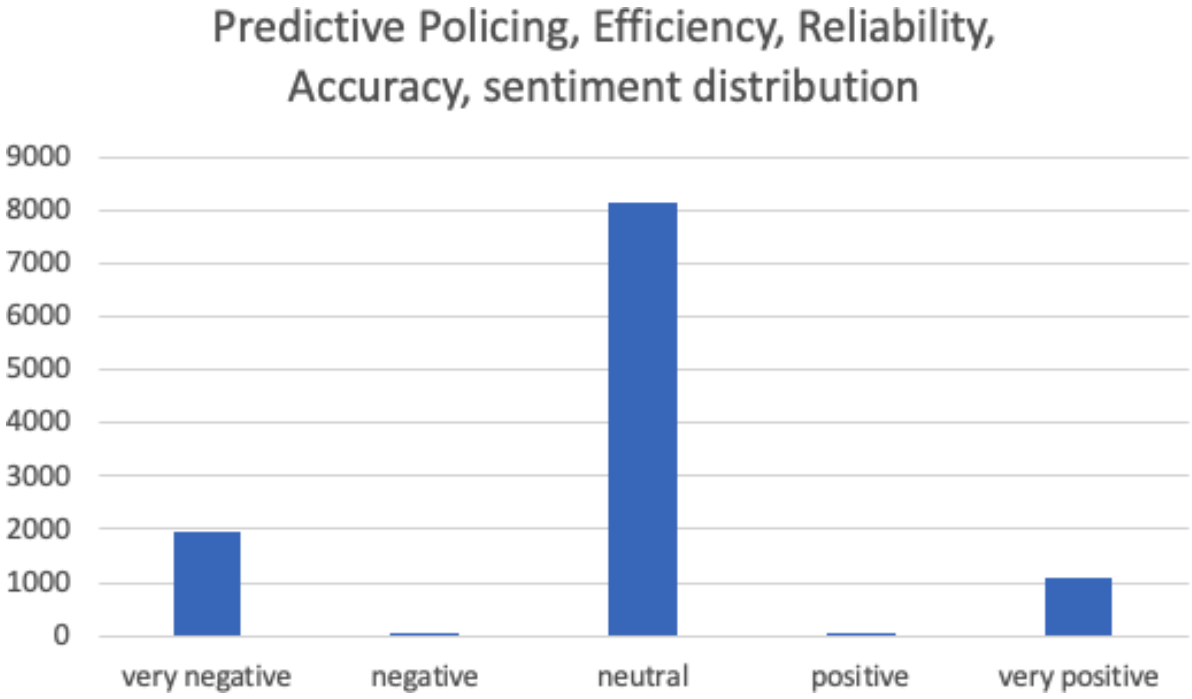


Figure 13 Predictive Policing, Efficiency, Reliability, Accuracy, sentiment distribution

Important takeaway

The increasing volume of negative discussions surrounding predictive policing algorithms, especially regarding perceived discrimination, indicates that citizens are becoming more aware of the potential harms associated with these tools.

The negative perception of predictive policing tools is likely due to the fact that they rely on historical data to make predictions about future criminal activity, which may perpetuate biases and discrimination in the law enforcement system.

2.2.3 Police Hacking

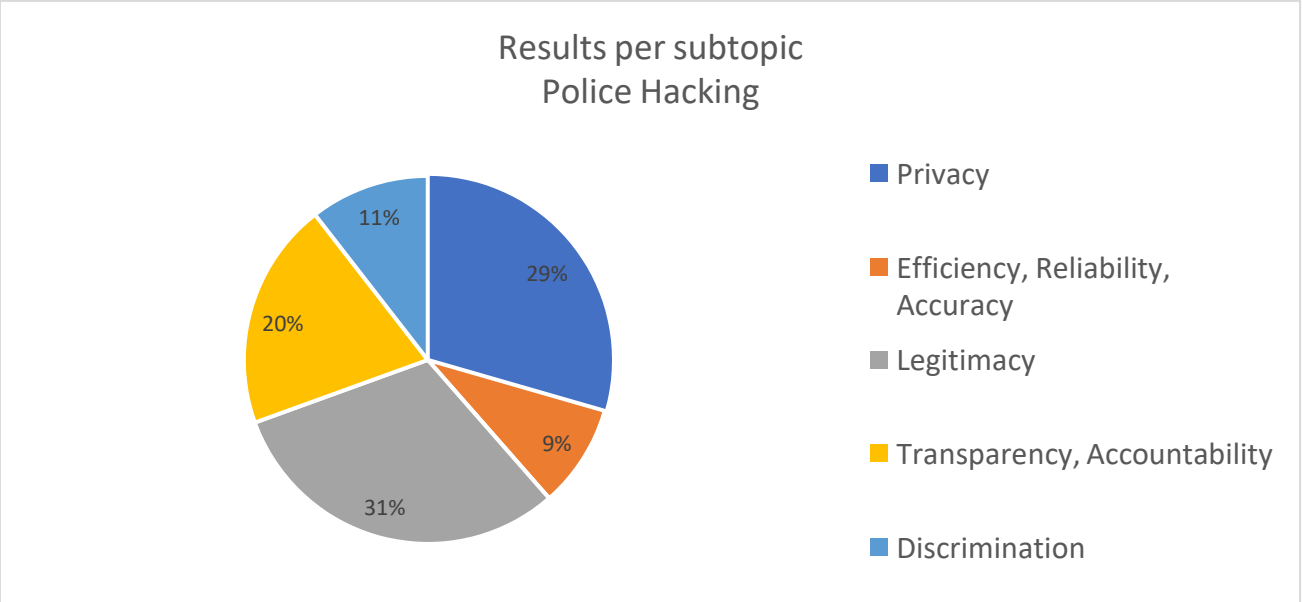


Figure 14 – Police Hacking, subtopic distribution

Within "Police Hacking", two subtopics generate the majority of public discourse, namely "Privacy" and "Legitimacy" with 29% and 31% respectively (Figure 14).

Our findings show that "Police Hacking" was the topic that generates the most negative attitudes in the online field. Over 36% of all results were classified as negative and the average sentiment generated was -0.233 (Figure 15). This can be attributed mostly to the subtopic with the highest weight, "Legitimacy", where negative results contribute to more than 45% of the total, producing an average sentiment of -0.305.

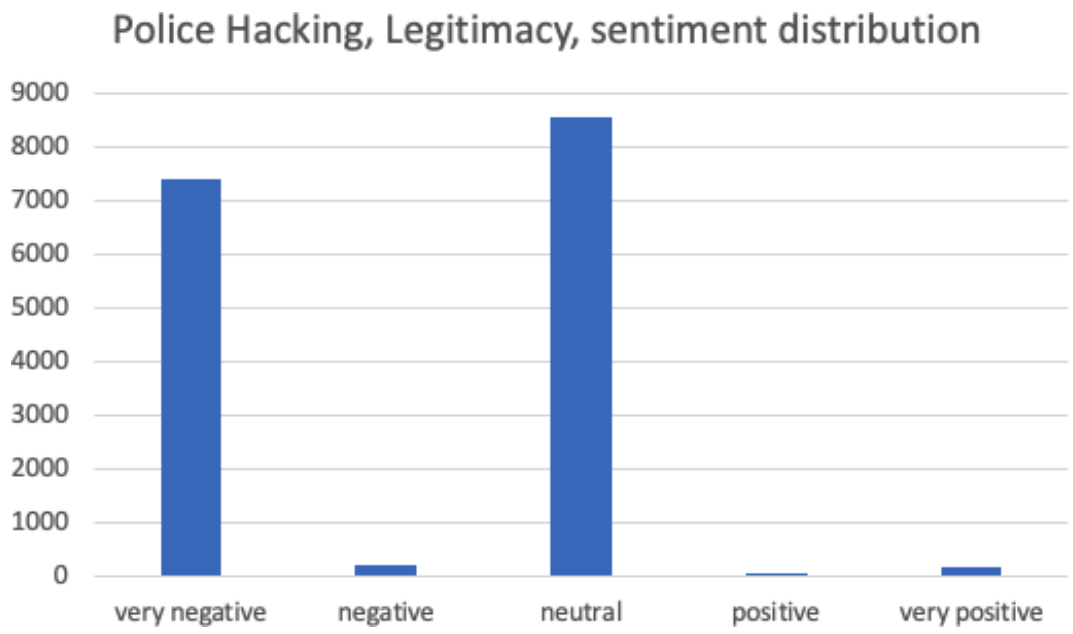


Figure 15 - Police Hacking, Legitimacy, sentiment distribution

"Discrimination" also contributes to "Police Hacking" having the lowest average sentiment score, with the same average of -0.305, but it forms a much smaller percentage of the overall results within the broader topic. **An explanation for this may be that the use of police hacking powers may also have a chilling effect on certain groups, leading them to self-censor or avoid online activities out of fear of being targeted or surveilled. This can further exacerbate existing disparities and perpetuate feelings of discrimination and bias.**

At the same time, as the general trend over time in the dashboard shows (Figure 16), the most of the results are generated in 2016, which is true for all topic-subtopic pairings in this category. This is most likely because of the aftermath of the 2015 and 2016 terrorist attacks in France and Belgium that sparked European-wide debate on encryption and police authorities' powers to access data to prevent or investigate security threats.

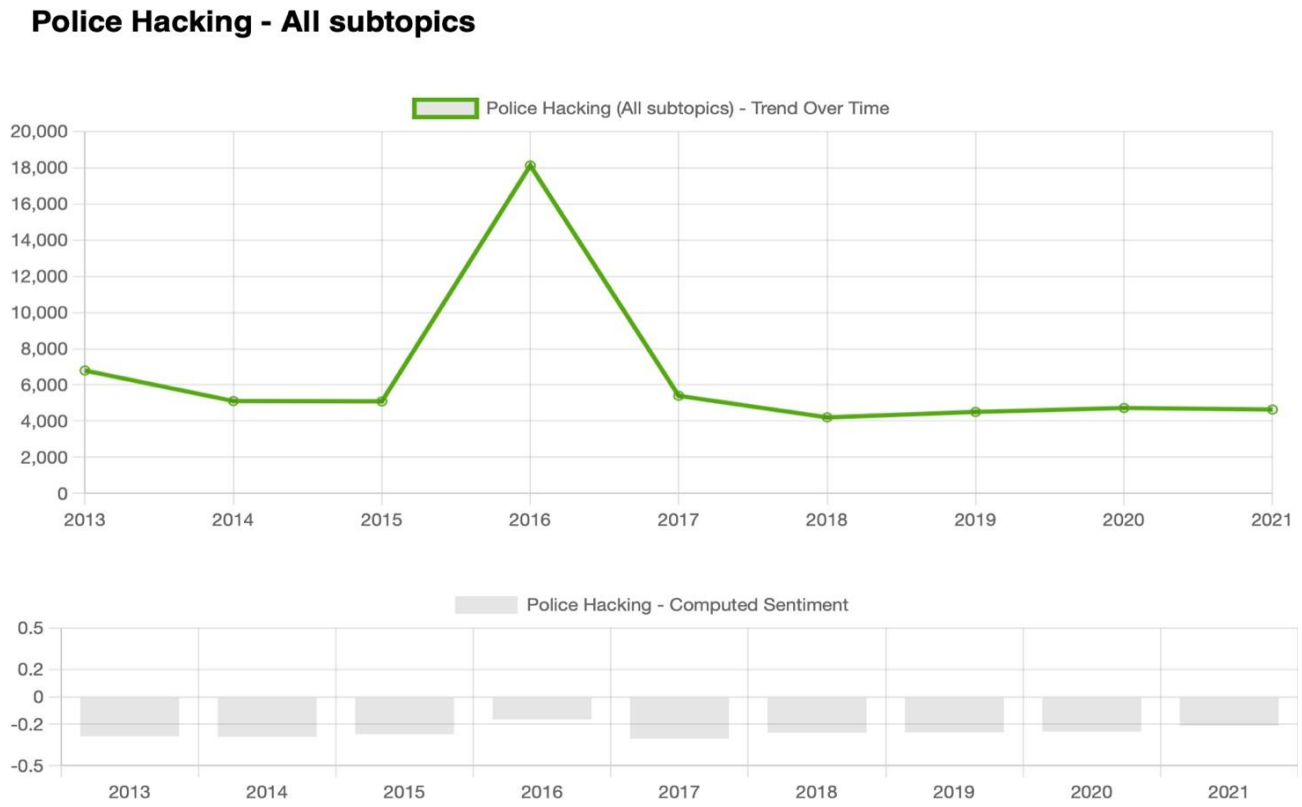


Figure 16 - Police hacking, trends over time

While sentiment is on the negative side of the spectrum across the timeframe, its average is the lowest in 2016, the same year that produced the majority of the discourse. This can be attributed to the overall prevalence of neutral results, which is true across the whole social listening dataset.

Important takeaway

The data shows that legitimacy and discrimination are the most concerning topics when it comes to online discourse. As technology continues to advance and become more complex, it can be difficult to ensure that police hacking powers are used appropriately and in compliance with existing laws and regulations, which is reflected in the results.

The notable increase in the period 2015-2016 can be attributed to a number of high-profile cases around the world. One such event was the legal battle between the Dutch government and internet service provider Ziggo over government hacking of a suspected criminal's computer. The case went to the Dutch Supreme Court and raised questions around the legality and oversight of police hacking powers in the Netherlands.

In the UK, the Investigatory Powers Act 2016 was introduced, which granted law enforcement agencies broad powers to intercept and hack into electronic communications. This sparked a debate around the balance between national security and individual privacy, as well as concerns around the potential abuse of these powers.

Additionally, the 2015 terrorist attacks in Paris and the subsequent increase in counterterrorism measures across Europe brought attention to the use of police hacking powers in investigations and intelligence gathering.

In the USA, one such event was the legal battle between Apple and the FBI over access to the iPhone of one of the San Bernardino shooters. This case brought attention to the issue of government access to encrypted devices and sparked a broader debate around the balance between individual privacy and national security.

2.2.4 Decision making in the justice system

The topic of AI tools being used in the justice systems is dominated by the discussion surrounding the issue of discrimination, which comprises 40% (Figure 17) of the total results under this category and is equal to the sum of the next biggest subtopics, “Efficiency, Reliability, Accuracy” and “Transparency, Accountability”.

