INTEGRATING KNOWLEDGE MANAGEMENT AND ARTIFICIAL INTELLIGENCE TO OVERCOME CONTEMPORARY CHALLENGES IN DETECTING AND PROVING CRIME

Alexandru Ioan[1], **PhD**

Department for Emergency Situations,Ministry of Internal Affairs, Romania
National School for Political and Administrative Studies, Bucharest, Romania

ABSTRACT

Purpose: This study explores how integrating knowledge management (KM) systems with artificial intelligence (AI) can effectively address contemporary challenges in detecting and proving crime, particularly concerning increasingly sophisticated criminal activities.

Design/Methods/Approach: The research employs qualitative analysis of recent case studies and literature review, focusing on existing KM frameworks and rapid AI-based analytic tools. This approach allows for swift assessment and immediate application in practical investigative contexts, suitable for short-term investigative requirements.

Findings: Preliminary results demonstrate that AI-driven KM systems significantly improve crime detection and evidence-gathering processes. Enhanced data analytics, predictive modeling, and automated evidence correlation provided by AI augment traditional investigative techniques, enable quicker response times and improved accuracy in criminal investigations.

Originality/Value: This paper uniquely bridges the gap between KM practices and contemporary forensic investigation methodologies by introducing AI capabilities as a central element of criminal justice frameworks. The approach presented here not only extends theoretical understandings but also offers practical implications for law enforcement agencies facing advanced crime threats, thereby contributing to safer communities.

Keywords: artificial intelligence, artificial knowledge, crime detection, forensic investigation, knowledge management, predictive analytics.

About the author

Major **Alexandru Ioan**, PhD, is a seasoned professional with extensive experience in law enforcement and management roles, excelling in leadership and organizational operations related to public safety and security. His expertise covers strategic planning, interpersonal communication, and criminal investigations, supported by advanced degrees in management, economics, and legal sciences. Actively engaged in continuous professional development through certifications and training in cybersecurity, law enforcement, and project management, Alexandru Ioan possesses a versatile skill set including digital competencies, technical proficiency, and multilingual capabilities, allowing effective contributions across organizational contexts.

1 aioan.mail@gmail.com

PURPOSE

The accelerating complexity of criminal phenomena, coupled with the exponential growth of digital data, requires law-enforcement agencies to evolve beyond traditional information management toward intelligent knowledge ecosystems. This study aims to explore how the integration of Knowledge Management (KM) and Artificial Intelligence (AI) can strengthen the processes of detecting and proving crime, while safeguarding ethical, legal, and evidentiary standards. Building upon the conceptual foundations of knowledge dynamics and organizational learning, the research investigates how AI-driven tools — such as explainable analytics, knowledge graphs, and human-in-the-loop systems — can enhance institutional knowledge flows and decision-making capabilities.

The paper positions AK as the convergence point between human cognition and machine intelligence, proposing that co-created knowledge can improve both the efficiency and transparency of criminal investigations. It also aligns this technological transformation with emerging governance frameworks, including the *EU Artificial Intelligence Act* and the *NIST AI Risk Management Framework*, ensuring responsible and accountable adoption. Ultimately, the purpose of this research is to articulate a coherent, ethically grounded model for integrating AI-enabled KM into contemporary policing and forensic practice.

LITERATURE REVIEW

This literature review synthesizes open-access and verifiable sources spanning KM in policing, AI in investigation and forensics, human–AI teaming, governance and ethics (EU AI Act, NIST AI RMF, HLEG), and convergent notions of AK. The objective is to ground a coherent conceptual and operational bridge between KM and AI for detecting and proving crime, while highlighting implications for evidentiary reliability, institutional learning, and cross-border cooperation.

