TENSOR
Reliable biometric tEchNologies to aSist Police authorities in cOmbating terrorism and oRganized crime

Funded by the European Union

# TENSOR

## Policy recommendations on biometric data use and sharing in EU law enforcement

January 2026

## Executive summary

The growing use of biometric technologies by European law enforcement agencies has changed how investigations unfold and how data moves across borders. These tools can make police work faster and more precise, but they also raise ethical and legal questions.

This paper examines these gaps through the experience of the TENSOR project, which develops tools to extract biometric evidence and enable secure cross-border data exchange. The paper draws from pilot activities, questionnaires, and interviews with law enforcement authorities, the paper identifies both progress and persistent challenges. It shows that technology alone cannot ensure justice without stronger legal clarity, operational consistency, and ethical safeguards.

From this effort two conclusions emerge. First, Member States need to align national laws and infrastructures to achieve real interoperability. Second, technological development must remain grounded in the principles of legality, accountability, and respect for fundamental rights. A harmonious European approach can ensure that innovation strengthens public safety without eroding public trust.

To support this balance, five policy actions are proposed.

1. An **EU certification scheme for biometric systems** would guarantee that technologies meet minimum standards for accuracy, security, and fairness.
2. **Standardised frameworks for data sharing** would give LEAs common templates and infrastructures that reduce fragmentation and speed up cooperation.
3. **Mandatory training on AI ethics and fundamental rights** would help officers understand the risks and responsibilities that come with digital tools.
4. **Inclusion of safeguards for human oversight** in national legislation and procedures.
5. Finally**, a Biometric Use Forum** would create space for dialogue among law enforcement, regulators, and civil society to anticipate risks and share good practices.

These measures reinforce the EU's robust legal framework by turning its principles into concrete action. Certification, standardisation, training, oversight, and open dialogue create the conditions for ethical and interoperable use of biometric systems. In doing so, they help align national practices with Europe's broader vision of secure, lawful, and rights-respecting innovation.

# 1. Introduction

Eighty-five percent of criminal investigations in the European Union now depend on electronic evidence (Wahl, 2025). This shift shows how digital transformation has reshaped criminal justice, complementing or in some contexts replacing traditional investigative methods with data-based approaches. However, as with any systemic change, its implementation demands a careful balance between innovation, ethical and lawful adoption.

As law enforcement authorities (LEAs) began to face these new realities, the European Commission (EC) moved to provide a common policy direction. Within the broader ProtectEU Strategy launched in 2025, the EC presented the *Roadmap for Effective and Lawful Access to Data for Law Enforcement* (European Commission, 2025). Both initiatives recognised that fragmented national practices and outdated cooperation mechanisms limited the benefits of data-driven investigations and could weaken the protection of individual rights. The *Roadmap* therefore outlined six key areas, in general to modernise digital forensics, strengthen interoperability among Member States, and ensure that access to data remains necessary, proportionate, and consistent with EU law.

In recognition of these emerging challenges, the TENSOR project was launched in 2023 under the Horizon Europe programme to address and anticipate the opportunities and challenges that came with the digital modernisation of law enforcement. The project brings together technical experts and practitioners who have recognised the need to strengthen the capacity of law enforcement authorities to use biometric and digital data responsibly. Its goal is to ensure that technology enhances investigations and enables secure cross-border data exchange while protecting fundamental rights.

Its work translates these shared European concerns on interoperability, accountability, and rights-compliant data use into practical solutions that complement the policy direction later consolidated in the ProtectEU Strategy and the Roadmap for Effective and Lawful Access to Data for Law Enforcement. Through this effort, TENSOR has contributed to the efforts in imagining public safety in a way that advances innovation without compromising privacy, justice, or the rule of law.

## 1.1 Purpose and scope of the document

This policy document is part of the TENSOR project's effort to turn its research findings into practical guidance for law enforcement and policy actors across Europe. It aims to show how TENSOR's work can support the responsible use of biometric technologies in criminal investigations and cross-border cooperation.

The document has two main objectives. First, it recommends ways to strengthen how LEAs collect and handle biometric evidence, ensuring that investigations remain fair, unbiased, and legally compliant at every step. Second, it proposes measures to support secure and privacy-preserving biometric data exchange among European security partners, facilitating cooperation while guarding fundamental rights. These objectives directly support the European Commission's 2025 roadmap on lawful data access and echo the EU's broader principles of justice, accountability, individual dignity and ethical innovation.

