MINISTÈRE
DE L'INTÉRIEUR
*Liberté*
*Égalité*
*Fraternité*

# *The impact and challenges of artificial intelligence* **for Gendarmerie type forces**

# *Edito*
# DGGN

Dear readers,

As Director General of the French National Gendarmerie and President of FIEP, I am honoured to introduce this final report on «Impact and challenges of artificial intelligence for gendarmerie-type forces».

In today's complex and interconnected threat landscape, the mission of protecting citizens entrusted to police forces has become a major challenge. This renewed requirement demands rapid response capabilities, constant adaptation, accurate risk anticipation, and, above all, innovation.

It is in this context that artificial intelligence (AI) is now emerging as an unavoidable revolution, offering unprecedented opportunities to meet these strategic challenges.

This report is the result of contributions from a panel of experts from FIEP member countries. Innovative in several areas, this work compares the experiences, visions, and challenges specific to each force. It illustrates how artificial intelligence is no longer a distant prospect or science fiction, but a concrete reality that is already transforming the practices and strategies of our institutions.

As we face rapid change, AI requires visionary leadership based on in-depth knowledge and genuine agility, in order to guarantee greater stability. It is in that regard paramount to prevent the risk of misuse from a techno-centric approach.

Through the various committees that make up the FIEP, experts approached this discipline from a variety of angles: the impact on human resources, regulatory frameworks, logistics, internal organization, and also the threats posed by the malicious use of AI by criminals. They also identified the concrete opportunities that this technology can offer to strengthen the effectiveness of law enforcement, improve public safety, and anticipate future developments.

Under the impetus of the French presidency of the FIEP, this initiative demonstrates the incomparable strength of international cooperation promoted by the FIEP. By sharing our knowledge and leaming from each other, we are strengthening our collective ability to make informed decisions, adopt the most relevant technologies for the immediate future, and prepare our institutions to meet the challenges of tomorrow.

Artificial intelligence, far from being a mere trend, is now establishing itself as a key element of defense and security strategy. Mastering it will be crucial to ensuring the safety of our fellow citizens and the sustainability of our institutions in an increasingly complex global environment. It is therefore together, through dialogue, rigour, and a shared vision, that we will succeed in integrating this technological revolution in the service of peace and security.

I want to thank all the experts who contributed their time and experience to this important work. I trust this document will support continued reflection and action within our respective organizations.

# INTRODUCTION

Artificial intelligence (AI) is now emerging as one of the most transformative technological developments for contemporary societies. Gendarmerie-type forces, faced with constantly evolving forms of crime, are on the front lines of this revolution. Advances in computing power, the capabilities of algorithms, and the massive availability of data offer new avenues for action, both in terms of prevention, investigation, and operational response. AI is not merely a modernization tool; it represents a paradigm shift in the way public security is conceived, enhancing the ability to anticipate and proactively respond.

Today's criminal landscape is characterized by its complexity and cross-cutting nature. Cybercrime, the rise of drug trafficking, the spread of radical ideologies online, transnational organized crime, as well as local delinquency, require police and gendarmerie services to strengthen their detection and anticipation capabilities. In this context, AI can help identify weak signals more rapidly, analyze large volumes of data from diverse sources, and reveal correlations invisible to the human eye. In this sense, it acts as a force multiplier, increasing the effectiveness of officers while freeing up time for missions that require significant human judgment and value. The impact of AI on crime can be assessed at several levels. On the preventive side, predictive systems can help identify high-risk areas or time periods, optimizing personnel deployment. In the judicial field, AI facilitates the analysis of images or intercepted communications, accelerating investigations and improving case-solving capacity. Finally, in terms of public safety, it allows for more efficient management of flows, whether during demonstrations, major sporting events, or the surveillance of sensitive areas. However, this new power raises ethical and legal issues that must be strictly regulated.

Indeed, the use of AI by gendarmerie-type forces cannot be conceived outside a robust regulatory framework. Protection of individual freedoms, respect for privacy, and transparency in algorithmic use must be guaranteed. The objectives of regulations in each country establish principles adapted to the governing authorities, regarding proportionality, purpose, and data governance. The challenge is to reconcile operational efficiency with the protection of fundamental rights, in order to maintain public trust, an indispensable condition for the legitimacy of law enforcement action.

This regulatory requirement must be accompanied by an appropriate internal organization. Integrating AI into the services requires a comprehensive strategy, ranging from officer training to the creation of multidisciplinary teams combining po-

lice officers, scientists, jurists, and analysts. Project governance, ensured by knowledgeable experts, must be clearly defined to prevent misuse, duplication, or loss of expertise. Furthermore, inter-service cooperation, as well as collaboration with the private sector and academic actors, is essential to maintain a high level of innovation and ensure national sovereignty in this highly strategic field.

Thus, AI represents both an opportunity and a challenge for internal security forces. It is an opportunity because it strengthens the fight against increasingly sophisticated and elusive criminal activity. It is a challenge because its use must be rigorously regulated, both legally and organizationally, to prevent infringements on liberties and ensure effective deployment. The future of public security will therefore depend on the ability to integrate these technologies responsibly, transparently, and efficiently, while always placing humans at the heart of the system.

The objective of the various commissions during the French presidency was to address the challenges and stakes of AI for better protection of populations through four commissions: human and logistical resources, international affairs, technological challenges, and finally service organization. In total, 22 gendarmerie-type forces gathered to exchange, share knowledge, better understand AI, and ultimately become more effective against crime.

*1st Commision : Human Ressources,*
*Chile from 10th to 13th December 2024*

# Exploring AI opportunities in the field of HR

## *Exploring AI opportunities in the field of HR*

**KEY POINTS**

- Talent recruitment and retention
- Human supervision
- Ethics and regulation rules
- Recruitment and Selection enhancement
- Employee Experience improvement
- Learning and Continuous Development

AI has considerable potential in the field of human resources, particularly for increasing productivity and improving the quality of recruitment, as well as in personnel management and development. At the same time, AI raises ethical questions and carries a number of risks of misuse. Managing these risks responsibly is essential for the successful and profitable use of AI in human resources. AI applications in human resources can be considered in relation to three main areas : management, development, and performance. In terms of management, AI can support time and activity management, recruitment processes, onboarding and integration of new employees, as well as administrative management. Regarding development, AI can enhance talent management, internal and external mobility, skills development and training, strategic workforce planning, employee experience, internal communication, quality of work life, corporate social responsibility, and management support. Finally, in the area of performance, AI can assist with overall management, managing the social climate, change management, remuneration management, and employee performance management.

The gains offered by AI have been the subject of numerous studies, and all agree in considering that thanks to AI, we notice a time saving by automating low value-added tasks, ever-changing legal and regulatory corpus simplification and a standardization of processes. Ultimately, the use of AI enables managers to focus in a human way on their core mission, which is managing people.

The aim of this commission is to examine the various possible applications of AI in the very specific field of human resources within each FIEP member country. It is also an opportunity for the MS to present their AI projects, those under development or planned for the short or medium term, and the limits observed. This provides an overview of the development and maturity of AI within gendarmerie-type forces. This commission also sought to assess the risks inherent in uncontrolled use and the need for highly qualified personnel.