KM in policing and criminal justice

Foundational KM research tailored to policing shows that law-enforcement agencies routinely generate and circulate both *tacit* (experience-based) and *explicit* (codified) knowledge, yet face structural barriers to capturing and reusing it at scale. Classic U.S. Department of Justice studies argued for treating frontline know-how as organizational intellectual capital and for integrating KM techniques into an interrelated system rather than isolated tools (e.g., after-action reviews, communities of practice, repositories) (Pendleton et al., 2001). These works emphasized leadership, culture, and workflow redesign to surface tacit insights and connect them to decision cycles. (Pendleton, Chavez, & Bueerman, 2001, pp. 1–3).

A systematic review of European studies (2000–2013) found research skewed toward intra-organizational sharing, criminal intelligence, and technology, with persistent impediments grouped into strategy/legislation, technology, culture, and knowledge loss; the review called for leadership attention and for bridging regional and institutional boundaries — an agenda that remains remarkably current (Griffiths et al., 2016).

Intelligence-Led Policing (ILP) codifies the KM–operations interface by linking information flows, analysis, and decision-making in a repeatable cycle. The OSCE ILP Guidebook sets out a process architecture (tasking, collection, evaluation, analysis, dissemination) and underscores legality, proportionality, and partnership working for knowledge exchange (OSCE, 2017). The United Nations DPO's *Manual on Intelligence-Led Policing* updates this for peace operations, emphasizing human-rights-com-

pliant collection, structured analytical products, and institutional learning loops — principles directly translatable to domestic policing KM and to cross-agency cooperation (UN DPO, 2025).

Within KM theory, Brătianu and Bejinaru reconceptualize knowledge beyond "stock/flow" metaphors by introducing *knowledge fields* and *knowledge dynamics* via a thermodynamics lens: rational, emotional, and spiritual forms of knowledge transform into one another; managing the *transformational* dynamics (not merely storage and transfer) is the key to organizational learning and innovation (Brătianu & Bejinaru, 2019, 2020). This energetic view is valuable in policing, where morale, sense-making under stress, and values shape evidence interpretation as much as rules and databases.

Recent work specific to KM and AI integration maps the research frontier. A bibliometric analysis highlights rapid growth and fragmentation in the KM–AI nexus and calls for robust conceptual scaffolding and empirical validation in core KM processes (creation, sharing, use) (Brătianu & Ioan, 2025). Complementarily, a systematic review proposes a research agenda to reconcile the "technology-centric" and "human-centric" poles of KM through AI capabilities while cautioning that barriers and risks remain under-studied (Nakash & Bolisani, 2024).

AI for detection, triage, and proof

Law-enforcement agencies in the EU collectively report accelerating adoption of AI for pattern detection, multimedia triage, language technologies, and resource optimization — while confronting acute issues of data quality, bias, explainability, and capability gaps (Europol Innovation Lab, 2024). Eurojust and eu-LISA extend this picture to judicial cooperation: AI promises efficiency in mutual legal assistance and evidence analysis, but admissibility, transparency, and due-process safeguards require early design attention and governance alignment (Eurojust & eu-LISA, 2022).

The INTERPOL–UNICRI Toolkit offers an operational playbook for "responsible AI innovation" in law enforcement, from problem framing and data governance to evaluation and human oversight. It operationalizes abstract principles into procurement, piloting, and deployment checklists that can be embedded in agency KM procedures (INTERPOL & UNICRI, 2023). In parallel, the U.S. federal guidance underscores validation, measurement, and accountability in criminal-justice AI, calling out risks for civil liberties and recommending governance mechanisms to scrutinize models used in forensic and investigative contexts (U.S. DOJ, 2024).

At the technical layer, explainability and auditability are essential to bridge AI outputs with evidentiary standards. An open-access study shows how explainable AI (XAI) techniques can clarify intrusion-detection system inferences, improving analyst trust and making algorithmic reasoning auditable — an approach generalizable to many investigative models (Hermosilla et al., 2025). Likewise, knowledge graphs combined with ML have been demonstrated to structure investigative entities, relations, and provenance, thereby supporting insight discovery and transparent evidence linking (Iyengar et al., 2024).