### 1.2 Structure of the document

The report continues with the following structure:

- **Section 2** provides an overview of the TENSOR project through the description of its main objectives and use cases. This section explains how TENSOR supports law enforcement agencies through advanced biometric tools and secure data exchange mechanisms. It establishes the project's relevance to the broader European agenda on lawful and effective access to data for law enforcement.
- **Section 3** looks at the European policies and laws that regulate the use of biometric data in law enforcement and cross-border cooperation. It also reviews how policymakers, researchers, and civil society understand the challenges of integrating new technologies into police work. Together, these elements outline the current policy context and help identify where further actions and guidance are needed.
- **Section 4** presents insights from the TENSOR pilots. It summarises lessons learned, good practices, and challenges observed across the project's use cases in practical scenarios
- **Section 5 outlines** evidence-based policy recommendations. They draw on Section 3 research and on empirical findings from the TENSOR pilots, including questionnaire responses from end users and qualitative insights gathered through semi-structured interviews with law enforcement authorities.

In sum, the paper provides policy recommendations that are meant to be actionable, specific to both LEAs and tech providers and usable in data exchange practices.

## 2. TENSOR overview

This section introduces the TENSOR project by outlining its objectives, core components, and use cases, placing the project within the wider European Union (EU) effort to support lawful and effective access to data for law enforcement.

TENSOR stands for *Reliable biomeTric tEchNologies to asSist Police authorities in cOmbating terrorism and oRganised crime (GA No. 101073920).* The project supports European law enforcement agencies by developing advanced biometric tools and secure data-exchange mechanisms that enhance criminal investigations. These, while safeguarding fundamental rights and developing privacy preserving tools.

TENSOR focuses on two core priorities. The **first goal** is to improve the accuracy and reliability of biometric evidence extraction so that digital traces gathered in investigations are robust and verifiable. The **second goal** is to strengthen cross-border cooperation through secure data-sharing mechanisms that make the exchange of evidence faster, more consistent, and compliant with European legal standards.

To meet these objectives, TENSOR advances technologies that extract, process, and analyse several types of biometric data, including facial, voice, and behavioural traits. This approach is known as **multimodal biometrics** (ScienceDirect, 2025). Multimodal systems combine more than one biometric modality, such as fingerprint, face, iris, or voice, to confirm identity even when single modalities are partial or unclear. The combination of different biometric modalities may increase the accuracy and reduce errors in identification processes. The project also examines

**soft biometrics**. These are traits that are too general to identify a person on their own, such as gender, age, ethnicity, or height. When used with other evidence, they add context without replacing strict identifiers (Mordini, 2021).

TENSOR embeds transparency features using a guided-workflow assistant and explainable AI features to help investigators clearly interpret results and explain how results are produced. Investigators and oversight bodies can review and verify the steps taken, which supports fairness and legitimacy.

In addition, the project advances the capabilities of digital forensics by offering tools that enable LEAs to extract and analyse data from seized devices and technically complex environments, including encrypted mobile phones. It supports the identification of device owners and the retrieval of forensic-relevant information such as app-usage patterns and location traces. At its core, TENSOR aims to demonstrate that innovation in biometric and forensic technologies can strengthen investigations while being privacy-preserving and legally compliant.

## 2.1 Pilots in TENSOR

To test its technologies and assess their operational relevance, TENSOR carried out a series of pilot activities that replicated real investigative conditions. The pilots were organised around three use cases that reflect different dimensions of law enforcement work. Together, they show TENSOR's complete tools and capabilities. Below is a brief overview of each use case:

- **Use Case 1 – Evidence collection through behavioural and physiological biometrics:** Led by the Policejní Prezidium České Republiky (PCR), this use case tested TENSOR's capacity to identify and verify suspects by correlating behavioural and physiological traits derived from CCTV footage. It showed how combining different biometric sources can increase reliability and reduce the likelihood of false matches in complex investigative settings.
- **Use Case 2 – Digital forensics and orphan device owner identification:** Under the leadership of the Ministry of the Interior of Finland (MOI), this use case demonstrated how TENSOR's digital forensic tools can identify the owner of a seized device when no user information is available. The system extracted relevant biometric and behavioural data, such as typing rhythm or device interaction patterns, that could associate a device with its owner.
- **Use Case 3 – Cross-border data protection and exchange:** This use case, coordinated by the Ministério da Justiça (PJ) of Portugal and the Inspectoratul General al Poliției (GPI) of Moldova, explored TENSOR's European Biometrics Data Space for secure information exchange between jurisdictions. It tested the system's ability to manage interoperability and data protection simultaneously, showing how transparent data-sharing mechanisms can speed up cross-border investigations while preserving individual rights.