### 1. Projects already up and running in gendarmerie type-forces

Most projects rely on chatbots based on algorithmic artificial intelligence. They work in a relatively simple way: a vast set of pre-recorded

questions and answers is integrated into the tool, providing a minimal basis for dialogue. When a user makes a request, the chatbot matches it to the closest question in its database and provides the corresponding answer. If the answer is unsuitable, the user can inform a moderator, who then takes over and provides a relevant response. The new question and answer are then integrated into the chatbot, gradually enriching its knowledge base. This approach has an immediate advantage: it saves a considerable amount of time. Since most requests are simple, users can quickly access the information they are looking for and managers avoid having to repeatedly answer the same questions. However, setting up such a system requires a significant initial investment in human resources and, in the medium term, regular and comprehensive updating of the question/answer corpus, particularly in a constantly changing regulatory environment. The future therefore lies in the use of chatbots that implement generative AI in order to limit the negative aspects listed above, while benefiting from the possibilities offered by the use of AI.

## 2. Potential and perspectives of AI for HR in Gendarmerie type-forces

During the commission, a wide range of projects were presented, illustrating the potential applications of artificial intelligence at every stage of personnel management. These initiatives highlight both the opportunities offered by AI and the challenges that must be addressed to ensure its successful integration into human resources processes. In the area of recruitment, AI has the capacity to transform selection procedures by analyzing large volumes of applications in order to identify candidates whose profiles most closely match the requirements of specific positions. Beyond

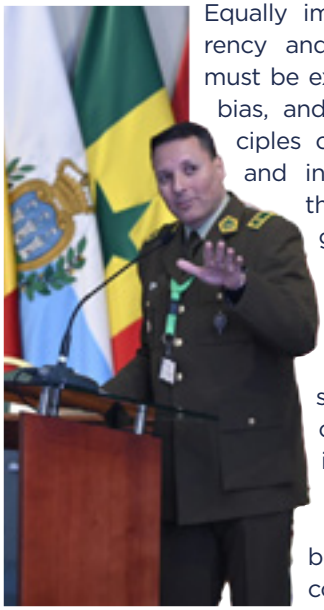
simple filtering, such systems can also detect high-potential individuals and emerging talent that may not be immediately visible through traditional evaluation methods. The gains in efficiency are substantial: considerable time and human resources can be saved, enabling recruitment teams to focus on more strategic aspects of candidate assessment. Nonetheless, a critical issue remains unresolved—the extent to which AI is capable of recognizing and respecting the unique military identity and culture of each security force. Without this, the risk is that recruitment becomes technically efficient but strategically misaligned with the institution's values and operational requirements.

When it comes to career mobility management, AI can bring real added value in navigating the complexity of annual transfer processes. These processes must reconcile numerous factors, including individual aspirations, the availability of positions, the broader interests of the institution, and the personal and family situations of service members. Traditionally, balancing these sometimes competing priorities requires significant manual effort and judgment. AI, by integrating and processing these parameters holistically, could support more transparent, equitable, and optimized decision-making, ensuring that mobility policies serve both organizational efficiency and personnel satisfaction.

In the domain of everyday HR management—covering training, promotion, and long-term skills development—AI opens the door to a more ambitious and data-driven approach to human capital management. A concrete example can be found in the French Gendarmerie Nationale, which is currently developing an integrated tool within its HR information system (HRIS). Over time, AI will act as a connective layer across the different modules of the HRIS, allowing service members to map out personalized career paths. These paths will be constructed on the basis of skills already acquired, the competencies required for future positions, and the broader strategic needs of the institution. For managers, this integration offers the possibility of greater agility and foresight in HR planning: quickly addressing shortages in critical roles, anticipating the need for rare technical expertise, and ensuring a closer match between the profiles sought and those actually recruited. Finally, in the sphere of medical monitoring, AI presents promising opportunities to strengthen the well-being and resilience of personnel. By providing objective indicators on stress levels, workload distribution, and potential health risks, AI could serve as an early warning system, alerting the chain of command before issues escalate. Such tools could help safeguard operational readiness while also promoting a healthier work environment. However, this area also raises particularly sensitive concerns, notably around the protection of medical confidentiality and the ethical handling of personal health data. Without robust safeguards, there is a significant risk of undermining trust between personnel and the institution.
Taken together, these initiatives illustrate both the transformative potential of AI in personnel management and the careful balance required between technological innovation, ethical responsibility, and institutional culture.

## 3. Key Success Factors for Effective AI Implementation in HR

The successful implementation of AI in Human Resources depends on several key conditions. First, organizations must clearly recruit and manage specific talent in AI, this is not a necessity, this is an obligation. They also must define the objectives and use cases ((recruitment, onboarding, talent management, training, payroll, employee experience), ensuring that AI addresses real business challenges rather than serving as a technological showcase. This requires a strong foundation of reliable, well-structured HR data and robust governance to guarantee security, privacy, and compliance with regulations such as GDPR.



Equally important is transparency and ethics: algorithms must be explainable, free from bias, and respectful of principles of fairness, diversity, and inclusion. To achieve this, HR teams, managers, and employees need to be actively involved from the start, trained in how to use AI tools, and supported through change management initiatives that ease concerns about automation. AI should be positioned as a complement to human expertise rather than a replacement, automating repetitive tasks like CV screening or handling routine inquiries, thereby freeing professionals to focus on more strategic and human-centered responsibilities. For long-term success, the system must remain adaptable and scalable, with regular updates to reflect evolving regulations, business needs, and technological advances. Finally, impact measurement is crucial: defining clear KPIs—such as time savings, cost efficiency, recruitment quality, and employee satisfaction—allows organizations to evaluate effectiveness and refine solutions over time. In essence, successful AI in HR is built on reliable data, ethical practices, human involvement, adaptability, and a clear vision of added value.

## 4. Workshop dedicated to constraints and solutions

A time was set for collective work. This enabled us to list a number of difficulties linked to the implementation and development of AI, and to propose some solutions. The results are summarized in the table below :

| AI Difficulties | Solutions |
|---|---|
| Resistance to change | Acculturation and training |
| Legal issues | Involment on regulation debate and discussion |
| Lack of skills | Exchanges with non-military or specialists<br>Recruitment of high-qualified specialists |
| Infrastructures : costs | Sharing infrastructures |
| Chief sponsoring : the will | Responsible view of AI |
| Accountability / Responsability | Human supervision<br>Policies guidelines<br>Code of Ethics |
| Adaptation – technical question | Step by step, program by program |

## 5. Conclusion

AI in human resources offers extraordinary potential for exploitation across numerous sub-domains. The benefits of sensible use are strategic: greater employee satisfaction, increased talent retention, targeted skills development and the implementation of solid succession plans. By integrating these tools, police forces also gain in agility and competitiveness, thanks to better anticipation of changes in skills requirements. Furthermore, employees who are actively involved in building their career paths often prove to be more creative, more innovative and more committed to collective success. Finally, this efficient use of AI can only be achieved if it is supported by experts in the field and, above all, if it places humans above machines, because there can be no human resources without humans !

# *KEYNOTE SPEAKER PRESENTATION*

## PART 1 : Strategic Vision of Artificial Intelligence in Police Operations

General Enrique Villarroel Valencia, Director of the Directorate of Information and Communication Technologies of Carabineros, opened the session by presenting the strategic and conceptual framework guiding the adoption of artificial intelligence (AI) in police functions. His presentation established the foundation upon which current technological projects are being developed.

