Organization for Security and Co-operation in Europe

USING NEW TECHNOLOGIES TO **STREAMLINE ORGANIZATIONAL PROCESSES IN POLICING**

SUMMARY PAPER FROM AN EXPERT ROUNDTABLE DISCUSSION AT THE AUSTRIAN MINISTRY OF THE INTERIOR IN VIENNA, AUSTRIA (8-9 OCTOBER 2025)

Disclaimer: This paper summarizes a roundtable discussion held under the Chatham House rule. The views, opinions and conclusions presented herein reflect a synthesis of the roundtable dialogue and do not necessarily represent the official position of the Organization for the Security and Co-operation in Europe (OSCE) and/or its participating States. This document is intended to capture the essence of the discussion without attribution to specific participants or their affiliations. The OSCE does not endorse or verify the accuracy of individual statements made during the round table. Readers should consider this paper as a reflection of the diverse perspectives shared during the event rather than an authoritative statement on the topics discussed.

OSCE Secretariat
Transnational Threats Department
Strategic Police Matters Unit
Wallnerstrasse 6
1010 Vienna, Austria

E-mail: SPMU@osce.org
www.osce.org/policing

Table of contents

Introduction

New and emerging technologies have transformed almost all aspects of human life. From big data analytics and machine learning algorithms through the Internet of Things (IoT), smart sensors and autonomous drones to artificial intelligence (AI) – the current pace of technological innovation is unprecedented. This development has prompted discussions around the benefits and risks associated with the use of new technologies in various professional domains.

In the context of crime and policing, much of the debate has focused on concerns about the threats that such technologies may pose, especially their misuse for criminal purposes. However, the potential of these technologies to revolutionize how law enforcement operates and to enhance both its effectiveness and efficiency is equally significant. There is substantial and varied scope for the integration of new and emerging technologies in the work of law enforcement. For example, they can help to analyse trends and patterns, monitor security risks and threats, assist in identifying suspects and solving crimes, or streamline various administrative processes and procedures. At the same time, achieving a balance between leveraging technological advancements and safeguarding human rights and fundamental freedoms is an important task that raises ethical, legal and practical questions.

Against this backdrop, the OSCE Secretariat's Transnational Threats Department/Strategic Police Matters Unit launched a series of expert roundtable discussions on the use of new and emerging technologies by law enforcement. The discussions aim to identify opportunities for law enforcement to harness new and emerging technologies to support their work, to help formulate policy recommendations and to explore potential OSCE capacity-building support in this area.

This paper summarizes the key points and outcomes of the fourth and final round table, which shifted the focus from *what* law enforcement do to *how* they are organized to do it. The event was dedicated to the use of new and emerging technologies to streamline organizational processes within law enforcement agencies and took place in Vienna, Austria on 8 and 9 October 2025. The round table was organized in co-operation with the Austrian Federal Ministry of the Interior and brought together thirteen experts from law enforcement authorities, academia, the private sector, civil society and international organizations.

Optimizing processes through digital transformation

New and emerging technologies have significant potential to strengthen internal organizational processes within law enforcement, including in areas such as human resource management, strategic and operational planning, monitoring and reporting, and various administrative functions. If effectively integrated into day-to-day work, these technologies could have a truly transformative impact.

In the context of law enforcement agencies, much of the discourse focuses on the operational impact of the

use of new technologies. However, technology-enabled or -driven processes have the potential to enhance institutional resilience, accountability and the sustainability of policing reforms.

There are significant opportunities in each area — from using AI-enabled tools to support more objective and inclusive recruitment, to leveraging analytics for resource planning and optimization, automating routine documentation and reporting, and deploying virtual reality for immersive scenario-based training. In each case, integrating digital technologies into organizational processes requires significant adaptation and careful organizational change management. Three key issues need particular consideration.

First, adoption of any new technology must be a deliberate and well-thought-out process that is driven first by identifying existing problems or gaps and only then searching for an appropriate technological solution. In other words, strategy needs to guide technological innovation, not the other way around. Any new tool should demonstrate a clear added value and respond to a pre-defined need, gap or operational shortcoming.