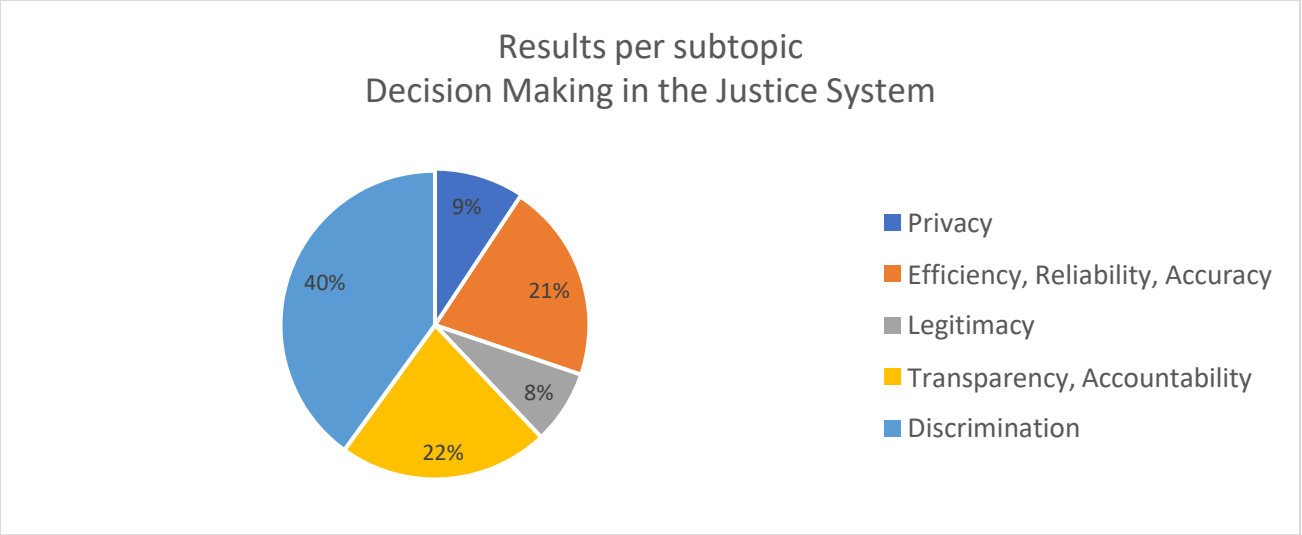


Figure 17 - Decision Making in the Justice System, distribution by subtopic

The overall attitudes of the sourced results show that the discourse is very close to neutral, with less than 30% (Figure 18) of opinions being negative and an average score of -0.152.

Most of the negativity is attributed to the subtopics of "Legitimacy" and "Discrimination". In "Legitimacy" the majority of the results have been classified as such. Nevertheless, this subtopic is also the one that generated the least discourse. On the other hand, "Discrimination", being also the largest subtopic, comprised of almost 36% negative discourse and has an average sentiment of -0.226.

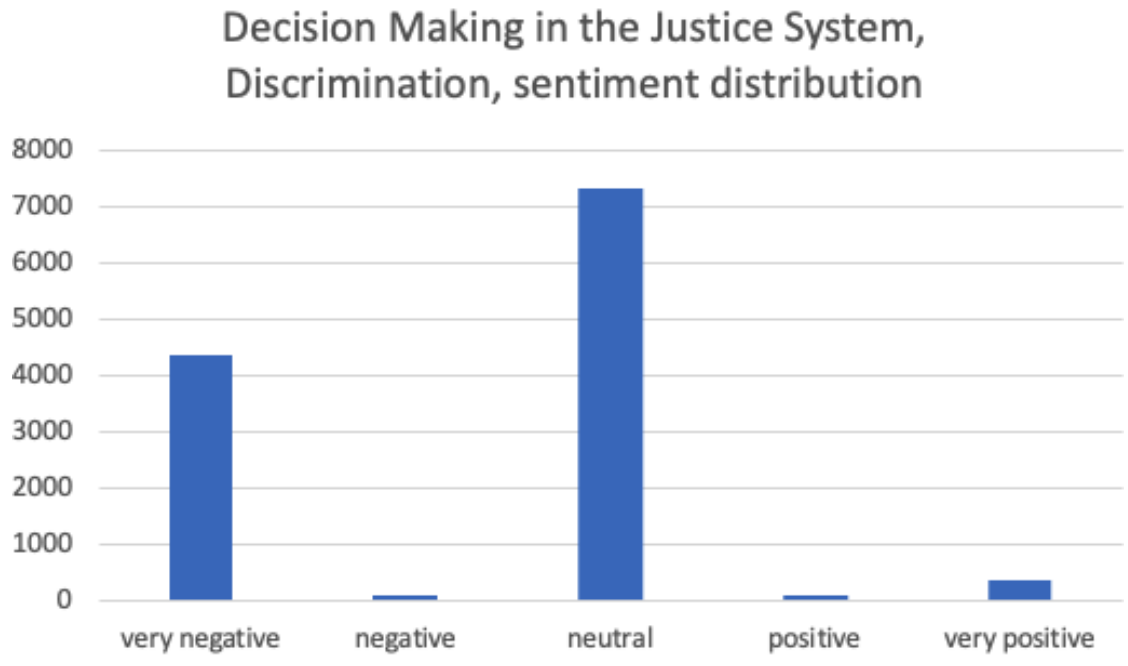


Figure 18 - Decision Making in the Justice System, Discrimination, sentiment distribution.

Using the dashboard to view the distribution of the discourse over time, we find that the "Discrimination" subtopic (Figure 19) has generated progressive interest through the years, which is true for all other subtopics under this category. Still, unlike other subtopics, the increasing discourse volume correlates to a negative trend when it comes to the average sentiment.

Figure 19 - Decision making in the Justice System - trends over time

Important takeaway

The online discourse shows that citizens believe that algorithms being used to aid the decision-making process in the justice systems are more likely than not biased and discriminatory. This is also reflected in the subtopic on legitimacy, where the conversation is extremely negative, i.e people do not see algorithms as a legitimate factor in judicial decisions.

As algorithms are increasingly introduced in the justice systems, there may be a growing awareness and concern around the potential impact of these tools on individual rights and freedoms. This leads to increased scrutiny and criticism of these systems, particularly in relation to their potential for perpetuating discrimination.

2.3 General findings across topics and subtopics

Multiple important findings stem from the dataset and comparisons between topics, subtopics and their pairings. Firstly, when it comes to ranking the topics based both on the average sentiment and the percentage of negative results:

Cyber Operations

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

As discussed previously, the volume of discourse under "Cyber Operations" was statistically insignificant and should not be regarded as part of the ranking order.

With regard to the subtopics, "Discrimination" produced the most negative sentiment across all topics, as such results comprised 48% of the data sourced. It also is the lowest-averaging subtopic with a score of -0.299. This can be attributed to the fact that three of the topics ("Biometric Identifiers", "Predictive Policing" and "Decision Making in the Justice System") deal with algorithms that are connected to profiling, thus there is a possibility of producing racial, gender, socioeconomic or other bias. The second-lowest ranking subtopic across all topics was "Legitimacy" where the share of negative results and the average sentiment were 40% and -0.256 respectively.

Still, the overall average sentiment and the majority of neutral results (in absolute terms) of the dataset shows that the discussion is largely in the middle, while online discussions which clearly show negative attitudes towards AI in the security domain are more and more negative than the positive ones.

3 Crowdsourcing activity

3.1 Methodology

Crowdsourcing is an e-participation method used worldwide and more specifically as a means of enhancing democratic engagement in the EU. Crowdsourcing can be a complementary tool to existing frameworks in order to expand the number of contributors to EU policy-making, remove potential barriers to participation and "engage the unengaged" throughout Europe.

In the framework of popAI, crowdsourcing is employed as the primary tool for actively engaging citizens with the topic of AI in the security domain, as opposed to social listening which is a tool to passively tune in to the conversations happening online. ECAS' crowdsourcing methodology consists of three phases, each one informing the next:

- Phase 1, Problem mapping – researching how citizens perceive the topics and different aspects thereof. The purpose of this phase is to identify the most concerning AI tools as per respondents and the specific features (e.g., invasion of privacy) that cause the most negative sentiment.
- Phase 2, Idea generation – analysing the results of the previous phase, the AI topics and their negatively perceived features are presented to citizens. Respondents are asked to share their ideas and proposals in improving the perceived shortcomings.
- Phase 3, Idea selection – citizens are asked to rank the proposals and solutions from the previous phase.

Between Phases 1 and 2, results of the crowdsourcing were cross-referenced with the outcomes of the social media listening. This ensures that the topics presented for idea generation were based on a larger, more representative dataset, and did not reflect the opinions of active and interested citizens only. Subsequently, law enforcement partners in the project reviewed the multitude of ideas generated in Phase 2, filtered the relevant ones and aggregated them in policy recommendations.

Several limitations and challenges of this methodology are identified, especially with regard to extremely complex topics which only sporadically become part of the popular discourse[1]. As AI tools used by law enforcement is a technically-heavy topic that does not directly affect citizens' everyday lives, explanations and information must be provided to respondents before they engage in the crowdsourcing activity. This needs to be simple and short so as to be understood by the general public, but also needs to provide enough background so that participants can formulate an informed answer. Secondly, topics must be presented in a neutral language in order to prevent instilling bias respondents. As controversies are intrinsically negative, the preparation of the questions for the first phase was done by Eticas and Trilateral research in a way that describes the AI tools in general terms.

To protect citizen's privacy, the Ethics Board decided that anonymous responses to all three phases would be accepted. While this indeed provides a sense of security to respondents, it also prevents re-targeting of citizens who took part in previous phases. Only less than 10% of respondents chose to create an account with an email address. In this regard, all data on participants is stored on GDPR-

[1] As opposed to, for example, the topic of climate change, which most citizens have a baseline understanding of and opinions on.

compliant servers rented by ECAS and a Privacy Policy informs citizens on how their information is collected and processed, including a mechanism for users to contact the GDPR officer of ECAS.

3.2 Results analysis

3.2.1 Phase 1 – Problem mapping

In preparation for Phase 1, research partners reviewed work done on controversies and taxonomy in order to select a range of topics and aspects of AI systems in the security domain to be put forward to citizens and gather their sentiment. Five topics were identified:

1. Biometric identification;
2. AI systems used to prevent crime (predictive policing);
3. AI systems used in cyberoperations;
4. Police hacking;
5. Justice decision-making tools.

These broad topics were introduced by a short informational paragraph to provide some background information and help citizens with little prior knowledge understand the subject matter on a basic level.

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

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

Respondents had to place a numerical value to a statement on each of the eleven aspects, ranging from 1 (totally disagree, highest concern) to 7 (totally agree, least concern) and 4 is neither agreement nor disagreement, for example:

- Biometric identification tools are reliable;
- Biometric identification tools have enough human oversight;
- Biometric identification tools are accountable;

The only question that is an exception to the rule is the one on prejudice and discrimination. Following the example above, for the question "Biometric identification tools reinforce prejudice and discrimination" full agreement (7) would mean that the respondent has a negative attitude, while full disagreement (1) would indicate a response that shows no concern. This is discussed in the findings for each topic where relevant.

This totalled 55 questions (5 topics, each with 11 aspects/sub-topics), along with a voluntary, introductory demographic questionnaire at the beginning. Questions were translated by the partners so they are available in all languages of the consortium. Please see the full questionnaire in Annex 3 "Crowdsourcing Phase 1 questions".

A total of 189 responses were gathered during this phase. Based on the contributions, the five topics were ranked from the most to least concerning:

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

Below is a visual overview of the results for each topic which shows the mean/average and the overall score distribution:

1. Biometric identifiers:

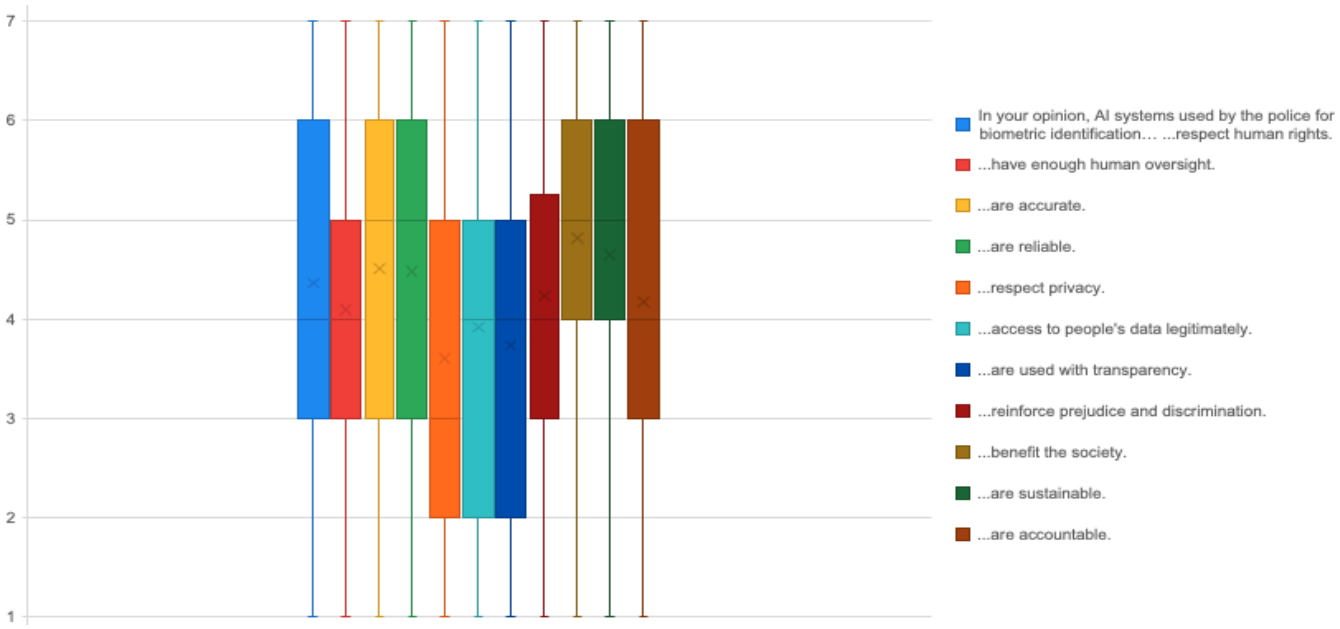


Figure 20 - Biometric Identification, distribution of votes

Respondents identified the respect to privacy, access to people's data and the level of transparency as the three most problematic areas of using biometric identification tools in the security domain. These form a *de facto* "cluster of negativity", as visible from the overall distribution as well (Figure 20). Generally, respondents' answers were largely neutral, and the whole topic of Biometric Identification averages extremely close to the absolute middle with a score of 4.24 on the scale of 1 to 7.

Interesting to note is the general feeling of participants that, although there are shortcomings in other aspects, tools for biometric identification are beneficial to society, where the average score lies much higher (almost a full point) than the absolute middle, and the overall distribution of answers clearly lies above it. In comparison, it is interesting to note that the lowest ranking subtopics forming

the “cluster of negativity” barely average 0.3 points below the 4-point neutrality mark, and distribute the sentiment much more evenly across the range.