### Global and Local Context of AI

General Villarroel explained the classification of AI —from Artificial Narrow Intelligence (ANI) to Artificial Superintelligence (ASI)— emphasizing that today's practical applications correspond to ANI, already having a direct impact on public safety. Drawing on the OECD definition, he described AI as a system capable of generating predictions, recommendations, or decisions that affect real or virtual environments, which marks a progressive transformation in the exercise of police work.

### The Impact of AI on Work and Society

Using international data, he highlighted how AI is reshaping the labor market :

- Around 25% of current tasks could be automated in the U.S. and Europe.
- 67% of companies already use AI, with growing adoption over the past year.

These trends, he argued, also apply to public safety, where automation can strengthen operational efficiency, though always within ethical, regulatory, and cybersecurity frameworks.

### Enabling Factors for AI Adoption in Carabineros

The General identified three key pillars for incorporating AI into police operations:

- Enabling Factors: investment in infrastructure and data governance, along with the strengthening of human capital through continuous training programs and collaboration with universities and academies that prepare officers in new technological skills.
- AI Development and Adoption: fostering collaboration between the State and the private sector, while modernizing institutional processes.
- Ethics and Regulation: safeguarding privacy and reinforcing cybersecurity.

### Concrete progress already includes :

- The construction of a dedicated Data Center, soon to be inaugurated.
- Collaborative work with academic and governmental institutions leading to the SITIA project.
- A strong focus on public safety, privacy protection, and citizen trust.

### Political and Institutional Support

He stressed that this process has solid state backing :

- President Gabriel Boric promoted Chile's first AI-powered teleprotection system to combat crime.
- The National Artificial Intelligence Policy provides guidelines on enabling conditions,
- adoption, and ethical governance, reinforced in the latest presidential address.

### Toward a New Era of Police Work

In conclusion, General Villarroel emphasized that AI is not a distant promise but a present reality already transforming police operations. The challenge lies in its responsible adoption, ensuring interoperability, strengthening both human and technological capacities, and using AI as a strategic tool to protect citizens more effectively while reinforcing institutional legitimacy.

Following the presentation by General Enrique Villarroel Valencia, the General introduced the presentation of Engineer Cristopher Álvarez Jaramillo

## PART 2 : Use of Artificial Intelligence in Police Operations

Cristopher Álvarez Jaramillo, Project Manager at the Directorate of Information and Communication Technologies of Carabineros, presented a comprehensive overview of how artificial intelligence (AI) is being used as a key tool in transforming police work in Chile. The presentation began by highlighting government support for these initiatives, framed within the national AI policies promoted by the 2023 presidential address. This institutional backing has enabled the development of innovative projects aimed at effectively combating crime and enhancing public safety.

### The SITIA Project: A Strategic Innovation

The core of the presentation focused on the SITIA Project, a flagship initiative in the use of AI in police operations. This project combines advanced technology with ethical principles and regulations to ensure responsible implementation. SITIA is structured into three fundamental stages :

- Integration: Consolidating multiple video streams from various public and private sources.
- Data Convergence: Centralizing information into a single platform to facilitate interoperability and data analysis.
- AI Analytics: Employing AI to conduct advanced analyses, generate predictive models, and support real-time strategic decision-making.

It was emphasized that these stages form the foundation upon which all practical applications of the project are built, showcasing a methodical and scalable approach.

### Practical Applications and Operational Transformation

Specific cases were presented to illustrate how AI has revolutionized police operations:

- Video Centralization: The integration of public and private video streams has optimized information management, fostering effective collaboration between the public and private sectors.
- License Plate Recognition: AI is used to identify patterns in vehicle license plates, improving the detection of stolen vehicles and the prevention of related crimes.
- Behavioral Analysis: Examples included pattern analysis in Santiago's Metro and areas near ATMs, enabling real-time measures against suspicious activities.
- Motorcycle Mugging Prevention: Predictive models have proven effective in identifying criminal networks specialized in this type of crime, strengthening operational response.

### Projections and New Areas of Application

The presentation also addressed future steps in the implementation of AI:

- Emergency Call System: Plans to integrate AI to automatically classify emergency calls,
- generate transcripts, and prioritize attention based on case severity. This improvement would significantly speed up responses to critical emergencies.
- Pedestrian Identification: Using AI to detect pedestrian behavior patterns, enabling the swift and accurate location of missing persons or the identification of fugitives.

Additionally, the success of the SITIA Patentes system was highlighted. This innovative platform integrates advanced technologies to combat vehicle theft. The process includes license plate capture, training machine learning algorithms, and utilizing predictive models for early decisionmaking, complemented by deep learning that identifies features such as vehicle type and color.

### Visualization Tools

A key aspect of the presentation was the explanation of the developed visualization tools :

- Crime Map: Facilitates the identification of crime patterns, high-incidence times, and problematic areas, optimizing operational planning and the use of police resources.
- Predictive Route Models: Analyzes routes used by criminals, such as tolls and highways, to anticipate movements and prevent escapes.
- Stolen Vehicle Visualization: Provides detailed information on vehicles involved in crimes,
- including type, model, and use in criminal activities.

These tools not only enhance analytical capabilities but also allow for faster and more precise strategic decision-making.

### Conclusion

The presentation concluded by emphasizing that artificial intelligence is not merely a future promise but a present reality transforming how police forces operate in Chile. Projects like SITIA demonstrate how technology can be a powerful ally in addressing public safety challenges, with the ultimate goal of protecting citizens more effectively.

These initiatives confirm that AI is not only a present reality but also a cornerstone for the future of policing in Chile.

*2nd Commission : International affairs,*
*The Netherlands from 7th to 10th May 2025*

# The Impact of International Regulation on AI in Law Enforcement

# *The Impact of International Regulation on Artificial Intelligence in Law Enforcement*

**KEY POINTS**

- Human Oversight and Accountability
- Bias Prevention and Fairness
- Cybersecurity and System Resilience
- Algorithm Transparency and Explainability
- Control and audit policy
- Data Collection and Use Governance

Artificial intelligence (AI) is revolutionising internal security practices, offering unprecedented capabilities in terms of surveillance, predictive analysis and risk management. However, the lack of an appropriate legal framework exposes societies to major abuses, justifying the urgent need for specific, rigorous and proportionate regulation, particularly in the field of internal security.

One of the central issues is the protection of fundamental rights. AI technologies, such as facial recognition, behavioural analysis and risk scoring systems, can, if misused, jeopardise individual freedoms, in particular the right to privacy, non-discrimination and the presumption of innocence. Without legal safeguards, these tools risk introducing intrusive surveillance, normalising arbitrary profiling or marginalising certain populations to the detriment of society's protection. Clear regulations tailored to the specificities of each culture must therefore define the limits of their use, ensuring that all applications comply with each country's fundamental rights principles.

