

AI-ASSISTED DECISION-MAKING IN PUBLIC SECURITY

Opportunities, Vulnerabilities and Professional Training Requirements

Colonel (ret) Professor George-Marius ȚICAL, Ph.D*
(Academy of Romanian Scientists, 3 Ilfov, 050044, Bucharest, Romania,
email: secretariat@aosr.ro)

Abstract: *The integration of artificial intelligence into public security is changing the relationship between data, analysis and professional decision-making. Algorithmic systems can process large volumes of information, identify patterns that are difficult to observe and support risk assessment or resource allocation. However, the same capabilities can produce effects contrary to legality and effectiveness when data are incomplete, models are opaque, results are affected by bias or users place excessive trust in technological recommendations. This article analyses the opportunities and vulnerabilities of AI-assisted decision-making in public security with reference to Regulation (EU) 2024/1689, Europol and FRA documents, and UNICRI–INTERPOL instruments. It argues that human oversight becomes effective only when the operator has the competence, authority and time required to verify and, where appropriate, reject the algorithmic output. As an original contribution, the article proposes the C.O.N.T.R.O.L. professional training model, focused on understanding the system, verifying data provenance, applying the relevant rules, testing the output, assuming responsibility, observing effects and drawing on lessons learned.*

Keywords: *artificial intelligence; public security; assisted decision-making; human oversight; algorithmic bias; professional training.*

DOI **10.56082/annalsarscimit.2026.3.72**

1. Introduction

The digitalisation of public order and safety activities no longer means merely computerising records or rapidly transmitting data. The development of artificial intelligence systems makes it possible to move from tools that describe the existing situation to tools that classify, estimate probabilities, identify links and formulate recommendations. In this context, the decision-maker interacts not only with raw information, but also with algorithmically processed outputs, often presented as a risk score, an alert, a prioritisation or a course of action.

Public security is a field in which the promise of technology is particularly attractive. Institutions must respond rapidly, manage limited

* “Andrei Șaguna” University, Associated Member of the Academy of Romanian Scientists, Entitled Member of The Academy of National Security Sciences, email: ticalgeorgem@gmail.com

resources, correlate heterogeneous sources and make decisions under uncertainty. Artificial intelligence can substantially enhance organisations' analytical capacity. Nevertheless, decisions in this field may affect liberty, privacy, equality, the presumption of innocence and access to an effective means of challenge. For this reason, effectiveness cannot be the sole assessment criterion.

The issue cannot be reduced to a simple opposition between human and machine. In practice, most relevant applications are sociotechnical systems: data are collected by individuals and institutions, the model is designed according to defined objectives, the output is interpreted within an organisational context, and the consequences are borne by individuals and communities. An error may originate in the data, the model's design, the way the output is presented or the user's conduct. Responsibility must therefore be examined throughout the system's entire life cycle.

The research question is: under what conditions can artificial intelligence support decision-making in public security without undermining legality, impartiality, accountability and fundamental rights? The article seeks to identify the principal opportunities and vulnerabilities, clarify the meaning of effective human oversight and formulate requirements for the initial and continuing training of personnel.

2. Conceptual and Methodological Framework

2.1. From Human Decision-Making to Assisted Decision-Making

AI-assisted decision-making must be distinguished both from exclusively human decision-making and from fully automated decision-making. In the first case, the algorithm plays no part in the reasoning. In the second, the system's output produces consequences without meaningful human intervention. Assisted decision-making lies between these extremes: the system formulates a prediction, classification or recommendation, while the competent person evaluates the output against the other information and assumes responsibility for the decision.

This distinction is normative, not merely technical. The formal presence of a person in the workflow does not establish the existence of human control. If the operator does not understand the system, lacks access to the information needed for verification, is constrained by time or lacks the authority to reject the recommendation, the intervention becomes a mere confirmation. In such a situation, the decision is effectively automated, even if a person's signature appears on the document. "Human judgment should be used when setting metrics for specific trustworthy AI characteristics."¹

¹ National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework* (AI RMF 1.0), NIST AI 100-1 (Gaithersburg, MD: NIST, 2023), p. 12.