To understand the significance of these developments and identify where policy recommendations can add value, it is necessary to examine the laws that regulate these technologies and the debates surrounding their use. The next section builds on this by presenting the European policy and legal context in which biometric data is used for law enforcement purposes.

# 3. Legal frameworks and existing practices and challenges

This section focuses on the main European instruments and policy debates that directly shape how law enforcement authorities handle data and cooperate across borders. It focuses on areas most relevant to TENSOR's objectives and is organised in three parts. The first two cover EU law on data protection, the handling of digital evidence, and the rules that enable information exchange between Member States. The third summarises how academia, policymakers, and civil society view the ethical and operational challenges in this field. These elements outline the current policy context and help identify where further action and guidance are needed.

## 3.1 EU Framework: Data protection and evidence extraction

The **General Data Protection Regulation (GDPR)** (Regulation (EU) 2016/679) is the core legal framework governing the protection of personal data within the European Union. It establishes binding rights for individuals and corresponding obligations for organisations, which ensures that the collection, use, and management of personal data uphold the fundamental right to data protection (Article 8 of the Charter of Fundamental Rights). For biometric systems used in policing, the GDPR sets the baseline rules for how information linked to a person can be extracted, entered into databases, reused, and shared.

A first set of obligations concerns the moment when evidence is collected and stored in digital files because biometric identifiers fall under special categories of personal data. Their processing is generally prohibited unless a specific legal exception applies. In the context of law enforcement activities, the processing of biometric data may be permitted under Article 9(2)(g) GDPR where it is necessary for reasons of substantial public interest, based on Union or Member State law, and subject to proportionality and appropriate safeguards. Member States also have the option to add stricter conditions applied in national law, and therefore biometric databases differ from country to country, according to what kind of biometric data is allowed to be collected and stored.

In practical terms, the GDPR influences every stage of biometric evidence handling. Data collected from suspects or crime scenes must be kept accurate and updated, retained only for as long as needed, and protected by robust security measures (Article 32 GDPR). Importantly, individuals have a right not to be subject to decisions based solely on automated processing (Article 22 GDPR). In law enforcement, this means any match or identification suggested by an algorithm cannot be treated as final without human review. A facial recognition match, for example, must be verified by an officer or forensic expert before it precedes an arrest or prosecution. This is a safeguard that has become central to debates on policing technology and is embedded in TENSOR's design through human-in-the-loop safeguards.

Furthermore, the GDPR mandates transparency and accountability in data processing. In practice, that means that data subjects should be informed about the collection and use of their data (Articles 13–14) and, with some law enforcement exemptions, have rights to access or rectify their data and, in case of data misuse, seek remedies. Even when informing individuals is difficult, as in covert investigations or when data originates from third-party databases, authorities must balance investigative security with the public's right to know about surveillance practices. Transparency, even at an aggregate level, is key to public trust since its absence can increase concerns about overreach, or bias in biometric policing.

It should be noted that for processing by police and criminal justice authorities, the GDPR's principles are mirrored and specified in the **Law Enforcement Directive (LED)** (Directive (EU) 2016/680). The LED is a sector-specific law that governs personal data processing "for the prevention, investigation, detection or prosecution of criminal offenses" by competent authorities. While the GDPR and LED share common foundations (data minimisation, purpose limitation, security requirements, etc.), the LED tailors these to law enforcement needs. For example, by allowing certain restrictions on data subject rights when strictly necessary to avoid prejudicing an investigation. The LED provisions ensure that if police use biometric modalities, they do so with a clear legal basis and added care for sensitivity. In effect, processing is lawful only if it is necessary and proportionate for a legitimate law enforcement purpose and grounded in law.

It also emphasises data security, logging, and oversight. Agencies must keep detailed records of data accesses and transfers, implement role-based access controls, and conduct audits to prevent misuse. Any sharing of biometric data between authorities (national or cross-border) must likewise be logged and only occur if the receiving authority is authorised to handle that data for a compatible purpose. Such provisions directly affect systems like TENSOR's data platform, which must maintain traceability of biometric evidence. All actions should be recorded for accountability.

Despite its harmonising objective, **implementation across Member States remains uneven.** Findings from the European Parliament's 2022 assessment (Vogiatzoglou and Marquenie, 2022) shows that Member States interpret key notions such as "competent authority", "criminal offence" and "public security" differently. This leads to variations in how law enforcement bodies process data and apply safeguards. This study also identifies **weak oversight, limited use of data protection impact assessments, and insufficient technical guidance for automated or large-scale data processing**. The inconsistencies create uncertainty and limit the effectiveness of cross-border cooperation.

