




Organization for Security and
Co-operation in Europe

THE USE OF NEW & EMERGING TECHNOLOGIES FOR **CRIME** **INVESTIGATIONS**

SUMMARY PAPER FROM AN EXPERT ROUNDTABLE
DISCUSSION AT THE SECURITY & POLICING EVENT,
UNITED KINGDOM (11-12 MARCH 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 2025

All rights reserved. The contents of this publication may be freely used and copied for educational and other non-commercial purposes, provided that any such reproduction be accompanied by an acknowledgement of the OSCE as the source.

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	2
Criminal investigations transformed	2
Expanding sources of investigative leads and evidence	3
Revolutionizing investigative methods	3
Increasing productivity and efficiency	4
Avoiding innovation overload	5
Overcoming risk aversion	5
Rethinking training and skills development	6
Breaking down internal silos	7
Co-operation - the indispensable element	7
Public-private partnerships	8
Data sharing	8
The (changing) role of international co-operation platforms	9
Pacing the law	9
From analogue to digital	10
Regulating change	10
From capability to responsibility	11
Conclusion and policy recommendations	11

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

(TNTD/SPMU) 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 second round table, which was dedicated to the use of new and emerging technologies for crime investigations and took place in Farnborough, United Kingdom, on 11 and 12 March 2025. The round table was organized in co-operation with the United Kingdom Home Office and took place on the margins of the Security & Policing 2025 event.

Criminal investigations transformed

Nearly all criminal activities today involve a digital component, from drug traffickers using encrypted communication channels to arrange shipments and people smugglers advertising their services online to burglars monitoring the social media accounts of their potential victims. Law enforcement authorities across the world have embraced a broad range of new digital tools and techniques to adapt to this evolving criminal landscape, in turn reshaping criminal investigations. From a strategic perspective, the impact of digital technologies on criminal investigations is particularly notable in the following three main areas.

Expanding sources of investigative leads and evidence

Investigators are confronted with myriad devices and platforms which generate data that can be used for investigation purposes. They can range from laptops, smartphones and watches to home router traffic, IoT sensors in a household, Wi-Fi-enabled home appliances and data recorded by a car. All of these examples have previously been used in investigating serious crimes in various participating States across the OSCE. Experience shows that such data can often provide critical insights into the sequence of events, establish connections between suspects and criminal activity, corroborate witness statements or offer new avenues of inquiry. Its timely and lawful collection and analysis not only enhance investigative effectiveness, but are increasingly indispensable for building strong, evidence-based cases in court.

As people increasingly use online services and platforms in all aspects of their daily lives, they leave behind digital traces that can be leveraged for investigative purposes. Open-source intelligence (OSINT) has become an important part of the law enforcement toolbox, often complementing other traditional sources of investigative leads and evidence. While OSINT poses its own challenges, especially with regard to reliability and verifiability, the wealth of available data and information — and the speed with which they can be obtained — significantly enhances investigative effectiveness and contributes to building a robust evidentiary base for subsequent prosecution.

Digital technologies also allow law enforcement to involve the public in ongoing investigations in a more meaningful way by crowdsourcing investigative leads. By engaging the public, investigators can collect valuable tips, leads or evidence that might otherwise remain undiscovered. Whether it involves identifying suspects from surveillance footage, locating missing persons or tracking stolen property, crowdsourcing can mobilize community support and expand investigative reach. When used responsibly and with proper safeguards, crowdsourcing investigative leads can enhance public trust and participation, while supplementing traditional investigative methods with local community knowledge and insights.

Revolutionizing investigative methods

As most contemporary crimes include a digital component, the ability to harness digital evidence has become a core competence for law enforcement. Digital forensics is emerging as a cornerstone of modern criminal investigations, playing a similarly transformative role as the advent of fingerprint or DNA analysis did in the past. Just as DNA revolutionized the ability to link individuals to crimes with scientific precision, digital forensics enables investigators to recover, analyse and interpret electronic data to reconstruct events, uncover hidden connections and support evidentiary chains. In an era where most human activity leaves a digital footprint, digital forensics provides essential tools for uncovering the truth, strengthening cases and ensuring accountability.

Another area where the impact of modern technologies is transformative is the ability to quickly process large amounts of data through AI-enabled applications. Examples of AI being successfully employed during investigations include the automated analysis of CCTV footage and the processing of large datasets generated from the interception of encrypted communications between criminals. AI-based tools can support the interpretation and use of this data in investigations in a fraction of the time required for manual analysis. However, human verification is still needed to identify and mitigate potential bias in AI models. Currently, there is no international legal or policy framework to ensure transparency in the use of AI in investigative work. The large-scale deployment of AI in criminal investigations will necessitate mechanisms to follow AI reasoning and audit trails as they arrive at outputs.

