CYCLOPES

DEPLOYING AI IN LAW ENFORCEMENT: PRACTICAL GUIDELINES FOR EUROPEAN AGENCIES

FOR CYCLOPES BY:
SCHEER, GUNHILD
CYBERCRIME RESEARCH INSTITUTE

Funded by
the European Union

DECEMBER 2025

Table of Contents

CYCLOPES | Deploying AI in Law Enforcement:
Practical Guidelines for European Agencies

1. Introduction

Artificial Intelligence (AI) technologies are increasingly used by law enforcement authorities (LEAs) across Europe. From automated face recognition to predictive crime analysis, AI tools promise greater efficiency, but also raise significant legal and ethical concerns.

This guide provides investigators with a structured overview of how AI may lawfully be deployed in criminal investigations. It focuses on high-risk AI systems under the EU Artificial Intelligence Act (AI Act) and obligations stemming from the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED).

Special attention is given to risk classification and compliance requirements under the AI Act, data protection obligations under GDPR and the LED, liability and evidentiary risks for LEAs and their officers, and real-life case studies where unlawful AI use led to the exclusion of evidence or court intervention.

2. What Is "High-Risk AI" Under the AI Act?

The EU AI Act defines “high-risk AI systems” as those that pose significant risks to health, safety, or fundamental rights. For law enforcement, this includes AI used in **post-remote biometric identification**, the evaluation of evidence in criminal proceedings, predictive policing and risk assessment tools, and profiling individuals during investigations.

Real-time remote biometric identification in publicly accessible spaces is **prohibited**, except in narrowly defined exceptional cases (e.g. searching for victims, preventing terrorist threats, or locating suspects of serious crimes), and subject to strict legal safeguards.

These systems are subject to strict obligations under Chapter III of the AI Act, including mandatory risk assessments, data governance, transparency, human oversight, and conformity assessments before deployment. Article 6(2) AI Act in conjunction with Annex III AI Act specifically identifies AI systems intended for use by LEAs to evaluate evidence, predict criminal behaviour, or identify individuals during investigations as high-risk systems.

3. Common AI Applications in Law Enforcement

Artificial Intelligence (AI) is currently deployed by Law Enforcement Authorities (LEAs) across Europe in a growing variety of operational contexts. These include biometric identification (such as facial recognition), predictive policing, natural language processing (NLP), digital forensics, and large-scale data filtering.

Europol has reported[1] the use of AI across the following categories of tasks:

- **Text Classification and Clustering**: AI systems are used to analyse written communication, such as messages, documents, and emails, to detect relevant investigative themes or classify them into criminal categories (e.g. drugs, money laundering, human trafficking). Europol applies these technologies in cross-border investigations and intelligence processing.
- **Machine Translation**: Given the multilingual nature of European investigations, AI-based machine translation is increasingly essential. Europol uses these tools to translate seized material, witness statements, and communication records in real-time or near real-time, increasing processing speed and reducing dependency on human translators.
- **Generative AI**: LEAs have started to explore the cautious use of generative models, for example, to produce investigative leads or reconstruct incomplete digital artefacts. However, Europol explicitly warns that the operational use of such models must be carefully assessed to avoid the risk of hallucinated outputs or misleading evidence.
- **Automated Video and Image Analysis**: Computer vision tools support the detection of objects, persons, or behavioural anomalies in video footage. Europol notes their role in analysing seized media in child sexual exploitation cases and terrorism-related investigations.
- **AI in Digital Forensics**: AI models are increasingly used to accelerate the analysis of digital evidence from seized mobile phones, computers, and storage devices. Tools help identify relevant data (e.g. financial transactions, location data, communications) faster and with greater precision.

These use cases demonstrate the operational potential of AI in high-volume, transnational, and multilingual investigations. However, Europol consistently underlines the need for **structured oversight, explainability, and validation** to ensure these tools are legally and ethically sound.

[1] Europol, AI and Policing: The benefits and challenges of artificial intelligence for law enforcement, Publications Office of the European Union, Luxembourg, 2023, p.18–19. Available at: https://www.europol.europa.eu/cms/sites/default/files/documents/AI-and-policing.pdf.

4. Legal Framework: EU AI Act, GDPR, and LED

The deployment of AI by LEAs is primarily governed by three core legal frameworks. The EU AI Act categorises AI systems according to their risk level; prohibited, high-risk, limited-risk, and minimal-risk, and sets legal obligations accordingly. Since many AI applications in policing are classified as high-risk, they are subject to extensive compliance requirements.