Earlier U.S. NIJ work mapped AI opportunities across the justice chain — from video analytics to triage of digital evidence — and stressed co-design with practitioners and measurable benefit-risk trade-offs (Rigano, 2019). These practice-oriented lines complement the policy and governance literature, anchoring AI's role not as a black box "oracle," but as a decision-support layer embedded in KM workflows.

Human–AI teaming and the emergence of "artificial knowledge"

Two comprehensive surveys formalize *human-in-the-loop (HITL)* machine learning as a family of methods that systematically inject expert judgment into the model lifecycle (data curation, feature engineering, active learning, interactive labeling, post-hoc calibration), thereby improving performance,

safety, and acceptance in high-stakes domains (Wu et al., 2022; Wang, Guo, & Chen, 2022). From a socio-technical vantage, *team-centered AI* emphasizes role clarity, shared mental models, communication, and workload distribution in human–AI teams — critical to avoid automation bias and to ensure investigators retain agency over evidential reasoning (Hagemann, Kluge, & Zohren, 2023).

These developments converge with the AK concept. Brătianu and Bejinaru (2025) define AK as the product of AI systems — especially generative AI — coexisting with human knowledge within KM systems; they frame integration strategies that treat AK as complementary, not substitutive, with explicit attention to the different genesis and validation logics of human vs. machine outputs (Brătianu & Bejinaru, 2025). Brătianu (2025) further situates technology within societal and ethical ambits, arguing that managerial discernment, values, and foresight are needed to capture benefits without eroding human judgment or social trust.

A related strand explores *entropy-informed* perspectives: Mageed (2024) argues that entropy offers a unifying lens for uncertainty quantification in AI and for measuring *knowledge entropy* in organizations — useful for diagnosing where knowledge transfer (including intergenerational transfer) fails and where codification vs. personalization strategies should be prioritized (Mageed, 2024). Together, HITL, team-centered AI, AK, and entropy perspectives motivate a KM-first integration pattern: encode *who does what* (roles), *how knowledge flows* (process), and *how uncertainty is surfaced and reduced* (methods) so that AI outputs become auditable *knowledge objects* within the institution.

Ethical, legal, and risk-management frameworks

Three complementary governance anchors shape legitimate AI use in policing and justice: EU ethics guidance (HLEG), binding regulation (EU AI Act), and risk management frameworks (NIST AI RMF). The *Ethics Guidelines for Trustworthy AI* articulate seven requirements — human agency and oversight; technical robustness and safety; privacy and data governance; transparency; diversity, non-discrimination and fairness; societal/environmental well-being; and accountability — and provide an assessment list to operationalize them (HLEG, 2019). The *EU Artificial Intelligence Act* (Regulation (EU) 2024/1689) introduces a risk-tiered regime with obligations for high-risk systems, including risk management, technical documentation, data governance, logging, transparency, human oversight, and post-market monitoring; it also contains specific safeguards for certain law-enforcement uses (e.g., biometric identification) (European Parliament & Council, 2024).

The *NIST AI Risk Management Framework (AI RMF 1.0)*, although non-binding in the EU, is widely used as a practical scaffold. Its GOVERN–MAP–MEASURE–MANAGE functions align with ILP/KM cycles: governance policies and roles; context/impact mapping; measurement and evaluation (including bias, validity, security, and explainability); and risk treatment across the AI lifecycle (NIST, 2023). In law-enforcement contexts, adopting AI RMF-style profiles can harmonize procurement, testing, and deployment with the obligations of the EU AI Act while preserving traceability for evidentiary scrutiny.