The NIST standard thus supports a substantive, rather than merely formal, understanding of the operator's intervention.

2.2. Research Methodology

The research uses legal and institutional analysis, supplemented by scenario methodology and risk analysis. The principal legal framework is Regulation (EU) 2024/1689 on artificial intelligence. It is examined in conjunction with the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, the UNESCO Recommendation on the Ethics of Artificial Intelligence, and the NIST AI Risk Management Framework.

The operational dimension is grounded in Europol reports on artificial intelligence in policing, algorithmic bias and technology assessment in law enforcement. Reports issued by the European Union Agency for Fundamental Rights are used for the fundamental-rights dimension. Training requirements are considered against the UNICRI–INTERPOL Toolkit for Responsible AI Innovation in Law Enforcement.

The analysis does not assess a specific operational application and does not use classified data or information from actual cases. Its conclusions are conceptual and normative and seek to construct a framework applicable to professional training and institutional assessment.

3. Applications and Opportunities in Public Security

3.1. Data Analysis and Pattern Identification

One of the major advantages of AI is its capacity to analyse volumes of data that personnel could not examine in full within a useful timeframe. Systems can correlate persons, locations, times, objects, transactions and *modi operandi*, flagging relationships that require further verification. Europol shows that these capabilities can support intelligence analysis, digital investigations, fraud detection, image recognition and the management of digital evidence. “Facial recognition technology (FRT) makes it possible to compare digital facial images in order to determine whether they belong to the same person.”²³

The probabilistic nature of the match nevertheless requires confirmation through independent information.

Operational value does not lie in turning correlation into certainty, but in directing the analyst's attention. A useful system narrows the search space and proposes verifiable hypotheses. It becomes dangerous when

² Europol, *AI Bias in Law Enforcement: A Practical Guide* (Luxembourg: Publications Office of the European Union, 2025), p. 8.

³ European Union Agency for Fundamental Rights, *Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement* (Luxembourg: Publications Office of the European Union, 2019), p. 1.

correlation is treated as evidence or when a probability score is converted into a presumption concerning a person.

3.2. Risk Assessment and Resource Allocation

Analytical tools can support patrol planning, the identification of high-incidence periods, risk analysis at public events and resource allocation. In emergency management, AI can combine meteorological data, geographical information, traffic flows and field reports. The advantage lies in the capacity to update the operational picture rapidly.

A prediction concerning a place or phenomenon must, however, be distinguished from an assessment of individual risk. Area-based data may reflect not only the actual distribution of crime, but also the historical intensity of police checks. Repeatedly directing resources to the same places generates new recorded incidents, which subsequently reinforce the initial prediction. This creates a feedback loop that may confuse the level of policing activity with the actual level of the phenomenon.

3.3. Reducing Repetitive Tasks

AI can be used for transcription, semantic search, document classification, preliminary translation, anonymisation or the organisation of materials. The time saved may allow personnel to focus on activities that require professional judgment, empathy and human interaction. This benefit is real only if generated outputs are verified and automation neither introduces non-existent information nor alters the meaning of documents. “Additionally, AI systems can automate the analysis of digital evidence, enabling investigators to quickly identify relevant clues from emails, online conversations, and forensic databases.” (“Additionally, AI systems can automate the analysis of digital evidence, enabling investigators to quickly identify relevant clues from emails, online conversations, and forensic databases.”)⁴

3.4. Training and Scenario Simulation

In professional training, generative systems can construct dynamic scenarios, adapt difficulty to the trainee's level and simulate the evolution of operational situations. Their use can develop the capacity to anticipate, compare alternatives and provide reasons for a decision. In this context, AI is valuable not because it provides the “correct” answer, but because it enables a wider range of learning situations and an examination of the consequences of different choices.