## 3.2 EU Framework: Cross-border data exchange

Beyond data protection and extraction, several EU instruments govern how biometric data and other evidence can be shared across agencies and countries in criminal cases. As seen in this section, the most pertinent are the new Prüm II Regulation, the European Investigation Order (EIO) (Directive 2014/41/EU), and the Europol Regulation ((EU) 2016/794, amended 2022).

The **Prüm II Regulation** is the EU's main legal instrument for automated data exchange among law enforcement authorities. It entered into force the 25 April of 2024 and it enables the cross-border sharing of biometric and identification data, including DNA profiles, fingerprints, facial images, and vehicle registration information. The regulation aims to enhance interoperability and mutual access to national databases to facilitate faster and more reliable investigations.

In operational terms, Prüm II affects how biometric evidence is compared and shared rather than how it is initially collected. Once fingerprints, DNA or facial images are stored in national systems, Prüm II provides the structured procedure that determines whether a query in one Member State can trigger a search in another State's system. According to the Regulation's architecture, an automated search may identify a potential match, after which the requesting authority can access additional information once human confirmation is given. This separation of automated query

and manual action creates both access and accountability conditions for cross-border forensic workflows.

The Regulation also governs how biometric information is exchanged between authorities. Exchanges must employ standardised formats and secure communication channels. Member States are required to log queries, record who searched which dataset and on what legal basis and ensure that the recipient authority is authorised to process the data for a compatible purpose. These measures create procedural and technical safeguards around the flow of biometric evidence.

Although intended to harmonise data exchange, the Regulation still faces criticism from civil society and parliamentary reports for leaving key problems unaddressed. EDRi (2024), for example, argued that the Prüm II reform **lacked a clear demonstration of necessity and proportionality for the expansion of data categories**, particularly facial images and police records, and raised concerns about automated large-scale searches that could weaken the presumption of innocence.

The **European Investigation Order** complements Prüm II by setting a unified procedure for law enforcement and judicial authorities to request and obtain evidence across Member States. Based on the principle of mutual recognition, it ensures that decisions on evidence gathering issued in one Member State are recognised and executed in another. For TENSOR, the EIO provides the legal mechanism that allows biometric data obtained or analysed through project technologies to be requested and transferred lawfully across borders. It connects the technical capacity to extract and process evidence with the judicial authority to exchange it. However, while the EIO simplifies cooperation, differences in procedural law, time limits, and technical infrastructure among Member States continue to slow down data transmission. Integration with emerging digital evidence frameworks also remains incomplete, which limits intended purpose.

The **Europol Regulation** establishes the mandate of the EU Agency for Law Enforcement Cooperation. It allows Europol to support Member States in data analysis, criminal intelligence, and operational coordination, including through large-scale data processing and the use of advanced analytical tools. While the regulation strengthens cooperation at the EU level, the integration of national and EU data infrastructures remains limited. National authorities still vary in how they format, transmit, and validate information, which limits full interoperability with Europol's central systems. These gaps underscore the broader issue TENSOR also addresses: the difficulty of reconciling innovation and efficiency with legal consistency and data protection safeguards across jurisdictions.

## 3.3 Ongoing debates on lawful and ethical use

While the EU's legislative framework is robust, numerous experts, non-governmental organisations (NGO), and academics have pointed out practical gaps and risks in how biometric technologies are being adopted by law enforcement. It is vital to consider these critiques to ensure that new policies address not just the letter of the law, but also public trust and ethical use. Key concerns include:

- **Private Vendor Involvement and Data Access:** Many law enforcement agencies rely on private companies for biometric systems (e.g. facial recognition software or fingerprint

databases). The Center for Democracy & Technology (Vallee, 2022) warns that this "reliance on private vendors" can create privacy risks, as companies may gain access to sensitive biometric information and even other personal data across agencies. For example, if one contractor provides face recognition services to multiple police forces, that vendor could potentially compile cross-agency data on individuals. This raises fears of surveillance outside direct public oversight. As a result, there is a clear need for strong rules on data sharing and auditing of vendors to prevent the erosion of public trust.

- **Accuracy and transparency:** Organisations like AlgorithmWatch (Kayser-Bril, 2019) noted in 2019, that at least 11 European police forces were using facial recognition, but details were scarce on their accuracy or how citizens could challenge mistakes. A consistent critique is the absence of mechanisms for individuals to appeal or correct false biometric matches. Moreover, civil society calls for more public disclosure about what tools are used and with what safeguards. This could include annual transparency reports by LEAs, disclosures to courts when algorithmic systems were used in an investigation, or even community consultations when new tech is introduced. Some law enforcement officials interviewed in TENSOR noted that openness is beneficial to address these concerns. Openness about how a technology works is essential, as **transparency makes public trust and acceptance more likely**.