Second, maintaining appropriate human oversight while harnessing efficiency gains from automation is critical. Law enforcement authorities need to distinguish between functions suitable for automation — such as data cleaning, scheduling and routine reporting — and those requiring human judgment, including consequential decisions related to personnel, discipline and case outcomes. Digital transformation is also fundamentally a cultural and leadership challenge: technology evolves faster than organizational culture, and sustainable innovation depends as much on trust, transparency and change management as on the tools themselves. Efficiency gains without accompanying additional ethical safeguards would merely be acceleration — technologies that make law enforcement more efficient should also make it more accountable.

Last but not least, high-quality data and well-designed processes are essential foundations for any successful optimization through digital technologies. Organizations must understand their own circumstances and realities before digital solutions can add value. Technology itself cannot fix fundamentally flawed workflows or compensate for poor, incomplete or irrelevant data. The more comprehensive and reliable the data, and the better designed the workflows, the greater the potential impact of automation on efficiency and effectiveness. At the same time, it should be acknowledged that more detailed data and improved workflows can increase transparency and accountability, but that this could also create or exacerbate sensitivities within an organization.

Innovating human resource management

Human resource (HR) management is among the most promising areas for digital transformation. AI and other digital tools offer opportunities to make recruitment, professional development, as well as actions to promote staff wellbeing more inclusive, compliant, effective and efficient. The digitalization of HR functions goes beyond increasing internal efficiencies and represents a strategic lever for integrity, inclusion and trust in law enforcement institutions.

At the same time, particularly in the case of AI, a clear legal basis and governance framework for its use in HR processes is essential — this applies to law enforcement agencies just as to any other organization. There needs to be a clear distinction between critical HR functions that should remain under human control and those that can be appropriately supported or automated through digital tools. Critical functions include, for example, personal interviews, subjective assessment and final selection decisions. Areas suitable for automation may include pre-screening of candidates, scheduling interviews, routine communication with candidates, and objective scoring. Computers may actually be more effective and efficient in such tasks, where automation can improve consistency and timeliness. This can in turn free up the capacity of HR staff for tasks that require more meaningful human interaction.

Talent acquisition

In recruitment, digital technologies — in particular AI — can support law enforcement authorities through several applications. These may include profiling candidates against defined role requirements, analysing previous recruitment outcomes to refine selection criteria, recording and analysing candidate interviews, and maintaining consistent and timely communication with candidates throughout the process.

An AI-supported system could be used to assist recruitment boards when interviewing candidates for demanding roles in law enforcement, for example. This could draw on a system trialled by some law enforcement agencies, which analyses responses during suspect interviews and suggests follow-up questions to investigators. AI tools could also be used to generate scenario-based exercises and provide more structured and comparable evaluations of the performance of different candidates. Furthermore, AI-powered recruitment assistants may be particularly valuable for automating routine "touch points" in HR processes where humans often lack time, helping avoid "ghosting" candidates and ensuring consistent and timely communication of key information to all applicants throughout the recruitment process.

Professional development

In the training domain, e-learning, virtual reality and scenario-based training are particularly promising applications of new technologies.

E-learning is already widely recognized as a way to make professional training and development for law enforcement practitioners more flexible, inclusive, accessible and scalable. While not all competencies can be developed through e-learning, foundational knowledge and skills education in many thematic areas can be effectively delivered digitally and provide a solid basis for more advanced and specialized in-person training.

Immersive virtual training environments can prepare officers for situations that would be difficult, dangerous or costly to recreate physically, such as crime scene management or responses to high-stress situations. When designed appropriately, such approaches can ensure compliance with the “do-no-harm” principle while still offering realistic and repeatable training experiences.

Gamification and serious gaming are also being used effectively for scenario-based professional training and development in

different thematic areas, including to identify specific skill gaps or performance issues that may require additional development or support.