It must also provide for independent oversight mechanisms and effective remedies for citizens, in order to prevent abuse and restore trust in institutions. Transparency and accountability are another essential pillar. Algorithms used in internal security often function as 'black boxes', making their decisions opaque and difficult to challenge. However, it seems necessary that any measure affecting individuals' rights should be understandable, justifiable and subject to scrutiny. Appropriate regulation must therefore enable authorities and companies to account for the functioning of their systems, explain the criteria used and allow for audits. This means not only documenting the databases and methods used, but also designating those responsible in the event of errors or malfunctions, in order to avoid impunity. Furthermore, algorithmic biases pose a serious threat to the fairness and effectiveness of security systems. AI systems, trained on data that is sometimes biased or incomplete, can reproduce and amplify existing discrimination, leading to miscarriages of justice or unjustified targeting.

Regulations must therefore allow for regular assessments of bias risks and non-discrimination tests to ensure that these technologies serve the public interest without reinforcing inequalities. The security of the infrastructure itself is also at stake. The growing integration of AI into internal security systems makes them vulnerable to cyberattacks, manipulation and misuse. Robust regulations must govern the design, deployment and maintenance of these tools, imposing high standards of cybersecurity and resilience. They must also provide for strict protocols for the collection, storage and sharing of sensitive data in order to prevent leaks or malicious use. The aim of this commission is to understand the various practices in different Member States with a view to improving systems for better protection of citizens and populations. Consistent regulation, inspired by best practices and ethical standards, would make it possible to reconcile technological innovation with respect for values, while facilitating international cooperation on security.

In conclusion, regulating AI applied to internal security is not a barrier to innovation, but rather an essential condition for leveraging it to protect citizens, while respecting their rights and the rule of law. This is all the aim of this commission.

**Insights from the Commission's Work**

The commission provided an international overview of national regulations and their impact on AI projects under development in each country. The two days were particularly rewarding, with each presentation providing an element to take into account when mastering the entire AI value chain. These highly complementary approaches have demonstrated the need to continue exchanging on this subject, either through very specific projects or through joint training courses.

These approaches concerned:

- **Technical aspects,** including the challenges of data accessibility and infrastructure funding.

- **Operational dimensions,** covering needs, applications, and practical implementation.
- **Human resources considerations.**
- **Governance and audit frameworks.**
- **The cyber domain,** underlining the importance of developing AI specifically for this sector, with the strong ambition to effectively protect both individuals and infrastructures.

These different approaches have revealed a shared concern: the protection of personal data and several legal challenges, including :

- the evolution of existing national legal frameworks to take account of AI technology and its specific features in terms of data accessibility and availability;
- the issue of data sharing, which is essential for developing AI systems;
- the ability to anticipate the requirements of the AI Act, in terms of compliance, training, and organisation.

In addition to these regulatory questions, the commission was an opportunity to work on **ethics in AI,** through four major values: justice, autonomy, beneficence, and non-maleficence. Divided into groups of different nationalities, the committee engaged in a highly instructive discussion on the practical meaning of these values. The exchanges demonstrated the need to combine current and future regulations with a shared ethical vision adapted to the missions and values of gendarmerie type forces.

Each participant emphasised that artificial intelligence regulation is a key issue for the operational deployment of this technology in the service of law enforcement.

### Operational Implications for Law Enforcement Agencies

In this regulatory environment, law enforcement agencies face a transformation of governance and practice. Chains of responsibility must be explicitly defined, with oversight roles embedded from project conception through operational use. Biometric identification must be divided clearly between emergency deployments and routine applications, each with its own authorisation and review procedures.

Procurement contracts will need to evolve, embedding obligations for data quality, auditability, explainability, and update mechanisms. Training in AI literacy becomes indispensable, enabling officers not only to use systems but also to recognise their limitations, interpret their outputs, and preserve human judgment as the ultimate safeguard.

Most importantly, the challenge of data accessibility and availability must be addressed systematically. Without adequate lawful datasets, compliant and effective AI in law enforcement will remain elusive. This tension—between the ambition of regulation and the reality of operational data—is perhaps the defining challenge of the coming years.

### AI regulation from Europe

Because the European commission has produced

a specific regulation, it appeared interesting for the FIEP commission to propose a overview of the main principles of this regulation called : the AI Act. The field of law enforcement is shaped by different regulatory approaches. However, at the global level, the Council of Europe's Framework Convention on Artificial Intelligence (2024) establishes the world's first legally binding international treaty on AI, applicable both to public authorities and to private actors acting on their behalf. Complementarily, the UNESCO Recommendation on the Ethics of AI (2021) and the OECD AI Principles (2019), though non-binding, remain influential by providing guidance on accountability, robustness, and human oversight. These instruments underline the urgency of coordinating standards across regions despite divergent legal traditions, political priorities, and economic contexts. A common concern cutting across these initiatives is the protection of personal data and privacy, which remains central to the responsible use of AI in law enforcement.

Within this fragmented landscape, the European Union has introduced the first comprehensive regulation of its kind: the AI Act, which entered into force in 2024. Built on a risk-based approach, it is particularly noteworthy as, if properly understood, it may not only ensure safeguards but also support innovation. For law enforcement agencies, the AI Act establishes binding requirements while also acknowledging their specific missions through a system of exceptions. It thus represents both a regulatory framework and a governance model, demanding that security forces adapt their organisational practices to new standards while navigating the balance between operational needs and fundamental rights.

The AI Act prohibits certain practices outright, such as biometric categorisation based on sensitive traits, social scoring, or indiscriminate scraping of facial images. It strictly limits real-time biometric identification in public spaces, permitting it only under narrowly defined exceptions and always subject to prior authorisation. Post-event biometric searches remain possible, but they require proportionality, justification, and rigorous documentation.

Beyond these prohibitions and exceptions, the AI Act introduces a quality and risk management philosophy into policing technologies. AI systems used for law enforcement purposes are generally classified as high-risk. This classification brings with it a demanding set of obligations :

- Risk Management Systems. Agencies must establish structured processes to identify, evaluate, and mitigate risks throughout the lifecycle of AI systems. This includes testing for accuracy, robustness, and bias before deployment, as well as continuous monitoring in operation.
- Quality of Data. Training and validation datasets must be complete, representative, and free of discrimination. Data governance thus becomes a cornerstone: agencies must verify the provenance of datasets, ensure lawful collection, and document measures taken to address gaps or biases.

- Technical Documentation. Every high-risk system must be accompanied by detailed documentation describing its design, training data, intended purpose, limitations, and known risks. This requirement ensures that systems can be audited and that accountability is traceable.
- Protocols for Explainability and Transparency. Agencies must be able to explain how systems operate, what inputs lead to what outputs, and what safeguards are in place. This does not imply that every algorithm must be fully interpretable in scientific terms, but that the use of AI in a policing context must remain intelligible to supervisors, judicial authorities, and, where appropriate, the public.
- Human Oversight. The Act insists that AI tools cannot replace human judgment. Clear protocols must specify the role of human operators, the conditions under which they may override system outputs, and the mechanisms for recording such interventions.

These requirements are not merely bureaucratic burdens; they are conditions for trustworthiness. In law enforcement, where legitimacy depends on respect for rights and procedural fairness, trustworthy AI is not optional but essential. The AI Act therefore pushes agencies to embed governance, documentation, and transparency into the very fabric of their technological adoption. Yet this transition is far from simple. Implementing quality and risk management systems requires resources, expertise, and organisational adaptation.