- **Bias:** It is well documented that some biometric systems perform unevenly across different populations. Academic studies and experts have raised high concerns about racial bias and other inaccuracies. For instance, facial recognition algorithms have shown higher false match rates for people with darker skin tones or for women, as compared to white males, in multiple evaluations (Buolamwini & Gebru, 2018). Naturally, if not addressed, this could lead to discriminatory outcomes. The Georgetown Center on Privacy & Technology (Garvie et al, 2016) recommended that police facial recognition technology should only be used when officers have an individualised suspicion of criminal conduct. This principle of requiring reasonable suspicion is in line with constitutional traditions and is now echoed in the AI Act's stance against indiscriminate biometric surveillance.

- **Oversight and Redress**: Finally, civil society organisations (CSOs) emphasise that independent oversight is essential wherever powerful biometric tools are deployed. This includes both external oversight (data protection authorities, courts, or ethics boards reviewing law enforcement programs) and internal accountability (clear policies within LEAs on who can access systems, with logs and audits). The European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS) have, in various opinions, stressed the need for systematic audits of algorithms and for human review of biometric identification before decisions are made (EDPB & EDPS, 2021; European Data Protection Board, 2022). NGOs have also called for moratoria or strict limits on certain uses like live facial recognition until robust safeguards are proven (SHARE Foundation et al., 2021). While EU law is moving toward stronger regulation, gaps remain in practice. One idea raised in policy circles is to establish **certification schemes** (at EU level) so that any biometric system sold to police meets security and bias mitigation standards.

These gaps identified by experts and the community inform the recommendations ahead. Effective policy must ensure that tools like TENSOR are adopted in a way that genuinely improves efficiency and security, and justifiably preserves the rights and trust of individuals. The next

section will consider how the TENSOR pilot experiences align with or highlight these broader issues, leading to targeted policy recommendations.

# 4. Insights from TENSOR pilots

This section summarises the main insights gathered from TENSOR's pilot activities. The analysis draws on observations from the pilot demonstrations, questionnaires implemented by project partners, and semi-structured interviews conducted with LEAs. Together, these sources provide a view of how TENSOR's technologies function in practice and how end users perceive their value and limitations.

## 4.1 Successes across the pilots

- **Automation of routine tasks:** Evaluation questionnaires show that LEAs believe that routine or pre-expert work could be partly automated by TENSOR. This frees experts to focus on interpretation rather than data preparation. This reallocation of human effort could leave forensic examiners to spend resources only on the top candidates instead of scanning thousands of files.
- **Centralised platform:** Integrating multiple biometric modalities in one system was viewed as a major advantage. Investigators could compare fingerprints, facial images, voice samples, and apply phone forensics in a single interface, which both saved time and facilitated cross-referencing. This centralisation enabled investigators to identify links across evidence types that might otherwise have been overlooked.
- **AI assistance with human oversight**: The pilots confirmed that AI can help parse data and support preliminary identification, but human verification remains essential. TENSOR's "human-in-the-loop" design, requiring experts to confirm automated results, proved effective. Agencies agreed that this balance improved efficiency while maintaining legal reliability and accountability.

## 4.2 Challenges throughout the Use Cases

Despite the positives, the pilots encountered challenges that highlight areas for improvement:

- **Legal fragmentation and uncertainty.** Differences in national legislation remain one of the main barriers to deploying biometric technologies consistently across Europe. Although all bound by the GDPR, individual partners embrace different levels of national laws that expand upon the GDPR, and LEAs may impose additional in-house policies, making the processing and sharing of biometric data challenging between countries. For example, Czech and Portuguese teams noted that their laws did not yet recognise newer biometric modalities, such as voice or gait, raising questions about evidentiary admissibility. This uneven legal landscape reflects the very gap that the EU's harmonisation efforts seek to close. As discussed in Section III on Legal frameworks and existing practices and challenges, national disparities continue to delay the full realisation of EU policy efforts.
- **Technical integration and scalability.** The pilots revealed that not all law enforcement agencies operate with compatible IT infrastructures. While the pilots were tested in

modern, controlled environments, real-world deployment would require integrating TENSOR with legacy systems and upgrading hardware to handle computational demands. This interoperability gap, already noted in European policy debates, demonstrates the importance of EU-level investment to ensure all Member States have the technological capacity to adopt AI-supported forensic systems. To address this, the EC has recently announced the launch of the shared biometric matching service (sBMS), which is meant to enhance interoperability with a focus on improving law enforcement (Directorate-General for Migration and Home Affairs, 2025). This could provide the start of a shared biometric system with adopted legislation.