2. Predictive policing

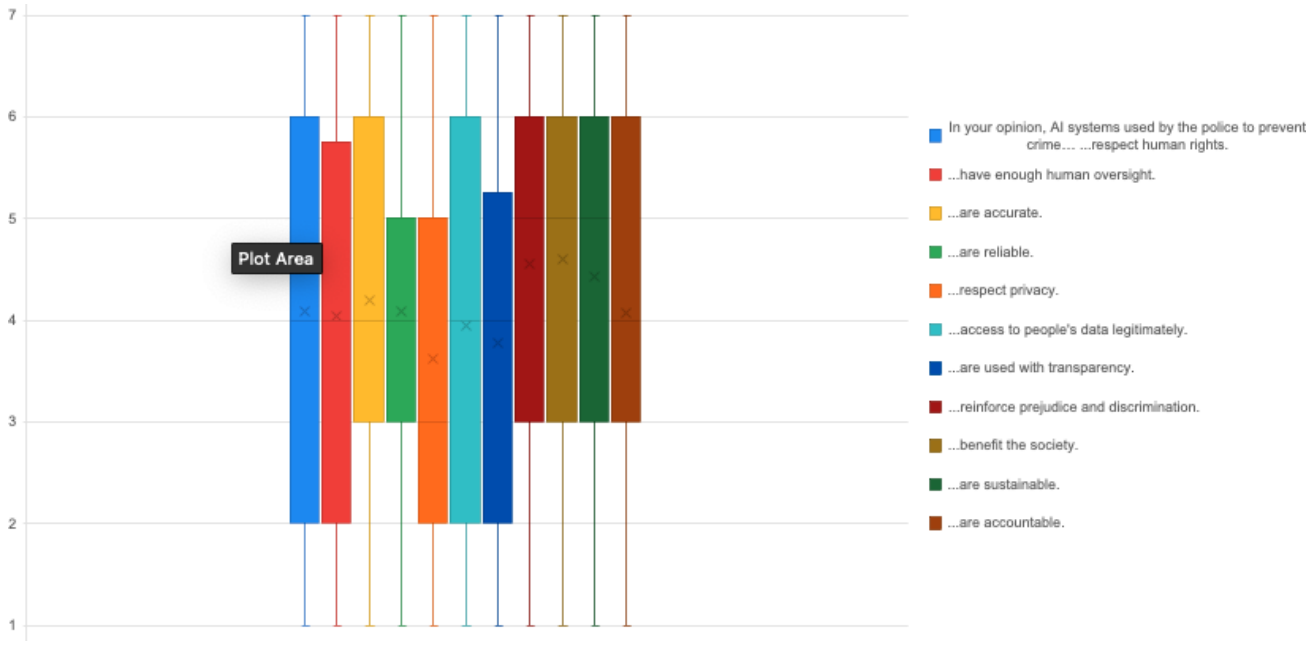


Figure 21 - Predictive Policing, distribution of votes

The attitudes of citizens about predictive policing tools being use in the context of law enforcement were both fairly evenly distributed and the averages tended to be close to the neutrality mark (Figure 21). With this in mind, discourse distribution on the topics of respect to privacy and transparency (orange and blue colours in the middle of Figure 21 leans noticeably towards the negative end of the spectrum, and does not spread towards the higher ranges as frequently. This is limited evidence for the rigidity of the “negative cluster” discussed in the previous topic, “Biometric identifiers”.

Here it must be taken into account that the question on reinforcing prejudice and discrimination should be taken with the opposite values, therefore the deviation of 0.55 points from the neutrality mark is the most significant negative within the topic of predictive policing.

Again, citizens value the benefit to society and sustainability aspects of such AI systems as distinctly positive. Combining all subtopics, the average score for “predictive policing” was almost exactly on the neutrality mark – 4.10.

3. Cyber operations

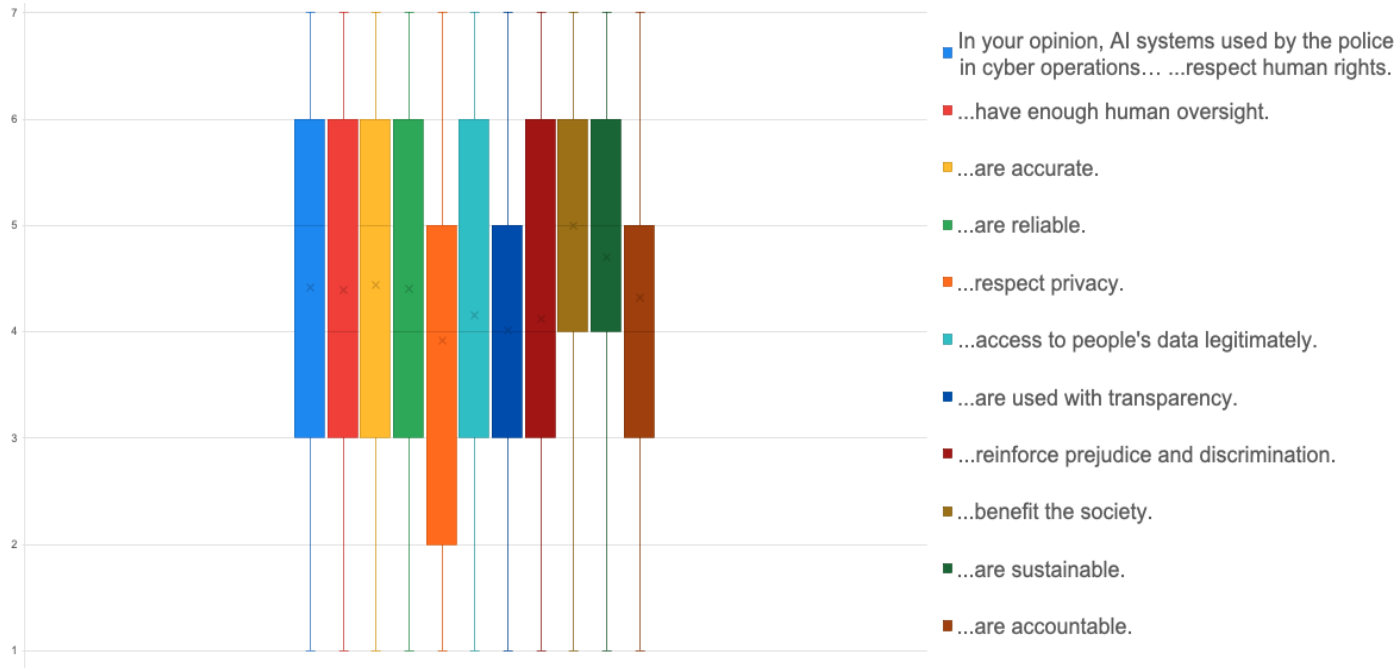


Figure 22 - Cyber Operations, distribution of votes

Cyber operations were the topic where the least negative sentiment was observed, the discourse is most evenly distributed, and the overall topic average of 4.40 shows that citizens favour such tools (Figure 22). The single negative subtopic is the respect to privacy, as seen in the other four areas as well. Unsurprisingly, benefit and sustainability not only average the highest but also keep the data distribution well in the positive end of the spectrum.

4. Police Hacking

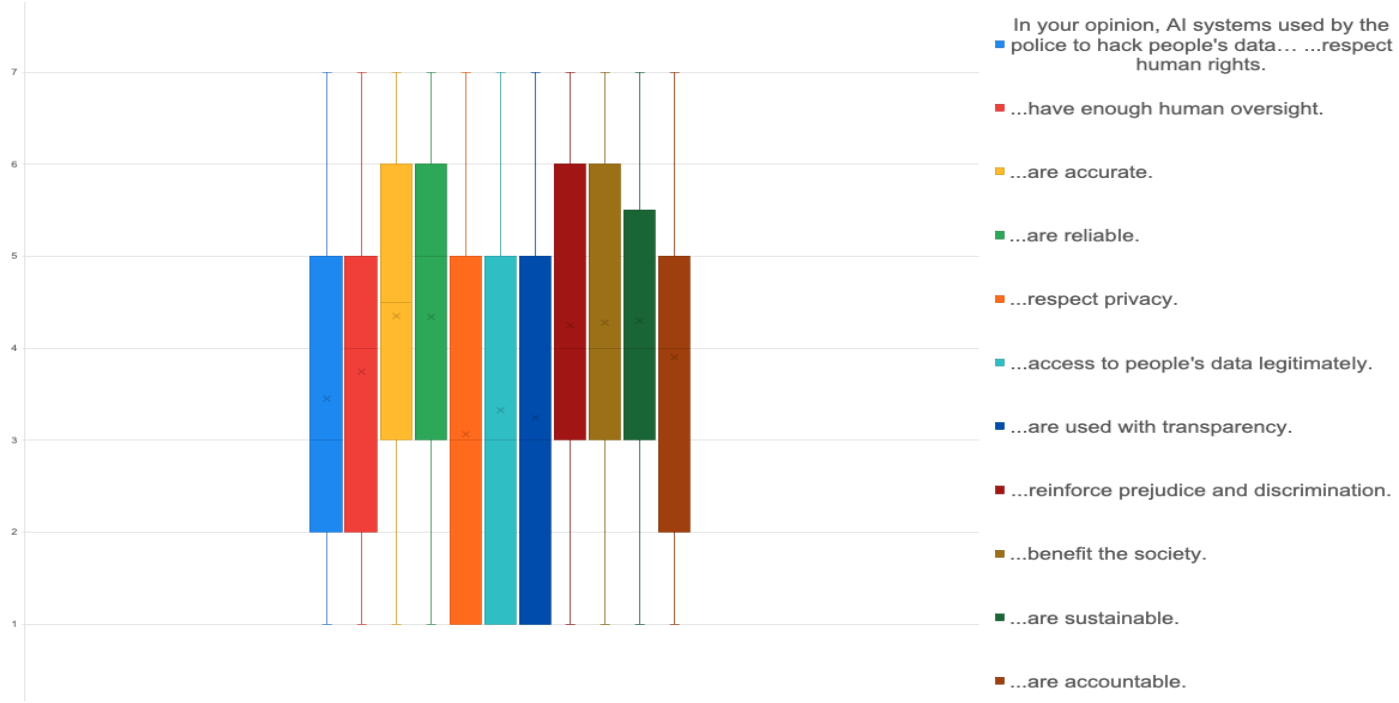


Figure 23 - Police Hacking, distribution of votes

Police Hacking was the topic that showed the most concern in citizens' answers. The respect of privacy, legitimate access to data and transparency again formed a cluster of most negative aspects, while the traditionally positive results of benefit to society barely averaged above the value of neutrality, although still keeping the discussion range on the positive side (Figure 23). This is the only topic falling below the value of neutrality with an average score of 3.85.

5. Decision-making in the justice systems

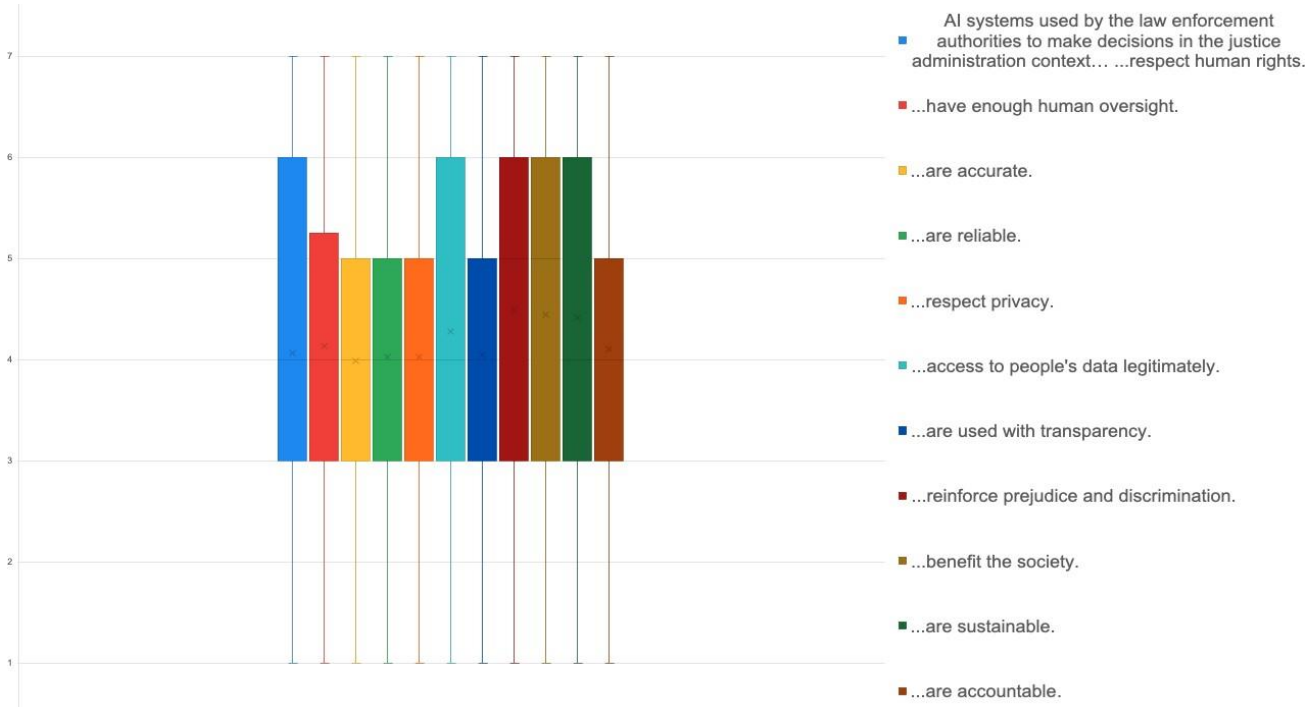


Figure 24 - Decision-Making in the Justice System, distribution of votes

The topic of AI systems that help in the administration of justice is the one with most even discussion spread, where 5 out of 11 topics are evenly distributed within one point of the middle value (Figure 24). The topic average score also confirms this, measuring 4.22.

Considering that the score of the "prejudice and discrimination" subtopic must be reversed, this constitutes the single feature that places the discussion range between 2 and 6 and has a negative value of 0.45 points below the neutral mark of 4.

3.2.2 Phase 2 – Idea generation

Based on the results in Phase 1, and by cross-referencing it with the data gathered in the social listening activity the following topics and subtopics were put forward in Phase 2 (Figure 25), where citizens provide solutions and ideas:

1. Biometric identification and Privacy:
Within the topic, the respect to privacy has the lowest average score. This combination of topic-subtopic is by far the most talked about online (as evidenced by the social listening

results), which arguably also makes it the most accessible for non-experts. Furthermore, social listening results show that most of the conversation in this pairing lies in the middle and there is a sizable swayable majority of citizens, who can form a positive opinion towards using biometric identification tools in the security domain.

2. Police hacking and Legitimacy:
   Police hacking is the category that causes the most negative discourse in the crowdsourcing and social listening activities. Within the topic, legitimacy, transparency and privacy have almost exactly the same results both in terms of distribution and average value placed by respondents, therefore choosing the subtopic to put forward for idea generation had to be determined by other factors. First and most important of these was to overlay the data sourced by the social listening on these categories. It showed that "Legitimacy" was the subtopic that fetched the most results (therefore is also most popular in the public domain), as well as the largest percentage classified as negative.