Duty of care and staff wellbeing

Digital tools can support officers' wellbeing throughout their careers and help law enforcement authorities fulfil their duty-of-care responsibilities. For example, they can monitor indicators of stress and help HR professionals to proactively identify officers who may need psychological support, such as those who have attended multiple traumatic incidents within a short period or have been repeatedly exposed to high-stress situations. Such early-warning systems can help prevent, or enable earlier responses to, stress-related disorders and other similar challenges. Another useful application includes digital dashboards that help track and identify patterns in workload (e.g., excessive overtime), training completion or key career milestones. This can support both individual wellbeing and organizational retention strategies, provided that safeguards are in place to ensure appropriate use, confidentiality and oversight.

HR strategy and oversight

Digital innovation in HR provides an opportunity not only to streamline existing processes but to rethink how law enforcement agencies define workforce needs and recruitment priorities. The profiles required for modern policing are changing — many agencies increasingly need data scientists, analysts and other specialists with different mindsets and skill sets alongside traditional operational roles. AI-enabled analytics can help agencies interrogate their data and assess whether current recruitment and retention approaches are evidence- and needs-based or driven by inherited assumptions and perceptions. AI can also support oversight by identifying patterns that may indicate discrimination based on race, gender or other protected characteristics. Used responsibly, such approaches can help decision-makers detect and reduce bias rather than perpetuate it. However, any such use requires a clear legal basis, robust safeguards and meaningful human supervision.

Smarter strategic and operational planning

Strategic and operational planning is another area where digital technologies can have a transformative impact. Predictive analytics and automation can help law enforcement agencies optimize resource allocation, from shift scheduling and personnel deployment to budget planning and longer-term strategic forecasting. Used effectively, such tools can significantly increase both organizational efficiency and operational effectiveness.

Data quality and management

As noted above, high-quality data is a prerequisite for automating any process. In the context of resource allocation and planning it is particularly critical. Many law enforcement authorities struggle with incomplete, inconsistent or poorly structured data that would require significant time and capacity to clean and organize manually. Digital tools can make a substantial difference: some law enforcement agencies have used machine-learning techniques to support

data cleaning, turning previously unusable datasets into valuable resources for planning and optimization.

Given the volume and diversity of data generated today, it is also important to establish clear data management policies and practices. This remains a task for human process designers and managers, who need to define the full data lifecycle: first, strategic decisions on what data is needed; then how this data will be collected, stored and documented (including appropriate metadata); followed by analysis to extract actionable insights; and, finally, dissemination so that findings inform both operational decisions and future collection priorities. This cycle of improvement depends on deliberate strategic choices at each stage.

Once reliable data is available and an appropriate data management system is in place, digital tools can support optimization across a wide range of strategic and operational planning functions. At the same time, it is important to reiterate that workflows must be well designed before automation is introduced: technology cannot compensate for fundamentally flawed processes.

Operational optimization

Digital tools can optimize strategic and operational planning in many ways. One common application is the use of digital dashboards to provide near-real-time oversight of key performance indicators and organizational "health" metrics such as response times to incidents, case backlogs, workload distribution across units, overtime levels, budget execution, and the utilization of vehicles, equipment and other material resources. When designed thoughtfully, such dashboards can help leadership identify bottlenecks and emerging pressures early, enabling targeted interventions and more efficient resource allocation. At the same time, overreliance on performance indicators carries the risk of making organizations too rigid, potentially preventing them from adapting flexibly to evolving operational situations and environments.

Another potential application involves predictive modelling to support patrol planning and personnel deployment. Such tools may be particularly useful for certain offences where patterns are relatively stable and location-specific, such as burglaries, but may be less effective where patterns are weak, rapidly changing or predominantly digital. Many law enforcement agencies still operate through highly standardized routines. However, contemporary policing increasingly requires flexibility, as the police must respond to both traditional crimes and emerging threats, often requiring different skill sets and operational models. Digital tools can support this shift, but only if introduced in ways that preserve professional judgment and allow operational commanders to override model outputs.

