FLASH REPORT 09

AI ACT AND LAW ENFORCEMENT

Main Authors
Isabela Maria Rosal (KU Leuven)
Dorothea Tsatsou (CERTH)
Vincent Perez de Leon-Huet (EOS)

December 2025

ENACT.
European Network Against Crime and Terrorism


AI

03

About ENACT

ENACT is a knowledge network focused on the fight against crime and terrorism (FCT). The network is funded under the Horizon Europe Framework Programme in Cluster 3 – Civil Security for Society. The project addresses the call topic HORIZON-CL3-2022-SSRI-01-02 'Knowledge Networks for Security Research & Innovation', aiming to collect, aggregate, process, disseminate and make the most of the existing knowledge in the FCT area.

The project aims to satisfy two major ambitions,

- Provide evidence-based support to the decision-makers in the EU research and innovation (R&I) ecosystem in the FCT domain, targeted explicitly at enabling more effective and efficient programming of EU-funded R&I for the fight against crime and terrorism.

- Act as a catalyst for the uptake of innovation by enhancing the visibility and reliability of innovative FCT security solutions.

Report Feedback

We're collecting feedback on this report through the EU Survey Platform, if you'd like to share your thoughts anonymously please click on the link below.

https://ec.europa.eu/eusurvey/runner/enact-report-feedback

Funded by
the European Union

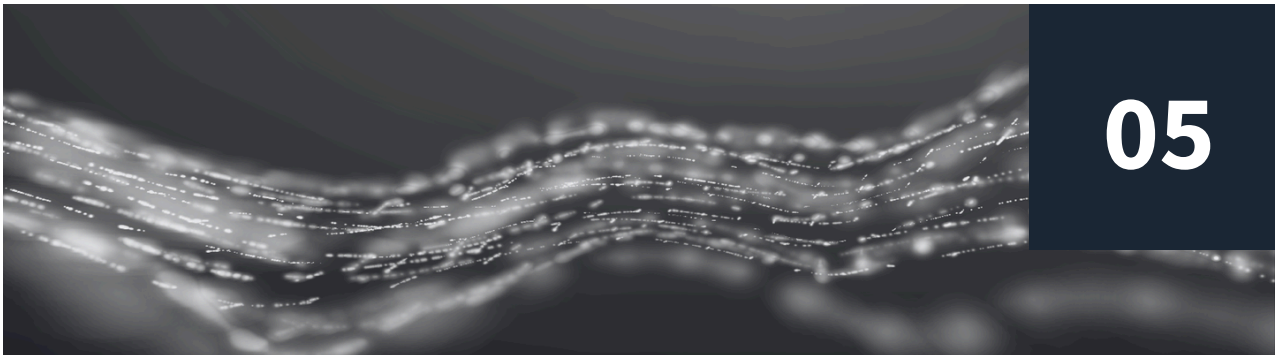
Disclaimer

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Copyright

Acronyms

AI	Artificial Inteliigence
AP4AI	Accountability Principles for Artificial Intelligence
CAGR	Compound Annual Growth Rate
ELS	Ethical, Legal, Societal
EC	European Commission
FCT	Fight against Crime and Terrorism
FRIA	Fundamental Rights Impact Assessment
GenAI	Generative Ai
GPAI	General Purpose AI
JRC	Joint Research Centre
LEAs	Law Enforcement Agencies
LED	Law Enforcement Directive
PETs	Privacy Enhancing Technologies
RBI	Remote Biometric Identification
R&D	Research & Development
SIS	Smart Information System
SKB	Structured Knowledge Based
XAI	Explainable AI



05

Scene Setter

The legislative process [1]

In 2019, the then candidate for President of the European Commission (EC), Ursula von der Leyen, proposed to move forward an Artificial Intelligence (AI) Regulation within her first 100 days in office [2]. After her election, even though a legal proposal was not presented within the foreseen timeline, the EU Commission published a White Paper on AI [3], with a major influence from the Guidelines for Trustworthy AI from the High-Level Expert Group on AI [4]. After a short period, in April 2021, the EC published the proposal for a Regulation laying down harmonised rules on AI [5]. This was the origin of what was to come - the AI Act. Following the ordinary legislative process, but in a short timeframe, the European Council formally adopted the EU AI Act in May 2024, and the final legal text was officially published in July 2024 [6].

Application

After a short period, the AI Act entered into force on 1st August 2024. If nothing changes, the norm will be fully applicable as of 2nd August 2026, with certain exceptions:

- Prohibitions and AI literacy obligations entered into application on 2nd February 2025.
- Governance rules and obligations for General-Purpose AI (GPAI) models became applicable on 2nd August 2025.
- Rules for high-risk AI systems, embedded into regulated products, have an extended transition period until 2nd August 2027 [7].

[1] For a detailed overview of the legislative process and some of the discussions surrounding the AI Act, see, c.f.: Donatella Casaburo and Lorenzo Gugliota (2023) The EU AI Act proposal(s): Context and definition of AI. *CiTiP Blog* https://www.law.kuleuven.be/citip/blog/the-eu-ai-act-proposals-context-and-definition-of-ai/; EU Artificial Intelligence Act (n.d.) Historic Timeline. https://artificialintelligenceact.eu/developments/
[2] Ursula von der Leyen (2019) A Union that strives for more: My agenda for Europe. https://commission.europa.eu/system/files/2020-04/political-guidelines-next-commission_en_0.pdf
[3] European Commission (2020) White Paper on Artificial Intelligence – A European approach to excellence and trust. https://commission.europa.eu/system/files/2020-02/commission-white-paper-artificial-intelligence-feb2020_en.pdf.
[4] High-Level Expert Group on AI - European Commission (2019) Ethics Guidelines for Trustworthy Artificial Intelligence. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai
[5] European Commission (2021) Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts.
[6] European Union (2024) 'Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689.
[7] European Commission (2025) AI Act. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

When the deadline for implementation of rules around General Purpose AI (GPAI) models was approaching, pressure mounted for a possible delay on the implementation, especially because the elaboration of a Code of Practice for GPAI models took longer than expected [8]. However, even under industry pressure, the deadline did not change, and the GPAI rules began to apply on 2nd August 2025 [9] after the publication of the GPAI Code of Practice on 10th July 2025 [10]. This discussion on GPAI rules is an interesting example to showcase the importance of codes of practice, standards and other soft law instruments in the application of the AI Act.

