EUROPOL

AI and policing

The benefits and challenges of artificial intelligence for law enforcement

An Observatory Report from the Europol Innovation Lab

AI AND POLICING
THE BENEFITS AND CHALLENGES OF ARTIFICIAL INTELLIGENCE FOR LAW ENFORCEMENT
An Observatory Report from the Europol Innovation Lab

PDF | ISBN 978-92-95236-35-6 | ISSN 2600-5182 | DOI: 10.2813/0321023 | QL-01-24-000-EN-N

Neither the European Union Agency for Law Enforcement Cooperation nor any person acting on behalf of the agency is responsible for the use that might be made of the following information.

Luxembourg: Publications Office of the European Union, 2024

© European Union Agency for Law Enforcement Cooperation, 2024

Reproduction is authorised provided the source is acknowledged.

For any use or reproduction of photos or other material that is not under the copyright of the European Union Agency for Law Enforcement Cooperation, permission must be sought directly from the copyright holders.

While best efforts have been made to trace and acknowledge all copyright holders, Europol would like to apologise should there have been any errors or omissions. Please do contact us if you possess any further information relating to the images published or their rights holder.

Cite this publication: Europol (2023), The Second Quantum Revolution – The impact of quantum computing and quantum technologies on law enforcement, Europol Innovation Lab observatory report, Publications Office of the European Union, Luxembourg.

This publication and more information on Europol are available on the Internet.

www.europol.europa.eu

Contents

6 Foreword

7 Executive Summary

8 Introduction

8 Background

9 Objectives

10 Key takeaways for law enforcement

12 Applications of AI in law enforcement

12 Data analytics

- Large and complex data sets
- Predictive Policing
- OSINT and SOCMINT
- Natural Language Processing (NLP)

20 Digital forensics

21 Computer vision and biometrics

- Video monitoring and analysis
- Image classification
- Biometrics
- Biometric categorisation

28 Improved resource allocation and strategic planning

29 Generative AI

31 Technological limitations and challenges

32 Ethical and social issues in AI for law enforcement

32 Data bias and fairness

33 Privacy and surveillance

34 Accountability and transparency

36 Human Rights and Discrimination

37 The EU Artificial Intelligence Act: overview and context

37 Objectives, scope and key provisions

- Prohibited uses of AI
- Law enforcement exceptions to prohibited practices
- High-Risk AI Systems
- The filter mechanism for the evaluation of high-risk systems

43 Implications for law enforcement agencies
46 Innovation and regulatory sandboxes

47 Balancing the benefits and restrictions
47 Addressing concerns of bias and discrimination
48 Safeguarding privacy and data protection

49 Future outlook and recommendations
49 Potential for technological advancements
50 Building public trust and acceptance
51 Strengthening collaboration and knowledge sharing within LEAs

53 Conclusion

54 AI Glossary

56 Endnotes

Foreword

Artificial Intelligence (AI) will profoundly alter the landscape of law enforcement, offering innovative tools and opportunities to enhance our capabilities in safeguarding public safety. This flourishing technological field promises to revolutionise how we analyse complex data sets, improve forensic methodologies, and develop secure communication channels.

However, alongside these advancements, AI introduces new challenges and potential vulnerabilities, particularly in areas like data privacy and the integrity of AI-driven decisions. It is imperative that we navigate these advancements with a strategic approach, balancing innovation with the ethical implications and societal impact.

As Europol stands at the forefront of embracing technological innovation within law enforcement, we are acutely aware of the necessity to stay ahead of these developments. This Europol Innovation Lab Observatory report, serves not only as a testament to our commitment to embracing AI responsibly, but also as a guide for the European law enforcement community as we step into this new era of digital policing.

I hope that this report will contribute to shed light on the intricate dynamics of AI for policing, providing valuable insights for our stakeholders and helping the law enforcement community on its path towards adopting AI's potential responsibly. Together, we embark on this journey, ready to face the challenges and seize the opportunities that the AI revolution presents, ensuring that we continue to protect and serve our communities in an increasingly digital world.

Catherine De Bolle
Executive Director of Europol

Executive Summary

This report aims to provide the law enforcement community with a comprehensive understanding of the various applications and uses of artificial intelligence (AI) in their daily operations. It seeks to serve as a textbook for internal security practitioners, offering guidance on how to responsibly and compliantly implement AI technologies. In addition to showcasing the potential benefits and innovative applications of AI, such as AI-driven data analytics, the report also aims to raise awareness about the potential pitfalls and ethical considerations of AI use in law enforcement. By addressing these challenges, the report endeavours to equip law enforcement professionals with the knowledge necessary to navigate the complexities of AI, ensuring its effective and ethical deployment in their work. The report focuses on large and complex data sets, open-source intelligence (OSINT) and natural language processing (NLP). It also delves into the realm of digital forensics, computer vision, biometrics, and touches on the potential of generative AI.

The use of AI by law enforcement is increasingly scrutinised due to its ethical and societal dimensions. The report attempts to address concerns about data bias, fairness, and potential encroachments on privacy, accountability, human rights protection and discrimination. These concerns become particularly relevant in the context of the EU's Artificial Intelligence Act (EU AI Act), an overview of which is detailed in this report, as well as its broader context. The report emphasises the significance of the forthcoming regulation, detailing its objectives, scope, and principal provisions. The Act's implications for law enforcement agencies are also discussed, emphasising the balance between fostering innovation and ensuring ethical use beyond compliance.

Central to the report is the assessment of how law enforcement can maintain a delicate balance between leveraging AI's benefits and addressing its inherent restrictions. Strategies for addressing bias, privacy concerns, and the pivotal role of accountability frameworks, are elaborated. The report highlights the importance of innovative regulatory environments.

The concluding section forecasts the trajectory of AI in law enforcement, underscoring the potential technological advancements on the horizon. It also emphasises the need for public trust and acceptance, and the importance of collaboration and knowledge sharing. This comprehensive document serves as both a guide and a reflective tool for stakeholders vested in the confluence of AI and law enforcement within the European landscape.

Introduction

Background

In the ever-evolving landscape of law enforcement, artificial intelligence (AI) has emerged as a transformative tool, bringing capabilities that could completely reshape policing. Law Enforcement Agencies (LEAs), both in the European Union (EU) and globally are confronted with increasingly complex challenges. From the exponential growth in data generated by digital devices and online services to the complex nature of modern criminal activities, it is evident that traditional policing methods alone are not sufficient as a response. Moreover, the globalisation of crime[1], marked by cyber threats, cross-border trafficking, and international terrorism, presents an increasingly challenging landscape that calls for advanced and innovative solutions.

In light of this, AI offers a promising alternative. By employing state-of-the-art technologies law enforcement can address many of these pressing challenges. The power of AI in processing vast amounts of data, and filtering for relevant content, its data modelling capabilities, and its ability to identify patterns and trends previously undetectable by human investigators highlight its transformative potential. Beyond that, the use of AI for repetitive and resource-intensive tasks, allows LEAs to work more efficiently with their limited resources and lets police officers focus on and prioritise their most important tasks.

Nonetheless, this comes at a cost, as certain applications of AI in policing raise concerns over privacy, bias and discrimination. There are concerns that these complex and somewhat opaque systems may do more harm than good. Further deepening the complexities of this new reality is the novel EU regulatory framework – referred to as the EU AI Act[1]. This regulatory framework introduces a set of new guidelines and standards that will impact AI systems in use in the European Union. While theAct aims to establish robust and ethical practices across the board, law enforcement agencies will need to review, and possibly modify, their existing and future AI tools to ensure compliance. Certain applications of AI, such as biometric identification – a longstanding law enforcement practice - are expected to be strictly limited[2]. The EU AI Act will also influence the development of future systems, making it imperative for police to collaborate closely with AI researchers, developers as well as ethical and privacy experts, to ensure new systems are in line with regulatory guidelines.

Within this perspective, innovative methods such as regulatory sandboxes and data spaces[3] can serve as an

1 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)

adaptive mechanism in those cases in which the application of AI-based technology could cause harm to the rights and freedoms of data subjects. By creating controlled environments where new AI tools can be tested and refined using representative data, without real-world consequences, law enforcement agencies can ensure that these tools meet both operational and regulatory standards before being deployed. This flexible approach allows for real-time adjustments and fosters an innovative environment of continuous improvement, positioning European law enforcement at the forefront of AI-driven policing.

Objectives

The primary objective of this report is to provide an overview of the benefits and challenges associated with the adoption of AI by law enforcement. The report is intended to serve as an informative resource primarily for LEAs operating across the EU, although the foundational principles should be globally applicable. Nonetheless, the report is a valuable asset for a diverse array of readers. This includes policymakers, technology developers, academics, civil rights advocates, and the general public, both within the EU and globally. Through delving into the potential advantages of AI integration, this report seeks to highlight how this rapidly evolving technology can contribute to enhancing the efficiency, effectiveness, and overall performance of law enforcement operations, while upholding ethical and legal standards.

While the emphasis of this report lies in understanding the applications, implications, benefits, and challenges of AI in law enforcement, it does not explore the intricate technical details of how AI algorithms or systems are developed, trained and operated. This decision has been made to maintain the report's accessibility and to prioritise its primary objectives. Readers interested in a deeper technical exploration of AI systems, their architectures, and underlying mechanics are encouraged to consult specific technical resources. Such sources can be found throughout the endnotes.

Key takeaways for law enforcement

AI has the ability to significantly transform policing; from advanced criminal analytics that reveal trends in vast amounts of data, to biometrics that allow the prompt and unique identification of criminals.

The integration of large and complex datasets and Natural Language Processing into policing applications allows for the extraction of actionable insights from vast datasets, improving resource forecasting and operational efficiency. Simultaneously, these technologies can protect and uphold individual privacy rights.

AI-driven tools, including in the context of OSINT and SOCMINT, process unstructured data to provide real-time insights and enhance the ability to tackle urgent situations such as crimes against children and terrorism more effectively and efficiently.

Technologies like machine translation are crucial to facilitate international collaboration among law enforcement agencies.

The fusion of AI and biometrics can enhance criminal identification accuracy while protecting the privacy of non-relevant individuals.

Generative AI represents the next leap, moving from passive analysis to active creation. For law enforcement, it offers a treasure trove of possibilities. Yet, like any tool, its power lies in its judicious and ethical application, balancing innovation with responsibility.

The effective development and deployment of AI technologies requires substantial technological infrastructure and expertise, presenting significant challenges, particularly to smaller law enforcement agencies.

Law enforcement agencies must navigate complex legal and ethical landscapes while investing in training and raising awareness amongst their staff to ensure appropriate data handling and responsible data processing practices.

Compliance with the EU AI Act represents a crucial balancing act, as it requires law enforcement to adhere to stringent ethical, legal, and privacy standards, potentially necessitating the reassessment of existing AI tools.

The EU AI Act challenges law enforcement agencies to allocate additional resources and navigate the complexities of compliance. This is especially relevant for those agencies developing AI tools in-house, emphasising the need for a responsible and ethical approach to AI integration in law enforcement.

Police forces, which may already be utilising certain AI systems, will face the challenging task of re-evaluating these tools. Should any of these operational technologies fall within the prohibited category set by the EU AI Act, they would need to be deactivated, leading to potential challenges in maintaining operational continuity.

Addressing bias in AI is paramount, with a need for systems that are not only technically sound but also embody fairness, justice, and impartiality, ensuring that data collection and storage adhere to strict privacy guidelines.

Accountability, transparency and explainability, are essential not only for ethical and responsible AI use but also to ensure that evidence collected and analysed by AI systems withstands scrutiny, respect the rights to a fair trial and is deemed acceptable in court proceedings.

Regular audits of AI systems are essential to ensure compliance with established privacy and data protection standards, maintaining a balance between harnessing AI-driven insights and safeguarding fundamental rights and individual freedoms.

Applications of AI in law enforcement

AI technology has the ability to completely transform policing; from advanced criminal analytics that reveal trends in vast amounts of data, to biometrics that allow the prompt and unique identification of criminals. This section explores some of the major applications of AI within the field of law enforcement. Through this, we aim to provide insight into the present and future capabilities that AI offers policing, projecting a course for a more efficient, responsive and effective law enforcement model.

Data analytics

The ability to analyse massive amounts of information and to then promptly take efficient decisions, has become essential in the digital age. In fields like law enforcement, decisions often need to be made with limited resources in time-sensitive settings (e.g. during a police raid, abductions or hostage-taking scenarios). Thus, the inability to make sound decisions might have a profound societal impact and negative consequences for citizens' freedoms and rights.

At its core, data analytics entails the extraction of knowledge and actionable insights from unprocessed and raw data. It provides a way to identify patterns, trends, and links in vast datasets. The advent of AI has significantly boosted the capabilities of traditional criminal data analytics. The ability of AI systems to learn and adapt based on data, including historical and other criminal data that are available to law enforcement, allows criminal analysts to navigate through, process and analyse vast amounts of information more efficiently and accurately than any human ever could without this type of technical assistance.

For example, using AI-driven analysis tools, investigators can analyse millions of financial transactions and detect anomalies, such as suspicious movements of funds to identify fraud[4]. For law enforcement agencies, this translates to an enhanced ability to analyse and understand crime patterns, detect links between international investigations and develop tailored strategies to specific challenges.

This transformative power of AI not only facilitates data processing, but also enriches the quality of generated intelligence leads. For instance, where traditional analytics might merely point out the occurrence of a crime spike, AI-powered analytics could potentially identify underlying causes, correlations between external and unrelated events, or even subtle patterns that would go unnoticed in manual analysis. It should be noted that this is typically done in targeted use cases in the context of well-prepared and closed datasets.

Furthermore, in crime areas involving digital devices such as smartphones the amount of data to be analysed and acted upon is massive and intricate. In these scenarios, AI-powered data analytics becomes indispensable for effective analysis. Without the assistance of AI, law enforcement agencies may face significant challenges in deciphering vast arrays of data, leading to potential

oversights, prolonged investigations, and missed opportunities to apprehend criminals. For example, simply going through the volume of data generated by one single smartphone is impossible without technical assistance.

The following sections will delve into the concepts of large and complex datasets, OSINT/SOCMINT (Open Source Intelligence/ Social Media Intelligence) and Natural Language Processing (NLP) and how they can reshape modern law enforcement practices.

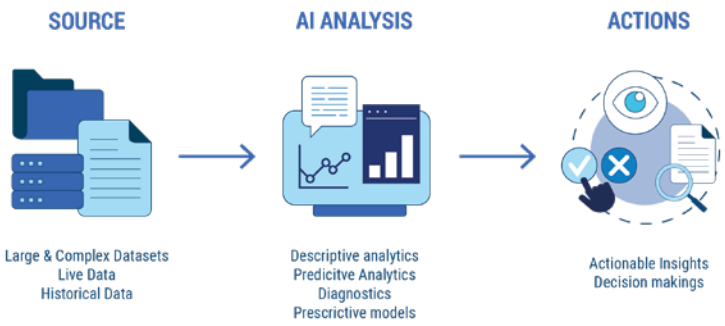
LARGE AND COMPLEX DATA SETS

Police more and more often are facing the challenge of navigating through large and complex datasets that cannot be easily managed and processed using traditional data processing tools. Handling the complexities such datasets require special techniques. Advanced database management systems and scalable search solutions, parallel processing[5], and cloud computing infrastructures are often employed to store, process and access massive data volumes. Moreover, AI models including machine learning algorithms play a crucial role in analysing and making sense of this data, especially when human analysis would be too slow or inefficient.

