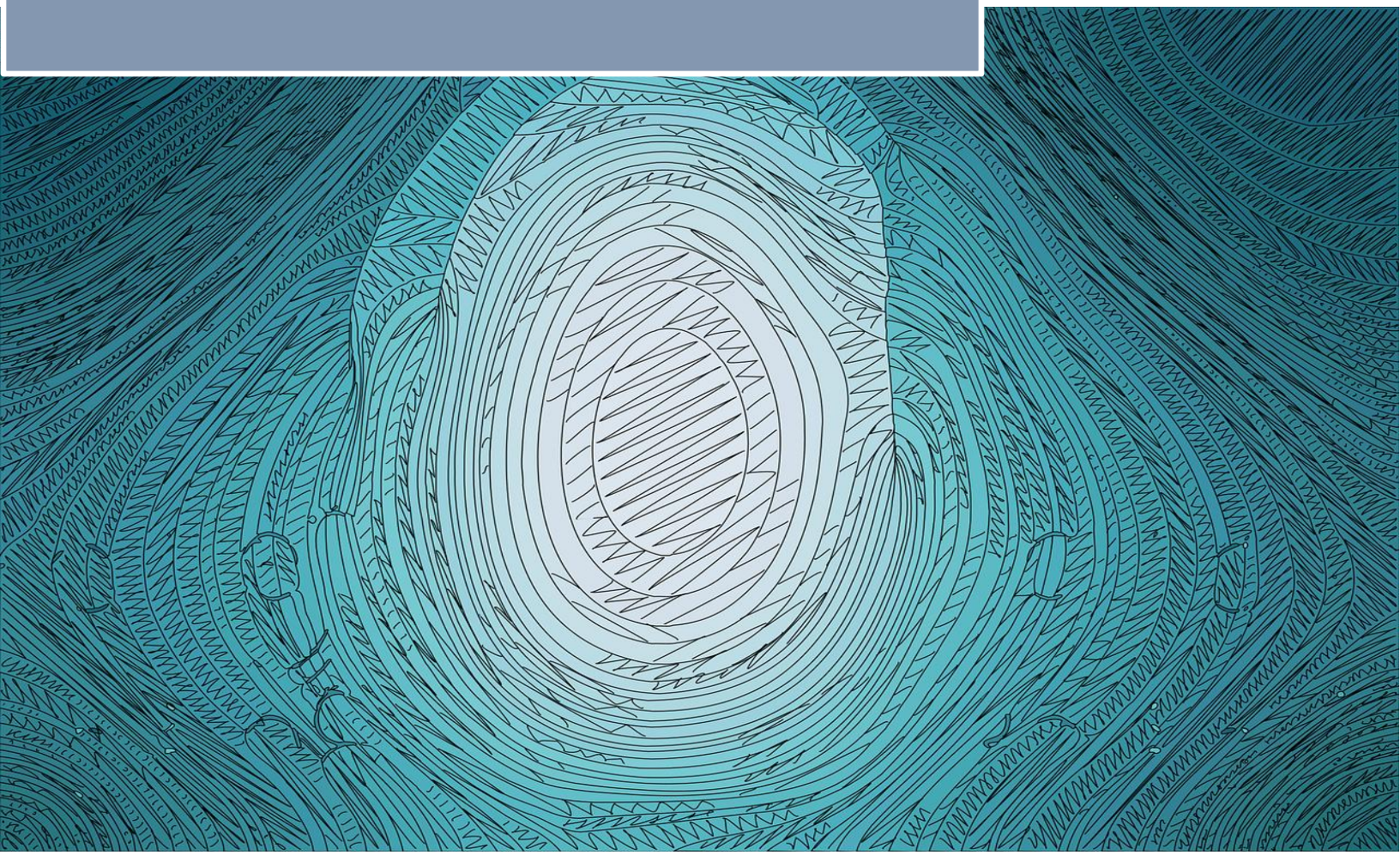
Neapolis University Pafos, Cyprus
AI-2-TRACE-CRIME
Jean Monnet Center of Excellence
Co-funded by the European Union

Policy Brief

Biometric Vulnerabilities and Law Enforcement

NUP Jean Monnet / UNESCO Policy Briefs

43/2026



Co-funded by the European Union

Neapolis University Pafos

UNESCO Chair in Human Development, Security & the Fight against Transnational Crime and Illicit Trafficking in Cultural Property

unesco Chair

The NUP Jean Monnet / UNESCO working papers and policy briefs can be found at:

https://www.nup.ac.cy

Publications in the Series should be cited as:

AUTHOR, TITLE, NUP UNESCO/JEAN MONNET WORKING PAPER or POLICY BRIEF NO. x/YEAR [URL]

Copy Editor: G. Pavlidis

Neapolis University Pafos, School of Law

Pafos, 8042, Cyprus

Biometric Vulnerabilities and Law Enforcement

Executive Summary

Europol's 2025 Innovation Lab report, 'Biometric Vulnerabilities: Ensuring Future Law Enforcement Preparedness', analyses the growing importance of biometric technologies in modern policing and border security, while highlighting critical vulnerabilities that could compromise their reliability and security. As biometric systems—such as facial recognition, fingerprint, iris, and voice identification—become central to law enforcement operations and EU-wide information systems, ensuring their integrity is a strategic necessity.