The General Data Protection Regulation (GDPR) applies where personal data is processed outside the scope of criminal investigations. Within criminal justice, the Law Enforcement Directive (EU) 2016/680 (LED) governs the processing of personal data by competent authorities. This includes core principles such as lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, and accountability. These principles must be reflected in every stage of an AI system's lifecycle, from design and procurement to deployment and review.

AI deployments must also comply with relevant national laws implementing these frameworks. The principle of proportionality and necessity is especially important when deploying intrusive technologies such as facial recognition.

5. Opportunities of AI in Criminal Investigations

AI offers substantial operational opportunities for LEAs. In times of persistent resource shortages, increasingly complex crime patterns, and rising volumes of digital evidence, AI systems provide a valuable means of supporting investigations efficiently and systematically.

AI tools can automate time-intensive tasks, such as screening large volumes of seized data, identifying relevant communication patterns, or conducting initial prioritisation of leads. This enables officers to focus their attention on critical tasks and strategic decision-making, which are not easily delegable to machines.

According to Europol, one of the most promising applications is **AI-supported multilingual processing**, particularly in the context of cross-border investigations. AI-powered **machine translation** significantly accelerates the review of evidence across languages and reduces dependence on human linguists, saving time and operational cost. Additionally, **text classification** algorithms can filter relevant case material, categorise records (e.g. by crime type), or link related documents to identify criminal networks.

Digital forensics is another domain where AI tools have demonstrated remarkable utility. Europol reports that in high-volume seizure contexts, such as large-scale financial crime or cybercrime cases, AI can sort, label, and highlight relevant data clusters for investigators to review more efficiently. This capability is particularly helpful in time-critical operations, for example when filtering media from child sexual exploitation investigations.

Moreover, **computer vision and image analysis** technologies are used to automate the detection of suspects, vehicles, or illicit objects in video footage. These systems can help process thousands of hours of surveillance material with minimal manual effort.

In some pilot settings, **generative AI tools** are being explored to reconstruct corrupted files or suggest narrative connections between disconnected data fragments. While this remains experimental, it highlights the growing role of AI as an interpretive rather than merely classificatory tool.

These advances demonstrate that AI can significantly **reduce the burden on personnel, improve operational speed,** and **enhance investigative accuracy,** provided the AI systems are legally compliant, carefully validated, and transparently used.

However, Europol also warns that the deployment of such AI systems must be framed by rigorous governance structures. Efficiency gains can quickly turn into operational or reputational liabilities, if AI systems are used in legally uncertain contexts or without adequate human oversight.

6. Key Risks Associated with AI Use in Criminal Investigations

Despite their promising capabilities, AI systems present serious risks in the context of criminal investigations. These risks do not only concern technological performance but also touch upon fundamental rights, institutional integrity, and the fairness of criminal proceedings.

A primary concern is algorithmic bias. Many AI systems rely on training data that reflects historical patterns, including discriminatory policing or societal inequalities. If not corrected, these biases are transferred into AI outputs, disproportionately targeting certain groups or geographic areas. This can result in unjust profiling, unequal treatment, and discriminatory impacts on already marginalised communities.

Another critical risk poses the opacity of many AI systems. So-called “black box” models may generate conclusions that are not understandable to investigators, defendants, or courts. This lack of explainability undermines accountability and may violate the right to a fair trial under Art. 47 EU Charter of Fundamental Rights (EU Charter) and Article 6 of the European Convention on Human Rights (ECHR). Defendants must be able to challenge the evidence used against them, which presupposes a degree of transparency.

Overreliance on AI systems also poses a structural risk. Investigators may develop a false sense of confidence in the technology’s output and neglect to verify or critically assess automated conclusions. This automation bias is particularly problematic in early case stages when investigative leads are generated or filtered by algorithms.

From a data protection perspective, AI systems often process large volumes of sensitive personal data, such as biometric identifiers or communications metadata. Without strong safeguards, this can lead to unlawful interference with privacy rights under the GDPR or the LED.

Furthermore, the admissibility of AI-detected evidence is under growing scrutiny. Courts in several European jurisdictions have rejected evidence derived from opaque or disproportionate AI applications, especially when legal authorisation or human oversight was lacking.

As Europol warns:

"If not carefully assessed, AI tools can reinforce inequality and erode public trust in law enforcement." (Europol, 2024, AI and Policing Report, p. 5)

This erosion of public trust is not an abstract risk. It directly affects the legitimacy of law enforcement and the acceptance of investigative outcomes by courts and the public.