- **Cost and resource constraints.** Agencies also highlighted the financial and human resource implications of deploying new tools. Beyond initial training and equipment costs, sustainable use would require ongoing professional development and infrastructure maintenance. Without dedicated EU or national funding streams, adoption risks being uneven, reinforcing existing disparities in digital capabilities among Member States.

In conclusion, the pilot experiences affirmed that technology can significantly aid law enforcement but only if accompanied by the right policies, training, and safeguards. The successes (automation, integration, AI assistance) can only be realised sustainably if the challenges (legal fragmentation, cost, inconsistency) are addressed. This evidences a need for the policy recommendations in the next section.

# 5. Policy recommendations

Based on the legal frameworks and existing practices and challenges (Section III) and the insights from TENSOR's pilots (Section IV), this section provides policy recommendations to ensure the adoption of biometric technologies is fair, unbiased, legally compliant, and privacy-preserving. The recommendations are grouped into two categories. The first focuses on measures to strengthen internal procedures of law enforcement agencies so that the technologies are used responsibly and effectively. The second measures to enable secure and rights-protective biometric data exchange between agencies and across borders.

## 5.1 Strengthening LEAs' Internal Procedures

***Recommendation 1:*** **Mandate training on AI ethics and fundamental rights for officers.**

The EU and Member States should require and fund regular training programs for LEAs on the use of AI and biometric systems, with a focus on ethics, data protection, and fundamental rights. This follows the approach used in the TENSOR pilots, where ethics workshops were held before new technologies were introduced to ensure all participants understood their legal and ethical obligations. Such practices help officers identify risks, apply safeguards, and ensure that innovation aligns with the principles of accountability and human rights.

Training should cover three core areas:

- **Data protection and legal compliance**, with modules grounded in GDPR and Law Enforcement Directive principles;

- **Non-discrimination and fairness**, addressing how bias can enter algorithms and how to identify or mitigate it;
- **Procedural justice and communication**, including how to explain technology use in court or to affected individuals.

Training must not be a one-time exercise. Officers should receive periodic refreshers, especially when new tools are introduced or existing systems are updated. To promote consistency, the EU could develop a shared curriculum with consultation of external experts, such as technologists, ethicists, and civil society representatives, would also strengthen the balance between operational needs and public trust. Ultimately, officers authorised to use biometric and AI systems should understand that these tools are powerful but sensitive instruments. Proper training ensures they can use them lawfully and effectively, preventing misuse, protecting fundamental rights, and reinforcing public confidence in technology-supported procedures.

### *Recommendation 2:* Enforce human oversight and decision-making in AI-assisted decisions within national regulation.

Policymakers should ensure that the principle of human oversight in AI-assisted decision-making is not only recognised at EU level but also embedded in national law enforcement policies and operational standards. Although the GDPR and the Law Enforcement Directive prohibit decisions based solely on automated processing and the AI Act (Article 14) reinforces this safeguard for high-risk systems, these provisions often remain abstract and unevenly applied across Member States. This recommendation builds on a key observation from the TENSOR pilots: human oversight remains vital even when technology performs well, as expert judgment provides the accountability and context that algorithms cannot replicate. In practice, every LEA using biometric AI should have a written policy that, for instance, "no arrest or search will be conducted based purely on an AI match without corroboration by a human investigator." National policing standards should explicitly include this safeguard as part of their operational protocols, supported by training that helps officers recognise the limits of algorithmic tools. Integrating this requirement into domestic practice will harmonise implementation across Member States and align national procedures with EU law.

### *Recommendation 3:* Improve transparency measures and public communication.

Recognising the concerns posed by CSOs regarding the transparency and accountability of mechanisms in place for technology driven or AI assisted systems, Member State authorities, supported by the European Commission, should establish consistent transparency frameworks for the use of biometric technologies in law enforcement. Public accountability is essential for maintaining trust, yet as highlighted by NGOs and researchers, information on how these systems are deployed, how often they are used, and with what results remains limited or fragmented.

Transparency does not mean disclosing sensitive operational data. Instead, it means offering structured, aggregate reporting that enables democratic oversight without compromising security. Each Member State should require law enforcement agencies to publish annual reports containing key indicators such as:

- the number of biometric searches conducted (e.g., facial recognition, fingerprint, or voice comparison);

- the number of positive identifications and confirmed false positives;
- summaries of audit findings, data protection assessments, or identified system errors;
- corrective actions or improvements made following internal or external reviews.