The ultimate goal of navigating large and complex datasets is to extract actionable insights. For law enforcement, this could mean transcribing thousands of hours of audio files, extracting entities such as names and phone numbers from text messages without necessarily going through the content of the message, thus it serves to restrict potential data protection violations and minimises the amount of personal data processing. Other relevant applications in policing include:

- detect patterns in criminal activity;
- identify correlations between different data types (like weather or seasonal patterns and crime rates, e.g. rate of burglaries increase during warmer months);
- forecast resource requirements based on past trends (e.g. a police department is trying to determine how many officers it should deploy in different precincts during different times of the day and week).

This list is not exhaustive. New use cases of analysing large and complex datasets within law enforcement will emerge as the technology and criminal landscape evolves.



Large and complex datasets in operations:

In 2020, the joint efforts of French and Dutch law enforcement, supported by Europol[6], led to the successful dismantling of the encrypted communications tool EncroChat. This operation not only dealt a severe blow to criminal networks, but also demonstrated the crucial role of analysing large and complex datasets in unravelling the intricate web of criminal activities at a global scale.

EncroChat, intended as a network for providing perfect anonymity, discretion, and no traceability to users, served as a key tool for organised crime groups (OCGs) worldwide. Encrochat-enabled phones, priced at approximately EUR 1000 each, offered features like automatic message deletion and remote device wiping capabilities, making them indispensable for criminals seeking secure communications. Since the dismantling, investigators managed to intercept, share and analyse over 115 million criminal conversations, by an estimated number of over 60 000 users. User hotspots were prevalent in source and destination countries for the trade in illicit drugs, as well as in money laundering centres[7].

The success of this operation underscores the transformative impact of analysing large and complex datasets. The vast dataset comprising millions of messages became a critical asset in dismantling criminal networks. Through advanced analytics, law enforcement agencies were able to identify patterns, connections, and hotspots, leading to the arrest of 6,558 suspects, including 197 High Value Targets. The scale of this data-driven approach is evident in the seizure of criminal funds totalling EUR 739.7 million, the freezing of EUR 154.1 million in assets, and the confiscation of substantial quantities of drugs, vehicles, weapons, and properties.

The EncroChat takedown serves as a paradigm for the effective integration of large and complex datasets analytics in combating organised crime. Europol's commitment and collaboration with various stakeholders showcases the power of collaborative efforts and data-driven intelligence in disrupting criminal activities around the world. It shows that this can be done while adhering to European data protection and human rights standards, with consultation from the European Data Protection Supervisor (EDPS). This operation stands as a testament to the evolving landscape of law enforcement, where advanced analytics play a pivotal role in dismantling criminal networks and upholding the rule of law.

Making the most of what AI solutions have to offer does not rest solely on the technology itself. Crucially, AI systems may only run properly on appropriate, extensive technological infrastructure. This requires significant budget and specific expertise to create and run, which can be challenging to obtain, especially for smaller agencies8.

Furthermore, it is key to consider the implications of obtaining, processing and analysing data and be mindful to make sound legal and ethical choices at every step of the process[9]. Practically, the EU has strict regulations and guidelines in place to ensure that individuals' privacy rights are protected, and that data are processed fairly and lawfully for specified, explicit and legitimate purposes, such as the General Data Protection Directive (GDPR) and the Law Enforcement Directive (LED). Compliance with these regulations is paramount, if at times restrictive for data analysis.

Lastly, the exchange of information among different agencies and units within law enforcement can be a challenge[10]. Fragmented data systems, information silos, and limited interoperability between databases can obstruct the comprehensive analysis of large and

complex datasets. Collaboration and data sharing among agencies, as well as the development and adoption of common standards are vital to harnessing the full potential of data-driven insights, but achieving this in practice often proves difficult.

To overcome these challenges, law enforcement agencies may need to invest in training and infrastructure to enhance their data-handling capabilities. They must also continually navigate the complex landscape of legal and ethical considerations, ensuring that their data practices remain both responsible and effective.

Finally, fostering improved communication and collaboration among different agencies and units is critical for leveraging the full potential of analysing large and complex datasets in law enforcement while respecting the boundaries of data protection and ethics.

PREDICTIVE POLICING

Within law enforcement, decision-making processes are increasingly reliant on intelligence derived from large and complex datasets[11]. A recent advancement is "predictive policing", employing sophisticated statistical methods to extract valuable new insights from vast datasets, for instance on crime records, events and environmental factors identified in criminological insights. This approach empowers police agencies to identify patterns related to the occurrence of crime and unsafe situations, and to deploy forces according to these insights to minimise risks.

Predictive policing[12], leverages the capabilities of AI to enhance the effectiveness and efficiency of policing activities. Primarily implemented through rule-based machine learning models[2], predictive policing involves two fundamental steps: (a) data collection and (b) data modelling (prediction). In the data collection phase, police departments accumulate structured and unstructured data from diverse sources, including historical crime data (time, place, and type), socio-economic data, and opportunity variables[13]. This information is supplemented in some cases with data from probation and social services, among other relevant sources. Subsequently, machine learning algorithms are employed to analyse this data in training and prediction phases. The AI model identifies patterns within historical data, associating indicators with the likelihood of a crime occurring, and then generates risk scores as predictive outputs.

Predictive policing manifests in two main types: (a) area-based and (b) individual-based policing. Area-based algorithms identify

2 A system designed to achieve Artificial Intelligence (AI) via a model solely based on predetermined rules. Two important elements of rule-based AI models are "a set of rules" and "a set of facts" and by using these, developers can create a basic Artificial Intelligence model. These systems can be viewed as a more advanced form of robotic process automation (RPA). Rule-based AI models are deterministic by their very nature, meaning they operate on the simple yet effective 'cause and effect' methodology. This model can only perform the tasks and functions it has been programmed for and nothing else. Due to this, rule-based AI models only require very basic data and information in order to operate successfully (Source: https://wearebrain.com/blog/rule-based-ai-vs-machine-learning-whats-the-difference/).

connections between locations, occurrences, and historical crime statistics to forecast the likelihood of crimes occurring at specific times and places. For instance, they can predict increased crime rates during certain weather conditions or at major sporting events. Individual-based predictive policing anticipates persons most likely to engage in criminal activities. This approach has gained traction in various EU member states, including the Netherlands, Germany, Austria, France, Estonia, and Romania, with others exploring its potential implementation[14].

Real-world applications:

The Dutch Police, developed and operationalised the Crime Anticipation System (CAS)15 to address a range of crimes beyond initial targets, including domestic burglary, robberies, pickpocketing, car burglaries, violent crimes, commercial burglaries, and bicycle theft. The system conducts weekly analyses using both local and recent data, enhancing this with external information about neighbourhoods and their inhabitants. This is further enriched by the police's own insights into criminal activities, local conditions, and data from statistics in the Netherlands. It aims to identify crime patterns, such as a higher frequency of bicycle thefts in a specific area occurring between 9:00 p.m. and midnight. With these insights, the police can allocate their resources more efficiently and tackle these crimes more effectively, as reported by local news16.

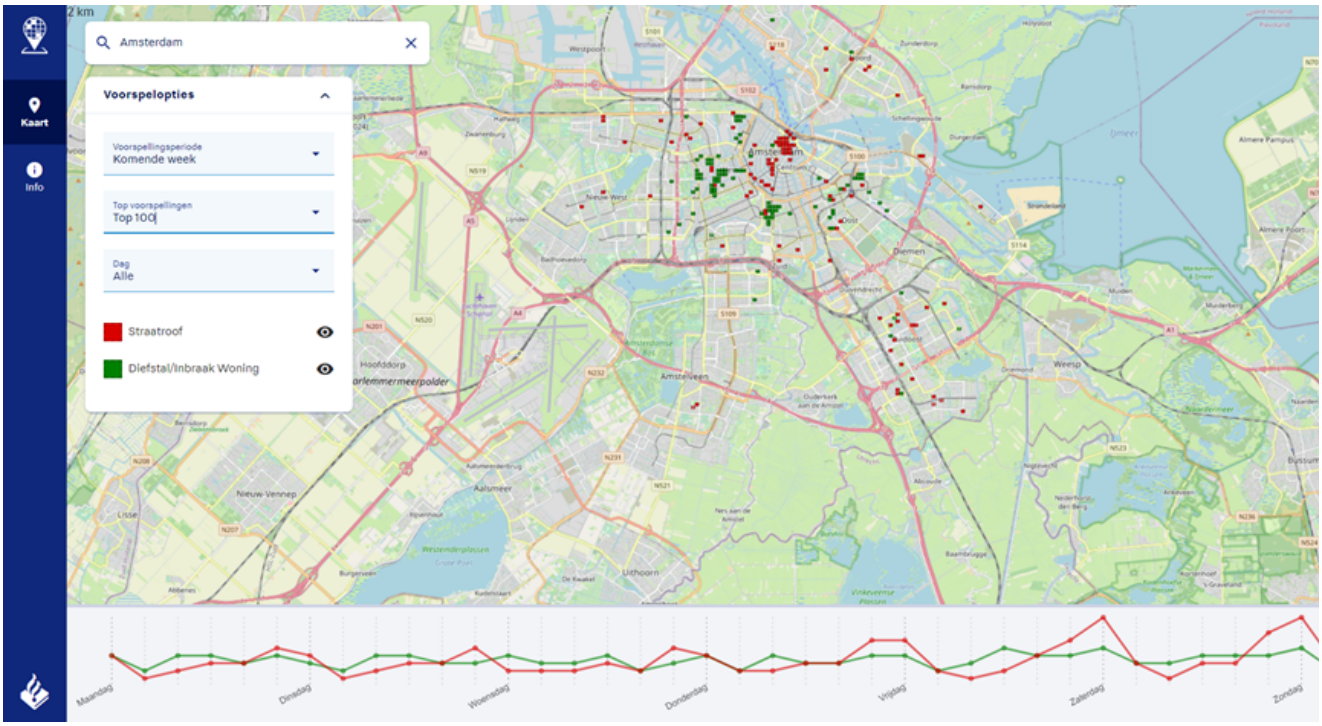


Image source: https://nl.wikipedia.org/wiki/Criminaliteits_Anticipatie_Systeem

Despite the potential benefits of predictive policing, concerns have been raised globally by policymakers and human rights groups regarding its potential to infringe upon fundamental human rights. The EU AI Act attempts to address these concerns; the relevant provisions will be discussed in Chapter 5.

In conclusion, predictive policing represents a transformative approach to law enforcement through the integration of AI technologies. As its implementation continues to evolve, policymakers must navigate the delicate balance between harnessing the potential benefits and addressing the ethical and legal concerns associated with this innovative policing tool.

OSINT AND SOCMINT

A sub-category of large and complex datasets originates from Open-Source Intelligence (OSINT) sources, especially in an era where the internet's data footprint is expanding rapidly.

After 2020, online traffic increased significantly. Enforced lockdowns, a result of the global pandemic, contributed to surges in internet users worldwide. This newly defined "normal" also paved the way for a spike in cybercrime[17] and led to a significant increase in violent extremist propaganda and terrorist content online[18]. In the vast expanse of the digital world, where cyber criminals act swiftly, traditional OSINT methods often struggle, confronted with the dilemma of 'overwhelming data, limited time'[19]. Delving into large, diverse, and unstructured data sets to extract valuable intelligence demands significant resources, such as time, personnel, and money – assets not always available to many law enforcement agencies.

The momentum is substantially shifting towards automation, optimising the use of resource and enhancing precision in decision-making. In the OSINT sphere, automation assists the user in uncovering and leveraging previously unidentified sources. Consequently, a rising number of global law enforcement agencies are adopting automated OSINT tools for investigative purposes. From investigating and reconstructing online criminal footprints to probing web applications and detecting cyber threats on social platforms, the applications of an automated OSINT paradigm are limitless. Automated OSINT tools provide insights that strengthen early-stage investigations, helping investigators shift from merely reacting to actively preventing.

Moreover, as already discussed, a major challenge remains; dealing with unstructured data. To meet this challenge, law enforcement may use automated, AI-enabled, multisource OSINT and Social Media Intelligence (SOCMINT) tools, adept at managing both structured and unstructured data. Empowered by self-learning machine learning models, these tools can reformat unstructured data, support targeted open-source searches and investigations, and offer real-time insights. Crucially, this must all be done at a speed that exceeds the speed at which criminals can erase their digital tracks.

Furthermore, Online Service Providers (OSPs) and Internet Referral Units (IRUs) can harness the power of AI to detect and counteract terrorist propaganda, disinformation, hate speech and illicit online content[20]. Utilising advanced AI and machine learning algorithms, they can analyse vast amounts of data at high speeds to identify patterns, keywords, or visual content associated with extremist

ideologies. Moreover, AI-enabled systems can be trained on known propaganda materials to proactively spot new content that shares similar characteristics and signal this to law enforcement officers, ensuring a more responsive and efficient takedown of harmful content before it spreads. It should be noted, under the new Digital Services Act (DSA), OPSs are not only encouraged but required to enhance their monitoring capabilities to ensure safer digital environments[21]. The DSA mandates a higher degree of accountability and transparency from platforms, pushing OSPs to disclose their content moderation practices and outcomes[22].

However, the use of AI for content moderation presents a complex challenge, particularly regarding the balance between the right to freedom of expression and freedom of thought, conscience, and religion (articulated in Articles 10 and 11 of the Charter of Fundamental Rights of the European Union) and the imperative to counteract disinformation, hate speech, and illicit content online. This balance is delicate, as the deployment of AI might inadvertently curtail legitimate expressions under the guise of content moderation, posing a threat to these fundamental freedoms.

NATURAL LANGUAGE PROCESSING (NLP)

Natural Language Processing, commonly abbreviated as NLP, is a branch of computer science and linguistics that focuses on the interaction between computers and human language[23]. It seeks to enable machines to interpret and generate human language in a meaningful and useful way. Research indicates that NLP methods are employed by law enforcement and police departments across various activities. These include administrative duties, forensic investigations, analysis of crime data, converting speech to text for reporting, and documenting criminal activities[24]. The vast amount of text-based data—ranging from interview transcripts, witness statements, online communications and social media posts extracted within the framework of criminal investigations—can be analysed swiftly and efficiently using NLP. This efficiency is particularly crucial when quick insights are needed in real-time situations such as abductions or hostage taking scenarios, during or in the aftermath of terrorist attacks and in investigating child abuse and exploitation cases. Key tasks performed by NLP in policing include:

- **Text classification**[25]: An analyst who processes textual data often marks crimes with keywords to help understand the circumstances surrounding a particular offence, like if an offender was under the influence of alcohol or drugs. As crime is constantly evolving, these labels may not be complete. One example of text classification is the assignment of different labels for subgroups of money laundering.
- **Clustering**[26]: Unlike text analytics that rely on predefined characteristics, clustering can help group similar crimes. Clustering maps texts into a high-dimensional space so that

similar texts are close to each other. In this task, no labels are required. Additionally, clustering can also consider factors such as time and location, to provide a holistic view of crime trends. For example, in burglary scenarios, clustering could reveal emerging methods, like hooking keys through letterboxes or exploiting particular lock weaknesses.