Real-world examples underscore the gravity of these concerns:

- **Netherlands – SyRI (System Risk Indication)**: In 2020, the Dutch District Court of The Hague declared the use of SyRI unlawful due to a lack of transparency, inadequate safeguards, and disproportionate data use. The system was aimed at detecting welfare fraud through automated risk profiling. SyRI was not AI-based in the technical sense of machine learning, it functioned as a rule-based automated risk scoring system. Its opacity and social impact made it comparable in effect to modern AI-driven profiling tools, and it was declared incompatible with Article 8 ECHR by the District Court of The Hague (ECLI:NL:RBDHA:2020:1878).
- **United States – COMPAS Algorithm**: Although not a European case, the COMPAS system's racially biased risk assessments (exposed in a 2016 ProPublica investigation) remain a cautionary tale for AI developers and law enforcement worldwide (Machine Bias: Risk Assessments in Criminal Sentencing," **ProPublica** (23 May 2016).

These cases illustrate how technically advanced tools can produce **legally unsustainable outcomes** and cause **reputational damage** to authorities when used without sufficient legal and ethical vetting.

7. Duties and Responsibilities of Law Enforcement Officers

The deployment of AI systems by Law Enforcement Authorities (LEAs) is not only a matter of institutional compliance. Individual officers also bear professional and, in some cases, legal responsibility for how AI tools are used during investigations.

The **AI Act**, the **Law Enforcement Directive (LED)**, and, depending on context, the **GDPR**, set out obligations that directly affect daily policing practice:

- Officers must ensure that AI systems are used only **within their intended purpose** and **in accordance with applicable legal authorisation**.
- Outputs generated by AI must be **critically assessed**, not blindly adopted. Human oversight is not a formality, it is a substantive duty of review and verification.
- The use of AI tools must respect the principles of **necessity and proportionality**, especially where fundamental rights (e.g., privacy or presumption of innocence) are affected.
- Personal data processed via AI must comply with **data quality standards** (accuracy, up-to-date, relevance) and **purpose limitation** as required by Articles 4 and 5 of the LED.

While institutions are responsible for procuring and maintaining lawful AI systems, **individual investigators remain accountable** for ensuring that these tools are used correctly and lawfully in operational settings.

Europol emphasises:
"Officers must understand both the operational capabilities and the legal boundaries of AI tools. Misuse—intentional or negligent—can undermine the validity of investigations and the legitimacy of the authority itself." (Europol, 2024, AI and Policing Report)

In practice, this means that officers need **basic training** in how the respective AI systems work, what limitations exist, and how to document and justify their use. Poor documentation or uncritical reliance on AI tools can compromise the **chain of evidence** or violate **disclosure obligations** towards the defence.

Distinction Between Institutional and Personal Responsibility

It is essential to distinguish between **institutional accountability** (i.e. that of the LEA) and **personal responsibility** of individual officers:

- The LEA is responsible for ensuring that any AI system it deploys is compliant with the AI Act, GDPR/LED, and national law. This includes performing conformity assessments, implementing risk mitigation, and ensuring ongoing legal review.
- The officer, however, is responsible for ensuring that the use of the tool in each case is lawful, proportionate, and documented. Officers cannot simply assume that a AI system is legally sound because it has been made available internally.

This distinction is particularly relevant in AI systems that operate with **a high degree of autonomy or opacity**, such as AI-based crime prediction or facial recognition in real-time surveillance. In such cases, improper deployment may lead to **disciplinary proceedings**, and in some jurisdictions even **personal liability** for rights violations.

Clarification: **disciplinary and civil liability consequences** for officers who misuse AI differ across Member States. Some countries have strict liability regimes for public servants, while others apply fault-based or good-faith exceptions. Therefore, national training and internal guidance remain crucial.

8. Liability of LEAs and Individual Officers

The use of AI systems in criminal investigations raises complex liability questions for both LEAs and individual officers. These questions become particularly acute when the use of AI results in rights violations, flawed investigations, or inadmissible evidence.

8.1 Institutional Liability

Law Enforcement Authorities (LEAs) are primarily responsible for ensuring that the AI systems they deploy:

- comply with the obligations of the **AI Act**, including conformity assessments and risk mitigation measures,
- are used in accordance with the **Law Enforcement Directive (LED)** or **GDPR**, particularly in relation to data minimisation, purpose limitation, and data security,
- are accompanied by internal policies, logs, and documentation mechanisms that allow for **auditability** and **accountability**.