Digital technologies are also transforming how crime scenes are documented and analysed. Using precision laser scanners, investigators can create highly detailed and accurate three-dimensional (3D) digital replicas of crime scenes, preserving spatial relationships, measurements and visual perspectives exactly as they were at the time of discovery. These reconstructions allow investigators, prosecutors and even juries to virtually revisit the scene, analyse trajectories or test hypotheses without being physically present. 3D scanning not only enhances the quality and integrity of crime scene documentation, but also reduces the risk of evidence being lost, altered or misinterpreted over time, making it a powerful tool in complex or large-scale investigations.

Increasing productivity and efficiency

The use of digital technologies can significantly reduce duplication of efforts and increase productivity in policing work. By digitizing workflows, automating repetitive tasks and enabling real-time data sharing across departments, law enforcement agencies can avoid redundant investigations, streamline case management, improve operational planning and make more informed decisions. For instance, centralized databases and automated case-tracking systems allow officers to see if similar cases are already under investigation elsewhere, saving valuable time and resources. They can also help to identify links between cases that may not otherwise be discovered.

Another prospective use case is the deployment of local AI agents trained on specific datasets (such as guidelines, manuals, legislation or case files) to provide practical guidance and advice to investigators, especially on technical matters. The deployment of such agents is currently being tested in the field of digital forensics, for example. Although the large-scale use of AI in live investigations will likely remain limited for the foreseeable future due to concerns about the integrity of evidence, its potential to serve as a “smart” technical assistant or adviser could significantly increase the productivity of individual investigators.

Ultimately, digital technology can help to shift policing efforts from manual, fragmented processes towards more co-ordinated, efficient and intelligence-led operations.

Avoiding innovation overload

While digital innovation presents enormous opportunities to enhance the effectiveness and efficiency of criminal investigations, it also presents significant challenges. Innovation in this context goes beyond the adoption of new tools — it requires a fundamental re-thinking of policing approaches, including the adaptation of organizational structures, procedures and institutional culture. Law enforcement authorities must continue to carry out labour-intensive activities across a wide range of policing services while simultaneously innovating to meet the demands of the shifting criminal landscape. In practice, the ideal of a smooth innovation process often clashes with the everyday reality of established practices, competing interests and reluctance to change.

Successful innovation requires a joint effort, willingness to learn and the acceptance that setbacks and failures are part of the journey. It is rarely a linear process and usually starts with a need to tackle a common problem rather than with a well-thought-out long-term strategy. When considering digital innovation in the context of criminal investigations, three areas deserve particular attention:

Overcoming risk aversion

Risk aversion is common in public sector settings and law enforcement is no exception. Police organizations are — for good reason — traditionally structured to minimize risk, ensure accountability and avoid errors. While such an approach is understandable given the need to maintain confidence in police work and

public trust, it can stifle innovation and slow down the adoption of new technologies. The assessment of risks associated with employing novel technologies is a major factor for law enforcement authorities in deciding whether or not to use them. Many officers and decision makers are hesitant to try unfamiliar tools or methods, fearing potential legal, operational or reputational consequences.

While responsible and robust risk management has to remain a priority for any law enforcement authority, it is important to ensure that risk avoidance does not become an inhibitor of necessary innovation. This requires building an institutional culture that encourages learning, tolerates controlled failure and rewards problem solving. This includes creating safe environments for testing new approaches, investing in pilot projects and promoting leadership that understands that not every risk is a threat — some are opportunities for progress. Too often, it is only tragic security incidents or failures that trigger the cultural shift necessary for innovation.

One example of risk aversion in law enforcement is a bias towards using established commercial tools. This is often due to their wide-spread popularity, which then translates into greater acceptability during criminal trials. Yet, in an environment of scarce resources, law enforcement officers increasingly need to rely on community-developed open-source solutions or even self-programmed tools to replace or complement the functionality of expensive commercial tools. Despite the greater potential to examine and audit the open code of such tools, there is often hesitancy to deploy them widely, as they are considered not

sufficiently tried and tested, and so more susceptible to legal challenges in a courtroom setting.

In principle, the scientific method should guide assessments of the impact and reliability of evidence and output emanating from the application of new technology-driven tools by observing replicability and verifiability of results in similar cases.