- **Text summarisation:** Text summarisation is a method used to produce a concise and accurate summary of lengthy texts, preserving the overall meaning. In the realm of NLP, two primary approaches[27] are employed: (a) extraction-based and (b) abstraction-based. Extraction-based summarisation involves extracting a subset of words or sentences that encapsulate the key points from the text, potentially resulting in grammatical inaccuracies. On the other hand, abstraction-based summarisation utilises advanced deep learning techniques to paraphrase and condense the original document, similar to human summarisation. By generating new phrases and sentences that encapsulate essential information from the source text, abstractive machine learning algorithms prove valuable help in addressing the grammatical limitations associated with extraction-based techniques. This technology is instrumental in assisting law enforcement in their work analysing extensive police reports and other information. This technology can provide law enforcement with concise summaries that capture crucial details without sacrificing accuracy.
- **Machine translation:** Automated translation systems facilitate the conversion of text from one language to another. These models take text in a designated source language as input and produce the corresponding text in a specified target language as output. Google Translate stands out as a well-known example of such a mainstream application. Machine translation systems play a vital role in law enforcement by enabling efficient analysis of multilingual communication data. These systems expedite the processing of large volumes of information, aiding investigators in uncovering potential threats and identifying criminal activities across language barriers. The technology enhances global collaboration among law enforcement agencies, allowing for smoother communication and information sharing during international investigations. Additionally, automated translation contributes to evidence collection by accurately translating diverse forms of evidence, thereby reducing language bias.

> Europol's own Secure Information Exchange Network Application (SIENA), the state-of-the-art communication tool that connects LEAs from 51 countries and 14 international organisations, already allows the possibility for end-users to translate text from their native language to English in real-time. The machine translation tool provides fast, accurate, and context-aware translations to break down language barriers and enhance communication amongst this rapidly evolving network of LEAs.

Real-world applications of NLP in policing are diverse and continually evolving. In cybercrime units, NLP aids in analysing

criminal communication, deciphering hidden meanings, or flagging potentially harmful online content. For example, major concerns in fighting cybercrime include spotting predatory communications, identifying internet criminals, and preventing child abuse and online grooming. NLP can be a game changer for policing in that regard[28]. A subtask of NLP, Named Entity Recognition (NER), assists analysts in labelling entities in crime reports, according to their type such as persons, organisations and vehicles. This allows for more refined crime grouping and analysis. In the context of burglaries, for instance, NER could distinguish between different entry methods, such as breaking a window versus tampering with a specific lock type. Furthermore, when sifting through massive databases of unstructured text, NLP tools can extract crucial information (entity extraction), allowing the police to act upon critical situations such as threats to life, promptly and efficiently.

In essence, NLP acts as a bridge between the highly context-dependent human communications and the performance of computational analysis, equipping law enforcement agencies with a powerful tool in their digital arsenal.

Digital forensics

Digital forensics has emerged as a critical discipline in the realm of law enforcement, given our increasingly digitalised world. With vast amounts of information being stored, communicated, and processed digitally, the ability to accurately investigate the digital footprint of criminals is crucial for the police. Central to the advances in digital forensics is the role of AI in modern digital investigations. AI provides an advanced capability to sift through vast data repositories, automating processes that would traditionally take human experts extensive periods[29]. For instance, while a human investigator might manually sort through thousands of files, AI can rapidly categorise, filter, and highlight relevant information based on predefined criteria or patterns (e.g. image classification or hash[3] values).

Several tools and techniques for data recovery and analysis have been developed with AI components. These tools can recover deleted files, access data from damaged devices, and restore fragmented pieces of information into coherent formats. Their efficiency lies in their ability to adapt and learn from each case, improving accuracy over time.

A significant concern in the digital space is cybercrime detection. Malicious activities, from hacking to phishing attempts, often leave subtle traces or are masked in regular web traffic. AI excels in identifying patterns and anomalies within this data[30].

3 Hash values are akin to digital fingerprints for files. By running a file's contents through a cryptographic algorithm, a distinct numerical identifier – the hash value – is generated that represents the file's content. Altering the content in any manner would drastically change this hash value. Presently, the MD5 and SHA-256 algorithms are the predominant methods for generating these hash values.

By continuously learning from new data, AI models can identify between regular network traffic and potential threats, even if the malicious activities evolve or employ new tactics.

Decrypting data is another area where AI has shown promise. Advanced encryption techniques can be serious obstacles for investigators. While traditional decryption might involve brute-force attempts[4] or seeking encryption keys, AI can predict potential encryption patterns or expedite the decryption process by narrowing down possible encryption keys based on pattern recognition.

Lastly, analysing digital footprints across devices and platforms has become paramount, especially with the proliferation of interconnected devices in the Internet of Things (IoT). A single individual might interact with multiple devices daily, from smartphones and laptops to smart home devices. AI can trace these interactions, building a comprehensive digital profile that aids investigators in understanding a subject's connections, or even propose additional elements for further analysis.

Digital forensics, fortified with AI capabilities, has transformed the investigative landscape, offering unprecedented depth and speed in analysing digital data. This not only amplifies the efficacy of investigations, but also positions law enforcement agencies to tackle evolving digital threats proactively.

Computer vision and biometrics

In this rapidly evolving landscape, computer vision and biometrics have emerged as game-changers for law enforcement, both from prevention and investigation standpoints. As cities and communities are facing a surge of digital imagery from sources like CCTV cameras to personal devices, it is essential to use this vast visual data[31] effectively. Coupled with biometric techniques that utilise the unique physiological traits of individuals, these technologies promise a new frontier in policing. The fusion of biometrics and AI can deliver a blend of efficiency and accuracy, offering in-depth insights to swiftly and effectively identify criminals while at the same time protecting the privacy of non-relevant individuals. As LEAs navigate the challenges and opportunities of the digital age, computer vision and biometrics stand out as invaluable allies.

VIDEO MONITORING AND ANALYSIS

4 A brute force attack employs a method of trial and error to crack login credentials, encryption keys, or locate concealed web pages. Attackers systematically try every possible combination in the hopes of making a correct guess. Such attacks are carried out using 'brute force', which involves continuous and forceful attempts to break into private accounts.

The advancement of imaging technology, coupled with AI including ML developments, has transformed the realm of law enforcement. Some of the potential applications for law enforcement include:

- **Real-time processing and anomaly detection:** Video monitoring has evolved beyond passive observation. With the integration of AI-driven algorithms, video feeds can be processed in real-time, scanning for predefined patterns or anomalies. This capability shines especially in security-sensitive zones. The system can promptly notify security personnel of suspicious activities, such as vehicles near sensitive locations, unattended objects like a forgotten bag at a transit hub, or unauthorised entries. Additionally, this real-time processing can be instrumental in traffic management, instantly detecting accidents or disruptions, facilitating immediate and informed responses.
- **Public safety and event management:** For events like public celebrations, concerts, or festivals, the safety and well-being of attendees are paramount. Safeguarding these events is fundamentally different from day-to-day policing. Instead of just traditional visual overviews, AI-enhanced video analysis can provide detailed insights into the general flow of participants. This allows for the early detection of potential areas of congestion and aids in proactive planning. Furthermore, the system can identify situations that might need attention, ensuring that everyone can enjoy the event peacefully.
- **Auto-reporting of incidents[32]:** One of the standout features brought by AI integration into video analytics is its ability to autonomously report incidents. If predefined conditions or scenarios are detected, such as public disturbances or potential safety hazards, the AI system can automatically generate detailed incident reports or/and send alerts to officers to assess the situation. This not only speeds up the documentation process but also ensures that even minor incidents, which might be overlooked in manual monitoring, are accurately recorded and addressed.

In essence, modern video monitoring and analysis amplify the capabilities of law enforcement. Police officers are not just observing - instead they actively understand and interpret the vast amounts of visual data at their disposal. From enhancing real-time traffic management to ensuring public safety at large-scale events, AI-driven video analytics represent a transformative leap in law enforcement capabilities, offering unprecedented speed and accuracy in detecting and responding to incidents, thereby fostering a safer environment for all.

IMAGE CLASSIFICATION

In the realm of computer vision, image classification is increasingly emerging as a critical field. Essentially, AI tools trained to categorise images based on the dominant content or objects they detect, help LEAs overwhelmed with imagery to promptly and effectively

analyse this data. Image classification helps swiftly sort through such data, categorising images into groups such as 'suspicious' or 'non-suspicious' or even organising them by different themes, events, or timeframes. This streamlined approach significantly expedites investigative processes.

The evolution of modern image classification tools, especially those powered by machine learning algorithms, has allowed for the rapid processing of vast volumes of data. Such tools not only segregate images with minimal manual intervention, but also ensure no piece of vital visual evidence goes unnoticed. Furthermore, the inherent precision in these systems ensures accurate categorisation, leading to more effective investigative outcomes. Beyond traditional applications, image classification is relevant in various law enforcement domains. For instance, during public events or crowded locations, image classification can identify potential threats or disruptions, helping law enforcement to take preventive actions.

A notable scenario that highlights image classification's potential is its application in forensic investigations; analysing data extracted from mobile communication devices. Frequently, these devices store thousands of images, which makes navigating them daunting and time-consuming. Additionally, this situation raises significant concerns about data protection when processing personal pictures. Through AI image classification, images extracted forensically from mobile devices can be rapidly sorted, minimising the need for manual review and the amount of personal data processed. By focusing only on relevant images, investigators can not only save valuable time, but also unveil crucial information that might have otherwise been overlooked in the vast volumes of data while fulfilling the principles of data minimisation, privacy-by-design and security-by-design. In essence, image classification is shaping the future of digital investigations in law enforcement, offering a blend of speed, precision, and efficiency.

BIOMETRICS

In an age where personal identification and verification are of paramount importance, biometric technologies have ascended as key instruments in the toolkit of law enforcement. Biometric technologies allow the identification of individuals, using their unique physiological (e.g. facial features, fingerprints, iris patterns) or behavioural attributes (e.g. gait[5], handwriting).

Facial Recognition: The technique of using facial images for criminal identification is as old as modern policing. Until the early 1960s, the procedure was primarily manual and relied on individual perception and human capacity to recognise familiar faces. However, advances in imaging technology and computer science[33]

5 Gait refers to the manner or pattern of movement of the limbs during locomotion over a solid substrate. Essentially, it is the way an individual walks or moves. Gait analysis is often used in medical, sports, and rehabilitation contexts to understand and address various issues related to movement.

allowed for Automated Facial Recognition (AFR)[34]; computer algorithms now assist the police, and digital images captured through various means have long replaced printed photographs.

This technology uses algorithms to extract and analyse certain facial features from images or video to match and verify identities. It has become an invaluable tool for law enforcement agencies. For instance, the technology helps swiftly identify suspects by comparing facial data collected within the course of a criminal investigation against historical data or databases of criminals available to the police. Additionally, it plays a crucial role in locating missing persons and children by matching unidentified individuals' images against databases of those reported missing. Moreover, outside the context of law enforcement, facial recognition offers enhanced security in controlled environments, eliminating the need for traditional authentication methods like physical access control.

However, the rise of facial recognition has also been followed by concerns. Notably, bias remains a topic of debate. Some studies have indicated discrepancies in the system's efficiency, particularly when identifying individuals from specific ethnic backgrounds, genders, or age groups[35]. Privacy and data protection stands out as another significant concern. As facial recognition systems become more ubiquitous, especially in public domains, they spark debates about surveillance's ethical bounds and potential misuse. Moreover, the data repositories that fuel facial recognition – vast databases of facial data – can be attractive targets for cyberattacks, emphasising the importance of robust data protection measures.

In this context, it is imperative to distinguish between systems used in real-time in public spaces (Live Face Recognition, LFR) and systems used retrospectively (post-event facial recognition). When used retrospectively, AFR helps the investigators to compare images of unknown persons, such as someone caught on CCTV footage, suspected of committing a crime or a mugshot of an arrestee, against a reference database. This reference database is typically supervised and lawfully stored, such as custody images or images collected during criminal proceedings.

Rather than focusing on one individual in pre-recorded imagery, LFR performs a real-time reading of all people passing a camera, regardless of their capacity, and compares them against a pre-determined closed watch-list of persons of interest. In some scenarios, the system will discard images that triggered no results immediately to avoid undue infringement of applicable data protection laws. LFR applications pose significant challenges both from a technical and a human perspective (system load, human capacity and biases, e.tc.). Police forces in the UK and in some EU countries have trialled LFR applications with varying degrees of success.

FACE RECOGNITION IN POLICING: REAL-WORLD USE CASES

1. Identification of an unknown person

- Biometric identification technologies, particularly facial recognition, play a crucial role in law enforcement for prompt and efficient identification of unknown persons. Two primary scenarios within this context:
- Solving cold cases: In the investigation of a murder case, CCTV footage identifies a suspect, leading to a facial image search against a database of known and unknown individuals. Initial results are negative, but the image is stored. Two years later, a biometric query triggers a match during another murder investigation, ultimately linking the suspect to the earlier case. This demonstrates the power of biometrics in solving cold cases over time.
- Uncovering child exploitation networks: In another scenario, police confiscate a child sex offender's computer, initiating a biometric analysis of extracted images. Matches with victims from previous investigations help unveil a broader network of criminals involved in child exploitation. This underscores the significant role biometrics play in combating heinous crimes and protecting vulnerable populations such as missing children.

2. Targeted searches of a known person

- Law enforcement relies heavily on targeted searches of known persons to validate identities and assess potential criminal involvement6. Various scenarios highlight the importance of biometric technologies in this domain:
- Unmasking terrorist connections: A citizen provides anonymous information linking a certain individual to serious crimes and terrorism. Traditional searches with biographic data yield no results, prompting a facial image search. This reveals a potential match with a wanted terrorist, illustrating how biometrics can enhance leads and aid in counterterrorism efforts.
- Uncovering criminal networks through mobile data analysis: Forensic experts analyse a suspect's smartphone, using face recognition to cluster media and narrow down targets. Subsequent searches against biometric databases of known or unknown persons reveal potential contacts, leading to the unravelling of a broader criminal network. This case demonstrates the synergy between technology and human analysis.
- Combatting financial fraud networks:In cases of ATM fraud, law enforcement employs facial recognition to connect a known perpetrator with a collection of images of unknown fraudsters. This targeted search helps assess the involvement of the known perpetrator in additional criminal activities.

Fingerprints: Fingerprinting is one of the oldest and most trusted biometric techniques in law enforcement. Each individual's fingerprint pattern, consisting of ridges, loops, and whorls, is unique

6 It is essential to clarify the circumstances under which biometric searches are allowed, especially when a person's identity is questionable or self-declared. Consideration should be given to cases where inconsistencies in identification, such as self-declared or fake identities, may necessitate biometric searches to ensure accurate identification and prevent potential threats.

and remains unchanged throughout life, making it a reliable means of identification. Traditional fingerprint analysis relied heavily on trained experts who would manually compare prints, which was time-consuming and sometimes subjective[36].