Where institutions fail to meet these requirements, they may face:

- **administrative sanctions**, including fines (under GDPR or national data protection laws),
- **judicial review or court sanctions**, such as exclusion of unlawfully obtained evidence,
- **civil liability**, particularly if individuals suffer harm (e.g. unlawful profiling or data exposure),
- **reputational harm**, which may undermine trust in law enforcement more broadly.

The AI Act (Articles 61–71) sets out enforcement powers, redress mechanisms, and complaint procedures that apply to providers and deployers of AI—many of which will be LEAs.

8.2 Individual Officer Liability

In addition to institutional responsibility, individual officers may be held accountable if they misuse or negligently apply AI tools, for example:

- applying AI in an unauthorised context (e.g. using face recognition without a legal basis),
- failing to verify or document AI outputs used in criminal charges,
- neglecting to disclose limitations or uncertainty in AI-generated evidence.

While most Member States place ultimate responsibility on the institution, some legal systems also allow for **personal liability** — especially in cases of **gross negligence** or **intentional rights violations**.

Example: In jurisdictions such as **Germany**, **France**, or **the Netherlands**, public officials can be personally liable under national civil service or liability laws, particularly if they knowingly breach legal obligations. Other countries apply more protective regimes, requiring proof of intent or denying personal liability where officers acted in good faith under superior orders.

In disciplinary terms, misuse of AI systems may trigger **internal investigations**, **warnings**, or even **suspension or dismissal,** depending on national public service law. Officers may also face **criminal liability** if their conduct meets the threshold for unlawful data processing, abuse of authority, or falsification of evidence.

Important clarification: The "**good faith exception**" known in U.S. law (where illegally obtained evidence may be admitted if the officer acted in good faith) **has no direct equivalent in the EU**. In Europe, good faith may be considered **within proportionality assessments** but cannot override explicit legal limits.

8.3 Case Example: Civil Compensation for Violations of Privacy Rights

The risk of liability is not merely theoretical. Several court decisions across the European Union demonstrate that individuals can and do succeed in obtaining compensation for unlawful data processing or privacy violations, even in the absence of financial loss.

Kočner v. Europol

In the 2024 judgment Kočner v. Europol (C-755/21 P), the Court of Justice of the European Union (CJEU) ruled that both Europol and the relevant Member State were jointly and severally liable for the unlawful disclosure of personal and sensitive data. The case concerned the dissemination of private messages and personal data during criminal investigations. The Court awarded 2.000,00 Euro in non-material damages to Mr. Kočner for the violation of his privacy rights (CJEU, 5 March 2024, C-755/21 P; curia.europa.eu).The CJEU determined that the unlawful processing and disclosure of personal communications by Europol constituted an infringement of the right to privacy and the confidentiality of communications under Art. 8 EU Charter. The Court confirmed that such an infringement may give rise to compensatory liability for **non-material damage**, even in the absence of measurable financial harm (CJEU, 5 March 2024, C-755/21 P).

9. Exclusion of Evidence: Consequences of Unlawful AI Use

Unlawful use of AI systems in criminal investigations may not only result in administrative or civil liability, but it can also lead to the **exclusion of evidence**, thereby affecting the outcome of entire proceedings. If investigative results are based on improperly used or non-compliant AI tools, they may be **inadmissible in court**, especially when fundamental rights of the suspect or third parties are infringed.

Under European fundamental rights law, notably **Articles 47 and 48 of the EU Charter**, evidence obtained in violation of essential legal safeguards, such as the right to a fair trial or the right to privacy, may be excluded from use in criminal proceedings. The **Law Enforcement Directive (LED)** and national criminal procedure codes also require that personal data be processed lawfully and proportionately. Evidence gathered through illegal data processing may be found to violate these principles and declared inadmissible.

In criminal investigations, the use of unauthorised facial recognition, predictive risk scoring, or profiling systems without proper legal basis and documentation could likewise result in **evidence being challenged or suppressed.** This can happen especially if the defence is not granted meaningful access to documentation or explanations necessary to challenge the AI system's outputs as required under Article 86(2) of the AI Act and the fundamental right to a fair trial (Article 6 ECHR).

Differentiated Consequences: Institutions vs. Officers

Where evidence is excluded due to unlawful AI use, the **investigative authority** may face institutional consequences, including criticism by oversight bodies, public mistrust, or even damage to the overall integrity of the proceedings. However, **individual officers** may also be affected if it becomes clear that:

- they deployed AI systems without legal authorisation,
- failed to document their use or methodology,
- ignored known limitations or compliance warnings.