3. Predictive policing and Discrimination:

   Predictive policing was the second ranking topic in both the crowdsroucing and social listening activities. In the crowdsourcing activity, the subtopic of discrimination produced the highest deviation from the neutral middle towards negativity across all 5 topics. This is confirmed by the social listening activity, where trends over time show that this pairing causes not only an increasing discourse volume, but, more importantly, this discourse is also increasingly negative.

Figure 25 - Topic-Subtopic parings, Phase 2

Again, the questionnaire started with a set of voluntary demographic questions. Each of the three questions was preceded by a short explanatory paragraph in order for citizens to be able to formulate informed ideas and proposals.

A total of 84 people contributed, although not every respondent provided a recommendation in each of the three categories. Most did, which means that the number of generated ideas is more than 200.

3.2.3 Phase 3 – Idea selection

With the help of the LEA partners, all collected ideas were filtered for relevancy and potential for practical implementation. Similar ideas were clustered together, and, if present, important aspects of their enactment were included in the description as bullet points.

Citizens were asked to rank the following ideas for the three topics (Figure 26):

1. **How can the police use biometric identification tools while maintaining the privacy of citizens?**

Proposal 1: Requirements on enhancing transparency**.** Create a framework and establish transparency and accountability mechanisms that allow for oversight and control of the use of biometric identification tools in order to create a framework that prevents unnecessary and malicious use of IT. This could be achieved by:

· providing citizens with appropriate information on the proper design and use of these IT systems, as well as on the purpose of their implementation by LEAs (which data is collected, under which legal procedures, avoiding illegal access to them by implementing appropriate security measures) ,

· the establishment of permanent periodic audits of the AI systems used by LEAs, by mixed teams including representatives of civil society, and audit reports to ensure that they comply with the requirements of transparency, privacy and human rights protection and, above all, to ensure a balance between privacy and security.

Proposal 2: Safeguarding data through secure installation and storage, encryption, pseudo-anonymisation techniques for any potential data breaches and immediate deletion of any legally unjustified material.

Obviously with proper design of these systems that takes into account issues of privacy, human rights, elimination of discrimination between citizens, transparent use by properly trained staff.

Proposal 3: Citizens' consent: Biometric data should only be collected with the consent of the individual. In this way, citizens are aware of the data being collected and can opt out if they do not wish to share their biometric data.

2. **How can we make sure police hacking operations remain within the boundaries of the law and not gather data illegitimately?**

Proposal 1: Regulation and oversight: - There should be an independent oversight mechanism to monitor these operations and ensure that they are carried out in a legal and ethical manner.This could be achieved by:

· Establish clear guidelines and policies for this type of business. These guidelines should be developed in consultation with legal experts and should be reviewed and updated regularly to ensure that they remain consistent with applicable laws and regulations.

· Establish oversight and accountability measures to ensure that these guidelines are adhered to. This may include independent audits and investigations, as well as having a designated person or group responsible for monitoring and reporting on police use of piracy.

· Audit by heads of other countries. For example, an idea here is that the head of the German police may check that his Hungarian counterpart was illegally targeting an opposition journalist, this would have a deterrent effect on the organisation that did wrong.

Proposal 2: Transparency and accountability: The police should be transparent about their hacking operations and how they gather data.

This could be achieved by:

· Reporting on the number of devices that were hacked, the methods used, and the outcome of the operation.

· Delegation of the role of depositary to independent authorities.

· Ensure that people are promptly informed of the surveillance and that procedures are in place to allow them to verify the legitimacy of the surveillance.

Proposal 3: Warrant requirement: Police should be required to obtain a warrant before they hack into a device or system. This warrant should be based on probable cause and provide specific details about the data that is being sought and the reasons for the request.

Proposal 4: Data protection: The AI Act will lay down the foundations to regulate this type of AI systems. National authorities have to demonstrate to regulators that the AI systems are compliant with regulations such as the AI Act and the GDPR, and build powerful cryptographic databases and platforms for AI systems.

Proposal 5: "Training and education": Police officers should be trained on the importance of privacy and data protection, and on the specific laws and regulations that govern their actions. This will help ensure that they are aware of their responsibilities and are able to carry out their duties in a responsible and ethical manner.

3. **How can we avoid discrimination and prejudice resulting from predictive policing algorithms?**

Proposal 1: Data collection and representation: Algorithms should be trained on a diverse and representative dataset, which accurately reflects the population it is meant to serve. This could be achieved by:

· Train and retrain the models on a regular basis with a variety of data in order to avoid discriminatory results. This includes not only demographic data, but also data on crime patterns, socioeconomic factors, and other relevant variables.

Proposal 2: Fairness and transparency: Algorithms must be designed and tested for fairness and transparency, with measures in place to detect and prevent discrimination. This could be achieved by:

· Full algorithm transparency and accessibility for experts and researchers;

· Rules must be set as to the display of error percentages, trust regions, etc., so that users / operators, etc. can have some indication as to how much the results can be trusted or not. Moreover, the results need to support (not to lead) the investigations.

Proposal 3: Auditing and evaluation**:** Regular auditing and evaluation of predictive policing algorithms must be performed to identify and address any biases or discrimination that may arise. This could be achieved by:

· Organize a formal AI algorithm check by authorized non-police persons/institutes. For instance, EU or National AI Ombudsman or independent Privacy Authority.

Proposal 4: Training on police officers: Targeted training actions to protect human rights and the principles of non-discrimination

How can the police use biometric identification tools while maintaining the privacy of citizens?	How can we make sure police hacking operations remain within the boundaries of the law and not gather data illegitimately?	How can we avoid discrimination and prejudice resulting from predictive policing algorithms?
• Strong data safeguards • Requirements on enhancing transparency • Citizens' consent	• Regulation and oversight • Transparency and accountability • Warrant requirement • Data protection • Training and education	• Fairness by design, error transparency • Training of police officers • Representative data; data actualisation • Algorithm auditing and evaluation

Figure 26 - Proposed ideas, Phase 3

A short voluntary demographics questionnaire preceded the three questions for which respondents were asked to rank the proposal. In order to ensure that no default ordering (i.e the order that the questionnaire administrator used to input the recommendations) would be submitted, all proposals appeared in random order for each new loading of the survey. A further measure was to require respondents to interface with the randomized ranking presented to them, even if the order of ideas happened do coincide with their preferences. Votes are counted as follows:

Placing an idea first gives it *n* points, where n= equals the number of proposals available for ranking;

The idea at second place receives n-1 points;

Third placed idea receives n-2 points;

And so on until the last placed idea which gets 1 point.

Furthermore, respondents had the chance to comment after the ranking question in order to express further preferences or justify their vote.

The total number of respondents for Phase 3 is 95.

3.3 Phase 3 results discussion

How can the police use biometric identification tools while maintaining the privacy of citizens?

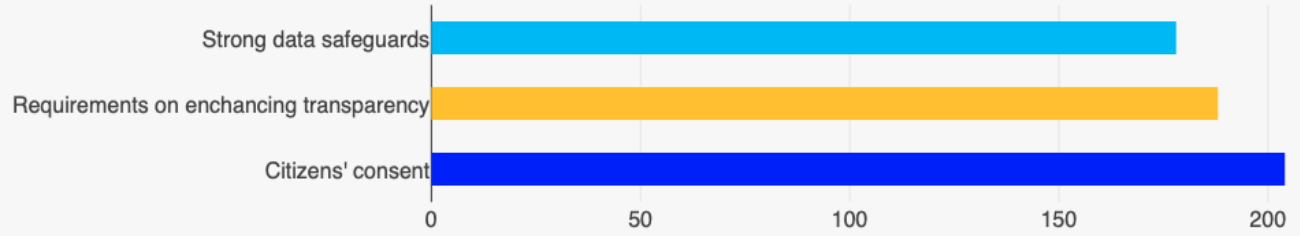


Figure 27 - First pairing, idea ranking

In this pairing (Figure 27), there is strong support for all three proposals, namely enhancing transparency, strengthening data safeguards and asking for citizens' consent. The majority of the respondents selected the idea that proposes asking for citizen's approval before biometric identification is applied or the option to opt out. While both social listening and crowdsourcing ranked biometric identification tools as the least concerning to people, the top selected idea does not support this. The implication here is that citizens would prefer to have the option of being totally "immune" to such AI systems, as compared to relying on a technology solution for better safeguards or an oversight solution for prevention. This is possibly due to the fact that citizens feel they can possibly be personally and directly subjected to such tools. Nevertheless, the ideas ranking second and third still score within the same range. Therefore, measures including informing citizens on what data is collected, for what purposes and what the legal justification is, along with designing the systems with greater focus on pseudo-anonymisation, encryption and more secure storage would make biometric identification more acceptable.

1. **How can we make sure police hacking operations remain within the boundaries of the law and not gather data illegitimately?**

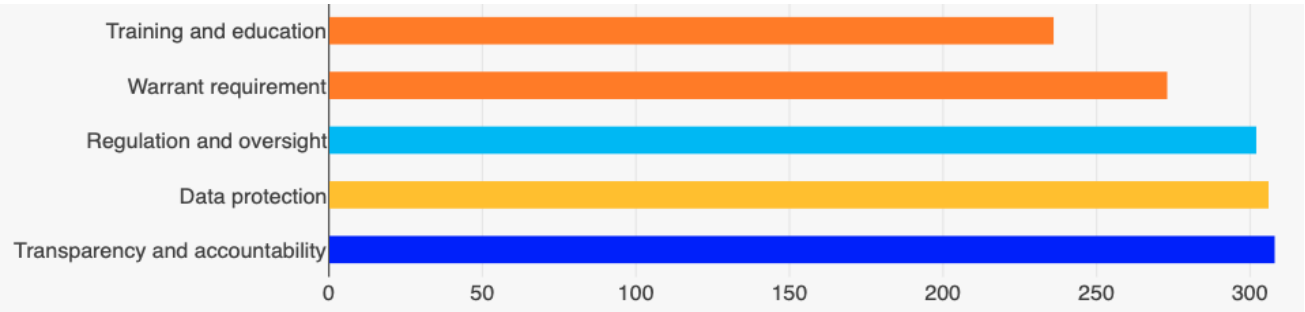


Figure 28 - Second pairing, idea ranking

The ranking of ideas under this topic is particularly important, as it was the one that generated the most negative sentiment within Phase 1 and the social listening activity. The idea of relying on training of law enforcement officers ranked last in all 5 proposals, which is an indicator that citizens think police operatives are not the problem in implementing hacking operations, i.e possible overstepping of authorities is not attributable to a personnel problem, but rather a systemic issue. Interestingly, the solution that is clearly "legal" in nature (requirements for a warrant prior to a

hacking operation) is not highly ranking. Both of these ideas would possibly have the potential to altogether prevent any illegitimate actions – either by a court denying a warrant or by a police officer deciding to not collect specific data. Opposite to the ranking discussed in the previous pairing (Figure 27), here we find that the two solutions that may fully stop the misuse of AI tools are placed at the bottom of citizens' priorities. The reason for this may be that citizens would not feel personally and directly affected by such operations, while they feel there is place for them in police work.

The top three ranking topics reinforce the somewhat positive attitude towards the benefit of police hacking, as they aim to only place it under a stricter framework of oversight and transparency, while increasing the protection of data gathered. This is a possible indicator that citizens think such operations contribute towards increased security, but are concerned of spill over of data gathering towards the wider population.

2. **How can we avoid discrimination and prejudice resulting from predictive policing algorithms?**

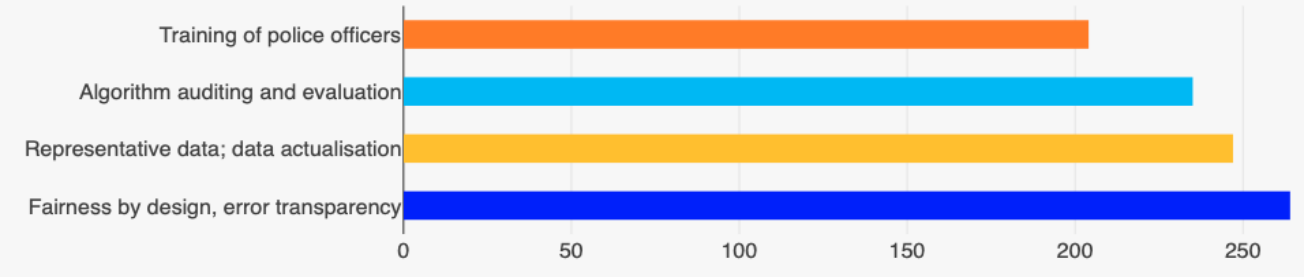


Figure 29 - Third pairing, idea ranking

In contrast to the previous two pairings, where the solutions focused on how the tools were implemented (biometrics) or regulated/controlled (police hacking), here citizens most often voted for the ideas that pertain directly to the very design of the AI systems in question. Again, the proper training of police officers is the lowest-ranking of all. Considering the training proposal from the previous paring was placed similarly, this is a clear indication that the public prioritises technical or regulatory solutions over personnel ones. In other terms, solutions should be directed towards *how* AI is implemented, by what standards and to what extent, not *by whom.*

The rest of the solutions are complementary to each other and are logically placed by the respondents to reflect the life-cycle of the AI system. The top-ranking solution underlines the need to have transparency built in the algorithms from the start, making them open to analysis from researchers and experts, and clearly indicating the probability for error in the computation. The second-best idea is to not only feed the predictive algorithms with data that is representative and non-discriminatory, but to update it regularly. Only after these two "technical" solutions, comes the "regulatory" one – that is the proposal for regular, independent auditing by authorised bodies in order to ensure oversight in cases of bias.

4 Passive Social Listening though Location-Based Searches

The analysis of information collected via social listening can be conducted in more than one dimensions, depending on its scope. Therefore, complementarily to the social listening and crowdsourcing activities presented in the previous sections 2 and 3, this section presents another dimension of social listening information analysis, related with the location-based searches. The aim of this location-based analysis is to uncover the areas in Europe that are mostly engaged/active on posting AI related information in social media platforms, and to highlight the sentiment extracted from these texts in order to identify the European areas that are reluctant to adopt AI technologies. Furthermore, the location-based analysis provides insights into areas where there may be low engagement, which could indicate low technological literacy.

During social listening, tweets posted on Twitter social media platform from November 2022 until March 2023 were collected, using AI-specific keywords. The selection of specific keywords was made with the aim of obtaining data related to this topic in a more general context. Given the purpose of the analysis, the data to be obtained had to have a more holistic overview, so as not to produce a biased result. The results of this analysis can be leveraged by the European Union in planning campaigns on AI technologies adoption in digitally illiterate areas, by giving additional emphasis on digital transformation of public administrations.