AI Act Approach

The AI Act follows a layered risk-based approach. The higher the risks posed by an AI application the higher-level the compliance measures imposed by the EU regulation.

Through the legal text, the AI Act already defines an AI risk qualification with the following layers:

- *Unacceptable risk:* defined prohibited practices (harmful AI-based manipulation, deception, and exploitation of vulnerabilities, social scoring, **individual criminal offence risk assessment or prediction, untargeted scraping of the internet or CCTV material to create or expand facial recognition databases**, emotion recognition in work and education places, **biometric categorisation to deduce certain protected characteristics**, and **real-time biometric identification for law enforcement purposes in publicly accessible spaces)**
- *High risk:* **AI uses that can pose serious risks to health, safety of fundamental rights**, but that are not prohibited (e.g., **AI use-cases in law enforcement that may interfere with people's fundamental rights**, including evaluation of the reliability of evidence, **AI use-cases in migration, asylum and border control management**, **AI solutions used in the administration of justice and democratic processes**) which are subject to strict obligations before they are put in the market (e.g., human oversight measures, logging of activities to ensure traceability).
- *Limited risk:* requires implementation of transparency measures (e.g., disclaimer for a user that they are interacting with a chatbot).
- *Minimal risk:* AI Act does not apply [11].

As illustrated with the summary presented above, several use-cases directly linked to LEAs and the Fight against Crime and Terrorism (FCT) community fall under the classifications of unacceptable or high risks. This requires a continuous engagement between LEAs and other stakeholders to ensure a prime implementation of the rules created by the AI Act. It is in this context that this Flash Report takes form. Leveraging from the observations and analysis in ENACT's Structured Knowledge Base (SKB) [12], the report will present certain trends and findings in the realm of AI Act application among LEAs. More than 400 (four hundred) observations fell under the criteria "Artificial Intelligence" in the "Relevant Technologies" classification.

[8] c.f., Henning, M. (2025) Airbus and other EU industry giants join calls to stop the clock on AI Act. *EURACTIV.* https://www.euractiv.com/section/tech/news/airbus-and-other-eu-industry-giants-join-calls-to-stop-the-clock-on-ai-act/; Mukherjee, S. (2025) Explainer: Will the EU delay enforcing its AI Act? *Reuters.* https://www.reuters.com/business/media-telecom/will-eu-delay-enforcing-its-ai-act-2025-07-03/.
[9] c.f., Moreau, C. (2025) The EU will ont budge on deadline for generative AI rules. *EURACTIV.* https://www.euractiv.com/section/tech/news/the-eu-will-not-budge-on-deadline-for-generative-ai-rules/.
[10] European Commission (2025) The General-Purpose AI Code of Practice. https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai.
[11] European Commission (2025) AI Act. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai
[12] ENACT (2025) Structured Knowledge Base (SKB) https://enact-eu.net/enact-fct-stakeholder-map/

TECHNOLOGY VIEW

07

Summary

The AI Act is already shaping how AI can be built and used by Law Enforcement Agencies (LEAs), for the FCT domain and beyond. The cascading enforcement of the Act has introduced the need to assess and classify, if applicable, AI systems used in law enforcement as high risk, and sometimes as unacceptable risk system, according to the definition of high risk systems in Annex III (referred in Article 6 (2)) and the classification rules of Article 6. As per the Act's requirements, the framework for high-risk systems (Articles 8-15), are governed under specific obligations including systematic risk management, data & data governance controls, technical documentation, system logging, transparency of operational context and concrete instructions of use, human oversight in all cycles of design and development, evaluation and benchmarking on accuracy, technical robustness and (cyber)security of models, system and data, and a conformity assessment to the Act. Additionally, the framework requires registration of high-risk systems in an EU database (Article 71) and a **Fundamental Rights Impact Assessment (FRIA) before deployment.**

Additional considerations and guidelines have since applied, notably: (a) the **Guidelines on prohibited AI practices** [12] (unacceptable risk systems), taking effect in February 2025, with detailed guidelines for high-risk AI systems and different provisions becoming available in February 2026 and full high-risk AI system obligations becoming mandatory, including harmonised standards, in August 2026 [13]. The guidelines ban systems that predict criminal risk based solely on profiling and tightly restricting real-time Remote Biometric Identification (RBI) in public spaces to narrow, pre-authorised law-enforcement scenarios (e.g., a specific imminent threat or targeted searches), with strict safeguards and prior judicial/independent authorisation. (b) The **GPAI code of practice** [14], published in August 2025, forming the basis for GPAI standards with a lookahead for adoption of these standards by August 2027 or later, outlining specific provisions for prohibited and high-risk GPAI systems.

The broader **high-risk systems regime timeline** mandates that AI developers and LE tech teams deploying AI systems must assume the guardrails are "live" for **GPAI and prohibited practices**, enforcing and applying relevant **operational and oversight structures.**

Technically, the bar is rising on how AI systems for the FCT domain and for use in law enforcement are engineered, tested, and monitored. Implementation guidance now emphasises data governance, bias mitigation and fairness enforcement, rigorous performance testing, security-by-design, detailed logging and traceability/accountability measures, human oversight, and post-market monitoring. These are core obligations for high-risk AI and relevant to LE use cases like biometrics-employing systems, digital-evidence analytics, forencsic analysis and investigation assistance, security of critical infrastructures, etc., including GenAI-assisted tools.