Predictive models, by definition, depend on historical data and will therefore always contain imperfections and biases. Even so, they can be valuable tools to support decision-making, helping anticipate pressures, explore "what if" scenarios and plan proactively rather than responding after problems have escalated. A practical approach is to pilot or test AI-enabled models on historical data in a controlled environment, comparing model outputs with later known outcomes to assess accuracy and identify systematic errors before any operational deployment. However, in

many jurisdictions legal and regulatory constraints — including privacy and data-protection requirements — can limit the ability to reuse historical datasets for model development and testing. This underscores the importance of clear governance arrangements, privacy-by-design approaches and early engagement with legal and oversight bodies when exploring predictive or AI-enabled planning tools.

Workforce implications

Any discussion about optimizing resource planning inevitably raises questions about its impact on the law enforcement workforce. While there are concerns that AI could render some roles unnecessary, overall staffing levels are not expected to be negatively affected. Rather than causing widespread job losses, the integration of AI and automation is more likely to change how law enforcement work is carried out, leading some roles to evolve or staff to be reassigned. Budget constraints, rather than technological innovation, are currently a more significant factor in driving some police forces to reduce staffing numbers. Digitalization may simply help police maintain similar performance levels with fewer people.

What is undoubtedly changing is the profile of a police officer. The typical perception of the police focuses on uniformed officers, with all other roles seen as "back office". However, today's police IT teams may be as crucial for organizational effectiveness as uniformed officers. Agencies are increasingly recognizing that technology and operations are now inseparable, and some have responded by integrating IT into operational units rather than confining them to traditional IT departments.

More accurate and transparent monitoring and reporting

AI-enabled analytics and automated reporting tools can enhance the accuracy, consistency and efficiency of law enforcement documentation. There are four primary areas where AI can add value to monitoring and reporting: (1) augmenting insights by integrating data to generate a richer understanding; (2) improving operational efficiency by enabling users to receive answers to complex questions in moments rather than hours or days; (3) improving accessibility to information through user-friendly interfaces for interrogating both structured and unstructured data; and (4) enhancing decision-making by encouraging deeper exploration of data and prompting further investigation.

In addition, there are three key levers for the successful deployment of AI in law enforcement documentation: (1) capitalizing on opportunities through effective workflow management and scalable infrastructure; (2) continuous monitoring to track fairness and accountability metrics, incorporate user feedback and detect data anomalies; and (3) risk mitigation through systematic bias reduction, purpose limitation and appropriate levels of human intervention and oversight.

Experience from some OSCE participating States suggests that, while many tools perform well in small-scale pilots, they face challenges when scaled to larger datasets and more complex operational

environments. Maintaining value, accuracy and consistency at scale therefore requires ongoing monitoring, auditing and refinement. While AI can add particular value in the continuous review of standardized reports and reporting outputs, establishing clear parameters and governance standards remains a prerequisite.

Data silos and fragmentation

A significant challenge in automating monitoring and reporting functions is the fragmentation of information across law enforcement agencies. In many agencies, there are multiple report formats, inconsistent data structures and disconnected IT systems. In principle, AI-enabled agents could help address this challenge by locating, retrieving and compiling relevant information from wherever it is stored, allowing data to remain in separate systems while providing users with a more unified means to access what they need. In practice, however, this potential is often constrained by internal and external access restrictions. Questions of data ownership, legal authority and access permissions can significantly limit the ability of AI tools to bridge silos within law enforcement.

There are nonetheless useful parallels in other sectors facing similar constraints. In healthcare, for example, sensitive data can be processed through intermediary layers that enable analysis and operational use while reducing the risk of identifying specific individuals. While the contexts differ, the underlying challenges of confidentiality, fragmentation and strict access controls are comparable, and approaches such as privacy-by-design, role-based access and controlled data environments may offer relevant lessons for law enforcement.

Ultimately, bridging fragmented data landscapes requires more than just technical solutions. Common standards are a key enabler of interoperability and meaningful integration. In this regard, INTERPOL initiatives such as the Unified Information Model provide shared standards and typologies for different categories of police information and can serve as a reference point when developing or adopting new digital systems. Such harmonization efforts help ensure that data from different sources can be integrated and analysed in a consistent and reliable manner.