In some Member States, this can trigger **disciplinary action** or a **formal reprimand**, especially if internal policies or legal training have been disregarded.

Legal Variation Across Member States

The rules governing the **exclusion of unlawfully obtained evidence** differ across EU Member States:

- Some countries apply a **strict exclusionary rule**, meaning that any unlawfully obtained evidence is automatically inadmissible.
- Others allow for a **balancing test**, assessing whether the legal violation was serious enough to affect the fairness of the trial.
- A few jurisdictions may consider whether the officer acted in **good faith** or under an honest misunderstanding of the law.

Clarification: While the "good faith exception" known from U.S. law does not exist as a formal doctrine in the EU, some Member States may consider the officer's intent or diligence as part of a broader proportionality test. However, this cannot override explicit legal limits or mandatory safeguards.

This legal fragmentation underscores the importance of **internal legal review** and **documentation**. AI-generated evidence must always be linked to **lawful, proportionate, and traceable procedures** to ensure admissibility and procedural fairness.

10. Practical Recommendations for Lawful AI Use

The deployment of AI in LEAs offers significant operational advantages. Properly implemented, AI can increase efficiency, support overburdened investigators, and accelerate complex casework. Especially in times of chronic understaffing and increasing digital complexity, AI systems offer a valuable opportunity to enhance the effectiveness of policing.

However, these benefits can only be realised if AI systems are used **within the boundaries of applicable law**. Poor implementation, insufficient training, or a lack of transparency may not only render AI outputs **inadmissible as evidence**, but also result in institutional liability, reputational harm, or public backlash.

Clarification: The legal risks of non-compliance are not limited to administrative sanctions. In some Member States, procedural errors involving AI tools may lead to exclusion of evidence, disciplinary consequences for individual officers, or even civil claims for damages by affected individuals.

To support lawful and effective use of AI in criminal investigations, the following good practices should be followed:

Checklist: Before Deployment

- **Legal Review**: Ensure the AI tool falls within a valid legal framework (e.g. under specific police act, data protection law, or special investigative power).
- **High-Risk Classification**: Determine whether the system qualifies as "high-risk" under the AI Act (Art. 6–29) and complete the required conformity assessment.
- **Procurement Compliance**: Verify that the provider has met the obligations for data quality, robustness, human oversight, and documentation.
- **DPIA / Fundamental Rights Assessment**: Conduct a Data Protection Impact Assessment (DPIA) or, where applicable, a Fundamental Rights Impact Assessment (FRIA) to identify potential infringements

Checklist: During Use

- **Training & Internal Guidelines**: Officers must be trained in how the AI system functions, its limitations, and the legal safeguards that apply.
- **Transparency in Use**: Keep an auditable record of when, why, and how the AI system was used during an investigation.
- **Human Oversight**: Maintain meaningful human involvement and never delegate final decision-making solely to the AI system.
- **Explainability**: Ensure that outputs can be interpreted and explained, especially when used to justify coercive measures (e.g. arrest, search, or surveillance).

Checklist: After Use

- **Evidence Traceability**: Document the link between the AI system and the investigative result. Ensure the chain of evidence remains intact and reproducible.
- **Defence Access**: Be prepared to grant defence lawyers access to technical documentation or explanations of the system when AI-based evidence is used in court.
- **Internal Evaluation**: Establish review mechanisms to assess whether the AI system contributed meaningfully and lawfully to the case outcome.

Operational Realities: Informal Use and Validation Gaps

Recent practitioner feedback, including from cross-border project meetings, suggests that AI tools are sometimes used in practice **without being formally declared as such**. In some cases, AI applications help generate leads that are then **replicated through manual methods** to avoid disclosure or legal complexity. While such practices may be intended to simplify procedures, they **raise serious questions about transparency, accountability, and evidentiary integrity**.

Furthermore, **validation practices for AI tools remain uneven across agencies**. It is unclear in many operational contexts:

- whether updated tools require new legal assessments or technical documentation,
- how validation responsibilities are distributed between providers and deploying authorities,
- and whether mutual recognition of validated tools across Member States is possible or advisable.

These uncertainties can lead to fragmentation and inconsistencies in legal compliance. Investigators may be unsure whether and how to document AI use, especially when tools evolve incrementally over time or are repurposed in different investigative contexts.

While the AI Act provides clear obligations for high-risk systems, **further operational guidance will be essential** to clarify:

- how agencies should handle minor updates,
- how informal or internal-use tools should be reported and evaluated,
- and how best to balance operational flexibility with legal and ethical safeguards.