Institution-specific guidance complements these frameworks. The INTERPOL–UNICRI Toolkit packages responsible-AI practices into checklists for problem definition, dataset audit, model assurance, and oversight — including community engagement and grievance mechanisms suited to sensitive policing deployments (INTERPOL & UNICRI, 2023). The Europol's analysis catalogues operational benefits and cautions and advocates shared EU competencies, training, and common testing facilities to reduce fragmentation (Europol Innovation Lab, 2024). Eurojust points to cross-border casework where AI can help with translation, classification, and prioritization but urges alignment with fair-trial rights and judicial independence (Eurojust & eu-LISA, 2022).

From artefacts to admissible knowledge

A recurring theme across technical and governance sources is the need to transform AI system outputs into *admissible knowledge objects* with provenance, context, and interpretability sufficient for courts and oversight bodies. Hermosilla et al. (2025) show that XAI can surface decision pathways and feature influences in IDS contexts; analogously, investigators can demand model cards, decision logs, and explanations in computer-vision or NLP systems used in digital forensics (Hermosilla et al., 2025). Knowledge-graph approaches help encode entities, relationships, and supporting evidence with timestamps and sources, making linkages auditable and falsifiable (Iyengar et al., 2024).

The EU AI Act documentation, logging, and human-oversight provisions directly support evidentiary defensibility, while HLEG's transparency and accountability requirements frame institutional duties to explain and justify (European Parliament & Council, 2024; HLEG, 2019). NIST's MAP/MEASURE activities recommend explicit identification of harms, impacted communities, and measurement strategies — inputs that can be mirrored in case files and disclosure packs (NIST, 2023). The U.S. DOJ report likewise recommends rigorous validation and auditing regimes tailored to justice applications — reinforcing that *model evidence* becomes *case evidence* only when governance, testing, and documentation close the gaps (U.S. DOJ, 2024).

Organizational capability building: culture, leadership, and learning loops

The shift from tools to knowledge systems is cultural as much as technical. The DOJ COPS volume underscored innovation leadership and the necessity to integrate KM techniques into a coherent system (Pendleton et al., 2001). The European systematic review urged leadership-driven strategies, procedural clarity, and training to build the motivation and skills for sharing (Griffiths et al., 2016). ILP handbooks (OSCE; UN DPO) illustrate how to embed knowledge capture and feedback in operational tasking cycles and to formalize analyst–operator dialogues that prevent siloing (OSCE, 2017; UN DPO, 2025).

In KM theory, treating knowledge as dynamic fields reframes capacity building as enabling *transformations* (e.g., from emotional to rational knowledge during briefings; from rational to spiritual knowledge when values and legitimacy are at stake) (Brătianu & Bejinaru, 2020). For AI integration, this supports interventions such as pre-mortems (to surface tacit concerns), red-team reviews (to stress-test models), and structured debriefs that explicitly translate experiential insights into dataset improvements and model governance artifacts — linking HITL practice (Wu et al., 2022; Wang et al., 2022) to KM outcomes.

Finally, strategic reflections on technology's societal role counsel prudence: capture AI's productivity and insight gains without allowing them to displace human judgment, professional ethics, or community trust. Managers must design KM strategies that preserve human agency while leveraging AK as a complementary asset (Brătianu, 2025; Brătianu & Bejinaru, 2025).

Toward an AI-enabled KM framework for detecting and proving crime

Across these sources, four design imperatives recur:

- *Legibility and auditability of AI-derived knowledge*. Use XAI, knowledge graphs, model documentation, and logging to convert AI outputs into evidentiary objects with provenance and context (Hermosilla et al., 2025; Iyengar et al., 2024; EU AI Act; HLEG; NIST).