[13] European Commission (2025) Commission publishes the Guidelines on prohibited artificial intelligence (AI) practices, as defined by the AI Act. https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act
[14] Nemko Digital (2025) EU AI Act Delay Officially Ruled Out: Timeline Confirmed for Full Implementation. https://digital.nemko.com/news/eu-ai-act-delay-officially-ruled-out
[15] European Commission (2025) The General-Purpose AI Code of Practice. https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai

Exceptions to the application of the AI Act

According to Articles 2, 5, 27, 49, 46 and Annex II, there are certain narrow exceptions in the AI Act that affect LE use:

- *Full exception (Article 2):* Operation for national security, defence, military. Any AI system used exclusively for these purposes is outside the AI Act, no matter who operates it (including police acting for national-security purposes).
- *Full exception (Article 2):* Foreign authorities in cooperation cases. Public authorities in third countries (or international organisations) using AI under international law-enforcement or judicial-cooperation agreements with the EU or a Member State are out of scope, provided adequate fundamental-rights safeguards exist.
- *Prohibition with narrowly defined exceptions (Article 5):* RBI in public is allowed only if strictly necessary for one of the following objectives, and only with prior judicial (or binding independent authority) authorisation and additional safeguards (FRIA, database registration), with limited urgency overrides:
  - Targeted search for specific victims or missing persons
  - Preventing a specific, substantial and imminent threat to life/physical safety or a genuine (present/foreseeable) terrorist threat
  - Locating/identifying a suspect of a serious offence listed in Annex II
- *High-risk RBI:* Delayed (non real-time) RBI for e.g. post-event analysis is not banned but is considered, in all cases, high-risk and generally requires judicial authorisation linked to prosecution of serious crimes, while all such systems it must meet the high-risk obligations in the AI Act.
- *Narrow dataset handling exception for biometric categorisation (Article 5):* The ban on biometric categorisation to infer sensitive traits (e.g., race, religion, sexual orientation) excludes labelling of lawfully acquired biometric datasets or categorising biometric data in the area of law enforcement.
- *Emergency conformity assessment need lift (Article 46):* In exceptional public security situations (or imminent threats to life), a surveillance authority may authorise temporary use of a specific high-risk AI system before full conformity assessment; in urgent cases law-enforcement authorities may put it into service first, but must seek authorisation during or after use without undue delay. If later refused, the system must be stopped and outputs discarded.

Key References

- Giannini, A., & Tas, S. (2024). AI Act and the Prohibition of Real-Time Biometric Identification. *Verfassungsblog*. https://verfassungsblog.de/ai-act-and-the-prohibition-of-real-time-biometric-identification/
- Future of Life Institute (2025) High-level summary of the AI Act. http://artificialintelligenceact.eu/high-level-summary/
- Future of Life Institute (2024) EU AI Act: Tasks in 2024–2025 for Member States. https://artificialintelligenceact.eu/wp-content/uploads/2024/10/FLI-Tasks-Member-States-2024-25.pdf
- Erdogan, I. (2024). Diving into the Iceberg: Establishing Transparency in AI for Law Enforcement. *European Papers-A Journal on Law and Integration*, 2024(3), 956-977. https://www.europeanpapers.eu/system/files/pdf_version/EP_eJ_2024_3_SS1_3_Irmak_Erdogan_00794.pdf
- Borak, M. (2025) EU issues guidelines clarifying banned AI uses. *Biometric Update.* https://www.biometricupdate.com/202502/eu-issues-guidelines-clarifying-banned-ai-uses
- Sampson, F. (2025) Do the police ever forget a face? *Biometric Update.* https://www.biometricupdate.com/202503/do-the-police-ever-forget-a-face
- ICT Security Magazine (2025) AI Act: la Commissione UE pubblica le Linee Guida sulle pratiche proibite. https://www.ictsecuritymagazine.com/notizie/ai-act-linee-guida-ue/

09

Prohibited vs. narrowly-permitted use and biometrics in policing

The AI Act bans several LE-relevant practices outright (e.g., biometric categorisation by sensitive traits; untargeted scraping for face databases; individual-level predictive policing). Real-time remote biometric identification (RBI) in public spaces is generally prohibited but allowed in tightly-scoped, court-authorised exceptions (specific serious crimes, prevention of substantial threats, or searching for serious crime victims) with strict ex-ante approvals, time/location limits, and logging. Post-event biometric identification is usually accepted but still constrained and governed by regulatory checks.

Relevant R&D implications:

- Use case design should not include banned operations per the prohibited AI practices, while appropriate safeguards should be designed and embedded in the use case design, in order to prevent inadvertent prohibited operations (e.g., individual predictive scoring).
- If employing RBI in exceptional cases, pre-deployment approval workflows should be built, including conducting a FRIA, time and geographical scoping should be considered, and comprehensive audit logs must be built into the systems by design.

Key References

- Amnesty International (2025) Automated Racism. https://www.amnesty.org.uk/files/2025-02/Automated%20Racism%20Report%20-%20Amnesty%20International%20UK%20-%202025.pdf
- Sampson, F. (2025) Do the police ever forget a face? *Biometric Update.* https://www.biometricupdate.com/202503/do-the-police-ever-forget-a-face
- FairTrials (2025) Law and Policy on the use of Artificial Intelligence by Police and Criminal Justice Systems. https://www.fairtrials.org/app/uploads/2025/02/Report-Fair-Trials-Law-and-Policy_AI_2411.pdf
- Europol (2024) AI and policing - The benefits and challenges of artificial intelligence for law enforcement. *Europol Innovation Lab Observatory Report.* https://www.europol.europa.eu/publication-events/main-reports/ai-and-policing
- Europol (2025) Biometric vulnerabilities, Ensuring future law enforcement preparedness. *Europol Innovation Lab Observatory Report*. https://www.europol.europa.eu/publication-events/main-reports/biometric-vulnerabilities-ensuring-future-law-enforcement-preparedness
- NPCC (2025) Artificial Intelligence (AI) Strategy. *National Police Chiefs Council.* https://www.npcc.police.uk/SysSiteAssets/media/downloads/publications/publications-log/science-and-innovation/2025/npcc-ai-strategy.pdf
- Sampson, F. (2025) Surveillance, identity and the right to go missing. *Biometric Update.* https://www.biometricupdate.com/202503/surveillance-identity-and-the-right-to-go-missing
- Erdogan, I. (2024). Diving into the Iceberg: Establishing Transparency in AI for Law Enforcement. *European Papers-A Journal on Law and Integration*, 2024(3), 956-977. https://www.europeanpapers.eu/system/files/pdf_version/EP_eJ_2024_3_SS1_3_Irmak_Erdogan_00794.pdf