Smaller or less technologically equipped agencies may struggle to maintain the documentation, testing, and monitoring demanded. Moreover, the challenge of data accessibility and availability often makes it difficult to meet the Act's strict standards on dataset quality, further complicating compliance.

The EU has thus positioned itself not only as a regulator but as a standard-setter: the AI Act exports a vision of responsible, risk-managed AI that other jurisdictions may eventually adopt or adapt. For law enforcement agencies, this means that compliance is not simply about avoiding sanctions but about building explainable, transparent, and trustworthy systems that can withstand both legal scrutiny and public debate.

# KEYNOTE SPEAKER PRESENTATION

**Peter Kager - Chief Quality Officer - ICTRecht**

The presentation 'AI from a legal perspective' takes a critical look at the emergence and regulation of artificial intelligence (AI) from a legal perspective. The central premise is that the discussion on whether machines can think is actually of little relevance; much more important is how AI is applied in practice and what consequences this has for people and society. *This is aptly illustrated by a quote from Edsger W. Dijkstra, in which he emphasises that the question of whether a machine can think is as meaningless as the question of whether a submarine can swim.* The focus should therefore be on the concrete implications of AI and how laws and regulations can guide it.

In essence, the European approach to AI is to promote human-centred and trustworthy technology. Especially when deployed for law enforcement. It seeks to strike a balance that ensures a high level of health, safety and fundamental rights protection on the one hand, while leaving room for innovation and economic growth on the other. AI is increasingly being integrated across different sectors and applications, but this poses risks that require legal safeguards.

An important framework for this approach is the European AI Act, which categorises AI systems according to their risk. This distinguishes between systems that pose unacceptable risks, such as manipulative technologies or social scoring, and high-risk systems, such as AI

at border controls. AI applications with lower risk fall under lighter rules, where transparency is particularly important. This risk-based approach allows for tailoring and applying the right level of control depending on the impact of the technology.

Besides legal aspects, the ethical challenges posed by AI are also considered. Algorithmic bias is a major risk, as AI systems can reinforce existing biases and make discriminatory decisions. Privacy also plays a crucial role, as many AI applications rely on the collection and processing of personal data. Finally, transparency is a core requirement for maintaining public trust. Citizens must be able to trust that AI systems are deployed fairly, verifiably and responsibly.

***The presentation underlines that developing legally and ethically sound AI is not an easy task. It requires an integrated approach in which legislation, technology and ethical reflection go hand in hand. Only then can AI truly contribute to a society in which technology supports humans without losing sight of their rights and freedoms.***

*3td Commission : New Technologies and Logistics, France from 25th to 27th May 2025*

# AI for criminals vs AI for Gendarmerie type forces

# *AI FOR CRIMINALS vs AI FOR GENDARMERIE-TYPE FORCES*

**KEY POINTS**

- Human Oversight and Accountability
- Bias Prevention and Fairness
- Cybersecurity and System Resilience
- Algorithm Transparency and Explainability
- Control and audit policy
- Data Collection and Use Governance

Police forces operating under a Gendarmerie model are approaching emerging technologies from a dual perspective: while these tools are increasingly exploited for criminal purposes—as both instruments and targets—they also offer promising opportunities to combat crime and terrorism, streamline administrative processes, and enhance overall operational efficiency. Traditional criminal practices are also being transformed by emerging generative technologies. One particularly striking example is the sharp increase (+442%) in cyber attacks based on voice deepfakes and voice-based phishing scams, which have become more targeted and effective due to recent technical advances.

Artificial intelligence appeals to criminals because it offers them three decisive advantages: automation, which allows them to carry out large-scale attacks; personalisation, which makes each attempt more credible; and anonymisation, which makes operations much more difficult to attribute. The democratisation of open source tools and the availability of powerful models accessible online further reinforce this phenomenon. This criminal exploitation of AI undermines trust in digital exchanges, increases cybersecurity costs for businesses, and creates new hybrid threats combining information manipulation, financial fraud, and physical violence. It could open up new possibilities in the race between criminals and gendarmes.

In response to these risks, the solution lies in developing defensive AI capable of detecting falsified content and anticipating suspicious behaviour, as well as strengthening international cooperation to combat threats that cross borders. Finally, raising awareness among the general public and organisations remains an essential lever in preventing confidence in digital tools from collapsing. Gendarmerie type-forces have no choice to develop AI projects in various areas: data mining and image analysis, predictive policing, drone deployment, analysis of digital communication, dark web investigation, live translations using different models, personnel training and skill development, forensic investigation supported by open-source intelligence techniques, and the simplification of everyday administrative tasks.  The aim of this commission is to evaluate the development of AI in the field of crime as well as against crime.


**AI for criminals**

During the commssion, the different member states have explianed the main use of AI in the field of crime in their own country. What we notice is a real emergence of techniques based on AI espacially in the field of cybercrime.

From a criminal perspective, AI is primarily a tool for efficiency. Whereas traditional scams required time and limited human skills, AI systems now make it possible to automate and personalise attacks. For example, phishing campaigns, which used to be generic and easily detectable, can now be generated in mass with highly credible messages tailored to each target's profile. AI thus provides increased productivity and unprecedented precision in the execution of crimes. Secondly, AI facilitates the creation of convincing fakes. Deepfake technologies, by realistically reproducing voices or faces, pave the way for sophisticated manipulation: identity theft, financial fraud, political disinformation. For a criminal, the appeal lies in the ability to make lies indistinguishable from the truth, thus blurring the traditional markers of social trust. Then a very interesting point for criminal who use AI is the difficulties to highlight the responsability. AI can contribute to criminals evading responsibility. The use of automated systems blurs the lines between human intent and machine action. This raises a key question: who is responsible when an algorithm generates fraud or orchestrates a cyberattack? This ambiguity can be exploited to complicate investigations and delay justice. Through the different présentation we could make a non-exhaustive list of the use of AI in criminal activity.

- The rise of technology-enabled criminal networks
- Changing tactics, tools, and organizational structures of criminal networks
- The use of cryptocurrency for money laundering
- New forms of online child sexual exploitation
- Shifting routes and methods in migrant smuggling
- Diversification in drug trafficking operations
- Expansion of firearms trafficking via digital platforms
- Underestimated yet growing waste-related crimes
- The proliferation of counterfeit goods
- A marked increase in the use of proxies

Finally, AI introduces asymmetry between defence and attack. While Geandarmerie-type

forces must comply with protocols and operate within a legal framework, malicious actors are free to exploit the speed and adaptability of these technologies. They can analyse huge volumes of data, identify vulnerabilities and design tailor-made attacks, while reducing their own risk of exposure. In this way Gendarmerie-type forces have no choice to be engaged on the use of AI because each technological advance carries with it a duality: an instrument of progress for some, an opportunity for harm for others. The future will therefore depend on our collective ability to bridge this gap and prevent AI from becoming a lasting lever for crime.

### AI for Gendarmerie-type forces

Because artificial intelligence is indeed a demanding and unique scientific discipline that requires dedicated training, differentiated appropriation and specific implementation within a defined regulatory framework, its use by the Gendarmerie type forces must necessarily be part of a strategy. The reasons for the uniqueness of AI lie in its rapid evolution, which requires it to operate in an agile mode; its short-, medium- and long-term impact on society, which requires its development to be anticipated; its complexity, which requires expertise and responsibility; and its multiple dimensions, which require its implementation to be coordinated. The commission's various discussions have therefore highlighted the need to bring together a range of skills (science, law, training, international affairs) within a single institute dedicated to AI for homeland security. This is a necessary and essential condition for the sensible and responsible use of AI in homeland security.