Rethinking training and skills development

Technology can significantly amplify the effectiveness of criminal investigations, but it cannot replace the need for sound investigative reasoning and methods. Investigators must continue to operate with a clear understanding of the investigative process, while developing new skills to navigate an evolving digital landscape. As the volume and complexity of digital evidence increases, specialized training will become essential for all officers involved in criminal investigations so they can operate effectively in a technology-driven investigative environment.

Currently, many law enforcement agencies still rely solely on digital forensic specialists to handle anything related to digital technologies, which risks overburdening a limited pool of experts and creating bottlenecks in investigations. Instead, frontline officers and investigators need to be equipped with basic digital competencies — such as identifying, securing and preserving digital evidence during searches or arrests — so they can serve as digital first responders. They also need to be able to conduct simple tasks (for example, checking a Bitcoin address) so specialists can focus on more complex activities, such as recovering deleted data from a seized

hard drive.

While the knowledge and skills required for investigative roles will differ from technical roles, a fundamental understanding of digital technologies and a minimum level of digital skills is becoming a key competency. Continuous upskilling must be thus embedded into the professional development and career progression of all law enforcement personnel involved in investigations to ensure that their capabilities evolve in line with the technologies they encounter. The curricula of police academies also need to reflect this shift by integrating practical digital skills and digital forensic awareness into basic police training.

Given the complex nature of digital technologies and their continuous evolution, a structured and systematic approach to updating professional training and development is essential. Rather than relying on ad hoc or one-size-fits-all training courses, law enforcement agencies should develop training competency frameworks that clearly define who needs to know what, at which level and in which role. Such frameworks help to identify the specific competencies required for different functions — from frontline officers securing digital evidence to specialists conducting digital forensic examinations. By developing training programmes in line with these defined competencies, law enforcement agencies can better allocate resources, track progress and ensure that personnel are equipped to meet evolving operational demands in a consistent and sustainable manner.

Breaking down internal silos

The digital transformation necessary to address current and emerging security threats requires both a general understanding of technological change and a fundamental rethinking of established policing practices and processes. In many cases, however, law enforcement authorities tend to think about technological progress in terms of specific tools and not as a profound change to the environment in which they operate.

This narrow perspective is often reinforced by organizational silos, where units and departments operate in isolation, with limited communication or collaboration across domains. Such structures hinder the flow of information, reduce operational efficiency and obstruct innovation. Officers may be hesitant to adopt new technologies or approaches simply because they fall outside their familiar mandate or perceived area of responsibility. In some cases, technical experts want to retain control over specialized knowledge and tools, unintentionally creating dependency and limiting wider institutional learning.

At the same time, the growing complexity and volume of digital evidence in most types of crime make it clear that traditional investigative methods based solely on manual work are no longer sufficient. Even if law enforcement authorities had the resources to significantly expand the number of investigators, this would not address the problem. What is needed is a strategic combination of skilled personnel and increased automation. Automation can help to process large volumes of routine data and streamline repetitive tasks, freeing up investigators to focus on higher-value analytical work.

To be effective, automation must be implemented in a scalable, reproducible and legally sound and rights-respecting manner.

Breaking down silos requires a cultural shift towards networked collaboration, where expertise is shared, cross-functional teams are encouraged and problem solving is approached collectively. It calls for more integrated collaboration between operational units and technical specialists (such as digital forensic experts, data analysts and other IT professionals) to identify solutions that can be scaled across different cases and contexts and where human and technological capacities complement one another. Innovation must be seen not as the responsibility of a few individuals or departments, but as a shared institutional goal. Only by creating structures that support interdisciplinary co-operation, invest in scalable processes and foster a culture of openness and knowledge exchange can law enforcement agencies meet the demands of modern criminal investigations.

Co-operation — the indispensable element

In addition to embedding a culture of internal collaboration, effective co-operation with external public and private actors is increasingly essential to all law enforcement functions — ranging from public order and criminal investigations to highly specialized services. To carry out their duties, law enforcement authorities must engage with the public, other criminal justice authorities at all levels,

public institutions and the private sector. Trust remains a cornerstone of effective partnerships, especially in the context of policing and criminal justice.

Public-private partnerships

With digital components now common to most, if not all, crimes, law enforcement authorities need to further strengthen their co-operation with private sector actors. Technology companies, in particular, are key partners, as the platforms and tools they provide are often exploited by criminals.