Compliance-by-design and standardisation

As aforementioned, several activities should be incorporated by design in the high-risk, FCT related and LE deployed, AI systems' design, development, use and assessment lifecycle, as described in the HLEG's Ethics Guidelines for Trustworty AI[1], including risk management, the use of high-quality, representative and balanced/debiased datasets, technical documentation including precise description of the tools' operational context, risks and limitations, event logging, human oversight during the entirety of the afore-described lifecycle, conducting post-deployment monitoring and establishing communication means between LE agents and developers to ensure timely an actionable incident reporting. Additionally, since the AI Act's essential requirements are operationalised via harmonised standards, the EU AI Office and scientific panels (e.g. JRC, AI Watch) will steer relevant guidance, codes of practice and supervision for high-impact systems.

Relevant R&D implications:

- AI systems' developers need to build and provide fully detailed documentation, including model and dataset descriptions, model/system operational context and intended use (including use case/scenarios description), foreseen risks within intended use and preferably provisional risks when used out of operational context, logging including hazard logs and change logs, traceable MLOps and human-in-the-loop controls - from system design, to each development step, usage and assessment.
- Consider conducting or at least expecting conformity assessments (self-assessment vs. notified body) and align implementations to evolving CEN/CENELEC/ISO standards.
- AI design and development must map and design processes to requirements to emerging standards (e.g., risk management, data quality, transparency) and track AI Office outputs to keep systems conformant as guidance evolves.

Key References

- Pouget, H. (2025) EU AI Act - Institutional Context. *Future of Life Institute.* https://artificialintelligenceact.eu/context/
- Future of Life Institute (2024) High-level summary of the AI Act. https://artificialintelligenceact.eu/high-level-summary/
- European Commission (n.d.) Artificial Intelligence at the JRC. https://ai-watch.ec.europa.eu/artificial-intelligence-jrc_en
- Project Sherpa (n.d.) Recommendation: Include research findings on AI ethics in standardization. https://www.project-sherpa.eu/standardization/
- Project Sherpa (n.d.) Recommendation: Promote Ethics by Design for researchers in EC-funded projects. https://www.project-sherpa.eu/ethics-by-design/
- Project Sherpa (n.d.) Recommendation: Develop baseline model for AI impact assessments. https://www.project-sherpa.eu/ai-impact-assessment/

Transparency and access

Effective transparency of AI systems for LE use depends on the Law Enforcement Directive (LED) plus the AI Act's logging, documentation, and transparency obligations. In practice, fragmentation, prohibition exceptions, privacy preservation often impede access and oversight.

Relevant R&D implications:

- AI R&D needs to provision operator-facing traceability (decision trails, data provenance), disclosure documentation for regulators and LE operators, as well as access request support (where lawful).
- Trade secret vs. transparency conflicts must be anticipated, by building layered transparency tools, including explanations (i.e. versions for the public, for regulators only, internal for LEAs).

Key References

- Erdogan, I. (2024). Diving into the Iceberg: Establishing Transparency in AI for Law Enforcement. *European Papers-A Journal on Law and Integration*, 2024(3), 956-977. https://www.europeanpapers.eu/system/files/pdf_version/EP_eJ_2024_3_SS1_3_Irmak_Erdogan_00794.pdf
- FairTrials (2025) Law and Policy on the use of Artificial Intelligence by Police and Criminal Justice Systems. https://www.fairtrials.org/app/uploads/2025/02/Report-Fair-Trials-Law-and-Policy_AI_2411.pdf
- NPCC (2024) Covenant for Using Artificial Intelligence (AI) in Policing. https://science.police.uk/delivery/resources/covenant-for-using-artificial-intelligence-ai-in-policing/
- NPCC (2025) Artificial Intelligence (AI) Strategy. *National Police Chiefs Council.* https://www.npcc.police.uk/SysSiteAssets/media/downloads/publications/publications-log/science-and-innovation/2025/npcc-ai-strategy.pdf
- Muir, R. & O'Connell, F. (2025) Policing and Artificial Intelligence. *Police Foundation.* https://www.police-foundation.org.uk/wp-content/uploads/2010/10/policing-and-ai.pdf.pdf
- Project Sherpa (n.d.) Recommendation: Develop baseline model for AI impact assessments. https://www.project-sherpa.eu/ai-impact-assessment/

Data quality, bias and fairness

Data quality and dataset balance, debiasing dataset and models and documenting bias and employing relevant fairnesss feedback loops in predictive AI systems, while also considering inclusion and demographic variability of model accuracy, especially in face recognition technologies, is of paramount importance. Research shows explanations alone don't yield appropriate trust when the underlying system is biased. The AI Act requires representative, relevant, error-managed datasets and bias controls.

Relevant R&D implications:

- Treat fairness as a topmost objective, including debiasing, dataset balance, inclusivity and population-specific accuracy variability.
- Enforce representation audits, bias metrics, counterfactual and subgroup testing, continual monitoring for drift and disparate impact.
- Incorporate fairness considerations beyond mere explainability: mitigate both upstream (data design, labelling, feature selection) and downstream (thresholding, deployment rules).