Balancing automation and human oversight

As in previous examples related to HR management, a clear distinction is needed between tasks that can be handled through autonomous processing and those that require human intervention. Suitable candidates for automation include, for example, comparative (delta) analysis between different versions of reports, drafting case summaries, compiling deadlines and key dates, and supporting workflow scheduling. Human involvement remains essential for decision-making and for the review of substantive reports before they are finalized or shared. The key is to define in advance which tasks can be safely delegated to automation and which must remain subject to human judgment and accountability.

In reporting, AI-enabled tools can be particularly useful as drafting and quality-assurance support. They can help ensure

that documentation is structured consistently, follows required templates, and includes relevant data and information in the appropriate format. This can free up time for those aspects of reporting that require professional interpretation, contextual understanding and judgement.

At the same time, digitalization can introduce new risks. Experience in one OSCE participating State following the implementation of a fully electronic case-file system illustrates how convenience can weaken oversight: managers began approving reports electronically without reading them in full and the overall quality of reporting declined. Technology may streamline processes, but it can also encourage complacency if control mechanisms are not built into workflows. Safeguards such as mandatory review steps for specific report types, audit trails and targeted quality checks, therefore need to be systematically embedded.

In some contexts, it may also be more effective to position such tools as "smart assistants" or structured checklists rather than emphasizing "AI" as such. Framing them as aids that support completeness, consistency and proper formatting may reduce resistance and misunderstandings compared to presenting them as autonomous systems — including in judicial contexts where the admissibility and reliability of documentation and evidence are subject to heightened scrutiny.

Evidentiary considerations

The question of how far to automate reporting and monitoring, and what level of human oversight is required, is closely linked to the type of algorithmic approach being used — and to whether its outputs can be explained and defended in administrative and judicial settings.

Important distinctions exist between deterministic and statistical tools, as well as between supervised and unsupervised methods. At a basic level, deterministic tools follow explicit, predefined rules: given the same input, they will produce the same output, and it is usually possible to trace the logic step by step. Statistical tools, by contrast, generate outputs based on patterns learned from data and typically produce probabilistic results (for example, many machine-learning models). Their outputs may vary depending on model design, training data and parameter settings, and the reasoning behind a particular result may be harder to reconstruct. For these reasons, deterministic tools are still preferred in many settings, particularly where it is necessary to demonstrate how conclusions were reached and to enable meaningful oversight.

Similarly, in supervised learning, it is generally possible to document how a system was trained and to describe, at least in broad terms, how outputs are generated and assessed against known examples. With unsupervised approaches, explainability is often more difficult, which can create challenges in law enforcement contexts where processes must be traceable, reviewable and auditable — including for evidentiary purposes.

In this context, the added value of AI in policing may lie less in replacing specialized tools and more in acting as an interface between them. An AI-enabled layer can allow an officer to ask questions through a single, user-friendly interface, while the system co-ordinates underlying databases and applications, retrieves

relevant information, and generates summaries or visualizations. Used in this way, AI can support discovery and analysis while responsibility for interpretation, decision-making, and the execution of standard policing steps remains with the human officer.

At the same time, evidentiary considerations are likely to become more prominent as AI-assisted reporting expands in the future. Potential court challenges — including questions about how much of a report reflects an officer's judgment versus AI-generated content — may become increasingly widespread. Clear documentation of any AI involvement in report preparation, together with the application of appropriate human review, validation, and audit trails, will be important to safeguard evidentiary integrity and maintain trust in reporting outputs.

Embracing a culture of change

If the adoption of new and emerging technologies in the organizational processes of law enforcement authorities is to be sustainable, it must be complemented by a comprehensive and deliberate process of organizational change management. As technology evolves faster than culture, the success of digital transformation depends as much on people and institutional norms as on the technologies themselves. Discussions focusing on digital innovations often lead to broader discussions about processes, ethics, return on investment, biases and other complex issues: in many ways, it represents a paradigm shift for law enforcement agencies.