⁴ Țical G.M., “*Artificial Intelligence and Big Data Analysis in Crime Prevention and Combat*”, *Annals Series on Military Sciences* 17, no. 1 (2025), p. 48, <https://doi.org/10.56082/annalsarscimilit.2025.1.36>.

Opportunity	Associated vulnerability	Professional competence
Rapid data analysis	False correlations or unrepresentative data	Verification of data source, quality and relevance
Risk assessment	Turning probability into certainty	Probabilistic reasoning and testing alternative hypotheses
Image recognition	False-positive identifications and differences in accuracy	Independent confirmation and understanding error rates
Document automation	Fabricated information, omissions or loss of traceability	Editorial control, source citation and responsibility for content
Resource allocation	Feedback loops and over-policing of certain communities	Impact assessment, proportionality and continuous monitoring

Table 1. Relationship Between Opportunity, Vulnerability and Required Competence

Source: author's own elaboration based on Europol (2024, 2025), FRA (2022) and UNICRI-INTERPOL (2024)

4. Vulnerabilities and Effects on Decision-Making

4.1. Data Quality

An artificial intelligence system cannot transcend the limitations of the information on which it was built and the data supplied during use. Information may be incomplete, outdated, incorrectly labelled or unrepresentative. FRA emphasises that poor-quality data may produce outputs that affect the right to non-discrimination and other fundamental rights. In public security, this vulnerability is amplified by the heterogeneous nature of the sources and by time pressure.⁵

Historical data are not a neutral snapshot of reality. They reflect institutional priorities, reporting practices and the distribution of checks. A database of interventions shows where agencies intervened, not necessarily where all offences occurred. If this distinction is not understood, the algorithm may legitimise earlier practices and project them into the future.

4.2. Algorithmic Bias and Discrimination

Bias can arise at every stage of the life cycle: problem formulation, data selection, definition of the intended outcome, training, validation, deployment and interpretation. The Europol guide shows that historical and representational biases may lead to unfair outcomes, while improper use and excessive reliance on an output can turn a technical problem into a harmful

⁵ European Union Agency for Fundamental Rights, *Bias in Algorithms: Artificial Intelligence and Discrimination* (Luxembourg: Publications Office of the European Union, 2022), pp. 12–15.

operational action. “AI bias can occur at any stage of the system life cycle”⁶⁷

Verification therefore cannot be confined to the time of procurement or initial validation.

Fairness cannot be reduced to removing sensitive characteristics from the model. Other variables may act as proxies for ethnic origin, social status or place of residence. Assessment must therefore examine the system's effects on different groups and be repeated after deployment. “Biases in algorithmic systems can lead to discrimination”⁸

The FRA formulation warrants a legal examination of effects, distinct from the mere technical measurement of error.

4.3. Opacity and the Problem of Explainability

When presented with a score or recommendation, the user must be able to understand at least the system's purpose, the relevant data, its known limitations and the meaning of the output. Explainability does not necessarily require every user to have access to the source code; it requires the provision of the information needed for prudent use and for giving reasons for the decision. An output that cannot be explained is difficult to verify, challenge and defend in legal terms.

4.4. Automation Bias

Automation bias refers to a person's tendency to accept the system's recommendation and disregard contradictory information. The risk is high when technology is presented as objective, when the interface uses precise scores or when the organisation rewards conformity with the recommendation. Under such conditions, the expression “assisted decision-making” may conceal the effective transfer of reasoning to the system.

This phenomenon cannot be prevented by the generic statement that “the final decision belongs to the human”. The user must know the tool's limitations, receive information about uncertainty, be able to consult the sources and be encouraged to formulate alternative hypotheses. Reasoned disagreement with the system should be treated as an expression of competence, not as a departure from the technological workflow.

4.5. Cybersecurity and Technological Dependence

AI systems may be compromised through data manipulation, adversarial attacks, unauthorised access, supply-chain compromise or model alteration. In public security, the consequences may include misdirecting

⁶ Europol, *AI Bias in Law Enforcement: A Practical Guide* (Luxembourg: Publications Office of the European Union, 2025), pp. 9–11.