In terms of application, it quickly became apparent that a distinction needed to be made between operational AI, AI to assist police officers, and AI for support purposes.

### An operational AI

One of the primary contributions of AI lies in detection and prevention. Predictive analytics systems, fed by historical and real-time data, make it possible to anticipate criminal area, certain criminal behaviours or identify suspicious

patterns. In the field of cybersecurity, for example, AI helps identify traffic anomalies or intrusions before they cause significant damage. This early warning capability gives law enforcement agencies a decisive advantage in their protection mission.

AI also offers considerable advances in the processing of investigations. Automatic image and video analysis can speed up the use of surveillance cameras, enabling the rapid identification of a wanted individual or the tracking of a suspect's movements. Similarly, automated natural language processing facilitates the examination of documents, messages or witness statements, reducing the workload for investigators and improving the accuracy of searches.

**A Gendarme assistance AI**

Artificial intelligence for operational use will be complemented by organic artificial intelligence dedicated to force support and resource management activities. The aim is to improve the functioning of the institution by developing tools that help to reduce and simplify the administrative burden, speed up procedures and limit human error.

Applications based machine translation can assist gendarmes during operations, particularly in multilingual contexts or at major events. The development of Large langage model also offers new capabilities.  A locally deployed large language system built from open-source components, integrating multiple models to accelerate workflows—for example, by generating multilingual summaries of video content avoiding usual biases that can be inherent to LLMs as ChatGPT or DeepSeek. Particular attention was given to the development of intelligent agents designed to enhance training and support forensic work. One example includes the use of simulated personas to assist in identifying individuals involved in child exploitation.

Intelligent drones, equipped with real-time analysis capabilities, help to monitor areas that are difficult to access, while limiting officers' exposure to risk. Different presentations focuses on the drone development and the prevention of their malicious use. In this regard, some participants shared both pilot studies and successful field experiments targeting the use of drones by smugglers within their territories.

AI can also be used in the field of logistics like for instance to predic vehicle maintenance. It is a way to gain in term of performance as well as saving money. Finally the use of AI in the field of human ressources have also be considered but it was the theme of the 1st commission. The different member state insisted the necessity to establish a dedicated career tracks to attract, train, and retain talented personnel.

**A support purpose AI**

The development of AI requires appropriately scaled infrastructure, without which scaling up is compromised, as is the ability to perform the calculations necessary for operational AI. This means anticipating and planning for massive investments in dedicated infrastructure. The goal is to have the capacity to store, process, access and secure data. Storage requires anticipating the challenges of sovereign cloud computing to prevent dependence on foreign suppliers and help guarantee the security of strategic data. Edge computing should also be considered, as it allows data to be processed as close as possible to users, which will reduce latency and increase the performance of AI systems. This dual challenge should make it possible to satisfy AI integrated into business information systems on the one hand, and into entities closest to operational action on the other.

To conclude AI is a real game changer for criminals, who see a proliferation of opportunities for crime and areas of attack. Nevertheless, Gendarmerie type-forces, provided they incorporate AI into a comprehensive and integrated strategy, can make AI a game maker in the fight against crime. The only way is ta gather different skills in a same place to know where and how to go. A recurring theme across all interventions was the need for strong oversight of algorithmic behavior and rigorous protection of the sensitive data used in training processes. Given the confidential nature of many investigations, security and data integrity remain paramount. While partnerships with academia and the private sector are key to progress, participants emphasized that these collaborations must be complemented by the internal development of technical expertise. As a result, there is growing support for the integration of dedicated training modules into police academy curricula, aimed at equipping cadets with the skills required for future operations. Moreover, member states have invited on the reinforcement of the transnational cooperation, especially in developing a very active participation and cooperation. At the same time, concerns over sovereignty and data protection have prompted efforts to develop local alternatives, though achieving full autonomy across all system components remains a complex task.

# *KEYNOTE SPEAKER PRESENTATION*

**Françoise Soulié Hub France IA, Scientific Advisor**

**What is AI ?**

An AI system is a computer program, but it is not obtained as usual. In the family of AI techniques most used (digital or connectionist AI or Machine Learning - ML) in problems when we do not have an algorithm to compute an exact solution, we « learn » an approximate solution using a “ML algorithm” and data. Because these techniques produce only an approximate solution, the answermay sometimes be wrong. Neural networks, deep learning and transformers are particular cases of such techniques. The first wave of industrial applications came from Predictive AI (for example classifying an email as spam or non-spam). Since 2022, Generative AI (for producing content, be it text, images or videos) is deploying rapidly (the deep-fakes increase is due to Generative AI).

**AI & Crime**

Cyber-attacks are increasing every year (for example +15% per year for the global cost of cyberattacks[1]; + 3 000 % deep-fake fraud attempts in 2023[2]). Criminals increasingly leverage Artificial Intelligence (AI) to enhance their activities and, according to Europol[3], this is just the beginning as the AI expertise


of attackers increases. Meanwhile, AI provides powerful tools to enhance crime fighting, by enhancing efficiency, accuracy, and speed in various law enforcement and security operations. This is the first edge of the AI sword: attackers and defensors use it to do a better job (of attacking or defending) and are using it increasingly. The second edge is starting to appear and should develop rapidly too: AI systems open new potentialities for attacks by increasing the exposure surface, and they can be attacked specifically through new types of attacks. For example, LLMs (Large Language models) can be attacked by a manipulation of the prompt (prompt injection) which will make the system return a totally different / inappropriate

answer[4]. Understanding what AI is, what it can & cannot do is thus important for security forces.

**Attacks on AI**


An attack on AI is a cyberattack + an attack specific to AI. Protecting against such attacks thus requires 3 lines of defenses embedded as concentric circles :

1. Cyber defense protection: every attack on AI needs to penetrate the AI system, classical cyber security procedures must be in place;
2. Protections "AI secure-by-design": AI systems must be developed by obeying recommendations to avoid standard risks to AI systems;
3. Protections against specific AI attacks: these include very particular defenses (not very many measures are available yet).

Various documents have been published to address these issues by ANSSI, Mitre, NIST, and OWASP. We have used them to produce a document on "Attacks on AI"[5] where we describe attacks in fact sheets and give practical prevention methods for the three lines of defense. Developers of AI systems and defensors must learn to implement these methods.

**Conclusion**

In the field of crime, AI is more and more used in cyber attacks and AI-assisted cybercrime has growing significantly avec if it has just started: Gendarmerie type-forces have no other choise to learn about AI. Attacks on AI will multiply and coping with this increase will require expert knowledge. It is a strategic error Gendarmerie type-forces not to take into account the benefit of AI in the fight against crime and especially cyber crime.