Public-private partnership models are increasingly prevalent, offering structured platforms through which law enforcement can engage with key stakeholders. While such forums already exist at the international level in areas such as cybercrime and economic and financial crime, they hold potential for application across a wider range of crime types and industries. These partnerships enable law enforcement and private sector actors to build trust, establish protocols and formalize co-operation in a consistent framework. They can also serve as catalysts for innovation in policing.

Above all, public-private partnerships facilitate communication. Law enforcement agencies conducting complex investigations often need to access data from private entities. Engaging in strategic dialogue — both in the context of individual cases and broader operational needs — helps to foster mutual understanding and more effective collaboration. In some cases, law enforcement authorities may need to engage external experts to supplement internal capacity, particularly for very specialized or large-scale investigations. While such partnerships can be valuable, they must be underpinned by robust

vetting procedures and trust-based frameworks to safeguard the integrity of investigations and protect sensitive data. Building a balanced, scalable model for digital expertise — both internal and external — is key to sustaining investigative effectiveness in a rapidly changing technological environment.

Data sharing

The growing importance of digital evidence in modern investigations has, in theory, made data sharing faster and more straightforward. At least at the level of police-to-police co-operation, the shift towards digitalization has the potential to reduce reliance on lengthy legal procedures, allowing investigators to focus more on operational (cross-border) co-operation and joint activities — an area that is consistently growing in importance as crime becomes ever more transnational. However, in practice, there are still many challenges in accessing digital data held by third parties, especially if they are based in a foreign jurisdiction.

In many OSCE participating States, law enforcement agencies have long-standing relationships with certain data-holding entities such as Internet service providers, social media platforms or file-hosting services. Yet, the digitalization of daily life now means that entirely new categories of actors — such as car manufacturers or producers of IoT devices — also generate data that may hold investigative value. It is, therefore, imperative for law enforcement to expand their engagement with the private sector to include these actors. In some OSCE participating States, requesting digital evidence from private entities is still relatively novel and law enforcement agencies lack the institutional and procedural

framework, and practical experience, for obtaining such data.

From the perspective of private companies, data sharing with law enforcement can often feel one-sided, as they respond to requests but receive little feedback in return. Establishing feedback loops can improve motivation and mutual understanding, helping companies see how their data contributes to public safety. These exchanges may even inform product design and lead to improvements that benefit both public and private actors. The private sector can and should be encouraged to invest further in law enforcement co-operation by emphasizing social responsibility and highlighting the tangible value of their contributions.

While data protection is sometimes viewed as an obstacle to co-operation by law enforcement actors, well-defined and comprehensive data protection frameworks can in fact facilitate information sharing. By providing clear legal boundaries and a shared understanding of what is permissible, robust human rights frameworks help both law enforcement and private actors operate with greater confidence and accountability.

The (changing) role of international co-operation platforms

International law enforcement co-operation stands to gain considerably from the use of digital technologies. These tools can help to deconflict investigations, enhance cross-border data sharing, support operational co-ordination and streamline communication between agencies. International conventions such as the Council of Europe's Convention on Cybercrime and the United Nations Convention against Cybercrime provide common definitions, frameworks and

principles that help to harmonize procedures and manage expectations across jurisdictions. These instruments offer a shared language that is especially useful when law enforcement authorities engage in cross-border investigations.

International organizations such as INTERPOL, UNODC, the Council of Europe and the OSCE have a valuable role to play — not only by supporting co-operation, but also by promoting innovation through the exchange of good practices and success stories, including with regard to public-private partnerships. By serving as platforms for dialogue and joint capacity-building, they can help to avoid duplication of effort and ensure that lessons learned in one country benefit others. They can facilitate more equitable access to new technologies, especially for countries with limited resources and, in doing so, support a more balanced and collaborative innovation ecosystem that strengthens collective security and distributes the burden of innovation in the law enforcement sector.

Pacing the law

Investigative work is strictly regulated and governed by an ever-expanding body of legislation and case law, which determine practices, standards and requirements. The types of evidence generated through criminal investigations and used in criminal trials are evolving in line with technology. For instance, whereas phone call interceptions used to be a valuable source of evidence in high-profile organized crime prosecutions, criminals now share key information through encrypted online calls and messaging applications. This shift has profound

implications for investigators, who must now navigate more complex and decentralized digital environments to uncover evidence.