Key References

- Mehrotra, S., Gadiraju, U., Bittner, E., van Delden, F., M. Jonker, C., & L. Tielman, M. (2025). "Even explanations will not help in trusting [this] fundamentally biased system": A Predictive Policing Case-Study. In *Proceedings of the 33rd ACM Conference on User Modeling, Adaptation and Personalization* (pp. 51-62). https://doi.org/10.1145/3699682.3728343
- Amnesty International (2025) Automated Racism. https://www.amnesty.org.uk/files/2025-02/Automated%20Racism%20Report%20-%20Amnesty%20International%20UK%20-%202025.pdf
- Cerezo-Martínez, P., Nicolás-Sánchez, A., & Castro-Toledo, F. J. (2024) Analyzing the European institutional response to ethical and regulatory challenges of artificial intelligence in addressing discriminatory bias. *Frontiers in Artificial Intelligence*, 7, 1393259. https://doi.org/10.3389/frai.2024.1393259
- NPCC (2025) Artificial Intelligence (AI) Strategy. *National Police Chiefs Council.* https://www.npcc.police.uk/SysSiteAssets/media/downloads/publications/publications-log/science-and-innovation/2025/npcc-ai-strategy.pdf
- Etti, P. (2024) Exploring the use of synthetic data in the public sector: a framework and case study based on the example of the Estonian Police and Border Guard. *Tallinn University of Technology.* Master's Thesis. https://www.etis.ee/Portal/Publications/Display/7c4c4890-efec-44b0-9559-a386093a2b5d
- Sampson, F. (2025) Can AI predict who will commit crime? *Biometric Update.* https://www.biometricupdate.com/202504/can-ai-predict-who-will-commit-crime
- Muir, R. & O'Connell, F. (2025) Policing and Artificial Intelligence. *Police Foundation.* https://www.police-foundation.org.uk/wp-content/uploads/2010/10/policing-and-ai.pdf.pdf

Privacy preservation, data access and security

An important open matter in the AI R&D community for LE is enabling collaboration without exposing sensitive data (of individuals within investigation or the LEAs themselves). To this end, work and projects advocate federated learning strategies for model training and synthetic data and other privacy-enhancing technologies (PETs) such as differential privacy, secure multi-party computation and homomorphic encryption. Moreover, emphasis is placed in the provision against adversarial threats (poisoning, evasion, model extraction) and the need for secure-by-design AI systems and continuous monitoring.

Relevant R&D implications:

- PET pipelines are essential, if not obligatory for model training and testing and for evaluating systems' privacy.
- When using synthetic or real data, there's a need to validate privacy leakage, utility, and bias
- Using supervised regulatory sandboxes with auditable and responsible testing is highly encouraged.
- Need to integrate threat modelling, adversarial testing, data/feature integrity checks, and secure model supply-chain practices.

Key References

- Etti, P. (2024) Exploring the use of synthetic data in the public sector: a framework and case study based on the example of the Estonian Police and Border Guard. Tallinn University of Technology. Master's Thesis. https://www.etis.ee/Portal/Publications/Display/7c4c4890-efec-44b0-9559-a386093a2b5d·
- Baloukas, C. et al. (2024). A risk assessment and legal compliance framework for supporting personal data sharing with privacy preservation for scientific research. In *Proceedings of the 19th International Conference on Availability, Reliability and Security* (pp. 1-10). https://doi.org/10.1145/3664476.3670878
- College of Policing (2025) Building AI-enabled tools and systems. https://www.college.police.uk/guidance/building-ai-enabled-tools-and-systems
- European Commission (n.d.) Artificial Intelligence at the JRC. https://ai-watch.ec.europa.eu/artificial-intelligence-jrc_en
- Project Sherpa (n.d.) Recommendation: Undertake security analysis for machine learning systems. https://www.project-sherpa.eu/security/
- European Data (2025) Open data and AI: An update on the AI Act. https://data.europa.eu/en/news-events/news/open-data-and-ai-update-ai-act

Key References (continued)

- NPCC (2025) Artificial Intelligence (AI) Strategy. *National Police Chiefs Council.* https://www.npcc.police.uk/SysSiteAssets/media/downloads/publications/publications-log/science-and-innovation/2025/npcc-ai-strategy.pdf
- Project Sherpa (n.d.) Security Issues, Dangers and Implications of Smart Information Systems (SIS). https://www.project-sherpa.eu/security-issues-dangers-and-implications-of-smart-information-systems-sis/
- National Academies of Sciences, Engineering, and Medicine. (2025). Cyber Hard Problems: Focused Steps Toward a Resilient Digital Future. https://doi.org/10.17226/29056
- Pawlicki, M., Pawlicka, A., Kozik, R., & Choraś, M. (2024) Advanced insights through systematic analysis: Mapping future research directions and opportunities for xAI in deep learning and artificial intelligence used in cybersecurity. *Neurocomputing*, 590, 127759. https://doi.org/10.1016/j.neucom.2024.127759
- UNCCT and UNICRI (2021) Countering terrorism online with artificial intelligence. *United Nations Office of Counter Terrorism and United Nations Interregional Crime and Justice Research Institute.* https://unicri.org/sites/default/files/2021-06/Countering%20Terrorism%20Online%20with%20AI%20-%20UNCCT-UNICRI%20Report.pdf

Human oversight and explainability

As aforementioned, the AI Act requires effective human oversight in a continuous feedback loop in all 4 stages of AI systems' lifecycle: design, development, use/testing and evaluation, especially so in autonomous systems. Policing strategies stress transparency, fairness, proportionality and public confidence. Critical to effect human oversight is human-interpretable reporting, performance monitoring and decision making explanations. However, research on explainability underlines limits of XAI (eXplainable AI) as a trust fix and the need to define usable, role-appropriate explanations.