4.1 neralMethodology of Social Sensing

4.1.1 Data collection from social media

Social media platforms, such as Twitter, are valuable sources of real-time information on various topics, including artificial intelligence, due to their popularity and widespread use. Users from diverse backgrounds often express their opinions and share information on social media, providing a large volume of data that can be analyzed to gain insights into various topics, including the use of AI tools in Law Enforcement and the protection of privacy and fundamental rights.

In this specific case, the collection of tweets using a list of keywords such as "DataAct", "ArtificialIntelligence", "DataEthics", and "cybersecurity" previously presented in task D3.2 was facilitated by Twitter's publicly available Application Programming Interface (API). However, collecting data from social media platforms presented several challenges, including the tendency for users to discuss AI in various general sectors that were not always specific to actual applications. To address this issue, advanced search operators and filters were applied to the API to obtain a more targeted dataset based on the keywords list. Furthermore, the presence of extraneous information, such as links and URLs, necessitated pre-processing. Finally, after collecting the tweets related to AI, preprocessing was carried out to remove immaterialinformation, including location data. However, some tweets did contain valid location data related to AI, which could provide valuable insights. To identify these tweets, named entity recognition (NER) was applied to the location data. Only geographic entities, such as countries and cities, and other geopolitical entities (GPE), were retained for further analysis.

To conclude, the collection of Twitter data has allowed for the acquisition of a large dataset of opinions and emotions expressed by European citizens towards AI tools. Through the application of sentiment analysis techniques, valuable insights have been obtained, which can aid in the development of targeted solutions to promote trust in AI tools. These insights will be further detailed in the subsequent section.

4.1.2 Machine Learning approaches used to extract information

An analysis based on machine learning techniques was performed with the purpose of understanding the sentiment towards the use of AI tools, as well as the level of awareness of European citizens on the issue.

The type of sentiment analysis performed is based on the polarity of the collected data, supporting the identification of three main categories:

- Positive: A positive label corresponds to texts whose emotional tone indicates that the writer has a good opinion about the entity in consideration (e.g., a product, an object, a person, etc.).
- Neutral: A neutral label corresponds to texts whose writer has no opinion about the entity under consideration (for example, a product, an object, a person, etc.) or in texts that present ambiguity and lack of information.
- Negative: A negative sentiment label corresponds to texts whose emotional tone indicates that the writer has an attitude or view that is critical or disapproving about the entity in consideration (e.g., a product, an object, a person, etc.).

In the passive social listening approach, the neutral sentiment label corresponded to texts that either included no opinion or were irrelevant to the topic of interest.

The application of machine learning techniques on textual data requires performing a preprocessing procedure on the data, which is described below. The sentiment of each tweet was extracted with the use of the BERT algorithm. The next part of the analysis involved grouping the tweets based on their location and extracting the overall sentiment per region. The origin of each tweet was extracted with Named Entity Recognition (NER) techniques. Identifying the origin allowedperforming a more fine-grained analysis that involves a comparison between different European regions with regard to the sentiment and level of awareness on the use of AI tools.

1. The collected data underwent a thorough Preprocessing process, which included the removal of all punctuation, filtering out common words such as articles and pronouns, known as stop-words, and the application of lemmatization techniques. The removal of stop-words was particularly important to eliminate common words that do not contribute to the sentiment expressed in the tweets, while lemmatization allowed for the grouping of different inflected forms of the same word. Additionally, all characters were converted to lowercase to ensure consistency across the data. Finally, a location filter was applied to the data to ensure that only tweets originating from European locations were retained, which was essential to ensure the relevance of the sentiments expressed to European citizens.
2. Processing per tweet: The analysis of sentiment from social media is highly related with the opinion mining, since sentiments are connected to the feelings that people communicate in

various ways, such as through text, photographs, videos, links, and animated gifs, and opinion mining often deals with textual opinions given by the users. Thus, in order to identify the opinion of the users that post information about the AI related topics, the task of sentiment analysis has been performed, by applying the BERT model [2]. The input of this models is a tweet, and converts them into features. The converted into features textual data are then forwarded as input into the BERT model with a linear classifier on top. The output of the model is the predicted sentiment class along with the corresponding softmax probability. TheBERT model needs to be fine-tuned to the particular task of interest that has its own unique data distribution because it was pre-trained on Wikipedia and BookCorpus and has a significant quantity of generic information. In our instance, the sentiment classification task—a type of sequence classification task—was fine-tuned. At this point it should be noted, that in this case a pre-trained BERT model was used and it was further fine-tuned on the fine- grained (5-class) Stanford Sentiment Treebank (SST-5-standard) dataset [156] [3]. The datasetconsists of 11.855 film reviews samples. The labels of the samples, [0, 1, 2, 3, 4] correspond to the five different classes [very negative, negative, neutral, positive, very positive] with

regards to the sentiment expressed. This dataset is by default split into train, validation, and test sets. The corresponding sizes are 8.544 for the train set, 1.101 for the validation set, and 2.210 for the test set. The fine-tuned on the SST-5 dataset BERT model achieved an accuracy of 53.4 and an AUC score 0.6915 for the test set, and an accuracy of 49.65 and an AUC score 0.6787 for the validation set.

3. Post-Processing (Geographical analysis of sentiment and awareness): Named Entity Recognition allows the identification of entities of interest such as a person, a country, a product, etc., in a text. In this case, a NER algorithm was used to identify any mentioned valid European locations within each tweet. The origin of each tweet was extracted based on the extracted Geopolitical entities, for all the tweets that included such information. Next, the subset of tweets with known origin were grouped into belonging to four distinct European regions; Northern, Western, Southern, and Central-Eastern Europe. The number of tweets for each region was observed, and sentiment analysis was carried out for each group separately. This approach facilitated a more fine-grained analysis of the sentiments expressed within each region. In addition, it enabled a comparative analysis on the level of awareness on the issue between the different regions.

4.2 Results of Social Sensing

4.2.1 Sentiment analysis on European tweets

After the calculations, half of the population presented a mixed impression of the role of AI in security, while the other half expressed both positive and negative views. More specifically, nearly half of the tweets (43.3%) had neutral thoughts regarding AI in security systems, compared to 29.3% who were in favor of it, 3.9% who were extremely in favor of it, 19.3% who were against it, and 4.3% who were really against it.

According to Figure 30, this research revealed a sizable number of opposing views, both positive and negative, leading to the conclusion that it was divisive in society. However, the fact that the most considerable portion of people had a neutral opinion of AI in security systems emphasized the need of increasing the interest of people on the subject and focus on the benefits of AI tools to illustrate their effectiveness.

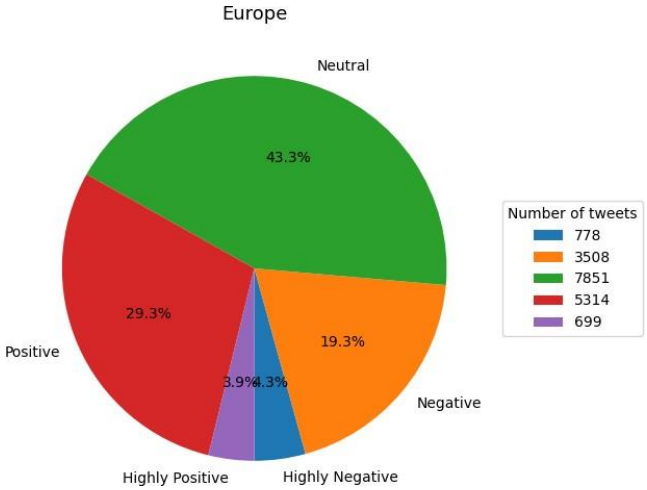


Figure 30 - Pie chart showing the results of Sentiment Analysis of 18,150 tweets from Europe

4.2.2 Dividing the dataset into 4 European Regions

In this subsection, an analysis of location data is illustrated, in order to compare the level of interest between different European regions. From the initial dataset that consisted of 754,713 tweets, 11% of them (83,019 tweets) included locations, and 2.4% (18,150 tweets) included locations within Europe. The tweets that did not include locations were filtered out for this analysis.

The tweets were divided according to their location information into 4 European regions:

- Central and Eastern Europe: 'Albania', 'Bosnia and Herzegovina', 'Bulgaria', 'Croatia', 'Kosovo', 'Hungary', 'Poland', 'Romania', 'Slovakia', 'Slovenia', 'Serbia', 'Czech Republic'.
- Northern Europe: 'Denmark', 'Estonia', 'Finland', 'Iceland', 'Ireland', 'Latvia', 'Lithuania', 'Sweden', 'Norway', 'United Kingdom'.
- Southern Europe: 'Greece', 'Cyprus', 'Italy', 'Spain', 'Malta', 'Portugal'.
- Western Europe: 'Austria', 'Belgium', 'France', 'Germany', 'Luxembourg', 'Netherlands', 'Switzerland', 'Monaco', 'Liechtenstein'.

An analysis regarding the origin of the tweets is presented in Figure 31. The figure indicates notable disparities in the frequency of discussion on the subject of AI tools in law enforcement and privacy protection across various regions of Europe. The study revealed that the Northern and Western regions of Europe, encompassing countries such as the United Kingdom, France, Ireland, and Germany, recorded the highest number of tweets regarding this topic. To be more specific, 9558 tweets were from Northern Europe. Western Europe followed with 5499 tweets, while Southern Europe and Central-Eastern Europe were the least represented regions with 2094 and 999 tweets respectively. This raises the possibility of a potential bias in the sentiment analysis results obtained from Twitter data collected from these regions, particularly towards Northern and Western Europe, where a higher number of tweets were recorded. The high number of tweets from Northern and

Western Europe could indicate that citizens in these regions are more engaged and knowledgeable about the topic.

Overall, these findings provide valuable insight into the differences in conversation and interest across Europe on the topic of AI tools. The data may serve as a basis for policy decisions and initiatives aimed at promoting awareness and understanding of this subject across all regions of Europe.

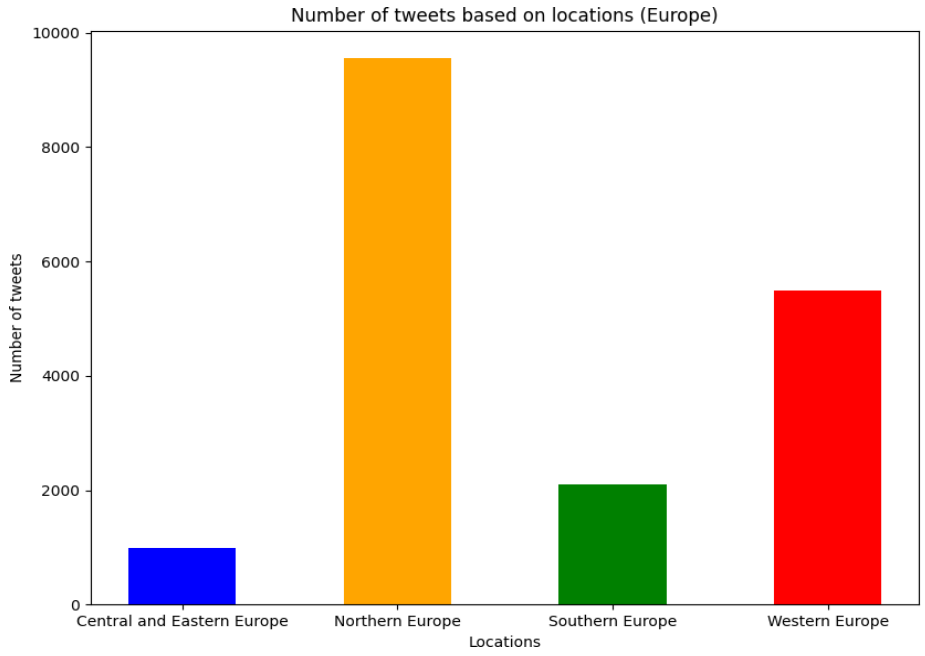


Figure 31 - Bar plot of number of tweets based on location, divided in 4 European Regions

4.2.3 Results of Sentiment Analysis on 4 European Regions

In order to achieve a more detailed examination of the sentiment towards AI tools across distinct regions of Europe, a separate sentiment analysis was conducted for each of the four regions: Northern Europe, Western Europe, Southern Europe, and Central-Eastern Europe. Upon analyzing the data presented in Figure 32 below, several observations were made. Firstly, it was noted that individuals across different European regions held varying opinions on the topic, which may be influenced by differences in technological literacy. In regions where individuals are more technologically literate, such as Northern and Western Europe, there was a higher frequency of neutral opinions and fewer highly positive or negative opinions. In contrast, in regions where individuals are less technologically literate, such as Central-Eastern Europe, there was a higher percentage of negative sentiments and a smaller percentage of positive sentiments.

Moreover, it was observed that Northern Europe, which had the highest number of tweets, presented relatively smaller differences between the sentiments expressed. This suggests that controversies on the topic were highly amplified in that region. Western Europe also had a large number of tweets, with a greater number of neutral opinions and fewer highly positive or negative opinions compared to the rest of Europe. These regions have already begun discussions on the topic of AI, therefore it would be beneficial to highlight the benefits of AI.

Conversely, citizens of Central-Eastern Europe presented the highest percentage of negative sentiments, and the smallest percentage of positive sentiments. Furthermore, the observation that this region released the smallest number of tweets, is indicating a lack of interest or knowledge on the topic, which may be attributed to lower levels of technological literacy. In contrast, people from Southern Europe exhibited the lowest percentage of negative sentiments and the highest percentage of positive sentiments. However, they also had one of the lowest numbers of tweets, with opinions opposing those from Central-Eastern Europe. These observations suggest that there is a need for education to increase understanding and awareness of AI tools and their benefits in Central-Eastern and Southern Europe.

Overall, the data presented in Figure 32 highlights the need for targeted education and awareness campaigns to increase understanding and promote the benefits of AI tools in regions where individuals may be less technologically literate.