1 https://www.euronews.com/2024/05/08/cybercrime-on-the-rise-thanks-to-artificial-intelligence
2 https://thenextweb.com/news/deepfake-fraud-rise-amid-cheap-generative-ai-boom
3 https://www.europol.europa.eu/cms/sites/default/files/documents/Internet Organised Crime Threat Assessment IOCTA 2024.pdf
4 https://www.nature.com/articles/s41467-024-55631-x
5 https://www.hub-franceia.fr/wp-content/uploads/2025/04/25_03_27_Analyse_des_attaques_sur_les_systemes_de_l_IA.pdf. English version to appear in October 2025.

*4th Commission : Service organisation,*
*Roumania from 1st to 3rd July 2025*

# How AI could positively impact Gendarmerie type-forces service organisation ?

## *How AI could positively impact Gendarmerie type-forces service organisation ?*

**KEY POINTS**

- Transformation of Business Models
- Optimization of Operational Processes
- Augmented Decision-Making
- Evolution of Skills and Jobs
- Organizational and Cultural Shifts

Beyond the technical aspects, the subject reveals a deeper truth: AI must not be viewed merely as a technology to deploy, but as a profound transformation — one that reshapes the way work is carried out, decisions are made, and interactions with citizens and colleagues are structured. This transformation reflects three ongoing revolutions: social, organizational, and cultural, and highlights the need to construct a risk-based approach to guide and manage it.

Managing AI-related risks becomes a strategic lever — essential for preserving decision-making autonomy, reinforcing institutional resilience, and safeguarding the democratic legitimacy of our actions. Each of these three dimensions brings its own set of challenges, from integrating AI into daily operations to developing new working methods and building the ethical and operational frameworks needed to fully harness its potential.

**Facing the three revolutions driving AI integration**

- **Social Revolution : Adjusting the Human-Machine relationship**

Integrating AI means transforming our interactions with it. AI only creates value if humans understand its functioning, recognize its limits, and critically apply its insights. A techno-centric approach is insufficient; the human must remain central to design and use.

Key enablers include :

1. Continuous training and critical engagement.
2. Collective reflection on AI's role.
3. Governance based on support, ethical vigilance, and real-world testing.

AI must empower human autonomy and competence—not replace it.

- **Organizational Revolution: Structuring to perform**

AI exposes structural weaknesses. Without solid data governance, shared standards, and integrated processes, it risks reinforcing dysfunctions.

To harness AI as a lever for public performance, it is essential to :

1. Implement rigorous data governance (quality, traceability, accountability).
2. Adopt common technical and ethical standards.
3. Align legal, engineering, and strategic frameworks.

Properly structured, AI offers clarity, strategic control, and operational sovereignty rather than opacity or confusion.

- **Cultural Revolution: Deciding differently with AI**

AI challenges decision-making, authority, and responsibility. Rather than ceding judgment to machines, humans must decide with AI, maintaining informed control and continuous evaluation.

This demands :

1. A culture of discernment resisting algorithmic opacity.
2. Ethical vigilance regarding biases and systemic impacts.
3. Integrated, interdisciplinary governance of decision-making.

The AI Act formalizes this, requiring high-risk AI operators to structure governance (risk management, transparency, supervision) and establish independent, pluralistic external evaluation.

But governance effectiveness begins with a clear typology of AI risks, considering contexts, vulnerabilities, and balancing performance with safety.

**Embracing AI's Full Potential and Risks**

The commission's discussions were particularly rich, emphasizing the importance of predictive tools and conversational assistants in enhancing crime prevention and response. These technologies were identified as key levers for improving efficiency, responsiveness, and citizen engagement. Participants also underlined the importance of embracing the full scope of AI-related risks — not to avoid them, but to acknowledge that risk acts as an amplifier, capable of intensifying both benefits and harms. The importance of determining in advance the level at which the SIA is to be implemented was also emphasised. In other words, determining the target users.

- **Three levels : Operational, Tactical, and Strategic Levels of AI Application**

**1. Operational level :** Focused on day-to-day activities, such as improving interactions with the public through assistance technologies, supporting victims via procedural-assistance tools, and reinforcing operational readiness through predictive maintenance.
**2. Tactical level :** Enhances investigative capabilities by accelerating and refining data processing, enabling law enforcement and agencies to respond more effectively to evolving challenges.

**3. Strategic level :** Involves strengthening understanding of digital threats through predictive analysis to anticipate risks, guide policy decisions, and ensure long-term resilience.

- **Three Functions: From Reactive to Proactive and Predictive Law Enforcement**

Law enforcement agencies operate across three functional levels to manage and anticipate events effectively :

**1. Reactive capacity :** Responding promptly to incidents as they occur, using immediate actions such as automated alerts and real-time decision support.
**2. Proactive capacity :** Anticipating potential issues before they arise and implementing preventive measures to mitigate risks.
**3. Predictive capacity :** Leveraging data analysis to identify trends and forecast future events, enabling strategic planning and preemptive interventions.

Artificial Intelligence plays a crucial role in enabling law enforcement to implement and enhance these capacities by providing advanced tools and insights. This support helps improve responsiveness, resource management, victim support, and the ability to address evolving criminal behaviors.

Specifically, AI facilitates

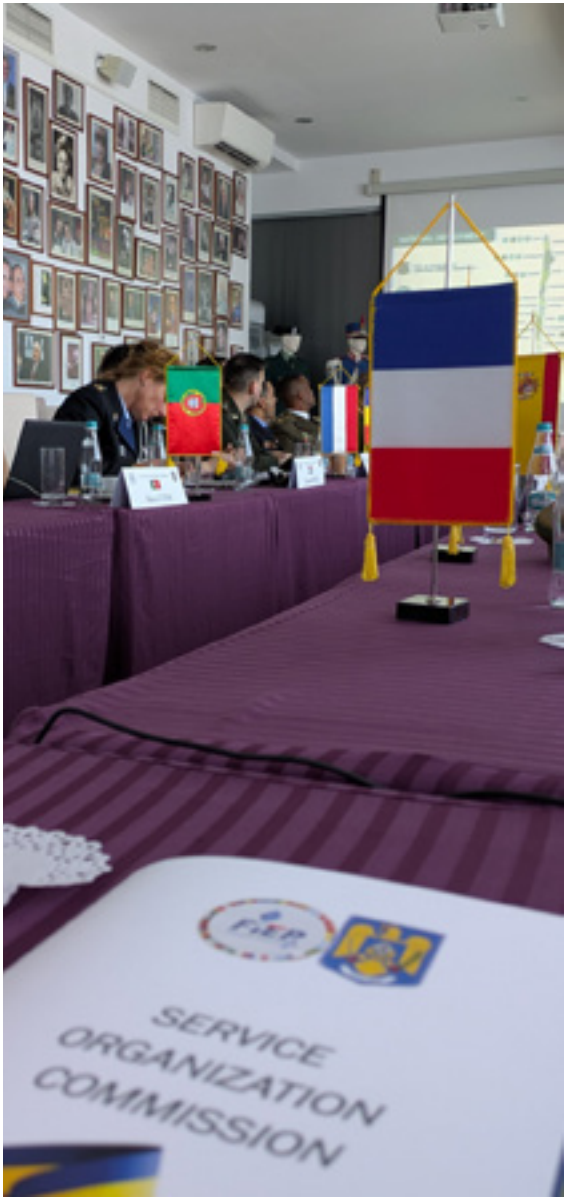
- Better interaction and trust with citizens, and improved victim assistance.
- Reduced administrative workload by anticipating operational needs through predictive maintenance and accelerating data processing to support human analysis.
- More effective reactions to crime evolution, by understanding emerging trends and ensuring the psychological well-being of agents in sensitive investigations.