Evolution not revolution

Lasting changes in policing will come through evolution rather than revolution. Different countries and agencies have varying levels of digitalization and IT capacity, and this diversity needs to be explicitly acknowledged and accommodated. Some countries are still working on the digitalization of case management systems, which constitutes a fundamental precondition for deploying AI and other automation tools. In such cases, support from international actors should focus on this foundational step, as only once these basic systems are in place can these countries benefit from the next stage of digital solutions. Managing expectations and being realistic about where organizations are in their digital evolution is essential.

When thinking about cultural change, transformation can also be also framed as a cultural evolution — a gradual process of adaptation rather than a dramatic break with the past. A shift from "knowing everything" to "being able to learn anything" reflects this evolutionary mindset. However, making people comfortable with accepting failures and learning from them represents a significant change in mindset, particularly in organizations where mistakes have traditionally been punished rather than viewed as learning opportunities. This is particularly true for law enforcement, where errors can have a serious and far-reaching consequences for victims, suspects, officers and the general public.

From pilots to scale

Experience suggests that the successful adoption of new digital solutions depends

primarily on three characteristics: user-friendliness, clear added value and readiness for operational use. If any of these elements is missing, uptake is likely to be limited and the solution risks remaining confined to pilot projects or niche use cases.

One practical approach is to rely on small, multidisciplinary development teams that work closely with operational units on an ongoing basis, building simple tools that solve concrete day-to-day problems. Such agile approach prioritizes solutions driven by operational needs rather than imposing top-down, generic solutions. This can build trust, shorten feedback loops and strengthen a shared understanding of operational requirements over time. Another model from the participating States with more decentralized law enforcement agencies is to establish dedicated mechanisms to share and distribute digital solutions across police forces.

Starting with proof-of-concept projects that demonstrate value on a small scale is recommended before broader rollout. Early "easy wins" can create momentum and confidence, while structured evaluations help identify what should be scaled, adapted or discontinued. The notion of "failing forward" reflects the reality that not all initiatives will succeed; learning from unsuccessful efforts can be as valuable as building on achievements. Embedding this approach often requires a cultural shift away from risk-aversion and towards a growth mindset that values experimentation and continuous improvement.

The role of leadership at all levels

Leadership is crucial for shaping institutional culture. Leaders at all levels must support good ideas so they can drive lasting change. Managers need to understand the strategic implications, while immediate supervisors play a critical role in shaping day-to-day practices and influencing how staff engage with new systems. The level of trust between supervisors and staff is often decisive a factor in determining whether the adoption of technology proceeds smoothly or encounters resistance.

At the same time, involving staff in the development and deployment process is equally important as people are more likely to use tools they have helped create. Analysts and operational officers require hands-on and sustained expertise with the tools they are being asked to use. Creating incentives for adoption and making new tools available through familiar and trusted interfaces can also help reduce resistance and foster ownership.

Digital transformation is fundamentally a values exercise — about what organizations *should* do, not just what they *can* do. The tools that make organizations more efficient must also make them more accountable. Innovation is sustainable only when it strengthens trust — both internally within institutions and externally with the public they serve.

Finally, effective implementation requires investment in both tools and the organizational capacity to use them. Many new and emerging technologies, including

AI, depend on a shared understanding of interdisciplinary collaboration across various domains. For law enforcement agencies shaped by traditional hierarchies and professional silos, this way of working can be unfamiliar and take time to embed, but it is a core part of successfully adopting new and emerging technologies, not an optional add-on.

Communication and interdisciplinary collaboration

As with leadership, how the adoption of new technologies is promoted and communicated — and who communicates it — can be as important as the technologies themselves. Credible messengers, clear messaging and carefully chosen entry points can all shape acceptance. Beginning with relatively uncontroversial use cases can help build trust and confidence, creating a basis for expansion into more sensitive domains once effectiveness and the meaningful application of safeguards have been demonstrated.