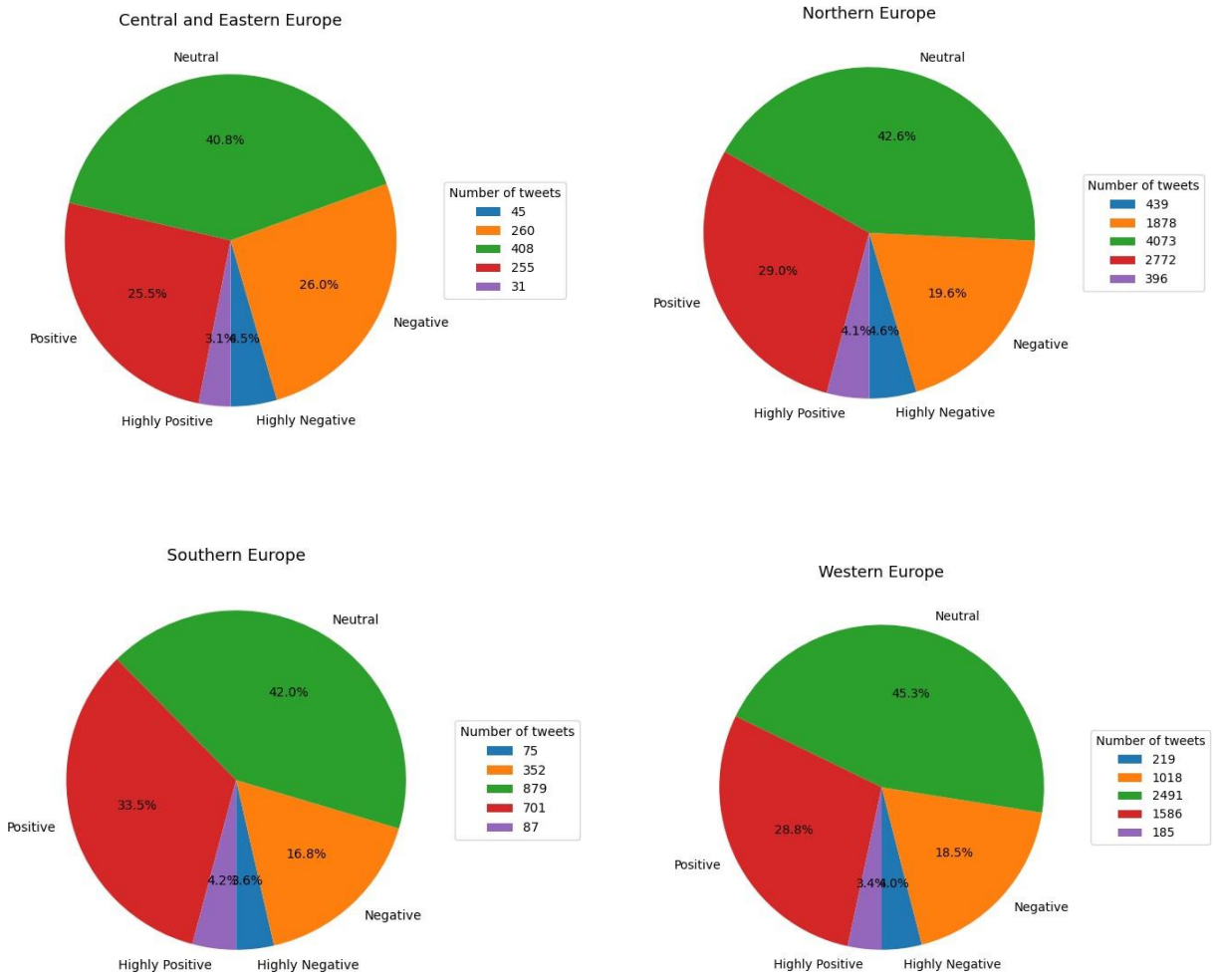


Figure 32 - Results of Sentiment Analysis on every European region

4.3 Conclusions

In conclusion, this analysis aimed to investigate the public conversation on the use of Artificial Intelligence tools, using social listening. The data was collected from Twitter using machine learning techniques and analytics, including text pre-processing, grouping, and visualization. The sentiment analysis on Europe showed differences in opinion across the continent, with the highest percentage of tweets expressing a neutral sentiment. To achieve a more detailed examination, sentiment analysis was conducted for each of the four regions: Northern Europe, Western Europe, Southern Europe, and Central-Eastern Europe. By conducting separate sentiment analyses for each of the four regions in Europe, the study achieved a more targeted examination of the sentiments expressed in each region.

Important takeaway

Based on the analysis conducted, and according to the scope of the passive social-listening approach presented in this section, the first outcome concerns the identification of the European area that is more active on posting AI related information in social media platforms. According to the results, Northern Europe seems to have a significant number of tweets posted within the data collection timeframe.

A second outcome of the analysis concerns the opinions shared within the collected data, regarding the AI use in different European areas. The results show that the opinions on AI tools vary across different European regions, and are likely influenced by differences in the area's technological literacy. In this scope, the sentiment analysis facilitated the further investigation of this topic. Central-Eastern and Southern Europe are both having a low number of tweets posted, and high percentage of neutral sentiment, indicating a need for education on the topic. In addition to this, and according to the negative sentiment's percentage presented, these areas seem also to be reluctant to adopt AI technologies.

Furthermore, the findings of this analysis suggest that Western Europe seems to be a slow adopter of AI, according to the numbers of tweets posted during these months and the high neutral sentiment extracted. This may impact its future competitiveness, despite the stimulus provided to AI adoption during the COVID-19 pandemic. [1]

As a recommendation, targeted education and awareness campaigns are suggested to increase understanding and promote the benefits of AI tools in regions with low engagement and lower technological literacy.

5 Citizen-produced recommendations. Next steps.

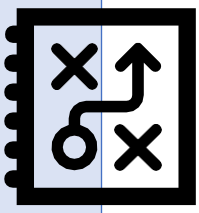
5.1 Biometric identification and Privacy

Policy action points

1. **Citizens' consent:**
- **Introduce legislation that requires law enforcement agencies to obtain explicit and informed consent from citizens before collecting, storing, or using their biometric data.**
- **Implement mechanisms for citizens to easily withdraw their consent and have their biometric data deleted.**
- **Provide clear and accessible information to citizens about the purpose and use of biometric identification tools, and the potential risks to their privacy and other rights.**

2. **Enhancing transparency:**
- **Require law enforcement agencies to publish regular reports on the use of biometric identification tools, including information on the number and types of tools used, the purposes for which they are used, and the outcomes of their use.**
- **Establish an independent oversight body to review the use of biometric identification tools and ensure that they are used in compliance with relevant laws, regulations, and ethical standards.**
- **Promote public education and awareness campaigns on the use of biometric identification tools and their potential impact on privacy and other rights.**

3. **Stronger data safeguards:**
- **Implement robust data protection and security measures to protect biometric data from unauthorized access, use, or disclosure.**
- **Develop clear guidelines and standards for the collection, storage, and use of biometric data by law enforcement agencies, and ensure that these are regularly reviewed and updated.**
- **Encourage the use of privacy-enhancing technologies such as encryption, anonymization, and pseudonymization to minimize the risks associated with biometric identification tools.**



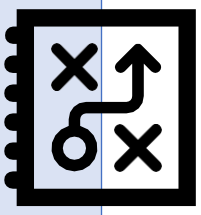
5.2 Police Hacking and Legitimacy

Policy action points

1. **Increased transparency and accountability:**
- **Regular reporting on the use of police hacking operations and the outcomes achieved.**
- **Establishing clear guidelines for police hacking operations, including the types of crimes that can be investigated and the circumstances under which hacking can be used.**
- **Creating an independent oversight body to review and monitor police hacking operations.**

2. **Better data protection:**
- **Requiring encryption of all data obtained through police hacking operations to prevent unauthorized access.**
- **Establishing strict data retention and deletion policies to minimize the risk of data breaches and misuse.**
- **Providing training to police officers on data protection and privacy laws.**

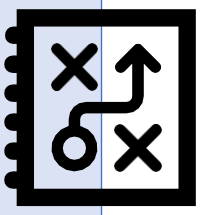
3. **Better regulation and oversight:**
- **Ensuring that all police hacking operations are conducted in compliance with the law and with respect for human rights.**
- **Establishing clear procedures for obtaining warrants and other legal authorizations for hacking operations.**
- **Providing training to judges and magistrates on the use of hacking as an investigative technique.**



5.3 Predictive policing and discrimination

Policy action points

1. **Fairness by design, error transparency:**
- **Establish guidelines and standards for developing and implementing predictive policing algorithms that are designed to ensure fairness and transparency.**
- **Require law enforcement agencies to regularly report on the accuracy, bias, and error rates of their predictive policing systems.**
- **Provide training and support for law enforcement agencies to help them identify and correct biases and errors in their systems.**
2. **Representative data, data actualization:**
- **Require law enforcement agencies to use data that is representative of the communities they serve, and to regularly update and audit their data to ensure it remains accurate and unbiased.**
- **Establish oversight bodies to monitor the use of predictive policing algorithms and to ensure that they are not being used in discriminatory or prejudicial ways.**
- **Promote the development of alternative data sources that can be used to supplement or replace biased or inaccurate data.**
3. **Algorithm auditing and evaluation:**
- **Require independent audits of predictive policing algorithms to evaluate their accuracy, fairness, and potential for bias.**
- **Establish a process for ongoing evaluation of predictive policing algorithms to ensure that they remain effective, accurate, and fair.**
- **Provide resources and support for law enforcement agencies to help them evaluate and improve their predictive policing systems.**



5.4 Next steps – connection to upcoming tasks

The most important purpose for the crowdsourcing activity and the social listening that underlines it is to feed into ***WP4.*** More specifically, it will form one of the primary sources for formulating recommendations and proposals directed to policy-makers, LEAs, civil society and technology developers. This will go beyond the expansion and refinement of the citizen-produced and ranked ideas. In the tasks under WP4, the data relating to citizens' concerns will be further examined as it relates to the deployment of AI in all of the five topics covered in this deliverable in order to identify gaps in policy. Furthermore, the data at hand will be used as a reference point for recommendations that are formed under other tasks, for example the Policy Labs in Task 3.4. The list of all citizen-produced proposals will serve as further source for novel ideas, even if some of them were not included in Phase 3 of the crowdsourcing. Lastly, the findings of this deliverable will serve ***WP5*** in producing content that either directly answers citizen's concerns or highlights instances where respondents' ideas were taken up, in order to reinforce positive attitudes toward AI in the security domain.

References

[1] Hradecky, D., Kennell, J., Cai, W., & Davidson, R. (2022). Organizational readiness to adopt artificial intelligence in the exhibition sector in Western Europe. International journal of information management, 65, 102497.

Annexes

Annex 1 "Social Listening keywords"

Biometric identifiers

1. Privacy – negative
    - Keywords position 1: biometric identification | facial recognition | biometrics | biometric* authentication | fingerprint mapping | retina scan* | iris scan*
    - Keywords position 2: police | law enforcement | security agencies | enforcement agencies
    - Keywords Position 3: disrupts|impedes|does not acknowledge|not sensitive|harm*|abuse|restrict
    - Keywords Position 4: privacy
    - Exclusions: -Analytica- Autonomous vehicle - CBD Hemp

2. Privacy – positive
    - Keywords position 1: biometric identification | facial recognition | biometrics | biometric* authentication | fingerprint mapping | retina scan* | iris scan*
    - Keywords position 2: police | law enforcement | security agencies | enforcement agencies
    - Keywords position 3: acknowledge | promote | respect | safeguard | by design | upholding
    - Keywords position 4: privacy
    - Exclusions: -no safeguard -lacks safeguards -doesn't promote privacy -does not respect -doesn't respect -protectionCloud
3. Privacy
    - Keywords position 1: biometric identification | facial recognition | biometrics | biometric* authentication | fingerprint mapping | retina scan* | iris scan*
    - Keywords position 2: police | law enforcement | security agencies | enforcement agencies
    - Keywords Position 3: privacy
    - Exclusions: -Analytica- Autonomous vehicle - CBD Hemp

4. Efficiency, Reliability, Accuracy – positive
    - Keywords position 1: biometric identification | facial recognition | biometrics | biometric* authentication | fingerprint mapping | retina scan* | iris scan*
    - Keywords position 2: police | law enforcement | security agencies | enforcement agencies
    - Keywords Position 3: effectively | efficient | reliable | accurately | accurate | fight crime | prevent crime | increased security | support crime preventionKeywords
    - Exclusions: -low efficiency -low reliability -not reliable -not efficient -not accurate

5. Efficiency, Reliability, Accuracy – negative
    - Keywords position 1: biometric identification | facial recognition | biometrics | biometric* authentication | fingerprint mapping | retina scan* | iris scan*

- Keywords position 2: police | law enforcement | security agencies | enforcement agencies
- Keywords Position 3: ineffective | inefficient | not reliable | not accurate | inaccurate | unreliable

6. Efficiency, Reliability, Accuracy
    - Keywords position 1: biometric identification | facial recognition | biometrics | biometric* authentication | fingerprint mapping | retina scan* | iris scan*
    - Keywords position 2: police | law enforcement | security agencies | enforcement agencies
    - Keywords Position 3: efficiency | reliability | accuracy | efficient | reliable | accurate
    - Exclusions:

7. Legitimacy – positive
    - Keywords position 1: biometric identification | facial recognition | biometrics | biometric* authentication | fingerprint mapping | retina scan* | iris scan*
    - Keywords position 2: police | law enforcement | security agencies | enforcement agencies
    - Keywords Position 3: legitimacy | legitimate | is legitimate
    - Exclusions: -not legitimate -low legitimacy

8. Legitimacy – negative
    - Keywords position 1: biometric identification | facial recognition | biometrics | biometric* authentication | fingerprint mapping | retina scan* | iris scan*
    - Keywords position 2: police | law enforcement | security agencies | enforcement agencies
    - Keywords Position 3: not legitimate | illegal

9. Legitimacy
    - Keywords position 1: biometric identification | facial recognition | biometrics | biometric* authentication | fingerprint mapping | retina scan* | iris scan*
    - Keywords position 2: police | law enforcement | security agencies | enforcement agencies
    - Keywords Position 3: legitimacy | legitimate | lawfulness | lawful

10. Transparency, Accountability – positive
    - Keywords position 1: biometric identification | facial recognition | biometrics | biometric* authentication | fingerprint mapping | retina scan* | iris scan*
    - Keywords position 2: police | law enforcement | security agencies | enforcement agencies
    - Keywords Position 3: disrupts|impedes|does not acknowledge|not sensitive|harm*|abuse|restrict
    - Exclusions: -low transparency -no transparency -no accountability -no oversight -lack of oversight -lack of accountability

11. Transparency, Accountability – negative
    - Keywords position 1: biometric identification | facial recognition | biometrics | biometric* authentication | fingerprint mapping | retina scan* | iris scan*
    - Keywords position 2: police | law enforcement | security agencies | enforcement agencies
    - Keywords Position 3: no | lack | deficient | weak | ineffective | lack of
    - Keywords Position 4: transparent | accountable | transparency | accountability | oversight

12. Transparency, Accountability
    - Keywords position 1: biometric identification | facial recognition | biometrics | biometric* authentication | fingerprint mapping | retina scan* | iris scan*
    - Keywords position 2: police | law enforcement | security agencies | enforcement agencies
    - Keywords Position 3: transparent | accountable | transparency | accountability | oversight

13. Discrimination – positive
    - Keywords position 1: biometric identification | facial recognition | biometrics | biometric* authentication | fingerprint mapping | retina scan* | iris scan*
    - Keywords position 2: police | law enforcement | security agencies | enforcement agencies
    - Keywords Position 3: no discrimination | impartial | do not discriminate