- *HITL and team-centered operations*. Design workflows that institutionalize human oversight, feedback, and shared mental models to mitigate automation bias and support learning (Wu et al., 2022; Wang et al., 2022; Hagemann et al., 2023; INTERPOL–UNICRI).
- *KM-first integration*. Embed AI within ILP/KM cycles and organizational culture (tasking–collection–analysis–dissemination–review), aligning with DOJ COPS guidance, OSCE/UN DPO ILP, and Europol/Eurojust recommendations for cross-border contexts (Pendleton et al., 2001; OSCE, 2017; UN DPO, 2025; Europol, 2024; Eurojust & eu-LISA, 2022).
- *Conceptual coherence*. Adopt thermodynamics-based KM (knowledge fields/dynamics), entropy-informed uncertainty management, and AK as the human–machine synthesis layer — ensuring AI augments, rather than substitutes, professional judgment (Brătianu & Bejinaru, 2019, 2020, 2025; Mageed, 2024; Brătianu & Ioan, 2025; Nakash & Bolisani, 2024).

Together, these strands justify an integrated *AI-enabled KM framework* for modern investigations: (i) governed by ethics, law, and risk controls (HLEG; EU AI Act; NIST), (ii) operationalized through ILP/KM processes and cross-border cooperation (OSCE; UN DPO; Europol; Eurojust), (iii) tooled with explainable, knowledge-graph-aware analytics (Hermosilla et al.; Iyengar et al.), and (iv) sustained by human–AI teaming practices and learning loops that cultivate AK as a traceable, admissible, and *useful* addition to institutional memory (Wu et al.; Wang et al.; Hagemann et al.; Brătianu & Bejinaru; Brătianu & Ioan; Nakash & Bolisani).

DESIGN/METHODS/APPROACH

The methodological design of this study follows a qualitative, interpretive research strategy aimed at exploring how the integration of KM and AI can address contemporary challenges in detecting and proving crime. Given the conceptual nature of the topic and the extensive availability of recent scholarly and institutional sources, a systematic qualitative document analysis (QDA) was employed. This approach allows the extraction, comparison, and synthesis of theoretical constructs, operational principles, and policy implications across multiple open-access publications, reports, and regulatory documents.

Research design

The study adopts an exploratory-descriptive design, intended to map and interpret relationships among three central constructs — *Knowledge Management*, *Artificial Intelligence*, and *Artificial Knowledge* — within the broader framework of criminal investigation and forensic evidence management. The investigation relies on secondary qualitative data, consisting exclusively of peer-reviewed articles, institutional manuals, international frameworks, and policy documents published between 2017 and 2025. This design aligns with prior interpretive KM research that privileges conceptual depth and contextual understanding over statistical generalization (Brătianu & Bejinaru, 2019; Nakash & Bolisani, 2024).

Data selection and analysis

A purposive sampling strategy was applied to identify documents that explicitly discuss:

- the role of KM in law enforcement or intelligence-led policing,
- the application of AI or machine learning in criminal justice, and
- theoretical or ethical frameworks addressing the human–AI knowledge interface.

Thirty open-access sources meeting these criteria were selected. They include academic journal articles, institutional manuals (e.g., OSCE, UN DPO, NIST), policy frameworks (e.g., EU AI Act, Ethics

Guidelines for Trustworthy AI), and technical or methodological studies (e.g., explainable AI, human-in-the-loop learning). Each document was reviewed in full to ensure relevance, credibility, and methodological transparency.

The qualitative analysis combined directed content analysis and conceptual synthesis:

Thematic coding. Text segments were coded using three overarching categories derived from the research objectives:

- *KM and organizational learning in law enforcement*;
- *AI applications and forensic investigation challenges*; and
- *Convergence through AK and human–AI teaming.*

Subcodes captured recurring patterns such as knowledge flows, explainability, human oversight, data governance, and evidentiary traceability.

Iterative interpretation. Through repeated reading and cross-document comparison, recurring theoretical propositions were identified — such as the complementarity of tacit and explicit knowledge (Brătianu & Bejinaru, 2020), or the need for explainable and auditable AI (Hermosilla et al., 2025; Iyengar et al., 2024). Concepts were then clustered into higher-order analytical themes that shaped the structure of the literature review and findings sections.