From analogue to digital

In many jurisdictions, digital evidence is still largely covered by the legal regimes established to regulate the use of physical evidence, with rules being applied by analogy. While this approach offers a degree of continuity, it fails to recognize the unique characteristics of digital evidence — such as its volatility, replicability and the difficulty of assigning clear jurisdiction. The transnational nature of digital evidence, where data is often stored on servers in multiple countries, presents further legal and procedural challenges.

To address these gaps, tailored legal provisions are needed to ensure clarity and consistency in how digital evidence is identified, collected, stored and used. Codifying key standards in national legislation — such as ensuring that digital evidence is gathered in a manner consistent with human rights and procedural safeguards — would contribute to greater legal certainty. At the same time, the principle of proportionality, which governs the use of physical evidence, must remain a guiding standard when dealing with electronic evidence. The scale and accessibility of digital data should not justify unnecessary or excessive intrusion into individuals' rights.

Many OSCE participating States, in particular those which are parties to the Council of Europe's Convention on Cybercrime, have already integrated procedures to use digital evidence in their criminal procedural codes and introduced relevant safeguards. Others are only

beginning this process.

Regulating change

Effectively regulating the use of emerging technologies — particularly AI — in criminal investigations and proceedings is one of the most pressing challenges facing criminal justice systems. While excessive regulation can risk stifling innovation, the absence of clear legal frameworks is equally problematic. Well-designed regulation provides transparency, protects fundamental rights and builds public trust. Legal safeguards can help to ensure that data collection and processing are limited, proportionate and driven by legitimate investigative needs. In addition, clear legal rules should enshrine privacy rights and offer whistleblower protections to encourage accountability and prevent abuse in digital investigations.

Developing legal and procedural frameworks for AI will also require establishing robust oversight mechanisms to monitor and guide its use — particularly in high-stakes settings such as law enforcement and criminal justice. Human oversight must be embedded into AI-enabled processes to ensure accountability and prevent over-reliance on opaque or unverified systems. Oversight bodies must be vested with sufficient authority, independence and resources to enforce compliance, akin to the regulatory models seen in the financial sector. Moreover, oversight should be proactive — anticipating potential misuse or systemic flaws, rather than reacting only after problems occur.

Regulation and oversight need to be complemented by practical knowledge within the justice system. One key aspect is ensuring that legal practitioners

understand how AI systems function, including the logic that drives their outputs and the risks they may pose for human rights and the rule of law.

From capability to responsibility

Ethical considerations have always been a core element of responsible policing, and their importance is only growing in the digital age. As law enforcement authorities gain access to increasingly powerful tools and vast volumes of data, they are confronted not only with the question of what they are legally permitted to do, but what they should - and should not - do. The mere availability of a technological capability does not automatically justify its use. Investigators and regulators alike must carefully weigh the potential benefits of a given tool against its impact on privacy, fairness and public trust.

At the same time, ethical questions also arise in cases where available technologies are not used, whether out of fear, inertia or institutional reluctance. When digital tools could significantly assist in preventing harm or solving serious crimes, inaction or the deliberate choice not to deploy them can carry their own consequences, particularly when lives and fundamental rights are at stake. Law enforcement agencies must, therefore, navigate a complex ethical landscape, balancing necessity and proportionality with transparency, accountability and respect for individual freedoms. To support this, clear guidelines and regular human rights training should become an integral part of digital transformation strategies in policing.

Conclusion and policy recommendations

The digital transformation is reshaping criminal investigations, offering unprecedented tools for increasing effectiveness and efficiency while raising operational, legal and ethical challenges. Digital technologies, including AI and big data analytics, are becoming indispensable, yet their use demands careful balancing between investigative efficacy and fundamental rights. Three key insights from the roundtable discussions are:

- **Adaptation is ongoing:** Investigations will continue evolving alongside technology, requiring agility in skills, co-operation and regulation.
- **Human oversight is critical:** While modern technologies such as AI can enhance efficiency, transparency and accountability mechanisms must safeguard against bias and overreach.
- **Collaboration is key:** Strengthening partnerships between law enforcement, the private sector and international bodies is essential to address cross-border and technical complexities.

Successfully navigating this landscape requires policymakers and practitioners to prioritize frameworks that harmonize innovation with rights protection, ensuring technologies serve justice without compromising public trust. In this context, OSCE participating States could consider the following policy recommendations.