Relevant R&D implications:

- Design, monitor and explain for operator awareness: alerts with actionable rationales, provide confidence and/or uncertainty information
- Human control in autonomous and non-autonomous systems: ensure error awareness alerts, error handling mechanisms and human override mechanisms by design

Key References

- Pavlidis, G. (2024). Unlocking the black box: analysing the EU artificial intelligence act's framework for explainability in AI. Law, *Innovation and Technology*, 16(1), 293-308. https://doi.org/10.1080/17579961.2024.2313795
- NPCC (2025) Artificial Intelligence (AI) Strategy. *National Police Chiefs Council.* https://www.npcc.police.uk/SysSiteAssets/media/downloads/publications/publications-log/science-and-innovation/2025/npcc-ai-strategy.pdf
- NPCC (2024) Covenant for Using Artificial Intelligence (AI) in Policing. https://science.police.uk/delivery/resources/covenant-for-using-artificial-intelligence-ai-in-policing/
- Stoykova, R., Porter, K., & Beka, T. (2024). The AI Act in a law enforcement context: The case of automatic speech recognition for transcribing investigative interviews. *Forensic Science International: Synergy*, 9, 100563. https://doi.org/10.1016/j.fsisyn.2024.100563
- Sachoulidou, A. (2024). Harnessing AI for law enforcement: Solutions and boundaries from the forthcoming AI Act. *New Journal of European Criminal Law*, 15(2), 117-125. https://doi.org/10.1177/20322844241260114
- Project Sherpa (2019) Guidelines for the Ethical Use of AI and Big Data Systems. https://www.project-sherpa.eu/wp-content/uploads/2019/12/use-final.pdf

Tool and projects view

Below is a non-exhaustive list of prominent, currently available, tools that can be used to assess the compliance of AI models and/or AI systems with the AI act:

- **EU AI Act Compliance Checker** (European Commission): An interactive questionnaire to assess and examine basic obligations that a model or system provider may have according to the AI Act [16].

- **AI Act Conformity Tool** (DIGITAL SME & EIT Digital): A basic questionnaire that guides providers/assessers of an AI system through the risk classification and returns a report with next steps [17].

- **EU AI Act Compliance Matrix** (IAPP): A comprehensive matrix that aids providers, deployers, product manufacturers, authorized representatives, importers and distributors of AI models/systems to navigate and map their obligations over each article of the AI act, offering a **full** and a **summarised** view of the respecitive correspondences between the Act's articles and the roles of the AI stakeholders [18].

- **AP4AI: CC4AI** (Europol Innovation Lab & CENTRIC): A web-based tool to support internal security practitioners to assess compliance of their AI systems with the requirements of the AI Act. Access is restricted, but offered freely to internal security agencies [19].

- **Compl-AI** (ETH): A technical assessment tool, to assess compliance of Generative AI models to the AI act against qualified benchmarks, under the 6 basic axes of the act. Assessment can be done locally, with the tool generating a comprehensive report [20].

Moreover, while a plurality of EU projects have provided – and continue to provide – methods, tools and assessments on own technologies and offer observations and insights on AI systems' ethical, societal, legal and technical assessment, it is valuable to mention an indicative selection which has contributed influential analyses, recommendations and frameworks relevant to the readiness and compliance of AI models/systems to ethical AI design and use (initially) and the AI Act in particular (subsequently).

[16] https://ai-act-service-desk.ec.europa.eu/en/eu-ai-act-compliance-checker
[17] https://www.digitalsme.eu/ai-act-conformity-tool/
[18] https://iapp.org/resources/article/eu-ai-act-compliance-matrix/
[19] https://www.ap4ai.eu/cc4ai-tool
[20] https://compl-ai.org/

Early research setters:

- **SHERPA** (H2020, GID: 786641): Although not an FCT/security project and completed long before the adoption of the AI Act, SHERPA conducted an extensive analysis of the ethical and human rights dimensions of Smart Information Systems (SIS), issuing a series of **recommendations** on AI Impact Assessment, Ethics by design, Standardization, Security, Regulatory framework, European agency for AI, among others, that are still prevalent, relevant and influential and can constitute best practices in all AI systems, including LE-relevant, high risk systems [21].

- **SIENNA** (H2020, GID: 741716): A non FCT-project that pivoted around the ethics, societal impact and impact on human rights of new technologies, including AI, offers a plurality of analyses, public views, surveys, recommendations, a general methodology for ethical AI, among others, for all domains of application of AI systems, including high-risks systems such as the biomedical and security domains [22].

- **DARLENE** (H2020, GID: 883297): DARLENE explored Augmented Reality technologies for the LE ecosystem. The project's meticulous and comprehensive impact assessment on data protection in Law Enforcement and deep analysis on best practices to address the legal and ethical implications of AI tech for the security sector are still flagship domain setters on the intersection of AI and Law Enforcement [23].

Noteworthy relevant work in recent projects:

- **LAGO** (HEU, GID: 101073951): With a goal to lessen obstacles in data access and governance issues of AI systems in the FCT domain, LAGO offers substantial analysis in barriers and solutions on data sharing in the FCT landscape, including identification or relevant challenges and recommendations, as well as a risk assessment and legal compliance framework for supporting personal data sharing with privacy preservation for scientific research [24].

- **STARLIGHT** (H2020, GID: 101021797): A major effort to empower LEAs with strategic autonomy in the use of AI models/systems, includes extensive work and analysis on the European institutional response to ethical and regulatory challenges of artificial intelligence in addressing discriminatory bias, a cybersecurity risk analysis framework for systems with AI components, as well as several technical solutions for AI components regarding trustworthiness in decentralised systems, bias detection and mitigation, person de-identification and anonymisation, among other [25].

- **EMPOWER** (DIGITAL, GID: 101102724): Dealing with AI-powered investigative tools for LEAs, EMPOWER has issued an extensive AI ethics framework analysis and published a code of ethics for both LEAs and AI developers/providers, to guide future deployment of AI models/systems in Law Enforcement [26].

A more conclusive listing and analysis on assessment tools, projects and relevant frameworks is planned for subsequent analytical report on this thematic.

[21] https://www.project-sherpa.eu/
[22] https://www.sienna-project.eu/w/si/
[23] https://www.darleneproject.eu/
[24] https://lago-europe.eu/
[25] https://www.starlight-h2020.eu/
[26] https://transgero.eu/empower/

MARKET & STANDARDS OBSERVATORY

Summary of market view

AI adoption in FCT security and law enforcement is growing. It focuses on:

- AI-enabled surveillance, forensic intelligence and cybercrime detection.
- Use cases include illicit trade monitoring (ANITA) [, environmental crime detection (PERIVALLON) [28], and predictive policing.