Triangulation. To ensure interpretive validity, insights were cross-checked between distinct document types (academic, regulatory, technical). For example, the *Ethics Guidelines for Trustworthy AI* (2019) and *Regulation (EU) 2024/1689* were juxtaposed with empirical analyses of policing practices (Europol, 2024; UN DPO, 2025) to derive consistent principles applicable to evidentiary contexts.

Analytical framework

The analytical process was guided by an integrative framework combining:

- *Knowledge dynamics theory* (Brătianu & Bejinaru, 2019, 2020), emphasizing transformational flows of knowledge;
- *Human-in-the-loop and team-centered AI models* (Wang et al., 2022; Hagemann et al., 2023), illustrating co-creation of AK; and
- *Governance and risk frameworks* (NIST, 2023; European Parliament & Council, 2024) that ensure legal and ethical compliance.

The synthesis of these dimensions enabled the formulation of a conceptual model situating AI-enabled KM within the investigative cycle — from intelligence collection and analysis to decision-making and evidentiary validation.

Methodological limitations

As a qualitative conceptual inquiry, this study does not include quantitative metrics or statistical validation. The conclusions rely on interpretive reasoning and triangulation rather than numerical generalization. Nevertheless, this approach provides depth, conceptual clarity, and policy relevance, laying a rigorous foundation for subsequent empirical validation through case studies or field applications in law-enforcement settings.

Ethical and quality considerations

All analysed materials were open-access or publicly available sources, ensuring compliance with academic integrity and intellectual property standards. Analytical transparency was maintained through systematic referencing, traceable citations, and alignment with recognized frameworks for qualitative research credibility — namely, dependability, confirmability, and transferability.

FINDINGS

The qualitative analysis of open-access academic and institutional sources revealed converging insights on how KM and AI can jointly enhance the detection and proof of crime. The results demonstrate that the effective integration of AI into law-enforcement knowledge ecosystems depends on (1) the maturity of organizational KM processes, (2) the degree of transparency and explainability embedded in AI systems, and (3) the establishment of ethical and regulatory safeguards ensuring human oversight and evidentiary integrity.

Table 1 below synthesizes the main conceptual contributions derived from the reviewed literature. Each thematic cluster reflects one of the three analytical axes of the study — *KM Foundations*, *AI and Forensic Innovation*, and *AK Convergence* — cross-referenced with key frameworks and representative sources.

Table 1: *Synthesis of Key Findings from the Qualitative Document Analysis*
(Source: Author's processing)

Thematic Cluster	**Key Insights**	**Sources**
KM in Law Enforcement	KM processes such as knowledge capture, sharing, and reuse remain fragmented across institutions. Tacit knowledge and experiential learning are undervalued but essential for intelligence analysis and operational coordination. ILP frameworks operationalize KM principles through the intelligence cycle (tasking–collection–analysis–dissemination–review).	Pendleton et al. (2001); Griffiths et al. (2016); OSCE (2017); UN DPO (2025)
Dynamic Knowledge Transformations	Knowledge behaves as an energy-like field undergoing transformations between rational, emotional, and spiritual states; effective KM strategies must facilitate these conversions to enable innovation and adaptive learning.	Brătianu & Bejinaru (2019, 2020); Brătianu (2025)
Integration of KM and AI	AI extends KM capabilities from data storage to semantic reasoning, predictive modeling, and decision support. Empirical gaps persist in validating these systems within law enforcement.	Brătianu & Ioan (2025); Nakash & Bolisani (2024)
AI for Crime Detection and Evidence Analysis	AI systems improve speed, precision, and pattern recognition in investigations but require human interpretive oversight to maintain accountability and admissibility.	Europol (2024); Eurojust & eu-LISA (2022); Rigano (2019)
Explainable and Auditable AI	Explainable AI (XAI) and knowledge graphs transform opaque algorithmic results into transparent, auditable evidence, supporting judicial scrutiny and chain of custody.	Hermosilla et al. (2025); Iyengar et al. (2024)