These reports would demonstrate accountability while addressing the current information gap identified by civil society. They should be complemented by communication strategies that explain to the public how such technologies are used, what safeguards apply, and what rights individuals have when their data is processed. At EU level, a central mechanism potentially coordinated the European Data Protection Board or EU-funded initiatives, could compile national reports to produce a comparative overview of biometric use across Member States. This would promote consistency, allow early identification of systemic risks, and help ensure that technological progress in policing remains transparent

***Recommendation 4:* A biometric forum for multi-stakeholder collaboration.**

A permanent Biometric Use Forum should be created at the EU level to facilitate structured dialogue between law enforcement authorities, data protection bodies, civil society, and technical experts. This forum would serve as a consultative platform for:

- Co-developing interpretive guidance on applying the Law Enforcement Directive, GDPR, and the AI Act to biometric technologies in policing;
- Sharing implementation challenges and best practices, allowing LEAs to exchange experiences on accountability, oversight, and proportionality;
- Feeding insights into legislative and policy development, ensuring that future EU reforms remain grounded in evidence and operational realities.

Unlike existing expert groups that focus primarily on data protection enforcement, this forum would bring together both regulators and end-users in a transparent setting and help shape customary law.

## 5.2 Biometric data exchange

TENSOR's vision of a European Biometric Data Space aligns with EU initiatives (like Prüm II) to improve cross-border cooperation. However, scaling up data exchange requires safeguards to ensure that sharing is proportionate. The following recommendations focus on the policy and technical measures needed to facilitate efficient yet rights-preserving exchange of biometric information.

***Recommendation 5:* Develop an EU certification scheme for biometric systems and vendors.**

Building on TENSOR's emphasis on privacy-respecting technology, it is important to strengthen how ethics and accountability are embedded in system design. The European Commission should establish an EU-level certification scheme for biometric technologies used by LEAs, modelled on the Cybersecurity Act's certification frameworks and consistent with the AI Act's risk-based approach. Certification should cover both technical systems and vendors. Systems would be tested and audited by external bodies to verify compliance with defined criteria such as:

- measurable accuracy and error rates across demographic groups,

- robust access controls, logging, and encryption,
- demonstrable bias testing results,

Over time, certification could become a condition for public procurement, ensuring that only "ethical and secure by design" systems are eligible for purchase. This initiative could be developed in collaboration with standards bodies (CEN/CENELEC, ISO), and privacy and fundamental rights experts.

***Recommendation 6:* Standardise frameworks and infrastructure for cross-border data sharing.**

To address the gaps of implementation found in the LED and Prum II, and to fulfil the objectives of the EU Roadmap for Effective and Lawful Access to Data for Law Enforcement (2025), the European Commission should promote greater standardisation of the operational and technical frameworks used for cross-border data sharing. The existing legal foundations (such as the Law Enforcement Directive, GDPR, and Prüm II Regulation) already set out clear rules on access, purpose limitation, and accountability. However, the TENSOR pilots revealed that their implementation remains fragmented, with Member States relying on incompatible templates, formats, and systems.

The EU should therefore coordinate the development of:

- **Common templates and procedures** for data-sharing agreements between law enforcement authorities;
- **Interoperable technical formats** and minimum cybersecurity standards to enable secure exchanges;
- **Targeted infrastructure support** for Member States with limited technical capacity, ensuring that all can participate equally in cross-border investigations.

Standardisation in these areas would turn existing legal principles into practice.

## 6. Conclusions

The deployment of biometric technologies in law enforcement stands at a crossroads. On one hand, projects like TENSOR demonstrate that innovative tools can greatly enhance investigative capabilities, helping LEAs to solve crimes more efficiently and collaboratively. On the other hand, these technologies raise legitimate concerns about privacy, bias, and legality. A recurring theme is the need for harmonisation and clarity in balancing the trade-offs between this. Variation in national laws and practices must be addressed to create a level playing field. Whether it's, how sensitive biometric data can be used, or how agencies request data from one another, clearer and more uniform rules will benefit everyone. The EU's 2025 Roadmap and strategies like ProtectEU already point in this direction, emphasising standardisation, interoperability, and modern legal frameworks. The policy steps recommended here serve to fill in the detail of those broad strategies in the domain of biometrics. Equally important is a rights-based implementation of technology. Europe's commitment to human dignity, freedom, democracy, equality, rule of law, and human rights is legally binding. Law enforcement, which operates at the nexus of state power and individual rights, must exemplify this commitment when introducing powerful tools.