Fingerprints and AI[37][38]:

The integration of AI into fingerprint could revolutionise this domain:

- **Automated matching:** AI-driven systems can sift through vast databases of fingerprint records in mere seconds, providing matches with a high degree of accuracy. This speeds up the identification process considerably, and is especially useful in scenarios where quick results are crucial.
- **Enhanced detail recognition:** AI algorithms can identify and highlight minutiae (specific points on a fingerprint, like bifurcations or ridge endings) with more precision than the human eye, leading to more detailed and accurate comparisons.
- **Latent print analysis:** AI is particularly beneficial when dealing with latent prints - fingerprints unintentionally left on surfaces. These prints might be partial, smudged, or low quality. Advanced algorithms can enhance such prints, fill in gaps, or even predict missing portions based on recognised patterns, enabling better matches from otherwise challenging samples.
- **Learning and adaptation:** One of the strengths of AI systems is their ability to learn. As they process more data, these systems refine their algorithms, becoming increasingly adept at recognising patterns or anomalies. This continuous learning ensures that the fingerprint analysis remains state-of-the-art and adapts to new challenges or techniques.
- **Integration/interoperability with other systems:** AI-driven fingerprint systems can be easily integrated with other digital databases or biometric systems, such as those large-scale EU systems available to internal security practitioners (SIS, VIS, Eurodac e.tc.). This allows for multi-modal biometric checks and comprehensive background verifications.
- **Incorporating AI into fingerprint analysis** not only boosts the accuracy and speed of the process but also brings a level of consistency and objectivity, minimising human errors or biases. It amplifies the strengths of traditional fingerprinting while mitigating its limitations, making it an indispensable tool in modern forensic and law enforcement contexts.

Voice recognition: Every individual has a distinct voice pattern, shaped by the anatomy of their vocal tracts and their unique way

of speaking. Voice recognition technology deciphers these minute differences, converting spoken words into digital models that can be compared against stored voiceprints. In law enforcement contexts, this can be utilised to match voice samples from phone calls or recordings, confirm identities in security systems.

Iris scans: The intricate patterns in the iris, the coloured part of the eye, are as unique as fingerprints. Captured through a simple photograph, these patterns offer a quick and non-intrusive means of identification. Although iris identification technologies were initially adopted for military applications such as biometric registration of vulnerable populations in battlefields[39], the adoption rates by law enforcement gradually increase[40].

Gait analysis: An emerging field, gait analysis studies the way an individual walks. Even subtle differences in posture, stride, and pace can be captured and analysed, offering a non-invasive way to identify individuals, especially useful in scenarios where facial or other recognitions are not feasible.

To distinguish between retrospective and real-time biometric identification applications, one should acknowledge the role of the latter in rapid response scenarios, especially its usefulness in preventing terrorist attacks, locating missing children and stopping or addressing serious crimes. However, one must also recognise the challenges and ethical considerations tied to real-time biometrics, which highlight the imperative need for responsible deployment and a regulatory overview to ensure privacy and prevent misuse.

Biometrics, with its myriad of modalities, stands as a testament to the innovative fusion of biology and technology. In law enforcement, it offers not just the promise of accurate identification but can also pave the way for more efficient services that respect the dignity of citizens while safeguarding their security.

BIOMETRIC CATEGORISATION

A further application of AI that holds potential for law enforcement; that of systems that facilitate the categorisation of individuals based on their biometric characteristics have become increasingly important. These systems, whose application is fundamentally different from systems used for identification, serve as invaluable tools for both prevention and investigation.

The primary drive behind employing these categorisation systems in law enforcement is to protect vulnerable segments of the population. For instance, biometric categorisation aids in detecting and redacting sensitive data from images, especially when it concerns minors or victims of severe crimes like child abuse or trafficking. Such technologies ensure that the privacy and dignity of victims are preserved during investigative processes.

It is important to understand the boundaries of biometric categorisation. Police do not leverage these systems to deduce or infer special categories of personal data such as sexual or

political orientations, religious beliefs, disabilities, or affiliations to trade unions. Instead, the focus primarily rests on age and gender estimation. Still, such estimations, especially when integrated into high-risk systems, necessitate robust regulatory overview, ensuring that the technology's potential is harnessed responsibly and ethically, especially considering data protection concerns.

For example, the challenge of handling vast amounts of video content, some potentially containing disturbing imagery of child abuse, underscores the urgent need for accurate age estimation systems. Without AI tools adept at identifying minors in videos with greater accuracy than human analysts, the task of manual review becomes nearly unfeasible due to the extensive resources needed. In this context, biometric categorisation tools, capable of quickly and accurately categorising individuals based on objective features such as their age, prove to be invaluable resources.

Alongside their utility, it is imperative to consider data protection aspects. Ensuring the privacy and security of individuals, especially minors, during the processing of such sensitive data becomes paramount. Balancing the urgency of accurate content moderation with robust data protection measures remains essential in upholding ethical standards and protecting the rights and privacy of individuals involved.

Improved resource allocation and strategic planning

The increasingly complex landscape of law enforcement necessitates a strategic approach to resource allocation. As threats evolve and cities expand, ensuring optimal use of resources—be it personnel, equipment, or time—is imperative. Artificial intelligence holds the potential to transform resource allocation from a reactive approach to a proactive, strategic one.

Understanding the need for optimal resource utilisation: LEAs operate often under constrained budgets and personnel limits. Yet, they are expected to ensure the safety of expanding urban spaces and tackle emerging threats. Ensuring every resource is utilised optimally is not just about efficiency—it is critical for public safety and trust.

AI-driven strategic planning: Beyond just daily deployments, AI plays a role in longer-term strategic planning. For instance:

- **Organising patrols**: Instead of generic routes, AI can design patrol routes that change based on the time of day, day of the week, or known patterns of activity, ensuring officers are where they are most likely to be needed.
- **Emergency response:** AI can help in planning rapid response to emergencies by proposing optimal routes, analysing real-time traffic data, or even forecasting potential secondary incidents or threats.
- **Public event security:** Large public gatherings, from concerts to sporting events or parades, can be security challenges. AI can

analyse past events, crowd dynamics, entry/exit bottlenecks, and even social media chatter to help design a comprehensive security plan.

Evaluating the effectiveness of policies/strategies: AI does not just offer tools for planning, it is also pivotal for evaluation. Post-incident reviews can be analysed to determine the effectiveness of deployments or anti-crime policies.

Were police officers positioned optimally? Did the AI outcomes match the actual patterns? Such evaluations can feed back into the system, ensuring continuous learning and reviewing policies/strategies.

In conclusion, AI-driven resource allocation and strategic planning elevate law enforcement's ability to safeguard communities. By turning vast amounts of data into actionable insights, and by continuously learning from both successes and failures, AI ensures that law enforcement agencies remain agile, proactive, and ever adaptive to the evolving challenges of the modern world.

Generative AI

The frontier of AI does not lie in just the analysis of existing data and information, but also in the creation of entirely new content. Generative AI, a rapidly advancing domain, employs algorithms to generate content, including texts, images and other forms of media. These technologies learn patterns, structures, and intricacies from vast datasets and then produce new data that adheres to the same patterns. For instance, after analysing thousands of images of cats, a generative model can create a new, synthetic image of a cat that, while entirely fictional, looks indistinguishably real. Some of the most prominent forms of Generative AI include Generative Adversarial Networks (GANs) and Large Language Models (LLMs).

Generative Adversarial Networks (GANs) are a class of machine learning frameworks where one neural network learns to generate as realistic synthetic data as possible while the other neural network learns to detect synthetic data. While the networks interact with each other, both are continuously improving their performance over time. GANs, more specifically the synthetic data generating networks are widely used in image generation, video generation, and increasingly in other domains like music.

GANs could offer law enforcement ways to evaluate the performance of biometric systems without compromising individual's privacy[41]. For example, GANs can help generate synthetic facial images, fingerprints, and other biometric data, which can be in turn used instead of real data, where real data may not be readily available, to assess the accuracy and robustness of recognition systems across diverse populations and conditions. Additionally, they enable the development of anti-spoofing technologies to combat identity fraud[42][43]. However, as these technologies are adopted, it is crucial for law enforcement

to balance the benefits with ethical considerations and privacy protections, ensuring that the use of synthetic media supports public safety while respecting individual rights.

Large Language Models (LLMs) refers to a form of generative AI with applications in Natural Language Processing (NLP). These models are designed to process and generate human language. By being trained on extensive text datasets, they are capable of executing various language-oriented tasks. These models mark a substantial advancement in the way machines grasp and produce human language with widespread implications across multiple sectors such as technology, entertainment, education, among others.

LLMs can offer substantial benefits to law enforcement agencies. These include supporting investigators to probe into unfamiliar crime areas, facilitating open source research and intelligence analysis, as well as the development of technical investigative tools[44]. Additionally, LLMs can help speed up numerous administrative tasks, such as the writing of reports and the summarisation of information. Nonetheless, the use of LLMs by law enforcement would require a secure environment that can be trusted with sensitive information, as well as thorough assessments concerning safeguarding fundamental rights and mitigating potential biases.

Despite their impressive abilities, LLMs have several limitations, such as the propensity to produce factually inaccurate or illogical content, commonly referred to as "hallucinations." **Retrieval-Augmented Generation** (RAG) emerges as a potential solution to some of these challenges. While many LLMs rely primarily on pre-existing knowledge or publicly accessible information to produce text, RAG goes a step further by integrating information retrieval mechanisms. This means that RAG models can actively search for and incorporate relevant information from pre-determined, authoritative knowledge sources, ensuring that the generated content is not only coherent but also contextually accurate and up-to-date. Organisations thereby have more influence over the produced textual content, while users have a better understanding of the process through which the LLM generates its response.

Exploring the capabilities of RAG in handling criminal investigations datasets is essential, yet it must be approached in a methodical and regulatory-compliant manner. In our current era, where information is paramount, there is an unprecedented demand for innovative methods to delve into and interpret complex data.

Generative AI represents the next leap, moving from passive analysis to active creation. For law enforcement, it offers a treasure trove of possibilities. Yet, like any application, its power lies in its judicious and ethical application, balancing innovation with responsibility.

Technological limitations and challenges

Despite the benefits for law enforcement, the integration of AI faces several technical constraints that challenge its effectiveness and efficiency:

Data quality and accessibility are fundamental to the effectiveness of AI in law enforcement, but challenges arise from disparities in data collection and storage practices across jurisdictions. These variations result in inconsistent datasets that may be incomplete or biased, compromising the integrity of AI outputs. Additionally, existing data often lacks the granularity required for AI applications, as it was not originally collected with AI in mind. For instance, police reports, though informative, may not capture unreported or undetected incidents, skewing AI training and outcomes. Standardised data collection protocols, coupled with data cleansing and enrichment processes are essential for creating comprehensive and unbiased datasets. Moreover, integrating robust data protection measures is crucial to safeguarding individuals' privacy and ensuring compliance with applicable data protection regulations. By addressing these issues, AI reliability in law enforcement can be improved, better reflecting and addressing the complexity of criminal activity while upholding ethical and legal standards.

Integration challenges: Integrating AI with existing law enforcement systems and data processing pipelines presents various technical hurdles. The incompatibility between modern AI solutions and older technological infrastructures can lead to significant integration issues, affecting data exchange and operational efficiency. Bridging this gap requires a dual approach: retrofitting legacy systems to enhance their compatibility with AI technologies and designing future AI solutions with a focus on interoperability and modular integration.

Scalability and performance under different conditions: The effectiveness of AI tools in law enforcement must be maintained regardless of the scale of data or complexity of operational scenarios. Variability in incidents and environmental conditions tests the adaptability of AI systems. Addressing these challenges necessitates the development of AI models that are not only scalable but also versatile, capable of adjusting to different data volumes and operational demands without compromising performance.

Maintenance and technical support: The rapidly evolving nature of AI technology demands continuous updates and maintenance to safeguard efficiency and security. However, the requisite ongoing technical support can strain the resources of law enforcement agencies, particularly those with limited access to IT expertise. Establishing dedicated support frameworks and leveraging partnerships with technology providers could offer sustainable solutions to these challenges, ensuring AI systems remain up-to-date and effective.

Addressing these challenges is not straightforward and requires an AI governance framework and a concerted effort from multiple stakeholders. Collaboration between law enforcement agencies,

technology developers, policymakers, and the community is crucial to navigate these technological limitations. Through such collaboration, innovative solutions can be developed, tested, and refined to enhance the efficiency, reliability, and overall effectiveness of AI applications in policing practices. Additionally, investing in research and development, focusing on ethical AI use, and fostering an environment of continuous learning and adaptation among law enforcement personnel are key steps toward overcoming these obstacles.

Ethical and social issues in AI for law enforcement

As the previous section demonstrated, Artificial Intelligence is becoming an increasingly vital tool for policing across the European Union. Nonetheless, this brings forth a multitude of ethical and social challenges that require meticulous analysis. This chapter delves into critical areas of concern: the potential for data bias and the subsequent implications for fairness; the fine line between surveillance for security and the infringement of individual privacy; the pressing need for accountability and transparency in AI deployments, with an emphasis on the 'black box' issue. Moreover, the chapter will discuss the potential for AI to either exaggerate or mitigate human rights issues and discrimination within the realm of law enforcement.

Data bias and fairness

Data is the core of any AI system, and the quality of the data directly influences the outcomes produced by the system. Any skew in data can unintentionally lead to unfair or biased outcomes. Fair and unbiased policing is a foundational pillar of democratic societies, and, therefore recognising and eliminating bias is of particular concern to law enforcement.

Bias in data can emerge from numerous sources. Historical data[45] used to train AI systems can embed longstanding societal biases, reflecting past prejudices and discriminatory practices. For instance, if a certain neighbourhood was historically over-policed due to racial or socio-economic biases, an AI system trained on this data might suggest that the area is more prone to criminal activity. Such outcomes might create a feedback loop[46], leading law enforcement to continue over-policing that area, thereby finding disproportionate numbers of crime and reinforcing the biases present in the data.

Beyond historical biases, there is also the challenge of representational bias[47]. If data does not adequately represent all segments of the population, the AI system can make flawed predictions. Overrepresented groups can be disproportionately affected. For instance, a study by the EU FRA[48] found that offensive speech detection algorithms, such as those for identifying hate speech or harassment, had higher error rates for certain socio-economic groups. A major contributing factor is the association of certain terms with ethnic groups (e.g., 'Muslim', 'gay', 'Jewish'), which can cause the algorithms to mistakenly classify non-offensive

phrases as offensive. Since these terms are more frequently utilised by the respective ethnic groups, there is an increased likelihood of their content being wrongly flagged as offensive and subsequently removed, due to their overrepresentation in the training data. On the other side, groups that are underrepresented in the data may not benefit from the same level of policing protection.

It is worth noting that there is not a universal agreement on the precise definitions of fairness. Various interpretations exist. In some instances, it is justified to use protected categories like gender and age; for instance, an AI system that deducts information about minors to ensure additional protection needs to be trained with relevant sensitive data. As such, these situations should be evaluated individually, and ultimately, humans must always determine how to act on the information provided by the AI.