At the same time, greater precision in language is increasingly necessary. "AI" has become an overused and often ambiguous term in public discourse, frequently presented as a generic solution rather than a set of specific methods with particular limitations. Being explicit about what is meant — for example, distinguishing between rule-based automation, machine learning, predictive analytics and generative AI — helps anchor discussions in practical reality. Many techniques now discussed under the label of "AI", particularly machine learning, have existed for some time and have been used in policing in different forms for several years. Much of the recent surge in attention has been driven by the conversational AI chatbots that emerged in 2020-2021, but the underlying capabilities are the result of incremental and cumulative development rather than a single sudden breakthrough.

Challenges

While new technologies offer significant opportunities for law enforcement to enhance organizational processes, successfully harnessing them requires the systematic identification of cross-cutting challenges:

- **Data quality and fragmentation:** Many agencies struggle with poor-quality historical data dispersed across multiple systems in different formats. Without significant investment in data cleaning, validation and harmonization, AI systems cannot deliver their potential value in producing complex and comprehensive business intelligence and may generate misleading results.

- **Starting with technology rather than problems:** Organizations too often invest in new technologies and then try to find applications for them. A problem-first approach, clearly defining what needs to be solved before selecting tools, leads to better outcomes.

- **Public-private expertise gap:** Salary differentials between public sector agencies and private technology companies make it difficult to recruit and retain staff with advanced technical skills. The profile of police personnel needs to evolve to include more data scientists, analysts and other digitally skilled professionals.

- **Regulatory compliance and legal basis:** The continually evolving regulatory environment creates uncertainty about permissible uses of AI. Clear legal frameworks for AI use in personnel decisions and internal processes are essential to create certainty and institutional confidence, and ensure compliance and adherence to human rights standards. One example is the European Union's AI Act, which is being used as a baseline by the EU member states for further decisions about development and deployment of AI in specific sectors, including law enforcement.

- **Organizational culture and stigma:** There is a stigma around AI in many organizations, with the default reaction being to focus on risks rather than opportunities. Traditional police culture may resist technological change that threatens established practices.

- **Balancing rigidity and flexibility:** Police forces often operate rigidly, but contemporary challenges require flexibility. Performance indicators and automated systems can make organizations more efficient, but also more rigid and less able to adapt to unexpected situations if not carefully designed and governed.

- **Different levels of digitalization:** Countries and agencies are at very different stages of digital development. For many, basic digitalization of case management and criminal justice systems must precede any deployment of AI. Expectations must be managed carefully and realistically.

- **Investment in enabling structures:** Digital transformation requires sustained investment in ICT and other enabling functions that may be targeted for cuts during budget constraints. Benefits take time to materialize, making it difficult to secure long-term commitment.

- **Complacency and quality control:** Technology can improve processes but also lead to reduced human attention. Checks must be built in to prevent technology from enabling laxness and exacerbating automation and confirmation bias.

Addressing these challenges requires not only technical solutions, but also strategic planning, institutional learning and a sustained commitment to responsible, rights-based innovation.

Conclusion and policy recommendations

Harnessing new technologies to streamline organizational processes offers significant opportunities for law enforcement agencies to become more efficient, effective, transparent and accountable. However, realizing these benefits requires careful attention to governance, ethics and change management. What matters most is clearly identifying the problems to be addressed and selecting the appropriate tools for those needs, not all of which necessarily involve AI. Being nuanced and precise about different types of technology, and avoiding treating AI as a generic silver bullet, helps ground policy discussions in operational and institutional realities.

The human element remains central. Human-in-the-loop approaches, both in setting narratives and in overseeing outputs, are essential for responsible deployment. Leadership and trust are critical for implementing new tools and processes, and organizations must create enabling environments that support innovation while maintaining consistency and effective oversight, and minimizing risk. Adoption of technology represents a cultural evolution rather than revolution, a paradigm shift that affects institutional processes, ethics standards, accountability framework and professional identities far beyond the technologies themselves.

In this context, law enforcement actors from the OSCE participating States could consider the following policy recommendations.

Strategic planning

- Begin with a clear problem definition: determine what needs to be solved, why and for whom, before selecting technological solutions. Avoid investing in technologies and then trying to find a practical application for them.