Together, these capabilities position law enforcement to act decisively and adaptively in an increasingly complex environment.

A critical factor in all these levels is data quality and utility. AI's performance depends on data that is reliable, representative, and ethically managed. It is crucial to identify what data is truly useful to ensure that AI systems are fed with information that supports sound decision-making and minimizes bias or error.

**Conclusion**

The social, organizational, and cultural revolutions are inseparable and foundational for responsible, controlled AI aligned with democratic values. The commission's reflections and operational priorities illustrate the urgent need to develop and test AI solutions. The time for hesitation has passed: it is imperative to act, iterate, and build AI systems that support public missions while managing risks thoughtfully and proactively.



# KEYNOTE SPEAKER PRESENTATION

**Work, People and Algorithms Redesigning Roles, Processes and Competences Dr. Eng. Ionuț Petre**

*Head of R&D Department – Digital Transformation and Governance National Institute for Research and Development in Informatics – ICI Bucharest*

Artificial Intelligence is no longer a distant vision and it is now reshaping how institutions work, how decisions are made, and how human resources are deployed. Across sectors, including law enforcement, AI is transforming not only operational tasks but also the roles and skills required. The transformation of work is driven by four main forces :

1. **Technological innovation** - AI, robotics, and platforms are changing how tasks are performed.
2. **Demographic shifts** - Ageing populations and urban migration reshape labor availability.
3. **Green transition** - Sustainable jobs emerge while high-emission roles decline.
4. **Geopolitical instability** - Conflicts and disruptions alter how and where work happens, demanding institutional resilience.

These forces affect both low- and high-skilled jobs. Routine and repetitive tasks, whether manual or cognitive, are increasingly automated. In parallel, new hybrid roles are emerging that combine technical, emotional, and cognitive abilities. The future workforce must be agile, continuously learning, and digitally fluent.

**Redefining Roles, Processes, and Competences**

By 2030, an estimated 170 million new jobs will be created in tech, green, and care-related fields, while 92 million jobs may disappear. The net effect is positive, but the transition will be uneven. Institutions must support career transitions, reskilling, and organizational redesign to manage this shift.

Key trends :

- Digital, human-centered, and sustainability-oriented roles are growing.
- Administrative, repetitive, and low-value tasks are declining.
- Soft skills (communication, empathy, leadership, emotional intelligence) become more valuable, as they are harder to automate.
- Competences are blended - jobs now require technical know-how, critical thinking, and interpersonal capabilities.

Upskilling is not a one-time effort but rather becomes a continuous loop, as many core skills are expected to change in the next decade.

### Implications for Law Enforcement and Gendarmerie Forces

AI is gradually altering how law enforcement operates. Key applications include predictive deployment based on crime data, real-time surveillance analysis using computer vision, automated report drafting for administrative efficiency or digital forensics for rapid analysis of large datasets. This frees up workforce to focus on high-value, human-centered duties such as community engagement, crisis negotiation, and ethical decision-making. But this evolution also redefines the identity of work - shifting expectations, workflows, and organizational cultures.

Integrating AI requires more than introducing new technologies, it demands a strategic shift in mindset and institutional culture. Leadership must be actively engaged to align vision and priorities, while long-term training frameworks need to equip officers at all levels with both technical understanding and ethical awareness. A successful transformation also relies on partnerships with academia and civil society, ensuring access to credible and up-to-date knowledge. Just as important is the institutionalization of ethical standards, transparency mechanisms, and public dialogue. Without these foundations, AI could undermine public trust instead of enhancing the effectiveness and legitimacy of the Gendarmerie.

Although Gendarmerie personnel does not need to become AI experts, but people will need to :

- Understand how AI tools function, including data risks and limitations.
- Critically interpret algorithmic outputs, rather than blindly trusting them.
- Communicate decisions transparently when AI plays a role.
- Maintain ethical awareness, emotional intelligence, and public accountability.

This new redefined basic of technical knowledge must be combined with a strong set of soft skills such as collaboration, judgment, adaptability in order to ensure responsible and effective use of AI.

The key risks and ethical challenges that must be considered include algorithmic bias, where flawed data reflects or amplifies social inequalities; automation bias, where humans defer to AI output even when it contradicts context or judgment, erosion of public trust, if systems are opaque or discriminatory. To prevent and mitigate these risks, the personnel must always be aware that AI should always support and not replace human decision-making. Clear human-in-the-loop protocols, ongoing audits, and ethical training must be institutionalized.

**The integration of AI into public security institutions is inevitable, but it must be deliberate, ethical, and inclusive. The Gendarmerie, like other critical institutions, faces a pressing choice - adapt proactively to the AI era, or fall behind. In the foreseen digital society, the success will be in human-AI collaboration, grounded in trust, competence, and a shared commitment to public service.**

# CONCLUSION

The work of the four commissions clearly demonstrates that artificial intelligence represents both a transformative opportunity and a profound challenge for gendarmerie-type forces. From human resources to international regulation, from the fight against crime to organizational restructuring, AI is already reshaping the way security institutions operate, make decisions, and engage with both their personnel and society.

On the operational side, AI strengthens the capacity to detect weak signals, anticipate threats, and accelerate investigations. In human resources, it supports more transparent and efficient recruitment, training, and career management, while also contributing to personnel well-being. In terms of international cooperation, it highlights the necessity of harmonized regulatory frameworks capable of protecting citizens while enabling innovation. Finally, from an organizational perspective, AI requires a rethinking of governance structures, data management, and institutional culture to ensure that technology truly serves the mission of public security.

Nevertheless, this transformation cannot occur without strong safeguards. AI tools must be embedded within a robust legal and ethical framework that guarantees transparency, fairness, accountability, and respect for fundamental rights. The protection of privacy, the prevention of bias, and the maintenance of human supervision are not optional—they are indispensable conditions for legitimacy and public trust. At the same time, internal strategies must prioritize the training and continuous upskilling of officers, the recruitment of technical experts, and the establishment of multidisciplinary teams combining legal, operational, and scientific expertise. The best way to be able to develop a reasoning and responsible AI is to create a dedicated center against crime
gathering in a same place expert of science, law, job, training and international affairs.

The future of AI in gendarmerie-type forces will therefore depend on a careful balance. On one side, the need to innovate, modernize, and keep pace with increasingly sophisticated forms of crime; on the other, safeguard liberties, and preserve human judgment at the core of decision-making. Striking this balance will be the decisive factor in turning AI into a genuine asset for security forces rather than a source of risk or mistrust.

In conclusion, artificial intelligence is not simply a tool—it is a strategic transformation. By approaching it responsibly, transparently, and collaboratively, gendarmerie-type forces can ensure that AI enhances operational efficiency, strengthens international cooperation, and contributes to the protection of citizens. Above all, it is by keeping humans at the center—officers, citizens, and institutions—that AI will fulfill its promise as a technology serving population in their collective as well as individual dimension.

Conception éditoriale et rédaction :
Crédits photographiques : ©MAJ Maurice Lehmann, ©GND Romain Culpin
Conception graphique : BRC Axel Goumillou