Privacy and surveillance

In law enforcement, striking the right balance between public security and individual privacy has always been a challenge. As AI integrates more deeply into policing methods, this balance becomes even more delicate.

Historically, law enforcement agencies across the EU operate within a robust legislative and regulatory framework. The introduction of regulations such as the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED) underscores the EU's proactive stance on safeguarding data protection and individual privacy rights. These regulations serve as foundational pillars governing the intersection of technology and citizens' rights, fortified by robust enforcement mechanisms, human overview, and avenues for redress. They are not merely legal frameworks but embody comprehensive measures to ensure the responsible handling of personal data, fostering transparency, accountability, and trust in digital interactions.

While AI offers significant advantages for law enforcement, such as the ability to process vast amounts of data and utilise biometrics for rapid criminal identification and threat assessment, it also brings with it complex challenges. Advanced technologies like facial recognition systems can dramatically enhance efficiency. However, without sufficient safeguards, such as human oversight to evaluate their outputs, these technologies risk infringing on fundamental rights, such as the right to private life and the right to personal data protection (Art. 7 and 8 of the EU Charter of Fundamental Rights). This could manifest as disproportionate surveillance of innocent individuals or the potential for misuse targeting specific groups, raising concerns about privacy and the necessity of such monitoring.

As the world copes with the implications of AI and surveillance, the EU, fortified by its stringent regulations, institutional ethos, and a history of prioritising its citizens, is uniquely poised to shape a path where technological advancements strengthen security without

compromising individual rights. This coexistence can serve as a global model, ensuring that technology remains a tool for the improvement of society.

Accountability and transparency

Accountability and transparency serve as cornerstone principles in democratic societies, ensuring that power structures remain in service to the community and function with integrity. As AI becomes a prominent tool within law enforcement, these principles must be at the forefront to maintain public trust and ensure justice.

Despite the benefits the technology brings, one of the primary concerns is the potential for decisions, predictions or recommendations made by AI to remain unexplained or unjustified. When the output of AI is used to support decision making in law enforcement – be it biometric identification, or threat assessment– it is crucial for both police officers and those affected by these decisions to understand the rationale behind. Without this clarity, the risk of mistrust, misuse, and potential injustices escalates.

In the EU, the demand for accountability and transparency is not new. However, AI's unique nature, where algorithms often operate with layers of complexity beyond human comprehension, introduces novel challenges.

> There is a pressing need for mechanisms that make AI's decision-making processes interpretable, especially in high-stakes environments like policing and criminal justice, not only in terms of how relevant evidence are collected, processed and presented before a court or tribunal, but also in a broader sense to ensure that citizens can comprehend, engage with, and challenge the use of AI.

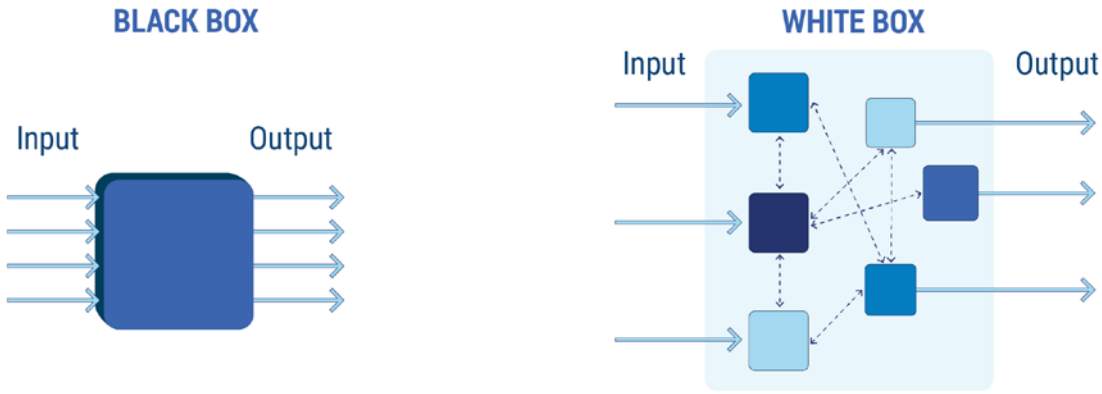
Ensuring accountability also entails setting clear responsibilities. When an AI tool is used to generate recommendations or make predictions, who is to be held accountable if there is an error or if it results in injustice? Is it the software developers, the law enforcement agency using the tool, or the overarching regulatory

body? The definition of responsibility is vital to ensure that AI tools in law enforcement remain both effective and just.

The Black Box Issue

In discussions surrounding AI transparency, a central and pressing concern is the puzzling 'black box' issue. At its core, the black box dilemma underscores the opacity inherent to complex AI algorithms, with a particular focus on the complexities of deep learning models[49]. These Machine Learning (ML) models are designed to emulate human information processing. Employing multiple layers of artificial neurons connected to a network to extract advanced features from the input data, they bear the label 'deep'. However, what raises profound questions is their capacity to make decisions or predictions lacking of a clear, linear explanation for their rationale. Much like an opaque sealed black box, these algorithms produce outcomes without exposing their inner workings to allow for an assessment of the applied logic.

In the law enforcement domain, this opacity poses a significant challenge. When an AI-driven system raises concerns about an individual's potential threat or recommends additional patrol officers in a specific area, it becomes imperative for law enforcement officers and the individuals affected by



Resolving the black box predicament is not solely a technical challenge; it is a profound ethical imperative. Innovative solutions, like explainable AI (XAI)[50], are actively under development to bridge this gap and render these algorithms more transparent and comprehensible. However, until such solutions become universally accessible and standardised, the black box issue remains an indispensable focal point in the ongoing pursuit for an AI-driven policing framework that is accountable, fair, and transparent to all stakeholders involved.

It should also be mentioned, AI algorithms can be opaque due to their protected status as trade secrets. Data controllers in these cases avoid sharing details of the inner algorithmic workings to protect trade secrets and avoid system manipulation.

Returning to the broader landscape, it becomes evident that for AI to truly benefit law enforcement in the European Union and maintain public trust, a rigorous commitment to accountability and transparency is essential[51]. The development of frameworks to explain AI's decision-making processes, together with well-defined regulatory standards and clarity in assigning responsibility, are indispensable for establishing this balance.

Human Rights and Discrimination

In the EU, where human rights are deeply embedded in our foundational values, integrating AI into law enforcement brings forth several challenges. The primary concern is AI's unintended reinforcement or amplification of societal biases due to reliance on historical data. As discussed, such biases can lead to unjustified targeting of particular social groups, leading to disproportionate policing.

Furthermore, AI's predictive capabilities can mistakenly categorise individuals based on broad data patterns. Such generalisations might risk infringing on the fundamental principle of "innocent until proven guilty," raising valid concerns about the right to fair trial.

To foster a balanced integration of AI within this critical paradigm, law enforcement has an array of options. Firstly, the significance of undertaking comprehensive audits cannot be overstated. Every AI system, before its active implementation in law enforcement, should undergo an in-depth assessment. While the technical robustness of these systems is essential, it is equally important to ensure their conformity to the relevant frameworks such as the ethics guidelines for trustworthy AI, introduced by the High-Level Expert Group on AI[52]. By locating and addressing any inherent biases at this stage, we can set the foundation for fair and unbiased AI implementations.

Equally crucial is the need to facilitate community engagement. Certain communities frequently find themselves excluded from the mainstream of technological advancements, often facing unintended negative impacts as a result. Through fostering continuous dialogue with these communities, law enforcement can gather unique perspectives other than purely technical evaluations. Proactive engagement not only improves trust but also ensures that AI systems are deployed in a way that resonate with the broader ideals of fairness, inclusivity, and justice.

Lastly, the dynamic nature of AI necessitates continuous monitoring and evolution. Technologies evolve, societal norms shift, and new challenges arise. In such a landscape, ensuring that AI applications in law enforcement are subject to ongoing monitoring becomes

The EU Artificial Intelligence Act: overview and context

essential. This iterative scrutiny and feedback enables real-time adjustments, ensuring that AI-driven initiatives in law enforcement consistently mirror and uphold the EU's dedication to equal rights, justice, and human dignity.

As the previous section highlighted, the increasing integration of AI systems into various facets of policing, raises concerns regarding their ethical, legal, and societal implications. The EU Commission, recognising the transformative potential of AI in all sectors of society, proposed in early 2021, a new legal instrument to regulate the use of AI horizontally, while balancing innovation with the protection of fundamental rights and societal values[53]. This legislative proposal is referred to as the EU Artificial Intelligence Act (EU AI Act). Following a lengthy consultation, the European Parliament and the Council of the EU, reached an agreement and adopted the Act which was published in the Official Journal on the 12th of July 2025 (Regulation (EU) 2024/168954). The Act will be fully enforced gradually, within two years, with certain exceptions: general provisions and the prohibitions will be enforced after 6 months, governance rules and obligations for general-purpose AI models will apply after 12 months. Finally, the rules for AI systems embedded in regulated products (Article 6(1)) will take effect after three years.

As AI systems are more and more widely adopted, regulatory frameworks are becoming increasingly important to clearly outline what use cases are legally permissible. In the EU, this legal framework has now been established via the EU AI Act. In specifying how AI can be used in the EU, the AIA provides aims to strike a balance between safeguarding core EU values, while still allowing law enforcement to leverage the opportunities offered by AI.

This section will delve deeper into the objectives, scope, and key provisions of the EU AIAct, exploring its implications for law enforcement agencies.

Objectives, scope and key provisions

The new regulations will be uniformly implemented across all Member States, based on a forward-looking definition of AI, ensuring a consistent application. According to the definition, 'an AI system is a machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments' (Art. 3 of the EU AI Act). The definition aligns closely with the work of international organisations working on artificial intelligence, notably the OECD.

The scope of the Act is very wide, covering systems developed with various approaches (machine learning, logic and knowledge-based approaches, and statistical or Bayesian approaches) that can

generate outputs such as content, predictions, recommendations, or decisions influencing 'environments they interact with'.

The main idea is to regulate AI based on its potential to cause harm to society following a 'risk-based' approach: the higher the risk, the stricter the rules. The 'unacceptable risk AI' category prohibits applications that are considered a clear and outright threat to European values and fundamental rights, such as social scoring or manipulation of human behaviour (e.g. toys using voice assistance to encourage dangerous behaviour among minors). Meanwhile, the "high risk AI" category includes specific systems which could jeopardise people's safety or infringe on fundamental rights; these systems will not be prohibited but rather face stringent mandatory requirements such as undergoing conformity assessments.

AI systems falling under 'limited risk' will only be bound by basic obligations, particularly in areas like transparency. For example, in the case of using AI systems like chatbots, it is important for users to recognise that they are engaging with a machine, enabling them to make an informed choice on whether to proceed or step back. All other AI applications, termed 'Minimal risk AI', can be developed and used within the EU without any additional obligations beyond existing legislation. On a voluntary basis, companies may nevertheless commit to additional codes of conduct for these AI systems.

The scope of the EU AI Act is extensive, encompassing systems developed using various techniques, which includes machine learning, logic and knowledge-based methods, as well as statistical or Bayesian methods[7]. These systems are capable of producing outputs like content, predictions, recommendations, or decisions that affect the 'environments they engage with[55]. Moreover, the Act applies and imposes certain obligations to a wide range of actors, including, providers (i.e. developers), deployers (i.e. users) and distributors of AI systems (Art. 2(1) of the EU AI Act).

In the sections below, we will break down the main provisions of the Act from a law enforcement perspective. While this is a non-exhausting analysis, by understanding these, we can better grasp how the EU plans to benefit from AI while making sure the technology is used fairly and transparently for everyone.

PROHIBITED USES OF AI

In recognising the potential pitfalls and harms associated with certain AI systems, the EU AI Act outlines certain AI practices that are strictly prohibited (Art. 5). These prohibitions aim to prevent the deployment of AI in ways that could cause potential harm, infringe on individual rights, or undermine the foundational principles of the EU. Applications that fall within this category include AI systems

7 Bayesian statistics is a method of data analysis that utilises Bayes' theorem to revise existing knowledge about model parameters using the information gained from observed data.

that manipulate human behaviour[8], social scoring systems[9] and AI systems used to exploit the vulnerabilities of people (due to their age, disability, social or economic situation).[10]

Moreover, the Act introduces a ban on real-time remote biometric systems (RBI), when these systems are used in public-spaces. Such systems are capable of capturing and analysing biometric data (like facial features, iris patterns, fingerprints, voice patterns, etc.) in real-time and from a distance, without the need for direct interaction or physical contact with the individual being identified. While these systems offer potential advantages for law enforcement and security applications, their application in public spaces might be considered intrusive, 'evoke a feeling of constant surveillance and indirectly dissuade the exercise of the freedom of assembly and other fundamental rights' (see Recital 18 of the EU AI Act). It should be noted that the Act foresees some narrow law enforcement exceptions (Art. 5(1)(h)). These exceptions will be discussed below.

Furthermore, Act prohibits the use of AI systems that allow the biometric categorisation of natural persons based on certain narrowly-defined attributes. These systems process biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs or sexual orientation. Such systems will thus be prohibited unless used to identify victims. Filtering of datasets based on biometric data in the area of law enforcement will still be possible (Art. 5(1)(g)).

One of the most critical additions has been the prohibition on individual predictive policing systems. As discussed already, such systems, designed to predict potential criminal activities based on events, locations or persons, have raised concerns. There is a fear that these systems might inadvertently reinforce biases, leading to unwarranted surveillance or interventions. In response to this, the EU AI Act introduces a partial ban of individual predictive policing. The ban covers systems which assess or predict the risk of a natural person to commit a criminal offence, based solely on the profiling of a natural person or on assessing their personality traits and characteristics. Use of AI systems that support the human assessment of the involvement of a crime that has actually occurred is allowed, as this is not considered a prediction but an evaluation based on objective and verifiable facts directly linked to a real criminal activity (Art. 5(1)(d))

While post-event remote biometric identification systems are not outright prohibited, their high-risk categorisation mandates a third-party conformity assessment process (Recital 125 of the Act). Furthermore, the Act imposes additional obligations for users of post-event RBI systems (Art. 26(10)). In particular, in the framework

8 AI applications that could potentially alter a person's decision-making by exploiting vulnerabilities or causing harm.

9 Systems that evaluate and classify the trustworthiness of individuals based on social behaviour or known predicted personality characteristics.

10 Any AI application designed to use subliminal techniques that a person might not consciously recognise but that could impact their behaviour.

of an investigation for the targeted search of a person convicted or suspected of having committed a criminal offence, the deployer of an AI system for post-remote biometric identification shall request an authorisation, prior to use, or without undue delay and no later than 48 hours. The authorisation should be carried out, by a judicial authority or an administrative authority whose decision is binding and subject to judicial review. No such authorisation is needed if the system is used for the initial identification of a potential suspect based on objective and verifiable facts directly linked to the offence. Moreover, the EU AI Act explicitly prohibits the untargeted use of post remote biometric identification in law enforcement.