- Conduct comprehensive assessments of existing data quality, systems and processes, recognizing that digitalized and interoperable systems are preconditions for AI deployment. For agencies still at the early stages of digitalization, focus on foundational digital reforms before pursuing AI applications.

- Establish clear frameworks for AI use in personnel decisions and internal processes, ensuring compliance with applicable employment law, data protection requirements and international human rights standards.

- Define the appropriate balance between AI autonomy and human oversight for different types of decisions, reserving critical decisions such as hiring, discipline and selection for human judgment while automating routine for standardized tasks.

- Invest in systematic improvement of data quality, including automated data cleaning and establish strategic data collection priorities with appropriate metadata standards.

Training and capacity-building

- Evolve the profile of police personnel to include data scientists, analysts and other digitally skilled staff, alongside traditional operational officers.

- Invest in AI literacy programmes for personnel at all levels, ensuring that users understand both the capabilities and limitations of different types of AI tools, including the distinction between deterministic and statistical approaches.

- Leverage virtual reality, gamification and scenario-based training to prepare officers for complex situations while ensuring compliance with do-no-harm principles.

- Develop unified e-learning platforms that can serve multiple agencies, including across borders, enabling them to share resources and ensure consistent approaches.

- Promote interdisciplinary collaboration between IT specialists, legal experts, ethicists and operational personnel through integrated team structures.

Change management

- Frame digital transformation as an evolutionary process rather than a revolutionary one, recognizing that organizations are at different stages of digital maturity and that gradual adaptation is often more sustainable than abrupt change.
- Start with low-risk and clearly defined applications to build policies, experience and trust, then gradually expand to more complex or sensitive areas.
- Involve staff at all levels in the development process and create incentives for adoption, recognizing that people are more likely to use tools they have helped create.
- Foster a growth mindset that embraces experimentation and views failure as a learning opportunity, moving from "knowing everything" to "being able to learn anything."
- Develop agile IT departments with small teams working closely with operational units to develop simple, useful tools that respond to real needs.

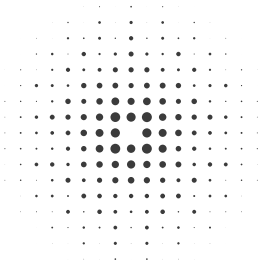
Governance and oversight

- Establish human rights-by-design principles, embedding ethical considerations into technology development and deployment from the earliest stages.
- Implement robust audit mechanisms for AI systems, including regular assessment of bias, accuracy and operational impact, with particular attention to preventing complacency as processes become automated.
- Develop clear internal policies and shared glossaries to ensure a common understanding of AI terminology, capabilities and governance requirements.
- Prepare for potential judicial scrutiny by establishing transparent documentation of AI involvement in reports and ensuring human review of all critical outputs, building toward judicial acceptance through gradual validation.
- Use AI-supported tools, where appropriate, to assist in detecting potential bias or discriminatory patterns in human decision-making, thereby strengthening oversight and accountability across both automated and non-automated processes.

Communication and trust-building

- Be transparent about what AI is used for and, equally importantly, what it is not used for, proactively addressing assumptions that may not align with reality.
- Conduct public research on attitudes toward AI in different policing contexts, calibrating communication strategies to public concerns and expectations and to inform communication approaches.

- Maintain the human factor in policing, recognizing that public trust often depends on human connection and communication — particularly keeping victims informed about their cases.



Co-operation

- Engage in multi-stakeholder dialogue among law enforcement, government, academia, the private sector and civil society to share experiences, lessons learned and emerging practices.

- Learn from other sectors facing similar challenges, such as healthcare, which have developed approaches to data-sharing and AI deployment under comparable confidentiality requirements.

Further reading

European Commission (2026): AI Act, https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

INTERPOL and UNICRI (2024): Toolkit for Responsible AI Innovation in Law Enforcement, https://unicri.it/Publication/Toolkit-for-Responsible-AI-Innovation-in-Law-Enforcement-UNICRI-INTERPOL

Accountability Principles for Artificial Intelligence, https://ap4ai.eu/

Organization for Security and Co-operation in Europe