⁷ Europol, *AI Bias in Law Enforcement*, p. 9.

⁸ European Union Agency for Fundamental Rights, *Bias in Algorithms*, p. 23.

resources, disclosing sensitive information and compromising investigations. Assessment must cover robustness, operational continuity, the traceability of changes and the possibility of reverting to alternative procedures.

Dependence on the provider raises distinct issues: access to documentation, updates, data location, auditing and termination of the contract. An institution cannot outsource responsibility for the legality of a decision merely because the tool belongs to a private company.

5. The European Legal Framework and the Requirement of Human Control

5.1. The Risk-Based Approach

Regulation (EU) 2024/1689 establishes a differentiated approach according to risk: certain practices are prohibited, high-risk systems are subject to extensive requirements, and other systems fall under transparency obligations. In the field of law enforcement, Annex III includes uses that may have significant consequences for individuals, while Article 5 sets limits on certain forms of individual prediction and biometric identification. “AI should be a human-centric technology. It should serve as a tool for people”⁹

For high-risk systems, risk management, data governance, technical documentation, record-keeping, transparency, human oversight, accuracy, robustness and cybersecurity are relevant. These obligations indicate that the technical output cannot be separated from the organisational context in which it is used.

5.2. Effective Human Oversight

Article 14 of the AI Regulation requires high-risk systems to be designed and used in such a way that they can be effectively overseen by natural persons. The overseer must understand the system's capabilities and limitations, identify anomalies, avoid automatic reliance and be able to disregard, override or reverse the output. This obligation is complemented by the requirements applicable to institutional deployers and by the fundamental-rights impact assessment.

Effective human control can be analysed through three cumulative conditions. The first is competence: the person must understand how the system is used and the risks involved. The second is authority: the person must be able to reject the output without unjustified organisational consequences. The third is genuine opportunity: the person must have the time, data and tools needed for verification. The absence of any of these conditions turns oversight into a formal ritual.

⁹ European Parliament and Council of the European Union, *Regulation (EU) 2024/1689*, recital 6, Official Journal of the European Union L 2024/1689 (July 12, 2024), p. 2.

5.3. Accountability and the Possibility of Challenge

The use of an algorithmic recommendation does not transfer legal responsibility from the institution or the competent decision-maker to the system. The decision must be reasoned on the basis of elements that can be communicated and verified. The affected person must be able to understand the significant role of the system and challenge the output, within the limits established by law and consistently with the protection of operational methods.

The Council of Europe Framework Convention reinforces this perspective through the principles of dignity, individual autonomy, transparency, oversight, accountability and non-discrimination. The UNESCO Recommendation adds the need for public and professional literacy, as well as ethical impact assessment throughout the life cycle. “...there should be adequate transparency and oversight requirements tailored to the specific contexts and risks”¹⁰¹¹¹²

The standard rules out the uniform application of purely declaratory safeguards.

6. Professional Training Requirements

6.1. AI Literacy

Article 4 of the AI Regulation makes artificial intelligence literacy an organisational obligation. In public security institutions, training cannot be limited to a general presentation of the technology or to reading instructions for use. Its level must be adapted to the role, the type of system, the risk and the possible consequences for individuals.

Minimum technical competence includes understanding the difference between probability and certainty, the role of training data, model limitations, error rates, and false-positive or false-negative outputs. The operator need not become a programmer, but must be able to interpret the output correctly and know which questions to ask. All of this “...requires certain processes, an enabling culture, and the right people and expertise to harness its potential effectively”.¹³

Individual training must therefore be supported by organisational preparedness.

¹⁰ UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (Paris: UNESCO, 2021), p. 17.

¹¹ Council of Europe, *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*, CETS No. 225 (Strasbourg, 2024), pp. 4–5.