Procurement evolution:

- European Commission's "Model Contractual Clauses for High-Risk AI" point to a maturing procurement framework [29].
  - Public authorities will have a common legal template when buying or deploying AI systems deemed "high-risk" under the AI Act.
  - Clearer obligations for suppliers

Downside of AI:

- A trend we see is the use of AI by criminals. AI is being employed to create realistic synthetic media (deepfakes), automate phishing campaigns, generate illicit content, and scale cyberattacks

Standardisation gap:

- A scan of ISO and CEN-CENELEC standards shows no dedicated standards yet for AI in FCT contexts.
- This highlights a disconnect between active research projects and the absence of harmonised technical standards.
- This opens a gap for future projects to focus on.

Market size

Current observations highlight the expansion of AI in security and surveillance markets:

- "La IA protagonizara la video vigilancia en 2025" [30] translates to AI will dominate video surveillance in 2025. Showing the rapid growth in AI-powered surveillance systems.
- Procurement as a Service and ProcurementIQ [31] indicate a rising spending on AI-driven procurement tools.

Data Gap:

- No quantified figures for total market size or CAGR in the FCT-AI segment.
- Further research needed via Eurostat or market analytics report.
- Market analysis can be challenging due to limited data transparency from AI providers.

[27] https://www.anita-project.eu/
[28] https://perivallon-he.eu/
[29] European Commission (2025) Procurement of AI: Updated EU AI model contractual clauses. https://public-buyers-community.ec.europa.eu/communities/procurement-ai/resources/updated-eu-ai-model-contractual-clauses
[30] Digital Security Magazine (2025) La IA protagonizará la videovigilancia en 2025, según Hanwha Vision. https://www.digitalsecuritymagazine.com/2025/01/15/ia-protagonizara-videovigilancia-2025-segun-hanwha-vision/
[31] https://www.procurementiq.com/

Investment in Relevant R&I

Indirect indicators like investment levels, compute resources, and model popularity are currently used to estimate AI market growth and competition

EU funded projects demonstrate active research streams:

- ANITA (AI for illicit trade monitoring).
- PERIVALLON (AI for environmental crime).
- AHEAD [32], POLIIICE [33], NIGHTINGALE [34], and STARLIGHT demonstrate investment in innovative research addressing real operational needs—from criminal communications interception to mass casualty management and crowd behaviour detection.
- DG Home Civil Resilience Report notes AI as a strategic R&I area in policing and forensics [35].

Standards gap

- Despite strong R&I activity, the ISO/CEN-CENELEC scan confirms no standardised AI frameworks for FCT, suggesting research is ahead of regulation.

Review of relevant funding opportunities

- H2020 and Horizon Europe (HE) on AI within FCT remain active
- Upcoming HE and DG HOME calls have a large focus on AI in security and law enforcement
- The ability of several companies to reach or approach the AI Economic frontier with significantly less funding suggests that current competitive advantage in model development extends beyond economies of scale and scope [36].

Review of relevant tender opportunities

National and EU tenders:

- Scientific Police Platform Tender (EL RADAR [37]) seeks a comprehensive forensic intelligence platform.
- National Police tenders include AI-driven forensic software and surveillance procurement.

Regulatory framework:

- Model Contractual Clauses for High-Risk AI likely to shape future AI tenders.

[32] https://he-ahead-project.eu/
[33] https://poliiice-project.eu/
[34] https://www.nightingale-triage.eu/
[35] European Commission: Directorate-General for Migration and Home Affairs (2024) Building resilience in the civil security domain based on research and technology: report of the CERIS Expert Group, November 2024. Publications Office of the European Union. https://data.europa.eu/doi/10.2837/06076.
[36] OECD (2025) Developments in Artificial Intelligence markets. *OECD Artificial Intelligence Papers.* https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/06/developments-in-artificial-intelligence-markets-new-indicators-based-on-model-characteristics-prices-and-providers_75e50b2a/9302bf46-en.pdf
[37] https://www.elradar.es/

ETHICAL, LEGAL & SOCIETAL OBSERVATORY

Summary of ELS view

In the observations collected, discussions around the AI Act represent most of the content. **Biometric methods, technologies and tools, anonymisation, trust** and **data security and privacy** are continuously part of this debate. Among functions, "**Data, information & intelligence gathering management, and exploitation**", and "**Security of information systems, networks and hardware**" are the most common classifications used.

Members of the law enforcement and FCT community are working on research and development of best practices and guidelines for specific use cases involving the use of AI. These should be considered alongside applicable legal framework.

Critical ethical and societal issues

AI and research

A relevant topic part of the discussion around AI use is the limits of possibilities of AI in research. While not a lot of observations go around this specific topic, certain projects and research results provide interesting insights for use of AI in research projects involving LEAs.

Key References

- DG Home (2024) Research projects help combat disinformation ahead of elections. https://home-affairs.ec.europa.eu/news/research-projects-help-combat-disinformation-ahead-elections-2024-05-30_en
- Darlene (2023) Responsible Research Brief. https://www.darleneproject.eu/wp-content/uploads/2023/12/DARLENE-Brief-1.pdf
- Project Sherpa (n.d.) Recommendation: Promote Ethics by Design for researchers in EC-funded projects. https://www.project-sherpa.eu/ethics-by-design/
- Aucouturier , E. & Grimbaum, A. (2023) D2.2: Recommendations to address ethical challenges from research in new technologies. *improving Research Ethics Expertise and Competences to Ensure Reliability and Trust in Science (IRECS).* https://irp.cdn-website.com/5f961f00/files/uploaded/Deliverable_2.2.pdf
- Hovy, D (2023) What does the EU AI Act mean for Research? *Institute for European Policing Making @ Bocconi University.* https://iep.unibocconi.eu/publications/what-does-eu-ai-act-mean-research
- DG REA (2025) Commission seeks feedback on the future Strategy for Artificial Intelligence in Science. https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/commission-seeks-feedback-future-strategy-artificial-intelligence-science-2025-04-10_en

Law enforcement and AI

As mentioned in the introductory parts of this report, several law enforcement AI uses are classified as unacceptable or high risk under the AI Act, which imposes prohibitions to the former and heavy obligations to the latter. Interesting to notice that while broader discussions around the AI Act focus on GPAI models, the narrow discussion on law enforcement and AI went beyond on other high-risk and prohibited uses. Facial recognition and border control still are main topics in the debate surrounding AI use by LEAs.