14. Discrimination – negative
    - Keywords position 1: biometric identification | facial recognition | biometrics | biometric* authentication | fingerprint mapping | retina scan* | iris scan*
    - Keywords position 2: police | law enforcement | security agencies | enforcement agencies
    - Keywords Position 3: promote discrimination | promote racism | racial bias | disproportionately | inequality
    - Exclusions: -CBD Hemp -metersBeyond

15. Discrimination
    - Keywords position 1: biometric identification | facial recognition | biometrics | biometric* authentication | fingerprint mapping | retina scan* | iris scan*
    - Keywords position 2: police | law enforcement | security agencies | enforcement agencies
    - Keywords Position 3: discrimination | impartial | bias | discriminate | race | minorities

Predictive policing

1. Privacy – negative
   - Keywords position 1: predictive policing | preventive policing | crime forecasting
   - Keywords position 2: disrupts|impedes|does not acknowledge|not sensitive|harm*|abuse|restrict
   - Keywords Position 3: privacy
   - Exclusions: -seekersBaiduBenefits

2. Privacy – positive
   - Keywords position 1: predictive policing | preventive policing | crime forecasting
   - Keywords position 2: acknowledges | promotes | respects | safeguards | by design | upholding
   - Keywords position 3: privacy
   - Exclusions: -no safeguards -lacks safeguards -doesn't promote privacy -does not respect -doesn't respect

3. Privacy
   - Keywords position 1: predictive policing | preventive policing | crime forecasting
   - Keywords position 3: privacy

4. Efficiency, Reliability, Accuracy – positive
   - Keywords position 1: predictive policing | preventive policing | crime forecasting
   - Keywords position 2: effectively | effective | reliable | accurately | accurate | fight crime | prevent crime | increased security | support crime prevention
   - Exclusions: -low efficiency -low reliability -not reliable -not efficient -not accurate

5. Efficiency, Reliability, Accuracy – negative
   - Keywords position 1: predictive policing | preventive policing | crime forecasting
   - Keywords position 2: ineffective | inefficient | not reliable | not accurate | inaccurate | unreliable

6. Efficiency, Reliability, Accuracy
   - Keywords position 1: predictive policing | preventive policing | crime forecasting
   - Keywords position 2: efficiency | reliability | accuracy | efficient | reliable | accurate

7. Legitimacy – positive
   - Keywords position 1: predictive policing | preventive policing | crime forecasting
   - Keywords position 2: legitimacy | legitimate | is legitimate
   - Exclusions: -not legitimate -low legitimacy

8. Legitimacy – negative
   - Keywords position 1: predictive policing | preventive policing | crime forecasting
   - Keywords position 2: not legitimate | illegal

9. Legitimacy
   - Keywords position 1: predictive policing | preventive policing | crime forecasting

- Keywords position 2: legitimacy | legitimate | lawfulness | lawful

10. Transparency, Accountability – positive
    - Keywords position 1: predictive policing | preventive policing | crime forecasting
    - Keywords position 2: transparent | accountable | transparency | accountability | oversight
    - Exclusions: -low transparency-no transparency -no accountability -no oversight -lack of oversight -lack of accountability

11. Transparency, Accountability – negative
    - Keywords position 1: predictive policing | preventive policing | crime forecasting
    - Keywords position 2: no | lack | deficient | weak | ineffective | lack of
    - Keywords Position 3: transparent | accountable | transparency | accountability | oversight
    - Exclusions: -Analytica- Autonomous vehicle - CBD Hemp

12. Transparency, Accountability
    - Keywords position 1: predictive policing | preventive policing | crime forecasting
    - Keywords position 2: transparent | accountable | transparency | accountability | oversight

13. Discrimination – positive
    - Keywords position 1: predictive policing | preventive policing | crime forecasting
    - Keywords position 2: no discrimination | impartial | do not discriminate

14. Discrimination – negative
    - Keywords position 1: predictive policing | preventive policing | crime forecasting
    - Keywords position 2: promote discrimination | promote racism | racial bias | disproportionately | inequality
    - Exclusions: -seekersBaiduBenefits

15. Discrimination
    - Keywords position 1: predictive policing | preventive policing | crime forecasting
    - Keywords position 2: discrimination | impartial | bias | discriminate | race | minorities
    - Exclusions: -seekersBaiduBenefits

Cyber operations

1. Privacy – negative
    - Keywords position 1: police | law enforcement | security agencies | enforcement agencies
    - Keywords position 2: cyber operations | cyber technolog*
    - Keywords Position 3: disrupts|impedes|does not acknowledge|not sensitive|harm*|abuse|restrict
    - Keywords Position 4: privacy
    - Exclusions: - foreign policy – war – military - international relations

2. Privacy – positive
    - Keywords position 1: biometric identification | facial recognition | biometrics | biometric* authentication | fingerprint mapping | retina scan* | iris scan*
    - Keywords position 2: cyber operations | cyber technolog*
    - Keywords position 3: acknowledges | promotes | respect | safeguards | by design | upholding
    - Keywords position 4: privacy
    - Exclusions: - foreign policy – war – military - international relations -no safeguards - lacks safeguards -doesn't promote privacy -does not respect -doesn't respect

3. Privacy
    - Keywords position 1: police | law enforcement | security agencies | enforcement agencies
    - Keywords position 2: cyber operations | cyber technolog*
    - Keywords Position 3: privacy
    - Exclusions: - foreign policy – war – military - international relations

4. Efficiency, Reliability, Accuracy – positive
    - Keywords position 1: police | law enforcement | security agencies | enforcement agencies
    - Keywords position 2: cyber operations | cyber technolog*
    - Keywords Position 3: effectively | effective | reliable | accurately | accurate | fight crime | prevent crime | increased security | support crime prevention
    - Exclusions: - foreign policy – war – military - international relations -low efficiency -low reliability -not reliable -not efficient -not accurate

5. Efficiency, Reliability, Accuracy – negative
    - Keywords position 1: police | law enforcement | security agencies | enforcement agencies
    - Keywords position 2: cyber operations | cyber technolog*
    - Keywords Position 3: ineffective | inefficient | not reliable | not accurate | inaccurate | unreliable
    - Exclusions: - foreign policy – war – military - international relations

6. Efficiency, Reliability, Accuracy
    - Keywords position 1: police | law enforcement | security agencies | enforcement agencies
    - Keywords position 2: cyber operations | cyber technolog*
    - Keywords Position 3: efficiency | reliability | accuracy | efficient | reliable | accurate
    - Exclusions: - foreign policy – war – military - international relations

7. Legitimacy – positive
    - Keywords position 1: police | law enforcement | security agencies | enforcement agencies
    - Keywords position 2: cyber operations | cyber technolog*
    - Keywords Position 3: legitimacy | legitimate
    - Exclusions: - foreign policy – war – military - international relations – not legitimate – low legitimacy

8. Legitimacy – negative
    - Keywords position 1: police | law enforcement | security agencies | enforcement agencies
    - Keywords position 2: cyber operations | cyber technolog*
    - Keywords Position 3: not legitimate | illegal |illegitimate
    - Exclusions: - foreign policy – war – military - international relations

9. Legitimacy
    - Keywords position 1: police | law enforcement | security agencies | enforcement agencies
    - Keywords position 2: cyber operations | cyber technolog*
    - Keywords Position 3: legitimacy | legitimate | lawfulness | lawful
    - Exclusions: - foreign policy – war – military - international relations

10. Transparency, Accountability – positive
    - Keywords position 1: police | law enforcement | security agencies | enforcement agencies
    - Keywords position 2: cyber operations | cyber technolog*
    - Keywords Position 3: transparent | accountable | transparency | accountability | oversight
    - Exclusions: - foreign policy – war – military - international relations -low transparency -no transparency -no accountability -no oversight -lack of oversight -lack of accountability

11. Transparency, Accountability – negative
    - Keywords position 1: police | law enforcement | security agencies | enforcement agencies
    - Keywords position 2: cyber operations | cyber technolog*
    - Keywords Position 3: no | lack | deficient | weak | ineffective | lack of
    - Keywords Position 4: transparent | accountable | transparency | accountability | oversight

- Exclusions: - foreign policy – war – military - international relations

12. Transparency, Accountability
    - Keywords position 1: police | law enforcement | security agencies | enforcement agencies
    - Keywords position 2: cyber operations | cyber technolog*
    - Keywords Position 3: transparent | accountable | transparency | accountability | oversight
    - Exclusions: - foreign policy – war – military - international relations

13. Discrimination – positive
    - Keywords position 1: police | law enforcement | security agencies | enforcement agencies
    - Keywords position 2: cyber operations | cyber technolog*
    - Keywords Position 3: no discrimination | impartial | do not discriminate
    - Exclusions: - foreign policy – war – military - international relations

14. Discrimination – negative
    - Keywords position 1: police | law enforcement | security agencies | enforcement agencies
    - Keywords position 2: cyber operations | cyber technolog*
    - Keywords Position 3: promote discrimination | promote racism | racial bias | disproportionately | inequality
    - Exclusions: - foreign policy – war – military - international relations

15. Discrimination
    - Keywords position 1: police | law enforcement | security agencies | enforcement agencies
    - Keywords position 2: cyber operations | cyber technolog*
    - Keywords Position 3: discrimination | impartial | bias | discriminate | race | minorities
    - Exclusions: - foreign policy – war – military - international relations

Police Hacking

1. Privacy – negative
   - Keywords position 1: police hacking | law enforcement hacking | security agency hacking | enforcement agency hacking | government hacking
   - Keywords position 2: disrupts|impedes|does not acknowledge|not sensitive|harm*|abuse|restrict
   - Keywords Position 3: privacy
   - Exclusions: - -Big Pharma -China CNI -climate change

2. Privacy – positive
   - Keywords position 1: police hacking | law enforcement hacking | security agency hacking | enforcement agency hacking | government hacking
   - Keywords position 2: acknowledges | promotes | respects | safeguards | by design | upholding
   - Keywords position 3: privacy
   - Exclusions: -no safeguards -lacks safeguards -doesn't promote privacy -does not respect -doesn't respect

3. Privacy
   - Keywords position 1: police hacking | law enforcement hacking | security agency hacking | enforcement agency hacking | government hacking
   - Keywords position 3: privacy
   - Exclusions: -Big Pharma -5GAerospaceAfghanistanAfricaAidAir -climate change

4. Efficiency, Reliability, Accuracy – positive
   - Keywords position 1: police hacking | law enforcement hacking | security agency hacking | enforcement agency hacking | government hacking
   - Keywords position 2: effectively | effective | reliable | accurately | accurate | fight crime | prevent crime | increased security | support crime prevention
   - Exclusions: -low efficiency -low reliability -not reliable -not efficient -not accurate

5. Efficiency, Reliability, Accuracy – negative
   - Keywords position 1: police hacking | law enforcement hacking | security agency hacking | enforcement agency hacking | government hacking
   - Keywords position 2: ineffective | inefficient | not reliable | not accurate | inaccurate | unreliable

6. Efficiency, Reliability, Accuracy
   - Keywords position 1: police hacking | law enforcement hacking | security agency hacking | enforcement agency hacking | government hacking
   - Keywords position 2: efficiency | reliability | accuracy | efficient | reliable | accurate

7. Legitimacy – positive
   - Keywords position 1: police hacking | law enforcement hacking | security agency hacking | enforcement agency hacking | government hacking
   - Keywords position 2: legitimacy | legitimate | is legitimate

- Exclusions: -not legitimate -low legitimacy – climate change

8. Legitimacy – negative
   - Keywords position 1: police hacking | law enforcement hacking | security agency hacking | enforcement agency hacking | government hacking
   - Keywords position 2: not legitimate | illegal

9. Legitimacy
   - Keywords position 1: police hacking | law enforcement hacking | security agency hacking | enforcement agency hacking | government hacking
   - Keywords position 2: legitimacy | legitimate | lawfulness | lawful
   - Exclusions: -We and our nominees -Traci Park

10. Transparency, Accountability – positive
    - Keywords position 1: police hacking | law enforcement hacking | security agency hacking | enforcement agency hacking | government hacking
    - Keywords position 2: transparent | accountable | transparency | accountability | oversight
    - Exclusions: -low transparency-no transparency -no accountability -no oversight -lack of oversight -lack of accountability

11. Transparency, Accountability – negative
    - Keywords position 1: police hacking | law enforcement hacking | security agency hacking | enforcement agency hacking | government hacking
    - Keywords position 2: no | lack | deficient | weak | ineffective | lack of
    - Keywords Position 3: transparent | accountable | transparency | accountability | oversight

12. Transparency, Accountability
    - Keywords position 1: police hacking | law enforcement hacking | security agency hacking | enforcement agency hacking | government hacking
    - Keywords position 2: transparent | accountable | transparency | accountability | oversight

13. Discrimination – positive
    - Keywords position 1: police hacking | law enforcement hacking | security agency hacking | enforcement agency hacking | government hacking
    - Keywords position 2: no discrimination | impartial | do not discriminate

14. Discrimination – negative
    - Keywords position 1: police hacking | law enforcement hacking | security agency hacking | enforcement agency hacking | government hacking
    - Keywords position 2: promote discrimination | promote racism | racial bias | disproportionately | inequality
    - Exclusions: -climate change

15. Discrimination
    - Keywords position 1: police hacking | law enforcement hacking | security agency hacking | enforcement agency hacking | government hacking
    - Keywords position 2: discrimination | impartial | bias | discriminate | race | minorities

Decision making in justice systems

1. Privacy – negative
    - Keywords position 1: AI | artificial intelligence | algorithm
    - Keywords position 2: justice system | court system | courts | judiciary
    - Keywords Position 3: disrupts|impedes|does not acknowledge|not sensitive|harm*|abuse|restrict
    - Keywords Position 4: privacy
    - Exclusions: - Kinsey Ancient

2. Privacy – positive
    - Keywords position 1: AI | artificial intelligence | algorithm
    - Keywords position 2: justice system | court system | courts | judiciary
    - Keywords position 3: acknowledge | promote | respect | safeguard | by design | upholding
    - Keywords position 4: privacy
    - Exclusions: -no safeguard -lacks safeguards -doesn't promote privacy -does not respect -doesn't respect
3. Privacy
    - Keywords position 1: AI | artificial intelligence | algorithm
    - Keywords position 2: justice system | court system | courts | judiciary
    - Keywords Position 3: privacy

4. Efficiency, Reliability, Accuracy – positive
    - Keywords position 1: AI | artificial intelligence | algorithm
    - Keywords position 2: justice system | court system | courts | judiciary
    - Keywords Position 3: effectively | efficient | reliable | accurately | accurate | fight crime | prevent crime | increased security | support crime preventionKeywords
    - Exclusions: -low efficiency -low reliability -not reliable -not efficient -not accurate

5. Efficiency, Reliability, Accuracy – negative
    - Keywords position 1: AI | artificial intelligence | algorithm
    - Keywords position 2: justice system | court system | courts | judiciary
    - Keywords Position 3: ineffective | inefficient | not reliable | not accurate | inaccurate | unreliable