Organizational management

- Promote a culture of innovation within law enforcement agencies that encourages experimentation, tolerates controlled failure and rewards problem solving.
 - Break down institutional silos by fostering interdisciplinary collaboration between operational units, digital forensic experts, data analysts and other law enforcement IT professionals.
 - Introduce dedicated innovation or digital transformation units within police agencies to identify, test and scale new technologies and methods, including in a controlled operational environment.
 - Develop scalable and reproducible investigative workflows that combine human expertise with automation to handle growing volumes of digital evidence.
 - Encourage leadership at all levels to champion adaptive change and lead by example in adopting new technologies and approaches.
- Include basic digital competencies and digital forensic awareness into core police training curricula for both basic police training and further professional development, equipping all officers to act as digital first responders.
 - Develop continuous upskilling programmes, including in partnership with academia and technology companies, to ensure that investigators keep pace with evolving technologies.
 - Promote interdisciplinary training that brings together law enforcement personnel, legal practitioners and technology experts to enhance mutual understanding and knowledge sharing.

Co-operation

- Expand and formalize public-private partnership frameworks, including with non-traditional actors such as IoT providers, car manufacturers and cloud service platforms, to streamline data sharing, with clear protocols for privacy and accountability.
- Establish feedback loops to inform private sector partners about how their co-operation supports investigations, building motivation and trust.
- Encourage joint pilot projects between law enforcement and private sector/academic institutions to co-develop solutions tailored to real investigative needs.

Skills and training

- Develop structured training competency frameworks for criminal investigations in the digital age that define skill requirements for different law enforcement roles.
- Develop dedicated strategies — or adapt existing training strategies — to integrate digital skills and awareness at all levels of law enforcement training and education. Such strategies should aim to:

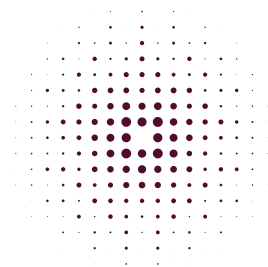
- Utilize international co-operation platforms and organizations to distribute the burden of innovation in the law enforcement sector by actively engaging in joint capacity-building and exchange of experiences and lessons learned.
- Explore opportunities for joint international projects to share the burden of developing and piloting AI technologies for use in criminal investigations.

Regulation

- Develop or refine national legal frameworks for the collection, handling and admissibility of digital evidence, ensuring consistency with human rights standards and alignment with relevant international standards and conventions.
- Introduce clear legal provisions governing the use of AI in investigations, including criteria for transparency, human oversight and auditability.
- Design data protection frameworks that support, rather than hinder, responsible data sharing within law enforcement and between the police and the private sector through clear procedures and safeguards.
- Promote the development of standardized legal agreements and procedures to facilitate cross-border access to digital evidence and data.

Human rights and oversight

- Establish guidelines for the human rights-compliant use of new and emerging technologies in criminal investigations, grounded in necessity, proportionality and fairness.
- Create and/or strengthen independent oversight bodies with the mandate and resources to monitor AI and other high-impact technologies used in policing.
- Integrate regular human rights and ethics training into law enforcement professional development programmes to build awareness of potential ethical dilemmas and responsible decision-making.
- Promote transparency in how digital tools and data are used during investigations to maintain public trust and accountability.
- Strengthen whistleblower protections and internal reporting mechanisms to ensure accountability in cases of misuse or overreach in digital investigations.
- Share experiences of effective strategies for ensuring human rights compliance in technology-facilitated investigations and discuss challenges and lessons learned in this area.



Further reading

EU Agency for Fundamental Rights (2019):

Facial recognition technology: fundamental rights considerations in the context of law enforcement,

<https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law>

EU Agency for Fundamental Rights (2022): *Bias in algorithms - Artificial intelligence and discrimination,*

<https://fra.europa.eu/en/publication/2022/bias-algorithm>

Council of Europe (2024): *HUDERIA - Risk and Impact Assessment of AI Systems,*

<https://www.coe.int/en/web/artificial-intelligence/huderia-risk-and-impact-assessment-of-ai-systems>

Europol (2024): *AI and Policing: The Benefits and Challenges of Artificial Intelligence for Law Enforcement,*

<https://www.europol.europa.eu/cms/sites/default/files/documents/AI-and-policing.pdf>

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>

Europol (2025): *AI bias in law enforcement - A practical guide,*

[https://www.europol.europa.eu/cms/sites/default/files/documents/AI bias in law enforcement - practical guide.pdf](https://www.europol.europa.eu/cms/sites/default/files/documents/AI%20bias%20in%20law%20enforcement%20-%20practical%20guide.pdf)

Accountability Principles for Artificial Intelligence,

<https://ap4ai.eu/>



Organization for Security and
Co-operation in Europe