The EU AI Act takes a firm stance on preventing the creation or expansion of facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage (Art. 5(1)(e)). Untargeted scraping (e.g. extraction of data from a website), is the collection of facial images without a specific, predefined purpose. It goes beyond the necessary and proportionate use of facial recognition technology, potentially amassing vast datasets without clear objectives. This prohibition is designed to address concerns related to mass surveillance and potential violations of fundamental rights, particularly the right to privacy.

LAW ENFORCEMENT EXCEPTIONS TO PROHIBITED PRACTICES

Considering the specificities of law enforcement activities, the co-legislators agreed on some exceptions to the prohibited AI practices, as discussed above. Subject to appropriate safeguards, these exceptions are meant to reflect the need to equip law enforcement with all available tools to be efficient against modern forms of crime, while also respecting the confidentiality of sensitive operational data in relation to their activities. For example, according to Article 46(2) of the EU AI Act, law enforcement or civil protection authorities can put a specific high-risk AI system into service urgently for reasons of public security or in the case of a specific, substantial, and imminent threat to life or physical safety of individuals. This can be done without prior authorisation, provided that an authorisation request is submitted during or immediately after the use of the system. If the authorisation is subsequently rejected, the use of the system must be stopped immediately, and all results and outputs from its use must be discarded.

Moreover, according to Art. 5(1)(h), the use of real-time remote biometric identification systems in public spaces is possible only for exhaustively defined law enforcement purposes. These purposes include the targeted searches of victims, the prevention of terrorist attacks and threats to life, and the localisation of criminals suspected to be involved in serious and organised crime.

The circumstances under which law enforcement agencies are allowed to use real-time RBI systems, are subject to specific conditions (Art. 5(2)(a)):

- **Specifically targeted individuals:** The use is limited to confirming the identity of specifically targeted individuals. This implies that real-time RBI should not be used for indiscriminate surveillance or broad identification purposes.
- **Limited scope:** The use of real-time RBI must be strictly necessary and targeted. This includes limitations on the individuals to be identified, the location, the temporal scope, and being based on a closed dataset of legally acquired video footage.
- **Fundamental Rights Impact Assessment (FRIA):** Law enforcement authorities are required to complete a fundamental rights impact assessment prior to using these systems. This assessment would evaluate the potential impact on the rights and freedoms of individuals.
- **Authorisation requirements:** The use of such systems in publicly accessible spaces for law enforcement purposes must be expressly and specifically authorised by a judicial authority or by an independent administrative authority. While the EU AI Act foresees exceptions to this rule[11], this authorisation should ideally be obtained prior to the use of the system (or within 24 hours).
- **National laws:** The exceptions for law enforcement use of real-time RBI will be possible only if there is national law in place explicitly foreseeing this, as outlined in the EU AI Act. As such, Member States have the flexibility to decide on whether the exceptions will be applicable in their country, introduce stricter conditions, or even a horizontal ban of such systems.
- **Notification of market surveillance authority:** The relevant market surveillance authority and the national data protection authority should be notified of each use of the 'real-time biometric identification system'.

The RBI exceptions outlined in the EU AI Act are welcomed from a law enforcement standpoint. These systems enable the targeted and effective interventions, while avoiding disproportionate stop and search measures based on race or ethnicity or any distinctive physical characteristics. This strategic shift towards a more focused use of technology not only enhances the ability of law enforcement agencies to maintain public safety but also significantly reduces the likelihood of discriminatory practices that have historically marred policing efforts.

However, while these exceptions are seen as a positive development, they also introduce a layer of complexity in the broader context of AI tool adoption and application within law

11 Exceptions are allowed in urgent situations where obtaining prior authorisation is not feasible, but even in these cases, the use must be restricted to the absolute minimum necessary. If such authorisation is rejected, the use of real-time biometric identification systems linked to that authorisation should be stopped with immediate effect and all the data related to such use should be discarded and deleted.

enforcement. While the Act is designed to ensure that relevant technologies are used in a way that upholds fundamental rights and fosters trust among the public, this may also slow down the adoption process, as law enforcement agencies must navigate through the additional regulatory requirements, ensuring that their AI tools are compliant with the new standards.

This careful balancing act between leveraging AI for enhanced law enforcement capabilities and adhering to the ethical, legal, and regulatory standards set forth by the EU AI Act will likely influence how AI technologies are upheld and implemented by law enforcement agencies across the EU. The success of this endeavour relies on finding a middle ground that allows for the innovative use of AI for policing purposes while safeguarding against the misuse of the technology in ways that could infringe upon individual rights and freedoms.

HIGH-RISK AI SYSTEMS

The EU AI Act identifies certain AI applications in the realm of law enforcement as 'high-risk' due to their significant potential to impact individual rights, freedoms, and safety. By classifying these systems as high-risk, the new regulatory framework mandates a set of stringent requirements to ensure their ethical and responsible use.

Among the applications considered high-risk are biometric systems used for unique individual identification tools like emotion recognition and polygraphs aimed at assessing a person's trustworthiness or emotional state. Other high-risk applications include some categorisation systems, as well as systems designed to evaluate the risk of victimisation or offending by analysing the likelihood of individuals becoming victims or perpetrators of crimes, including human trafficking, domestic violence, or cybercrime. Additionally, AI technologies employed to scrutinise the reliability of evidence during criminal investigations or for profiling purposes in detection and prosecution phases are subjected to these rigorous regulations.

Notably, despite their initial categorisation as high-risk, the final text of the EU AI Act excluded technologies for deepfake detection and crime analytics, reflecting a nuanced approach to balancing the benefits of these technologies against concerns related to privacy, ethics, and misuse risks.

In light of the categorisation of certain systems as high-risk, users, providers, developers and sellers of such AI systems, should follow some strict rules. Every application, for instance, must undergo an exhaustive risk assessment and mitigation process to understand and counter potential hazards (conformity assessment). A thorough fundamental rights impact assessment (FRIA) shall be performed as well. The foundational data driving these AI systems must be of the highest quality, not only to diminish risks but also to circumvent any discriminatory outcomes and algorithmic bias.

THE FILTER MECHANISM FOR THE EVALUATION OF HIGH-RISK SYSTEMS

The EU AI Act introduces a filter system to address concerns that the classification of high-risk for certain AI applications might be overly broad (Art. 6(3)). This system allows providers of AI systems which could fall in the high-risk category, but which do not pose a significant risk of harm to the health, safety or fundamental rights of natural persons, to conduct self-assessments. The filter mechanism focuses on AI systems tailored for less risky, specific functionalities, including those for narrow procedural tasks, review or enhancement of human-completed tasks, identification of decision-making patterns, and preliminary task performance in critical assessment preparation[12].

For law enforcement agencies employing AI, this filter mechanism could significantly benefit operations by reducing regulatory burdens for AI systems deemed lower-risk. For example, AI tools that assist in organising evidence or managing data, provided they do not directly evaluate the reliability of evidence or profile individuals. Another example would be AI systems that optimise the logistics of evidence collection or systems used to organise and cross-reference public records and case files, and aid in the initial stages of an investigation, which could also fall within this filter mechanism.

However, the operation of this filter system might pose practical challenges, including potential difficulties in determining the eligibility for exemptions and ensuring that the use of AI remains within legal bounds. This could lead to uncertainties regarding the scope of exemptions and the need for clear guidance and examples from the European Commission to ensure that law enforcement agencies can benefit fully, without compromising legal standards or ethical considerations.

Implications for law enforcement agencies

The introduction of the EU AI Act poses various challenges and implications for law enforcement agencies use of AI across the EU, specifically regarding the deployment and utilisation of AI-driven tools that include AI. Firstly, the Act's explicit position on prohibiting certain AI practices means there is an immediate imperative to stop deploying these technologies. Police forces, which may already be utilising certain AI systems, will now face the challenging task of re-evaluating these tools. Should any of these operational technologies fall within the prohibited category set by the Act, they would need to be deactivated, leading to potential challenges in maintaining operational continuity. This poses the question: how

12 The European Commission is tasked with developing guidelines for applying these filters, aiming to clarify and simplify the compliance process for AI system providers. It should be noted that AI systems used for the profiling of natural persons should always be considered as high-risk applications.

will the transition be managed for legacy systems under the new regulations?

Moreover, the process of conformity assessments for systems deemed high-risk by the EU AI Act will undoubtedly be intricate and time-consuming. LEAs will be required to comprehensively assess these systems against the stipulations set by the new regulation. In many instances, this could entail considerable modifications to existing systems to ensure alignment with the new standards. Consequently, not only does this suggest potential changes to software, but it also highlights the need to allocate additional resources, in terms of both finance and staff.

Furthermore, the influence of the Act is not restricted to only the newly deployed AI systems. Considering the dynamic nature of AI, its continuous evolution and updates, systems that are already in operation will also be subject to these regulations. The evolving nature of AI means that LEAs will be in a perpetual cycle of reviewing and modifying, ensuring that their systems, even if previously compliant, remain in line with the regulations, especially if updates alter their functions or associated risks.

A particularly challenging scenario emerges for LEAs that have taken the initiative to develop AI tools internally. These agencies will confront the dual responsibility of ensuring compliance both as users and as developers. This essentially indicates a substantial investment in guaranteeing that every stage of the process, from development, data collection, training, to deployment, is in strict adherence to the EU AI Act requirements.

Additional safeguards in the context of RBI for law enforcement.

Given the sensitive nature of RBI deployments and the implications on privacy and other fundamental rights, the EU AI Act foresees additional safeguards on the use of such systems. According to the regulation, law enforcement agencies using such systems, shall ensure that no decision that produces an adverse legal effect on a person may be taken solely based on the output of these post remote biometric identification systems (See Art. 26 (10) of the EU AI Act). Therefore, the new regulation mandates an additional layer of verification and confirmation.

Achieving this requires a combination of technological, procedural, and legal safeguards such as human validation, implementing multi-modal biometric systems, establishing appropriate confidence thresholds and educate human operators on the capabilities and limitations of biometric identification technology.

Moreover, the EU AI Act considers an enhanced human overview as a requirement for those systems so that no action or decision may be taken unless the output of the RBI system has been separately verified and confirmed by at least two natural persons, with the necessary competence, training and authority (Art. 14 (5)).

The requirement for a separate verification by at least two natural persons shall not apply to high risk AI systems used for the purpose of law enforcement, migration, border control or asylum, in cases where Union or national law considers the application of this requirement to be disproportionate. The mandate of the so-called 4-eyes principle, reflects the peer-review process which features prominently in the forensic sciences.

Nonetheless, adhering to this principle for rather basic investigative measures such as a criminal identification, presents potential challenges for law enforcement agencies such as operational efficiency, availability of resources, subjectivity in verification, expertise and training timeliness in critical scenarios and others.

As the model EU law enforcement Agency, Europol is leading efforts aimed at demonstrating compliance with the provisions of the EU AI Act. In that direction, Europol, jointly with selected partners[13] has co-developed CC4AI, a compliance checker tool for the AI Act. CC4AI is a step-by-step guide designed to support LEAs to evaluate whether existing or future AI applications used in policing meet the criteria set by the new regulatory framework.

With the CC4AI initiative, Europol seeks to contribute to ensure a harmonious adoption and implementation of the EU AI Act requirements across LEAs in the EU, thereby preventing inconsistencies that could potentially impede police collaboration in the future. Access to CC4AI will be offered freely to internal security agencies.

While the new regulation offers a comprehensive framework geared towards maximising the advantages of AI without compromising ethical standards and the safety of the public, it also introduces a complex set of challenges for LEAs. Successfully navigating this regulatory terrain will necessitate a profound understanding of AI's

13 EU JHA agencies (CEPOL, Eurojust, EUAA and EU FRA) from the EU Innovation Hub for Internal Security and the Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research (CENTRIC)

technological aspects, coupled with an increased awareness of its legal dimensions within the realm of law enforcement.

Innovation and regulatory sandboxes

Central to the EU AI Act and its innovative approach is the establishment of coordinated AI 'regulatory sandboxes' (Art. 57-60). These controlled environments are designed to allow developers to test and refine innovative AI products and services within a secure environment. The Act's emphasis on regulatory sandboxes is of great importance to law enforcement agencies. As extensively discussed, AI innovations, ranging from biometric identification to advanced data analysis, offer substantial benefits to LEAs. Regulatory sandboxes offer a unique opportunity for these agencies to explore these technologies, understand their implications, and identify any potential issues before implementation in real-life law enforcement contexts.

Furthermore, the Act encourages a harmonised approach across Member States, aiming to eliminate regulatory disparities. This ensures that LEAs across the EU can uniformly benefit from AI advancements, promoting consistent and effective use of technology in law enforcement operations.

Another critical aspect addressed in the EU AI Act is the intersection between sandbox activities and the EU's stringent data protection regulations, including the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED). The Act acknowledges the importance of balancing the need for experimentation with adherence to data protection principles, emphasising the need for transparency in the deployment and use of AI within sandboxes, especially in sensitive domains like law enforcement where public trust is crucial.

The provisions within the EU AI Act for regulatory sandboxes represent a forward-thinking approach, allowing law enforcement agencies to harness the potential of AI technologies. By addressing key concerns around liability, regulatory harmonisation, and data protection, the Act ensures that innovation can happen in a manner that is responsible, transparent, and aligned with the core values and rights upheld by the European Union. Already in 2022, the EU legislators had anticipated the use of sandboxes to allow Europol to process personal data for the purpose of its research and innovation projects to train, test and validate algorithms, in a separate, isolated and protected data processing environment (Art. 33a of Europol Regulation)[14].

14 REGULATION (EU) 2022/991 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation (Source: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R0991#d1e2572-1-1)

Balancing the benefits and restrictions

As highlighted throughout the report, the fusion of AI and policing promises enhanced efficiency, new or improved capabilities, and resource optimisation. However, it also brings critical issues to the fore, such as potential biases, potential infringements of fundamental rights and freedoms, and questions of accountability.

This section looks at the primary concerns and corresponding strategies, emphasising the significance of ensuring fairness, safeguarding individual rights, upholding stringent standards of accountability, and fostering an environment that promotes both innovation and stringent regulatory adherence.

Addressing concerns of bias and discrimination

Even though the foundational issues surrounding data bias and fairness in AI for law enforcement were elaborated in section 3.1, addressing these concerns goes beyond just the technicalities of data. The implications of bias and unfairness in AI systems resonate deeply within societal structures, trust dynamics, and the broader ideal of democratic governance.

> In law enforcement, where the consequences of decisions can be life altering and the goal is to contribute to fairness and justice, AI tools need to be more than just technically sound; they should embody the principles of justice, fairness, and impartiality.

The challenge thus extends from ensuring fairness at data level, to ensuring the equitable application and interpretation of AI outcomes in real-world scenarios. By adhering to these principles, law enforcement agencies can ensure that AI-processed evidence meets the rigorous standards required for court acceptance, thereby maintaining the integrity of the judicial process.

To address this multifaceted challenge, there is a need for a multi-disciplinary approach. While an AI system might be trained on unbiased data and might be using a fair algorithm, the way its outcomes are interpreted and applied by law enforcement officials could introduce bias. Ensuring that officers understand AI outputs and follow clear guidelines on how to act on them can prevent misapplications. For example, the output of a facial recognition system is merely an indication that two persons present similarities to a certain degree. Without human decision and corroboration of these findings with additional information (such as fingerprints or biographical data), this output should not be used as a probable cause for arrest.