¹² Council of Europe, Framework Convention, art. 8, p. 4.

¹³ UNICRI and INTERPOL, *Toolkit for Responsible AI Innovation in Law Enforcement: Organizational Readiness Assessment Questionnaire* (Turin/Lyon, 2024), p. 4.

6.2. Legal and Ethical Competences

Training must cover data protection, non-discrimination, the conditions for using high-risk systems, the statement of reasons for a decision, traceability and accountability. The ethical dimension concerns dignity, proportionality, the avoidance of stigmatisation and the preservation of professional autonomy. This knowledge must be applied in scenarios, not presented exclusively in theoretical terms.

6.3. Critical Thinking and Probabilistic Reasoning

A competent user asks questions about the output: what data were used, how current they are, what information is missing, what the error rate is, whether alternative explanations exist and whether the decision can be reasoned without merely invoking the score. Training must develop the ability to disagree with the system on the basis of verifiable arguments.

6.4. Scenario-Based Training and Competence Assessment

Scenarios may include correct recommendations, erroneous recommendations and ambiguous situations. The trainee is required to identify the necessary information, verify the output and give reasons for accepting or rejecting it. Assessment must measure not only speed or agreement with the recommendation, but also the quality of reasoning, the identification of uncertainty and respect for rights.

The 2026 INTERPOL training catalogue includes the T.R.A.I.L. programme – Training on Responsible AI Innovation in Law Enforcement – confirming that the responsible use of AI has become a distinct field of professional training. The UNICRI–INTERPOL Toolkit recommends developing competences, organisational culture and assessment procedures before systems are introduced into routine activities. It also lists “Training on Responsible AI Innovation in Law Enforcement – T.R.A.I.L. (EN) – one week”¹⁴¹⁵¹⁶

7. The C.O.N.T.R.O.L. Model – A Proposal for Professional Training

To translate the principles into an easy-to-use instrument, the C.O.N.T.R.O.L. model is proposed. It can serve as the structure of a training module, a pre-decision analytical framework or a tool for assessing a situation in which an algorithmic recommendation plays a significant role.

¹⁴ UNICRI and INTERPOL, *Organizational Readiness Assessment Questionnaire*, pp. 4–17.

¹⁵ INTERPOL, *INTERPOL I-Learn Catalogue* (May 2026), p. 14, available at <https://www.interpol.int/content/download/24489/file/INTERPOL%20I-Learn%20Catalogue%20May%202026.pdf>, accessed on September 15, 2026.

¹⁶ *Ibidem*, p. 14.

Element	Content	Control question
C – Comprehension of the system	Purpose, operation, limitations and intended use.	What can and cannot this system do?
O – Origin of the data	Source, currency, quality and representativeness of the data.	What information is the output based on?
N – Norms applicable	Legality, necessity, proportionality and fundamental rights.	Is the use permitted and justified in the specific situation?
T – Testing the output	Comparison with other sources and formulation of alternative hypotheses.	What elements confirm or refute the recommendation?
R – Responsibility of the human	Reasoning and assumption of the decision by the competent person.	Can I explain and defend this decision without invoking the authority of the algorithm?
O – Observation of effects	Monitoring errors, incidents and differentiated effects.	What consequences has use of the system produced?
L – Lessons learned	Reporting, reviewing procedures and updating training.	What must be changed for future uses?

Table 2. The C.O.N.T.R.O.L. Model

Source: author's own elaboration

The model does not replace institutional procedures or legal assessment. Its role is to create a cognitive routine through which the user avoids automatically accepting a recommendation. Its application must be adapted to the type of system and the level of risk. In situations with significant effects on individuals, the answers must be documented proportionately.

8. Empirical Research Proposal

To test the hypothesis concerning automation bias, a small-scale experiment may be conducted with students or trainees from public-order educational institutions. Participants are assigned to two groups and receive the same hypothetical situation. The control group analyses the data without an algorithmic recommendation, while the experimental group additionally receives a recommendation presented as having been generated by an AI system.