# 7. Bibliography

Buolamwini, J. and Gebru, T. (2018) 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification', in Proceedings of the 1st Conference on Fairness, Accountability and Transparency. Conference on Fairness, Accountability and Transparency, PMLR, pp. 77–91. Available at: https://proceedings.mlr.press/v81/buolamwini18a.html

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (2014) OJ L. Available at: http://data.europa.eu/eli/dir/2014/41/oj.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (2016) OJ L. Available at: http://data.europa.eu/eli/dir/2016/680/oj.

Directorate-General for Migration and Home Affairs (2025) (Commission announces launch of the shared biometric matching service - Migration and Home Affairs. Available at: https://home-affairs.ec.europa.eu/news/commission-announces-launch-shared-biometric-matching-service-2025-05-19_en

EDRi (2022) 'Respecting fundamental rights in the cross-border investigation of serious crimes', European Digital Rights. Available at: https://edri.org/wp-content/uploads/2022/10/EDRi-position-paper-Respecting-fundamental-rights-in-the-cross-border-investigation-of-serious-crimes-7-September-2022.pdf.

EDRi (2024) 'Automated data exchange in Prüm II: The EU's securitisation mindset keeps encroaching on our fundamental rights', European Digital Rights (EDRi). Available at: https://edri.org/our-work/automated-data-exchange-in-prum-ii-eu-securitisation-mindset-encroaching-on-fundamental-rights/

European Commission. (2025). Commission presents Roadmap for effective and lawful access to data for law enforcement. Migration and Home Affairs. https://home-affairs.ec.europa.eu/news/commission-presents-roadmap-effective-and-lawful-access-data-law-enforcement-2025-06-24_en

EDPB & EDPS. (2021). EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). https://www.edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en

European Data Protection Board. (2022). Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement | European Data Protection Board. Europa.eu. https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_en

Garvie, C., Bedoya, A, Frankle, J. 'Unregulated Police Face Recognition in America'. (2016) Perpetual Line Up. Available at: https://www.perpetuallineup.org/recommendations.

Kayser-Bril, N. (2019) 'At least 11 police forces use face recognition in the EU, AlgorithmWatch reveals', AlgorithmWatch. Available at: https://algorithmwatch.org/en/face-recognition-police-europe/.

Mordini, E. (2021) 'Ethics of Biometrics', Springer eBooks [Preprint]. Available at: https://doi.org/10.1007/978-3-642-27739-9_1504-1.

Multimodal Biometric - an overview | ScienceDirect Topics (n.d.). Available at: https://www.sciencedirect.com/topics/computer-science/multimodal-biometric.

SHARE Foundation, Hermes Center, Bits of Freedom, ARTICLE19, Homo Digitalis, & EDRi. (2021, February 15). Campaign "Reclaim Your Face" calls for a Ban on Biometric Mass Surveillance - European Digital Rights (EDRi). European Digital Rights (EDRi). https://edri.org/our-work/campaign-reclaim-your-face-calls-for-a-ban-on-biometric-mass-surveillance/

Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (2016) OJ L. Available at: http://data.europa.eu/eli/reg/2016/794/oj.

Regulation - EU - 2024/1689 - EN - EUR-Lex (n.d.). Available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC – Legal Text (2016) General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/.

Regulation (EU) 2024/982 of the European Parliament and of the Council of 13 March 2024 on the automated search and exchange of data for police cooperation, and amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, (EU) No 2019/817 and (EU) 2019/818 of the European Parliament and of the Council (the Prüm II Regulation) (2024). Available at: http://data.europa.eu/eli/reg/2024/982/oj.

Vallee, H.Q. la (2022) 'Public Agencies' Use of Biometrics to Prevent Fraud and Abuse: Risks and Alternatives', Center for Democracy and Technology, 7 June. Available at: https://cdt.org/insights/public-agencies-use-of-biometrics-to-prevent-fraud-and-abuse-risks-and-alternatives/.

Vogiatzoglou, P., & Marquenie, T. (2022). Assessment of the implementation of the Law Enforcement Directive Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies PE. https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740209/IPOL_STU(2022)740209_EN.pdf

Wahl, T. (2025). Commission Roadmap on Access to Data for Law Enforcement PurposeS. Https://Eucrim.eu/; EUCRIM. https://eucrim.eu/news/commission-roadmap-on-access-to-data-for-law-enforcement-purposes/#:~:text=The%20Commission%20reiterated%20that%2085,actions%20in%20six%20key%20areas

TENSOR is co-funded by the EU Horizon Europe research and innovation programme under Grant Agreement No. 101073920.



Funded by
the European Union