Moreover, human oversight and transparency mechanisms needs to be established. Engaging communities in the evaluation of AI-driven policing tools can be an effective way to gather trust and ensure that the systems are in line with societal values. Recursive cycles with communities can also help refine these tools to ensure they are more aligned with community needs. Additionally, continuous training of law enforcement personnel on the ethical dimensions of AI is imperative. Officers should be equipped not just to use these

tools but also understand their implications on society, ensuring that the technology is used responsibly.

In conclusion, while the technical aspects of bias and fairness are undeniably critical, the broader challenge lies in integrating AI into the ethos of law enforcement in a manner that upholds the values of justice, equity, and community trust.

Safeguarding privacy and data protection

As AI systems gain traction in law enforcement, concerns about privacy and data protection rise concurrently. The use of AI-driven analytics, predictive policing, and biometric identification systems underscores the acute necessity to protect individuals' personal data and privacy rights.

Key to addressing these challenges is the establishment of a robust data protection and AI governance framework. Data collection should be governed by the principles of lawfulness, fairness, and transparency, ensuring that only necessary and relevant data is processed. Furthermore, data storage duration, especially concerning personal information, must be limited strictly to what is necessary for the purposes for which the data is processed. Access to stored data should be restricted to authorised individuals or entities according to applicable laws to prevent unauthorised access.

Furthermore, encryption and other appropriate technical and organisational measures must be implemented as standard procedures to ensure the security and confidentiality of stored data, thereby protecting against breaches and unauthorised access. For AI systems that necessitate continuous data inputs, it is imperative to adhere to the principle of data minimisation, collecting only the data that is strictly necessary. This aligns with the requirements outlined in the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED), which emphasise the importance of limiting the processing of personal data to what is essential for the intended purposes.

Equally important is to guarantee the individual's right to information. Citizens should be informed about the nature of data being collected, its purpose, and the extent of its use. Moreover, individuals should have the right to access, rectify, or even erase their data under certain circumstances, in line with applicable data protection laws.

Ensuring appropriate human overview is essential. While AI systems are capable of processing and analysing vast amounts of data, human intervention is necessary to ensure that the interpretation of data aligns with legal and ethical standards. Conducting regular audits of AI systems can provide additional assurance of compliance with established privacy and data protection regulations.

Engaging with the public and fostering a culture of transparency can also help build trust. Open dialogue about the scope and limitations of AI in law enforcement, its implications on privacy, and measures taken to safeguard data will foster community trust and collaboration.

To summarise, as AI reshapes modern policing, safeguarding privacy and data protection is of utmost importance. It is a balance of harnessing the potential of AI-driven insights while ensuring that the fundamental principles of privacy and individual freedoms remain intact.

Future outlook and recommendations

Potential for technological advancements

In the swiftly evolving landscape of AI, the horizon for technological advancements remains vast. The intersection of AI with law enforcement is particularly ripe for innovation, promising to reshape traditional paradigms of policing and security.

- **Quantum Computing:** With quantum computing nearing development, the potential for handling complex computations of specific mathematical problems at unparalleled speeds could introduce new digital forensics and decryption methods. Quantum machine learning can improve computational speeds and performance of AI models at unprecedented levels. A recent report[56] published by Europol's Observatory sheds light into how quantum computing and quantum technologies will impact law enforcement and what should be done to prepare.
- **6G connectivity:** 6G is expected to become one of the first AI-native networks, integrating AI directly into the networking infrastructure. This integration will empower the network to self-learn and self-manage, enhancing its autonomy and reducing operational costs[57]. This will likely allow for even faster data transfer rates, facilitating real-time secure communication tools for law enforcement, ensuring that officers in the field have instant access to crucial information, enhancing on-ground efficiency and safety. Consequently, the increase in data volumes will likely require a new array of AI tools and methods to analyse this data.
- **Automated Drones and Robotics:** The future might hold a more widespread use of AI-powered drones and robots for search and rescue operations, or even securing large events, providing aerial insights or on-ground assistance without risking human lives.
- **AI chips:** The further development and integration of AI chips will significantly accelerate the progress and capabilities of AI technologies in the future. Specialised AI chips are designed to efficiently process AI and machine learning tasks, offering faster computation speeds and reduced energy consumption compared to general-purpose processors. Further advancement in this area will enable more complex and sophisticated AI

models to be trained and deployed, enhancing the performance of AI applications in law enforcement.

- **Edge computing:** By bringing computation and data storage closer to the location where it is needed, edge computing has the potential to revolutionise the future of AI. Edge computing can enable faster, more efficient, and real-time AI processing capabilities, which would reduce the dependency on cloud-based services and data centres. This can help minimise latency, bandwidth use, and the potential for data privacy breaches. For AI applications, this means the ability to process and analyse data on-device in real-time, which is crucial for applications which require instant decision-making such as autonomous vehicles, IoT devices, and smart city technologies. This could have a significant impact on law enforcement, by enabling a more seamless integration of AI at various operational levels. Edge computing could facilitate use cases ranging from facial recognition and mobile command centres to smart wearables, improved sensors, and enhanced deployment of unmanned systems, such as drones.

As these technological advancements come to the fore, it is imperative for law enforcement agencies to stay abreast, adapt, and integrate these tools responsibly. While the potential is significant, ensuring that these technologies are employed ethically and in line with the principles of justice and fairness will be paramount. The balance between harnessing technology and safeguarding rights will dictate the trajectory of AI's role in the future of policing.

Building public trust and acceptance

Public trust and acceptance are cornerstones for the successful integration of AI technologies into law enforcement. Without the collective confidence of the public, even the most ground-breaking advancements risk facing resistance, potentially impeding their effective utilisation. Investing in community engagement, education, and feedback mechanisms can significantly enhance public trust and cooperation in AI technology, ultimately leading to a more informed and supportive community. For example:

- **Community engagement:** Regularly engaging with the community can provide valuable insights into their concerns and expectations and foster mutual understanding. Hosting public forums, workshops, or open debates can help in demystifying AI, addressing misconceptions, collaboratively identifying areas of improvement. This dialogue is also essential to effectively navigate the trade-offs between privacy and security, especially in the context of high-risk AI applications in law enforcement.
- **Education and awareness:** Investing in public education campaigns about the benefits and limitations of AI can reduce fear and scepticism within the society. When people are informed about the positive impacts, such as reduced crime

rates or quicker response times, they are more likely to embrace the technology.

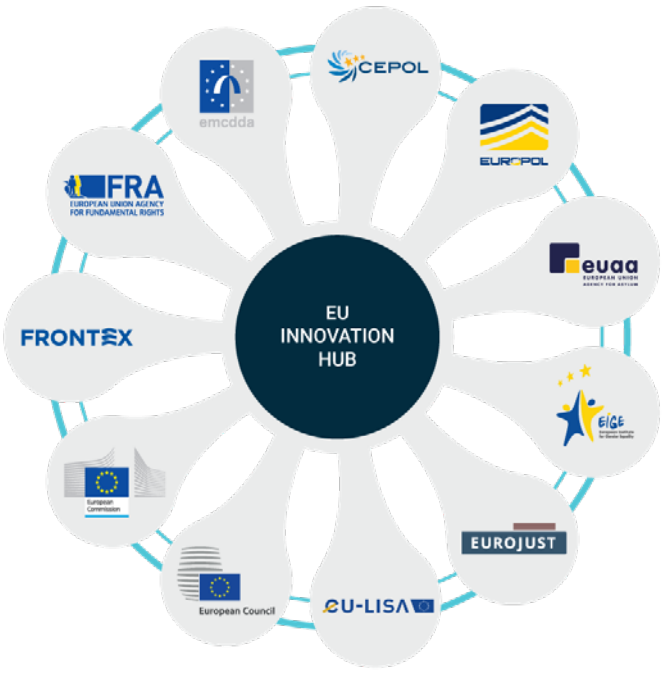
- **Feedback mechanisms:** Establishing channels where the public can voice their concerns, provide feedback, or even report potential misuse of AI could instil a sense of participation and co-ownership in the technology's evolution.

Building public trust is an ongoing process, demanding consistent efforts and open dialogue. As AI continues to shape the future of law enforcement, prioritising public trust and acceptance will not only validate technological progress but also ensure that society moves forward cohesively, with technology acting as an enabler rather than a divider.

Strengthening collaboration and knowledge sharing within LEAs

In this dynamic ecosystem, collaboration and knowledge sharing is of utmost importance. By fostering an environment of collective intelligence and open dialogue, law enforcement agencies can ensure that AI's potential is recognised in a manner that resonates with the collective good. This includes:

- **Inter-agency collaborations:** agencies across regions and countries can come together to pool resources, share insights, and co-develop AI tools tailored for diverse scenarios. Such collaborative endeavours can streamline efforts, reduce redundancies, and lead to more universally adaptable solutions. Such an initiative is the aforementioned EU Innovation Hub for Internal Security - a collaborative network of innovation labs that works to provide the latest innovation updates and effective



solutions to support the work of internal security actors in the EU and its Member States, including justice, border security, immigration and asylum and law enforcement practitioners.

- **Partnerships with academia and the industry:** By building alliances with universities and technology companies, law enforcement agencies can tap into cutting-edge research, methodologies, and tools. This collaborative spirit can accelerate the development and refinement of AI systems, ensuring they remain at the forefront of innovation.
- **Open-source AI:** Promoting open-source AI projects can facilitate access to advanced tools, enabling even smaller law enforcement entities to leverage the power of AI. Such initiatives can also foster a community-driven approach to development, enhancing the quality and applicability of tools.
- **AI Literacy:** Enhancing AI Literacy among law enforcement staff, in alignment with the EU AI Act, is pivotal for fostering an informed and ethical approach to AI integration in policing. Law enforcement personnel should become aware of the operational, ethical, and legal dimensions of AI technologies, ensuring they can effectively deploy AI tools while addressing concerns related to bias, privacy, and accountability. Similarly, it is crucial to engage the public in transparent discussions about AI's role in law enforcement, clarifying its benefits, limitations, and regulatory oversight as mandated by the new regulation. By promoting a deep understanding of AI's capabilities and the legal frameworks governing its use, this effort seeks to build trust, enhance collaboration between law enforcement and communities, and ensure AI's deployment aligns with societal values and fundamental rights.
- **Centralised knowledge repositories:** Establishing centralised databases or platforms where agencies can share case studies, research papers, toolkits, and best practices can serve as invaluable resources. Such repositories can ensure that knowledge is not just created but also made accessible to those who need it. A notable example is Europol's Platform for Experts (EPE)[15] and Europol's Tool Repository (ETR)[16]. The latter was created by the Europol Innovation Lab as a participatory platform for law enforcement agencies around Europe, to share innovative tools based on cutting-edge technology. The former, is a secure environment for specialists in a variety of law enforcement areas, including AI, enabling them to share – within their respective communities - knowledge, best practices and non-personal data on crimes. For the time being, there are over 18,000 members

15 Read more about EPE here: https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/europol-platform-for-experts

16 ETR is a secure and LEA-exclusive online platform to share non-commercial, cost-free software developed by LEAs and research and technology organisations. ETR was designed to avoid duplication of effort among LEAs. It allows all police forces in Europe to benefit from innovative tools and become more efficient in their work, thus enhancing the protection of EU citizens. AI tools available through ETR have already supported several operations across Europe, resulting in the arrests of organised criminals and the rescue of victims of human trafficking.

from more than 100 countries interacting and collaborating with each other in virtual communities.

- **Engagement with civil society:** Collaborating with civil actors' society and community organisations can provide unique perspectives on the ethical and societal implications of AI in policing.

Conclusion

The integration of AI into law enforcement, particularly within the European Union, presents a paradigm shift with profound implications for both operational efficiency and ethical considerations. This report assessed the multifaceted applications of AI in policing, ranging from data analytics and predictive policing to digital forensics, computer vision, and biometrics. The report highlighted the transformative potential these technologies hold for enhancing public safety and operational effectiveness.

However, this technological evolution does not come without challenges. The ethical and societal dimensions, including concerns over data bias, privacy, accountability, and human rights, are critical. The European Union's proactive stance through the development of the Artificial Intelligence Act underscores a commitment to balancing innovation with ethical considerations, aiming to foster an environment where AI's benefits in law enforcement can be harnessed responsibly.

The report emphasised the importance of addressing bias and discrimination, safeguarding privacy and data protection, and ensuring accountability and legal compliance. It outlined strategies such as fostering regulatory sandboxes, which allows for the safe exploration and development of AI technologies within a structured framework that respects EU values and fundamental rights.

Looking forward, the trajectory of AI in law enforcement is poised for significant technological advancements, including quantum computing and 6G connectivity, promising to further enhance the capabilities of law enforcement agencies. However, the successful integration of these technologies hinges on building public trust and acceptance, emphasising transparency, and strengthening collaboration and knowledge sharing within the law enforcement community.

In conclusion, the report called for a balanced approach to AI in law enforcement, where the benefits of technological advancements are leveraged to enhance public safety and operational efficiency, while simultaneously addressing the ethical, legal, and societal challenges. The EU's regulatory framework, including the Artificial Intelligence Act, provides a solid foundation for this endeavour, ensuring that AI's integration into law enforcement aligns with the EU's core values and fundamental rights. The future of AI-driven policing, therefore, lies in the harmonious integration of innovation with regulation, guided by principles of fairness, accountability, and transparency.

AI Glossary

ACCOUNTABILITY: The responsibility and explainability for the actions and decisions made by Artificial Intelligence systems. In the context of AI-driven policing, it involves ensuring that the use of AI in law enforcement adheres to ethical standards and legal regulations.

AI GOVERNANCE: The framework and set of rules and regulations that guide the development, deployment, and use of AI systems. It includes ethical considerations, accountability mechanisms, and compliance with legal standards.

AI OFFICE: The European Commission's function of contributing to the implementation, monitoring and supervision of AI systems, general purpose AI models and AI governance.

AI SYSTEM: AI system is a machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments (Art. 3 of the EU AI Act).

ALGORITHM: A set of sequential instructions applied on specific input(s) to reach a predefined goal, ranging from the output of a basic mathematical function to more complex tasks.

ARTIFICIAL INTELLIGENCE (AI): The development of computer systems that can perform tasks that typically require human intelligence. These tasks include learning, reasoning, problem-solving, perception, and language understanding.

BIAS: Systematic and unfair preferences or prejudices in the data or algorithms that can lead to discriminatory outcomes. Bias can arise from the data used to train AI models or the design of the algorithms themselves.

BIOMETRIC DATA: Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, such as facial images or dactyloscopic data (Art. 3 of the EU AI Act).

CHATBOT: Software designed to mimic conversation with humans.

CLASSIFICATION: A type of machine learning task where the algorithm assigns predefined categories or labels to input data.

CLOUD COMPUTING: The provision of computing services, such as storage, computational power, and software applications, via the internet.

CONFORMITY ASSESSMENT: The process of demonstrating whether the requirements set out in the EU AI Act relating to a high-risk AI system have been fulfilled.

COMPUTER VISION: A field of AI that enables machines to interpret and make decisions based on visual data. Computer vision is used for image and video analysis.