The recommendation must contain a detectable error or an insufficiently substantiated conclusion, without misleading participants about real risks. The acceptance rate, the amount of information verified, identification of the error, quality of reasoning, decision time and declared level of confidence may be measured. After the exercise, its purpose must be explained and the mechanism of automation bias discussed.

In a second stage, participants complete a training module based on the C.O.N.T.R.O.L. model and then solve a comparable situation. The difference between the two stages may indicate whether training reduces uncritical acceptance and improves the statement of reasons. The results should not be interpreted as an assessment of general professional aptitude, but as an indicator of a cognitive vulnerability specific to human–algorithm interaction.

9. Discussion

Introducing AI into public security is not merely a technological project, but an institutional change. A high-performing system used in an organisation without procedures, competences and mechanisms of challenge may produce poorer results than a transparent traditional method. Assessment must include fitness for purpose, the impact on rights, data quality, staff capacity and the possibility of monitoring. “While AI brings undeniable benefits to security, its use must be accompanied by strict measures to protect citizens' rights and prevent abuses.” (“While AI brings undeniable benefits to security, its use must be accompanied by strict measures to protect citizens' rights and prevent abuses.”)¹⁷

There is a risk that the requirement of human control will be used to legitimise systems without changing actual working conditions. If a person must validate hundreds of alerts, if the explanation is inaccessible or if departure from a recommendation must be justified disproportionately, control is not effective. Institutions must assess not only the technical interface, but also workload, incentives and the distribution of authority.

Professional training must be coordinated with procurement and governance. Staff vigilance cannot compensate for a system that is unfit for purpose or built on unsuitable data. Conversely, even the best system cannot eliminate the need for contextual reasoning. Responsibility is distributed across the process, but must not be diluted: providers are responsible for their obligations, management for the decision to adopt the system and organise control, and the user for the specific manner in which the output is integrated into the decision.

In public-order education, AI must be used both as an object of study and as a learning tool. Trainees must understand the technology they will encounter in professional practice and must also practise its responsible use. The aim is not to cultivate obedience to the system, but to develop the capacity for critical human–AI collaboration.

¹⁷ Tical GM, “*Artificial Intelligence and Big Data Analysis in Crime Prevention and Combat*”, p. 50.

10. Conclusions

Artificial intelligence can improve analysis, response speed and the use of resources in public security. It can identify patterns, organise information and generate scenarios that a decision-maker could not produce with the same speed. These benefits do not, however, turn an algorithmic output into truth or justify replacing professional judgment.

Vulnerabilities arise from data quality, bias, opacity, attacks, dependence on the provider and, above all, the way in which people interpret the output. Automation bias demonstrates that the formal presence of a human does not guarantee control. Oversight is effective only when the person has the competence, authority and genuine opportunity to verify the output.

Professional training must integrate technical, legal, ethical, operational and critical-thinking competences. The C.O.N.T.R.O.L. model offers a structure applicable to training and practice, directing the user towards understanding the system, verifying the data, applying the rules, testing the output, assuming responsibility, observing effects and drawing on lessons learned.

In public security, an artificial intelligence system is useful not when it decides in place of the professional, but when it helps the professional make a better-informed decision without diminishing judgment, independence or responsibility.



BIBLIOGRAPHY

- COUNCIL OF EUROPE. *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*. CETS No. 225. Strasbourg, 2024, available at <https://rm.coe.int/1680afae3c>;
- EUROPEAN DATA PROTECTION SUPERVISOR. *TechDispatch: Human Oversight of Automated Decision-Making*. Brussels, 2025, available at https://www.edps.europa.eu/system/files/2025-09/25-09-15_techdispatch-human-oversight_en.pdf;
- EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. *Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement*. Luxembourg: Publications Office of the European Union, 2019, available at https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf;
- EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. *Getting the Future Right: Artificial Intelligence and Fundamental Rights*. Luxembourg: Publications Office of the European Union, 2020,