The report underscores that while biometrics strengthen identification accuracy and support cross-border investigations, they are increasingly targeted by presentation attacks, synthetic identity creation, and data manipulation. Europol calls for enhanced awareness, testing, and resilience mechanisms to prevent exploitation by criminal actors and maintain public trust in these technologies.

It further anticipates that advances in artificial intelligence and quantum computing will shape the next generation of biometric authentication, presenting both opportunities for innovation and new risks for data protection and security.

Keywords

Europol, Biometrics, Facial Recognition, Fingerprints, Iris Scans, Presentation Attack Detection, Artificial Intelligence, Quantum Computing, Data Protection, Law Enforcement Preparedness.

Background

Biometric technologies—ranging from fingerprint and face recognition to iris and voice analysis—have become integral to EU law enforcement, border management, and judicial cooperation. They underpin large-scale systems such as the Schengen Information System (SIS), the Visa Information System (VIS), EURODAC, and the forthcoming Prüm II framework for cross-border biometric exchange.

These tools enable fast and reliable identification, support investigations, and strengthen public security. However, as biometric technologies become more embedded in operational workflows, they also expose new vulnerabilities—both technical and procedural. The Europol Innovation Lab, through its Observatory on Emerging Technologies, assesses these challenges to ensure that EU law enforcement remains prepared and resilient.

Key Findings

The report highlights several technical, procedural, and ethical vulnerabilities that could undermine the reliability and acceptance of biometric technologies:

• Presentation and Spoofing Attacks: Increasingly sophisticated techniques—such as high-resolution replicas, 3D-printed fingerprints, and facial masks—can deceive sensors and compromise authentication systems.

• Morphing and Deepfake Manipulation: Synthetic image creation and video morphing tools blur identity verification, posing challenges for both border control and forensic analysis.

• Data Security Risks: Large biometric databases are high-value targets for cyberattacks and data breaches, requiring encryption and strict access control.

• Bias and Ethical Considerations: Algorithmic bias in facial and demographic data may lead to false positives or discrimination, threatening public trust and compliance with EU data protection standards.

• Standardisation Gaps: While ISO/IEC standards for biometric performance and presentation attack detection exist, implementation remains inconsistent across systems and jurisdictions.

The report stresses that understanding these vulnerabilities is essential for ensuring operational reliability, legal compliance, and societal trust.

Operational Implications

For law enforcement agencies, the proliferation of biometric tools brings both enhanced capability and increased responsibility. Europol emphasises that preparedness requires not only technical solutions but also procedural safeguards, inter-agency cooperation, and continuous training.

Key operational implications include:

- Integration of liveness detection and anti-spoofing mechanisms into biometric systems;
- Establishment of dedicated units for biometric system testing and red-teaming;
- Close collaboration with research institutions and private sector developers to anticipate and mitigate new attack vectors;
- Development of ethical review mechanisms to ensure compliance with fundamental rights and proportionality standards.

The report encourages EU Member States to adopt a proactive approach—embedding risk assessments, resilience testing, and interoperability standards into the full lifecycle of biometric technologies.

Strategic Recommendations

Building on its findings, Europol proposes a series of strategic recommendations to strengthen biometric resilience and governance across the EU:

• Awareness and Training: Increase operational awareness of biometric vulnerabilities and enhance investigator training on technical and ethical aspects.

• Advanced Detection and Verification: Deploy multi-modal systems combining fingerprints, facial, and iris recognition, with integrated presentation attack detection.

• Secure Data Management: Ensure encrypted storage, decentralised architectures, and compliance with the EU's General Data Protection Regulation (GDPR) and Law Enforcement Directive.

• Public-Private Collaboration: Strengthen cooperation with industry, standardisation bodies, and academia to align on best practices and emerging security standards.

• Technological Foresight: Monitor developments in quantum computing, which may redefine encryption, data protection, and biometric matching capabilities. Policymakers are urged to anticipate these transformations by investing in post-quantum security measures.

These recommendations underscore the need for an integrated policy framework balancing innovation, security, and privacy protection.

Concluding Remarks

The Europol Innovation Lab's 2025 report underscores that biometric technologies are both powerful enablers of security and potential vectors of risk. Maintaining the integrity and trustworthiness of these systems requires anticipating vulnerabilities, promoting technical standardisation, and ensuring continuous adaptation to emerging technologies such as artificial intelligence and quantum computing.

Law enforcement preparedness will depend on harmonised EU guidance, investment in innovation, and transparent governance frameworks. By reinforcing resilience and ethical safeguards, the EU can ensure that biometrics continue to serve as a cornerstone of effective and rights-respecting security policy.

Further Reading

- Europol Innovation Lab (2025), 'Biometric Vulnerabilities: Ensuring Future Law Enforcement Preparedness' (link)