Recommendation: Law enforcement agencies should establish internal protocols not only for the deployment of officially procured AI systems, but also for **informal, experimental, or evolving tools** that influence investigative outcomes. Transparency and traceability are essential – even where the AI system is not directly cited in court.

Final Reflection

AI offers **enormous opportunities** for modern policing, from handling data volumes to identifying hidden connections and accelerating investigative processes. But the use of AI in criminal investigations is not a technical matter alone: it is a legally regulated activity, subject to strict standards of **necessity, proportionality, accountability**, and **respect for fundamental rights**.

AI becomes an asset to law enforcement only when it is **legally grounded, ethically used, and operationally controlled**. If these conditions are not met, the very tool meant to support investigations may become a liability, **jeopardising criminal trials, violating individual rights, and undermining public trust in law enforcement**.

11. Building Trust and Accountability in the Use of AI by LEAs

For AI to be effective in criminal investigations, **public trust** and **institutional accountability** must go hand in hand with technical capability. Even the most advanced AI systems cannot succeed in law enforcement environments if they are perceived as **opaque, discriminatory, or unregulated**. As highlighted in Europol's 2024 report "AI and Policing", trust is not merely an outcome, it must be **actively built** into the design, deployment, and oversight of AI systems.

11.1 Transparency and Public Communication

Transparency does not mean disclosing sensitive operational details. Rather, it means that law enforcement authorities must:

- Communicate clearly what types of AI systems are in use,
- Under what legal frameworks they operate,
- And how human oversight is ensured.

Proactive public communication helps counter fears of “black box policing” and demonstrates that AI use is neither arbitrary nor beyond scrutiny.

Note: The AI Act (Articles 13 and 14) requires that high-risk AI systems provide **clear information** to users and allow for **traceable and auditable decision-making**. These provisions are crucial to enabling meaningful transparency without undermining operational security.

11.2 Accountability and Redress Mechanisms

Accountability mechanisms ensure that individuals affected by AI-supported investigations have meaningful ways to challenge decisions or seek redress. This includes:

- Documentation of system use,
- Accessible complaints procedures,
- And independent oversight (e.g. data protection authorities, courts, or parliamentary bodies).

Failure to provide such mechanisms can lead to **strategic litigation, reputational damage**, or **policy reversals** — as seen in the Netherlands, where the SyRI system was abandoned following a court ruling and widespread criticism.

11.3 Internal Trust: Empowering Officers

AI systems must also earn the trust of the **officers who use them**. If investigators feel they lack training, cannot understand system outputs, or fear disciplinary consequences for misuse, AI tools will either be misapplied or underused. Building internal trust involves:

- Continuous training programs,
- Clear usage protocols,
- Legal clarity on roles and responsibilities,
- And shared ownership of results.

11.4 A Dual Obligation: Effectiveness and Legitimacy

LEAs face a dual obligation: to **leverage AI for greater effectiveness** while simultaneously **protecting rights and ensuring legitimacy**. The success of AI in policing depends not only on accuracy and speed but also on whether the public and the judiciary see its use as **lawful, fair, and proportionate**.

12. Conclusion

Artificial Intelligence presents a transformative opportunity for law enforcement authorities (LEAs) in Europe. When deployed thoughtfully under the constraints of the EU AI Act, GDPR, and the LED AI can significantly enhance investigative capacity, accelerate case resolution, and relieve workloads during periods of staffing limitations. These benefits include faster analysis of large or multilingual datasets, improved accuracy in identifying relevant leads, and better resource allocation, among others.

Yet, this potential comes with considerable responsibility. Improper implementation — whether through lack of transparency, unclear legal authorisation, failure of oversight, or insufficient regard for human rights — can lead to serious legal, operational, and reputational harms. Evidence may be excluded, officers may face liability, and public trust may erode if citizens perceive LEA practices as unfair or opaque.

Therefore, achieving the promise of AI for policing depends on striking a careful balance. The tools must be matched with robust governance, clear legal and ethical frameworks, ongoing training, and constant evaluation. Only under these conditions will AI serve as a force-multiplier rather than a liability. LEAs that commit to transparency, accountability, and human oversight are those best placed to harness AI's advantages without compromising fundamental rights or the rule of law.

CYCLOPES

JOIN THE CYCLOPES NETWORK

FOLLOW US

Project-Cyclopes

ProjectCyclopes

WEBSITE

https://cyclopes-project.eu

CONTACT

contact@cyclopes-project.eu

Funded by
the European Union