- available at https://fra.europa.eu/sites/default/files/fra_uploads/-fra-2020-artificial-intelligence_en.pdf;
- EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. *Bias in Algorithms: Artificial Intelligence and Discrimination*. Luxembourg: Publications Office of the European Union, 2022, available at https://fra.europa.eu/sites/default/files/fra_uploads/-fra-2022-bias-in-algorithms_en.pdf;
- EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. *Assessing High-Risk Artificial Intelligence: Fundamental Rights Risks*. Luxembourg: Publications Office of the European Union, 2025, available at https://fra.europa.eu/sites/default/files/fra_uploads/fra-2025-assessing-high-risk-ai-fundamental-rights-risks_en.pdf;
- EUROPOL. *AI and Policing: The Benefits and Challenges of Artificial Intelligence for Law Enforcement*. Luxembourg: Publications Office of the European Union, 2024. <https://www.europol.europa.eu/publication-events/main-reports/ai-and-policing>;
- EUROPOL. *AI Bias in Law Enforcement: A Practical Guide*. Luxembourg: Publications Office of the European Union, 2025, available at https://www.europol.europa.eu/cms/sites/default/files/documents/AI_bias_in_law_enforcement_-_practical_guide.pdf;
- EUROPOL. *Assessing Technologies in Law Enforcement*. Luxembourg: Publications Office of the European Union, 2025, available at <https://www.europol.europa.eu/cms/sites/default/files/documents/Assessing-Technologies-in-Law-enforcement.pdf>;
- HOBSON, ZOË, JULIA A. YESBERG, BEN BRADFORD, and JONATHAN JACKSON. “Artificial Fairness? Trust in Algorithmic Police Decision-Making.” *Journal of Experimental Criminology* 19 (2023): 1027–60. <https://doi.org/10.1007/s11292-021-09484-9>;
- INTERPOL. *INTERPOL I-Learn Catalogue*. May 2026, available at <https://www.interpol.int/content/download/24489/file/INTERPOL%20I-Learn%20Catalogue%20May%202026.pdf>;
- NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. NIST AI 100-1. Gaithersburg, MD: NIST, 2023, available at <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>;
- EUROPEAN PARLIAMENT AND COUNCIL OF THE EUROPEAN UNION. *Regulation (EU) 2024/1689 of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence*. Official Journal of the European Union L 2024/1689, available at https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=OJ:L_202401689;

- UNESCO. *Recommendation on the Ethics of Artificial Intelligence*. Paris: UNESCO, 2021, available at <https://unesdoc.unesco.org/ark:/48223/pf0000381137>;
- UNICRI. *Decoding Transparency: How to Foster Public Trust in Responsible AI Innovation in Law Enforcement*. Turin: UNICRI, 2026, available at https://unicri.org/sites/default/files/2026-04/-AI4Citizens-Decoding-Transparency-How-to-Foster-Public-Trust-in-Responsible-AI-Innovation-in-Law-Enforcement_1.pdf;
- UNICRI and INTERPOL. *Toolkit for Responsible AI Innovation in Law Enforcement: Organizational Readiness Assessment Questionnaire*. Turin/Lyon, 2024, available at https://www.interpol.int/content/download/20933/file/AI_Toolkit_Organizational_Readiness_Assessment_Questionnaire%5B1%5D.pdf;
- UNICRI and INTERPOL. *Toolkit for Responsible AI Innovation in Law Enforcement: Principles for Responsible AI Innovation*. Turin/Lyon, 2024, available at https://unicri.org/sites/default/files/2023-06/02_Principles%20for%20Responding%20AI%20Innovation.pdf;
- UNICRI and INTERPOL. *Toolkit for Responsible AI Innovation in Law Enforcement: Technical Reference Book*. Turin/Lyon, 2025, available at https://unicri.org/sites/default/files/2025-03/Tech%20Ref_Book_Mar25.pdf.