Key References

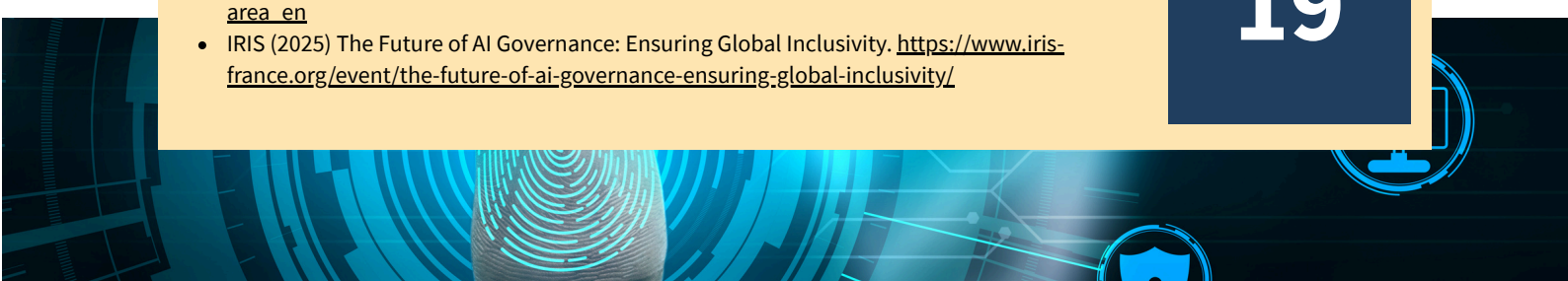
- Europol (2023) ChatGPT - The impact of Large Language Models on Law Enforcement, a Tech Watch Flash Report from the Europol Innovation Lab, Publications Office of the European Union, Luxembourg. https://www.europol.europa.eu/publications-events/publications/chatgpt-impact-of-large-language-models-law-enforcement
- Sachoulidou, A. (2024). Harnessing AI for law enforcement: Solutions and boundaries from the forthcoming AI Act. *New Journal of European Criminal Law,* 15(2), 117-125. https://doi.org/10.1177/20322844241260114
- Miniadou, K., Leonidis, A., Papadopoulos, G. T., & Stephanidis, C. (2024, May). Enhancing secure cross-border collaboration among law enforcement agencies for facial biometric search. In *2024 5th International Conference in Electronic Engineering, Information Technology & Education* (EEITE) (pp. 1-6). IEEE. https://doi.org/10.1109/EEITE61750.2024.10654447
- Papakonstantinou, V. & Zarkadoulas, E. (2023) Remote Biometric Identification and Emotion Recognition in the Context of Law Enforcement. *Eurocrim.* https://doi.org/10.30709/eucrim-2023-021
- Simmler, M., & Canova, G. (2025). Facial recognition technology in law enforcement: Regulating data analysis of another kind. *Computer Law & Security Review*, 56, 106092. https://doi.org/10.1016/j.clsr.2024.106092
- WeProtect Global Alliance (2023) Global Threat Assessment 2023. https://www.weprotect.org/wp-content/uploads/Global-Threat-Assessment-2023-English.pdf
- Stoykova, R., Porter, K., & Beka, T. (2024). The AI Act in a law enforcement context: The case of automatic speech recognition for transcribing investigative interviews. Forensic Science International: Synergy, 9, 100563. https://doi.org/10.1016/j.fsisyn.2024.100563
- Bertuzzi, L. (2024) AI Act: MEPs mull narrow facial recognition technology uses in exchange for other bans. *Euractiv.* https://www.euractiv.com/news/ai-act-meps-mull-narrow-facial-recognition-technology-uses-in-exchange-for-other-bans/

Soft law and best practices

Soft law and best practices occupy a central role in the discussion of AI Regulation. Allowing for more specific considerations, these instruments may add to the protection of fundamental values and rights and should be applied alongside legal instruments, such as the AI Act. Even though certain observations are prior to the adoption of the AI Act, discussions around AI regulation were already in course.

Key References

- Erdogan, I. (2024). Diving into the Iceberg: Establishing Transparency in AI for Law Enforcement. European Papers-A Journal on Law and Integration, 2024(3), 956-977. https://www.europeanpapers.eu/system/files/pdf_version/EP_eJ_2024_3_SS1_3_Irmak_Erdogan_00794.pdf
- Europol (2025), AI bias in law enforcement - A practical guide, Europol Innovation Lab observatory report, Publications Office of the European Union, Luxembourg. https://www.europol.europa.eu/publications-events/publications/ai-bias-in-law-enforcement
- EDRI (2024) How to fight Biometric Mass Surveillance after the AI Act: A legal and practical guide. https://edri.org/our-work/how-to-fight-biometric-mass-surveillance-after-the-ai-act-a-legal-and-practical-guide/
- EDPB (2023) Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. *European Data Protection Supervisor.* https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052022-use-facial-recognition-technology-area_en
- IRIS (2025) The Future of AI Governance: Ensuring Global Inclusivity. https://www.iris-france.org/event/the-future-of-ai-governance-ensuring-global-inclusivity/



ENACT.

European Network Against Crime and Terrorism

@enact-network

enact-eu.net

Scan the QR code to visit ENACT online and read this report in digital format.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.