DEEPFAKES: AI generated or manipulated image, audio or video content that resembles existing persons, objects, places or other entities or events and would falsely appear to a person to be authentic or truthful (Art. 3 of the EU AI Act).

DEEP LEARNING: Deep learning is a subset of machine learning and AI that mimics human knowledge acquisition to enable models to perform complex tasks like recognising patterns in various data types. Encryption The process of converting information into a code to prevent unauthorised access, particularly important for securing data in AI applications.

EXPLAINABILITY: The ability to understand and interpret the decisions and actions of AI systems, particularly in complex models like neural networks.

FAIRNESS: Ensuring that AI systems treat all individuals and groups fairly, without introducing biases or discrimination.

FOUNDATION MODEL: A pre-trained model that serves as the starting point for various downstream tasks in machine learning.

GENERAL PURPOSE AI (GPAI): An AI system which is based on a general purpose AI model that has the capability to serve a variety of purposes, both for direct use as well as for integration in other AI systems (Art. 3 of the AIA)

GENERATIVE AI: AI systems that can generate new content, such as images, text, or music, often using general purpose AI models.

HIGH-RISK AI: application AI applications with the potential for significant impact on individuals' rights and safety, requiring stricter regulatory scrutiny.

LARGE LANGUAGE MODEL: A type of AI model, like GPT-4, that is trained on vast amounts of text data and can generate human-like language.

MACHINE LEARNING: A subset of AI that focuses on the development of algorithms that enable computers to learn and make predictions or decisions based on data.

MARKET SURVEILLANCE AUTHORITY: A regulatory body responsible for monitoring and ensuring compliance with market regulations, including those related to AI applications.

NATURAL LANGUAGE PROCESSING: A subset of artificial intelligence, focusing on how computers and human languages interact, allowing machines to comprehend, decipher, and generate human language.

NEURAL NETWORKS: A set of algorithms, modelled loosely after the human brain, designed to recognise patterns. Neural networks are a key component of deep learning.

PROFILING: The process of analysing and classifying individuals based on their characteristics, behaviours, or preferences.

QUANTUM COMPUTING: Quantum computing is a rapidly-emerging technology that harnesses the laws of quantum mechanics to solve problems too complex for classical computers.

REGULATORY SANDBOX: A concrete and controlled framework set up by a competent authority which offers providers or prospective providers of AI systems the possibility to develop, train, validate and test, where appropriate in real world conditions, an innovative AI system, pursuant to a sandbox plan for a limited time under regulatory supervision (Art. 3 of the EU AI Act).

REMOTE BIOMETRIC IDENTIFICATION (RBI): system An AI system for the purpose of identifying natural persons, without their active involvement, typically at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database (Art. 3 of the EU AI Act).

ROBOTICS: The interdisciplinary field that combines computer science and engineering to develop, build, and operate robots.

SOCIAL SCORING: The use of AI and data analytics to assess and score individuals based on their behaviour, activities, or social interactions.

TRANSPARENCY: The openness and clarity in the functioning and decision-making process of AI systems, ensuring that users and stakeholders can understand the system's behaviour.

Endnotes

1 Europol, 2021, Serious and Organised Crime Threat Assessment (SOCTA) 2021, accessible at https://www.europol.europa.eu/publication-events/main-reports/europe-an-union-serious-and-organised-crime-threat-assessment-socta-2021

2 European Parliament press release, June 2023, MEPs ready to negotiate first-ever rules for safe and transparent AI, accessible at https://www.europarl.europa.eu/news/en/press-room/20230609IPR96212/meps-ready-to-negotiate-first-ever-rules-for-safe-and-transparent-ai

3 European Parliament, 2023, Study to support the technical, legal and financial conceptualisation of a European Security Data Space for Innovation, accessible athttps://home-affairs.ec.europa.eu/system/files/2023-02/Data%20spaces%20study_0.pdf

4 Y. J. Tan, S. Ramachandran, M. A. Jabar, et al., 2022, Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review, Applied Sciences, vol. 12, no. 19, pp. 9637, accessible at https://doi.org/10.3390/app12199637

5 K. Gülen, 2023, The parallel universe of computing: How multiple tasks happen simultaneously?, Dataconomy, accessible at https://dataconomy.com/2023/04/18/what-is-parallel-processing/

6 Europol press release, 2020, Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe, accessible at https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe

7 Europol press release, 2023, Dismantling encrypted criminal EncroChat communications leads to over 6 500 arrests and close to EUR 900 million seized, accessible at https://www.europol.europa.eu/media-press/newsroom/news/dismantling-encrypted-criminal-encrochat-communications-leads-to-over-6-500-arrests-and-close-to-eur-900-million-seized

8 A. Babuta, 2017, Big Data and Policing: An Assessment of Law Enforcement Requirements, Expectations and Priorities, RUSI, accessible at https://static.rusi.org/201709_rusi_big_data_and_policing_babuta_web.pdf

9 Ibid.

10 Ibid.

11 W. Hardyns, A.Rummens, 2018, Predictive Policing as a New Tool for Law Enforcement? Recent Developments and Challenges, Eur J Crim Policy Res 24(2018), pp. 201–218, accessible at https://doi.org/10.1007/s10610-017-9361-2

12 P. Walter et al., 2013, Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations, RAND, accessible at https://www.rand.org/pubs/research_reports/RR233.html

13 W.Hardynn & A. Rummens, 2017, Predictive Policing as a New Tool for Law Enforcement? Recent Developments and Challenges, Eur J Crim Policy Res 24(2018), pp.201-2018, accessible at https://doi.org/10.1007/s10610-017-9361-2

14 EUPCN, 2022, Artificial Intelligence and predictive policing: risks and challenges, accessible at https://eucpn.org/sites/default/files/document/files/PP%20%282%29.pdf

15 Dutch Police, 2021, Crime Anticipation System, accessible at https://www.politie.nl/wet-open-overheid/woo-verzoeken/landelijke-eenheid/woo-verzoeken-per-jaar/2021/crime-anticipation-system.html

16 S. Oosterloo and G. van Schie, 2022, The Politics and Biases of the "Crime Anticipation , System" of the Dutch Police, accessible at https://ceur-ws.org/Vol-2103/paper_6.pdf

17 Europol, 2021, Internet Organised Crime Threat Assessment (IOCTA) 2021, accessible at https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021

18 Europol, 2022, EU Terrorism Situation and Trend Report (TE-SAT) 2022, accessible at https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2022-te-sat

19 Medium, 2023, Using OSINT to Improve Your Competitive Intelligence Strategy, accessible at https://goldenowl.medium.com/using-osint-to-improve-your-competitive-intelligence-strategy-eeb6114f9c71

20 Cambridge Consultants, 2019, Use of AI in online content moderation, accessible at https://www.ofcom.org.uk/__data/assets/pdf_file/0028/157249/cambridge-consultants-ai-content-moderation.pdf

21 European Commission, 2023, The impact of the Digital Services Act on digital plat-

forms, accessible at https://digital-strategy.ec.europa.eu/en/policies/dsa-impact-platforms

22 Meta, 2023, New Features and Additional Transparency Measures as the Digital Services Act Comes Into Effect, accessible at https://about.fb.com/news/2023/08/new-features-and-additional-transparency-measures-as-the-digital-services-act-comes-into-effect/

23 DeepLearning.AI, 2023, Natural Language Processing, accessible at https://www.deeplearning.ai/resources/natural-language-processing/

24 P. Sarzaeim et al., 2023, A Systematic Review of Using Machine Learning and Natural Language Processing in Smart Policing, Computers 2023; 12(12):255, accessible at https://doi.org/10.3390/computers12120255

25 A. Dixon & D. Birks, 2021, Improving Policing with Natural Language Processing, In Proceedings of the 1st Workshop on NLP for Positive Impact, pp. 115–124, accessible at https://aclanthology.org/2021.nlp4posimpact-1.13.pdf

26 Ibid.

27 R. Abhijit, 2020, Understanding Automatic Text Summarization-1: Extractive Methods, Towards Data Science, accessible at https://towardsdatascience.com/understanding-automatic-text-summarization-1-extractive-methods-8eb512b21ecc

28 Roxanne project, NLP technologies against online crime, accessible at https://www.roxanne-euproject.org/news/blog/nlp-technologies-against-online-crime

29 J. M. James et al., 2022, Digital Forensics AI: Evaluating, Standardizing and Optimizing Digital Forensics Investigations, SpringerLink, accessible at https://link.springer.com/article/10.1007/s13218-022-00763-9

30 H. Ravichandran, 2023, How AI Is Disrupting And Transforming The Cybersecurity Landscape, Forbes, accessible at https://www.forbes.com/sites/forbestechcouncil/2023/03/15/how-ai-is-disrupting-and-transforming-the-cybersecurity-landscape/?sh=5aab864c4683

31 J.S. Hollywood et al., 2018, Using Video Analytics and Sensor Fusion in Law Enforcement, RAND, accessible at https://www.rand.org/pubs/research_reports/RR2619.html

32 Ibid.

33 A. Jain, K. Nandakumar & A. Ross, 2016, 50 Years of Biometric Research: Accomplishments, Challenges, and Opportunities, Pattern Recognition Letters, 79, doi: 10.1016/j.patrec.2015.12.013.

34 P. Grother et al.,2024, Face Recognition Technology Evaluation (FRTE). Part 2: Identification, NIST, available at https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf

35 P. Grother et al.,2019, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, NIST, accessible at https://nvlpubs.nist.gov/nistpubs/ir/2019/nist.ir.8280.pdf

36 J. L. Mnookin, 2003, Fingerprints: Not a Gold Standard, Issues, XX (1) Fall, 2003, accessible at https://issues.org/mnookin-fingerprints-evidence/

37 European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), 2020, The digital transformation of internal security in the EU, AI and the role of eu-LISA, accessible at https://www.eulisa.europa.eu/Newsroom/News/Pages/The-digital-transformation-of-internal-security-in-the-EU-AI-and-the-role-of-eu-LISA.aspx

38 Y. Rawat, et al., 2023, The Role of Artificial Intelligence in Biometrics, 2023 2nd International Conference on Edge Computing and Applications, pp. 622-626, doi: 10.1109/ICECAA58104.2023.10212224.

39 A. Mitchell, 2013, Distinguishing Friend from Foe: Law and Policy in the Age of Battlefield Biometrics, Canadian Yearbook of international Law/Annuaire canadien de droit international, 50, pp. 289-330, doi: 10.1017/S0069005800010869.

40 J. Thorpe, 2023, FBI amongst key adopters of innovative iris recognition technology for law enforcement, International Security Journal, accessible at https://internationalsecurityjournal.com/fbi-iris-recognition-law-enforcement/

41 J. Lunter, 2023, Synthetic data: a real route to eliminating bias in biometric, Biometric Technology Today 2023(1), accessible at https://www.magonlinelibrary.com/doi/

full/10.12968/S0969-4765%2823%2970001-5

42 A. Gomez-Alanis, J.A. Gonzalez-Lopez & A.M. Peinado, 2022, GANBA: Generative Adversarial Network for Biometric Anti-Spoofing, Applied Sciences, 12(3):1454, accessible at https://doi.org/10.3390/app12031454

43 Z.Zhang et al.,2023, An Improved GAN-based Depth Estimation Network for Face Anti-Spoofing, ICCAI '23: Proceedings of the 2023 9th International Conference on Computing and Artificial Intelligence, March 2023, pp. 323–328, accessible at https://doi.org/10.1145/3594315.3594661

44 Europol, 2023, ChatGPT - the impact of Large Language Models on Law Enforcement, A Tech Watch Flash Report from the Europol Innovation Lab, accessible at https://www.europol.europa.eu/publications-events/publications/chatgpt-impact-of-large-language-models-law-enforcement

45 P. Tomczak, 2018, Machine Learning and the Value of Historical Data, accessible at https://kx.com/blog/machine-learning-and-the-value-of-historical-data/

46 C. Veal, M. Raper & P. Waters, 2023, The perils of feedback loops in machine learning: predictive policing, Gilbert +Tobin, accessible at https://www.lexology.com/library/detail.aspx?g=c8fff116-2112-48dd-841c-f9d1688d722b

47 N. Shahbazi, Y. Lin, A. Asudeh, & H. V. Jagadish, 2023, Representation Bias in Data: A Survey on Identification and Resolution Techniques, ACM Computing Surveys (55)13, accessible at https://doi.org/10.1145/3588433

48 EU Fundamental Rights Agency, 2022, Bias in algorithms - Artificial intelligence and discrimination, doi:10.2811/25847

49 J. Burrell, 2016, How the machine 'thinks': Understanding opacity in machine learning algorithms, Big Data & Society, 3(1), accessible at https://doi.org/10.1177/2053951715622512

50 S. Ali et al., 2023, Explainable Artificial Intelligence (XAI): What we know and what is left to attain Trustworthy Artificial Intelligence, Information Fusion (99)2023, accessible at https://doi.org/10.1016/j.inffus.2023.101805

51 B. Akhgar, et al., 2022, Accountability Principles for Artificial Intelligence (AP4AI) in the Internal Security Domain AP4AI Framework Blueprint, accessible at https://www.ap4ai.eu/sites/default/files/2022-03/AP4AI_Framework_Blueprint_22Feb2022.pdf

52 European Commission, 2019, Ethics guidelines for trustworthy AI, accessible at https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

53 European Commission, 2021, Proposal for a Regulation laying down harmonised rules on artificial intelligence, accessible at https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence

54 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)

55 L. Edwards, 2022, The EU AI Act: a summary of its significance and scope, Ada Lovelace Institute, accessible at https://www.adalovelaceinstitute.org/wp-content/uploads/2022/04/Expert-explainer-The-EU-AI-Act-11-April-2022.pdf

56 Europol, 2023, The Second Quantum Revolution: the impact of quantum computing and quantum technologies on law enforcement, accessible at https://www.europol.europa.eu/publication-events/main-reports/second-quantum-revolution-impact-of-quantum-computing-and-quantum-technologies-law-enforcement#downloads

57 MIT Technology Review, 2023, AI-powered 6G networks will reshape digital interactions, accessible at https://www.technologyreview.com/2023/10/26/1082028/ai-powered-6g-networks-will-reshape-digital-interactions/

About the Europol Innovation Lab

Technology has a major impact on the nature of crime. Criminals quickly integrate new technologies into their modus operandi, or build brand-new business models around them. At the same time, emerging technologies create opportunities for law enforcement to counter these new criminal threats. Thanks to technological innovation, law enforcement authorities can now access an increased number of suitable tools to fight crime. When exploring these new tools, respect for fundamental rights must remain a key consideration.

In October 2019, the Ministers of the Justice and Home Affairs Council called for the creation of an Innovation Lab within Europol, which would develop a centralised capability for strategic foresight on disruptive technologies to inform EU policing strategies.

Strategic foresight and scenario methods offer a way to understand and prepare for the potential impact of new technologies on law enforcement. The Europol Innovation Lab's Observatory function monitors technological developments that are relevant for law enforcement and reports on the risks, threats and opportunities of these emerging technologies. To date, the Europol Innovation Lab has organised three strategic foresight activities with EU Member State law enforcement agencies and other experts.

www.europol.europa.eu