6. Efficiency, Reliability, Accuracy
    - Keywords position 1: AI | artificial intelligence | algorithm
    - Keywords position 2: justice system | court system | courts | judiciary
    - Keywords Position 3: efficiency | reliability | accuracy | efficient | reliable | accurate

- Exclusions:

7. Legitimacy – positive
    - Keywords position 1: AI | artificial intelligence | algorithm
    - Keywords position 2: justice system | court system | courts | judiciary
    - Keywords Position 3: legitimacy | legitimate | is legitimate
    - Exclusions: -not legitimate -low legitimacy

8. Legitimacy – negative
    - Keywords position 1: AI | artificial intelligence | algorithm
    - Keywords position 2: justice system | court system | courts | judiciary
    - Keywords Position 3: not legitimate | illegal

9. Legitimacy
    - Keywords position 1: AI | artificial intelligence | algorithm
    - Keywords position 2: justice system | court system | courts | judiciary
    - Keywords Position 3: legitimacy | legitimate | lawfulness | lawful

10. Transparency, Accountability – positive
    - Keywords position 1: AI | artificial intelligence | algorithm
    - Keywords position 2: justice system | court system | courts | judiciary
    - Keywords Position 3: disrupts|impedes|does not acknowledge|not sensitive|harm*|abuse|restrict
    - Exclusions: -low transparency -no transparency -no accountability -no oversight -lack of oversight -lack of accountability

11. Transparency, Accountability – negative
    - Keywords position 1: AI | artificial intelligence | algorithm
    - Keywords position 2: justice system | court system | courts | judiciary
    - Keywords Position 3: no | lack | deficient | weak | ineffective | lack of
    - Keywords Position 4: transparent | accountable | transparency | accountability | oversight

12. Transparency, Accountability
    - Keywords position 1: AI | artificial intelligence | algorithm
    - Keywords position 2: justice system | court system | courts | judiciary
    - Keywords Position 3: transparent | accountable | transparency | accountability | oversight

13. Discrimination – positive
    - Keywords position 1: AI | artificial intelligence | algorithm
    - Keywords position 2: justice system | court system | courts | judiciary
    - Keywords Position 3: no discrimination | impartial | do not discriminate

14. Discrimination – negative
    - Keywords position 1: AI | artificial intelligence | algorithm

- Keywords position 2: justice system | court system | courts | judiciary
- Keywords Position 3: promote discrimination | promote racism | racial bias | disproportionately | inequality
- Exclusions: - Assisted Living

15. Discrimination
    - Keywords position 1: AI | artificial intelligence | algorithm
    - Keywords position 2: justice system | court system | courts | judiciary
    - Keywords Position 3: discrimination | impartial | bias | discriminate | race | minorities

Annex 2 "Social listening – number of results by topics and sentiment"

Note: '--' signifies the number of results that were identified as very negative, while '–' signifies the number of results that were identified as negative; same is applicable to the positive and very positive results'; Fields showing the part of negative (very negative+negative) results as a percentage of the whole are colour-coded; darker colours signify a more negative overall discourse.

	Biometric identifiers					% negative	avg. sentimen
TOTAL RESULTS			177950				
	--	-	/	+	++		
TOTAL PER SENT. RANGE	40815	568	123660	232	12675	23.26%	-0.11
Privacy			66299				
	--	-	/	+	++		
	10766	191	52361	33	2948	16.53%	-0.079
Efficiency, Reliability, Accuracy			40582				
	--	-	/	+	++		
	9378	142	22879	130	8053	23.46%	-0.038
Legitimacy			12078				
	--	-	/	+	++		
	4300	32	7469	15	262	35.87%	-0.223
Transparency, Accountability			41319				
	--	-	/	+	++		
	8935	98	31375	36	875	21.86%	-0.127
Discrimination			17672				
	--	-	/	+	++		
	7436	105	9576	18	537	42.67%	-0.274

	Predictive Policing					% very negative	avg. sentimen
TOTAL RESULTS			40078				
	--	-	/	+	++		
TOTAL PER SENT. RANGE	12656	199	25092	63	2068	32.07%	-0.201
Privacy			2672				
	--	-	/	+	++		
	573	13	1956	0	130	21.93%	-0.11
Efficiency, Reliability, Accuracy			11287				
	--	-	/	+	++		
	1973	31	8141	31	1111	17.75%	-0.052
Legitimacy			1493				
	--	-	/	+	++		
	393	3	1063	2	32	26.52%	-0.169
Transparency, Accountability			8896				
	--	-	/	+	++		
	1421	65	6990	26	394	16.70%	-0.08
Discrimination			15730				
	--	-	/	+	++		
	8296	87	6942	4	401	53.29%	-0.394

	Cyber Operations					% very negative	avg. sentiment
TOTAL RESULTS			441				
	--	-	/	+	++		
TOTAL PER SENT. RANGE	222	0	190	0	29	50.34%	-0.294
Privacy			23				
	--	-	/	+	++		
	5	0	16	0	2	21.74%	-0.039
Efficiency, Reliability, Accuracy			190				
	--	-	/	+	++		
	98	0	82	0	10	51.58%	-0.313
Legitimacy			154				
	--	-	/	+	++		
	114	0	33	0	7	74.03%	-0.47
Transparency, Accountability			54				
	--	-	/	+	++		
	3	0	42	0	9	5.56%	+0.069
Discrimination			20				
	--	-	/	+	++		
	2	0	17	0	1	10.00%	-0.027

	Police Hacking					% negative	avg. sentiment
TOTAL RESULTS			52851				
	--	-	/	+	++		
TOTAL PER SENT. RANGE	19196	396	32474	41	744	36.32%	-0.233
Privacy			15574				
	--	-	/	+	++		
	3965	77	11327	3	202	25.46%	-0.16
Efficiency, Reliability, Accuracy			4796				
	--	-	/	+	++		
	1769	47	2783	13	184	36.88%	-0.224
Legitimacy			16343				
	--	-	/	+	++		
	7395	208	8564	20	156	45.25%	-0.305
Transparency, Accountability			10584				
	--	-	/	+	++		
	2522	41	7854	3	164	23.83%	-0.148
Discrimination			5554				
	--	-	/	+	++		
	3545	23	1946	2	38	63.83%	-0.305

	Decision making in justice management					% very negative	avg. sentiment
TOTAL RESULTS			30446				
	--	-	/	+	++		
TOTAL PER SENT. RANGE	8990	244	19053	95	2064	29.53%	-0.152
Privacy			2837				
	--	-	/	+	++		
	626	26	2043	0	142	22.07%	-0.102
Efficiency, Reliability, Accuracy			6359				
	--	-	/	+	++		
	1328	64	4004	15	948	20.88%	-0.035
Legitimacy			2353				
	--	-	/	+	++		
	1243	10	1017	2	81	52.83%	-0.327
Transparency, Accountability			6712				
	--	-	/	+	++		
	1436	63	4653	2	558	21.39%	-0.089
Discrimination			12185				
	--	-	/	+	++		
	4357	81	7336	76	335	35.76%	-0.226

Annex 3 "Crowdsourcing Phase 1 questions"

1. Landing page (open https://crowdsourcing.ecas.org/en/popai for references)

Exploring citizens' main concerns and attitudes with regard to the use of Artificial Intelligence by Law Enforcement Authorities (LEAs).

POP AI (A European Positive Sum Approach towards AI tools in support of Law Enforcement and safeguarding privacy and fundamental rights) is a project which aims to foster trust in artificial intelligence (AI) for the security domain via increased awareness, ongoing social engagement, consolidating knowledge on the topic and offering a unified European view across Law Enforcement Agencies (LEAs). The goal is to create an ecosystem that will form the structural basis for a sustainable and inclusive European AI hub for Law Enforcement.

Visit project's site

Newsletter

Learn about all our new projects, get updates on active ones and contribute where it is most needed!

2. Socio-demographic questionnaire

***Introductory paragraph*:**

In the framework of the Horizon2020 project POP AI, we are currently exploring citizen's main concerns and attitudes with regards to the use of Artificial Intelligence (AI) by Law enforcement Authorities (LEAs). With this questionnaire, we would like to solicit the opinion of citizens concerning selected topics related to the use of AI tools in policing. We would like to invite you to share your point of view and help us understand better how citizens perceive the use of AI in policing, what their main concerns and priorities are. Before starting, we would like to understand your living situation better. Thank you very much for filling in the following questions:

What is your gender?

· Female

· Male

· Non binary

What is your age group?

· Below 20 years old

· 20-34 years old

· 35-49 years old

· 50-64 years old

· Above 65 years old

What is the highest level of education that you completed?

· High school or equivalent

· Vocational training

· Bachelor or equivalent

· Master or equivalent

· Ph.D. or higher

What is your estimated household income?

· Less than 20.000 €

· 20.000 € - 39.999 €

· 40.000 € - 59.999 €

· 60.000 € - 79.999 €

· 80.000 € - 99.999 €

· More than 100.000 €

Would you consider yourself religious?

· I don’t have any religion

· Not religious

· Religious

· Somehow religious

· Very religious

In which country are you currently residing?

3. AI use cases questionnaires

1. Biometric identifiers

To support their operations on crime investigation, police authorities use people's unique features for identification purposes. These unique features are called biometrics. Biometrics are valuable personal data that are a powerful and immutable proof of identity. Biometrics can include fingerprints, facial recognition, voice recognition among others. People's biometric data can be extracted from images, videos, voice messages. For example, they can be extracted from CCTV cameras, drones images, and body-worn cameras images but also from personal digital devices such as mobile phones and computers.

All these personal biometric data can be used by the police to identify people and potential criminals. AI systems automatise this task by comparing the data of the person who needs to be identified with large datasets. The police use of AI based biometric identification has been been criticised as it is often not transparent - it is used without people knowing it-, it might infringe the laws that regulate the use of data (GDPR) and it can also show bias, where people of different races and gender tend to be misidentified more often. Recently, there has been some criticisms regarding such an AI based system of facial recognition used by the police without people's consent. This AI system has a database of billions of images taken from social media users (Facebook, Twitter, Linkedin). It compares the face of a person that needs to be identified by the police with public images of people from social media and online sources until a match is found.

Please indicate your level of agreement with the statements below.

Please bear in mind that there is no right or wrong answer.

Questions: (1 Totally disagree - 7 Totally agree)

AI systems used by the police for biometric identification…

- respect human rights
- have enough human oversight
- are accurate
- are reliable
- respect privacy
- access to people's data legitimately
- are used with transparency
- reinforce prejudice and discrimination
- benefit the society
- are sustainable
- are accountable

Is there anything else you'd like to share on the topic of biometric identifiers?
Feel free to comment in the field below if you want to express another concern or want to provide context on some of your answers.

2. Predictive policing

Law enforcement agencies increasingly use artificial intelligence (AI) systems to prevent crime, based on the promise that AI tools can help in the prediction and anticipation of crime. The AI algorithms used to predict crime rely on historical police data together with other data such as demographic, socio-economic data, as well as real time data from digital devices (mobiles for example). These data are merged together to create models that predict where crime is most likely to occur and also who may commit it. Serious concerns have been raised regarding the accuracy of AI in predictive policing. These concerns regard the data that are used and the accuracy of the output. The way data is used might breach data protection laws in terms of privacy and also lead to some erroneous output where people living in areas that are socio-economically disadvantaged are more targeted. In this way, the AI system in use reinforces discrimination. This has been considered a serious threat to human rights.

Please indicate your level of agreement with the statements below.

Please bear in mind that there is no right or wrong answer.

Questions:(1 Totally disagree - 7 Totally agree)

AI systems used by the police to prevent crime…

- respect human rights
- have enough human oversight
- are accurate
- are reliable
- respect privacy
- access to people's data legitimately
- are used with transparency
- reinforce prejudice and discrimination
- benefit the society
- are sustainable
- are accountable

Is there anything else you'd like to share on the topic of predictive policing?
Feel free to comment in the field below if you want to express another concern or want to provide context on some of your answers.

3. Cyber operations

AI tools can process vast quantities of data and discover patterns and correlations in the data unseen to the human eye, which can enhance effectiveness and efficiency in the analysis of complex information. AI tools are used to automatically detect and take down online Child Sexual Abuse Material (CSAM). Yet, there are strong oppositions due to privacy and surveillance concerns in relation to access to personal data or private databases. Activists have accused the abusive use of these AI tools that have been found to target artists and people belonging to marginalised communities who share innocent materials that is then reported as CSAM.

Please indicate your level of agreement with the statements below.

Please bear in mind that there is no right or wrong answer.

Questions:(1 Totally disagree - 7 Totally agree)

AI systems used by the police in cyber operations…

- respect human rights
- have enough human oversight
- are accurate
- are reliable
- respect privacy
- access to people's data legitimately
- are used with transparency
- reinforce prejudice and discrimination
- benefit the society
- are sustainable
- are accountable

Is there anything else you'd like to share on the topic of cyber operations?
Feel free to comment in the field below if you want to express another concern or want to provide context on some of your answers.

4. Hacking

AI tools can be used by the police for hacking purposes. Hacking by police through AI is aimed at preventing and identifying terrorists and criminals. However, AI has been used also to hack the smartphones of journalists, government officials and human rights activists in several countries. Protests took place in several countries over allegations that the government used AI tools to illegally monitor public figures. These AI tools are seen as unacceptable form of surveillance is carried out with a lack of transparency, without people being aware of it. The AI tools allowing the police to hack people devices can be seen as a form of oppression rather than a form of protection.

Please indicate your level of agreement with the statements below.

Please bear in mind that there is no right or wrong answer.

Questions:(1 Totally disagree - 7 Totally agree)

AI systems used by the police to hack people's data…

- respect human rights
- have enough human oversight
- are accurate
- are reliable
- respect privacy
- access to people's data legitimately
- are used with transparency
- reinforce prejudice and discrimination
- benefit the society
- are sustainable
- are accountable

Is there anything else you'd like to share on the topic of hacking?
Feel free to comment in the field below if you want to express another concern or want to provide context on some of your answers.

5. Decision making in justice management

AI tools can be used to support Law Enforcement Authorities in their decisions on whether a prosecuted person should be detained, released or whether it should be allowed to follow an alternative program. While these AI tools have been praised for making the decision process more efficient, they have criticised for reflecting discrimination against people with disadvantaged socio-economic backgrounds.

Please indicate your level of agreement with the statements below.

Please bear in mind that there is no right or wrong answer.

Questions:(1 Totally disagree - 7 Totally agree)

AI systems used by the law enforcement authorities to make decisions in the justice administration context…

- respect human rights
- have enough human oversight
- are accurate
- are reliable
- respect privacy
- access to people's data legitimately
- are used with transparency
- reinforce prejudice and discrimination
- benefit the society
- are sustainable
- are accountable

Is there anything else you'd like to share on the topic of AI in justice management?
Feel free to comment in the field below if you want to express another concern or want to provide context on some of your answers.