Thematic Cluster	Key Insights	Sources
Human–AI Collaboration	Human-in-the-loop and team-centered AI models demonstrate that the most reliable systems retain human agency for contextual judgment, bias correction, and situational awareness.	Wu et al. (2022); Wang et al. (2022); Hagemann et al. (2023)
AK as Convergence	AK represents the synthesis between human cognition and machine-generated insights; it is validated through interaction, not automation.	Brătianu & Bejinaru (2025); Mageed (2024)
Ethical and Legal Alignment	Trustworthy AI in policing requires adherence to risk-based governance (AI Act), ethical principles (HLEG), and documented accountability mechanisms (NIST AI RMF).	European Parliament & Council (2024); HLEG (2019); NIST (2023)
Organizational Learning and Change Management	Successful AI–KM integration depends on leadership commitment, inter-agency learning loops, and a culture that values transparency, documentation, and cross-domain collaboration.	Griffiths et al. (2016); UN DPO (2025); INTERPOL & UNICRI (2023)

Emerging Patterns

Three dominant patterns emerged from the analysis (Figure 1):

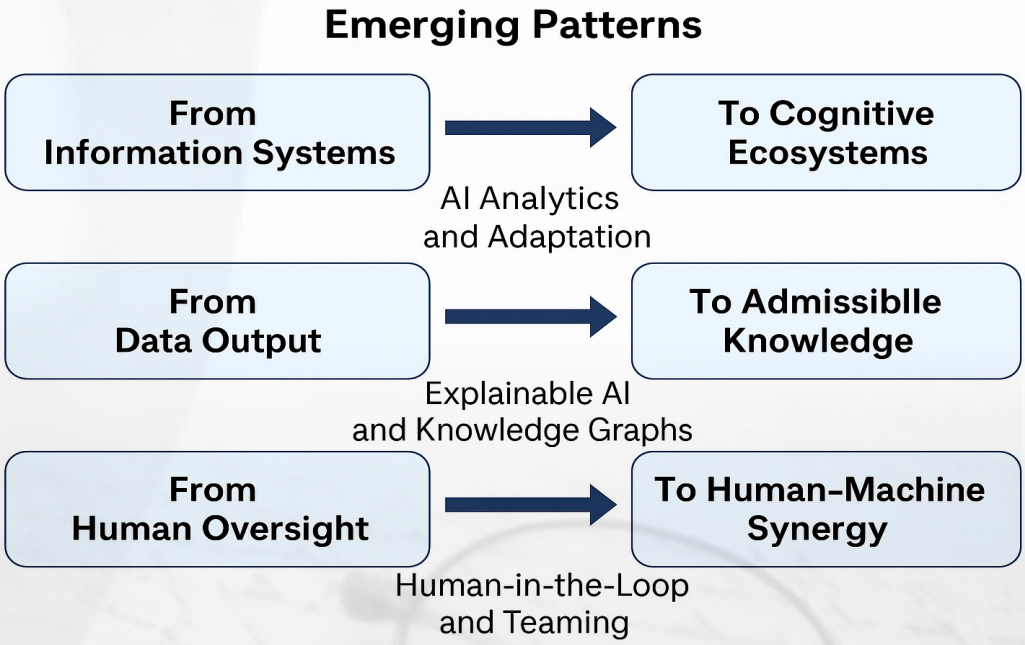

Figure 1: *Emerging Patterns* (Source: Author's processing)

From Information Systems to Cognitive Ecosystems. The integration of AI transforms KM infrastructures into *cognitive ecosystems* where human expertise, digital records, and algorithmic analytics coexist. Traditional KM tools (databases, reports, after-action reviews) evolve into interactive, adaptive systems capable of detecting patterns and generating hypotheses in near real time (Brătianu & Ioan, 2025; Nakash & Bolisani, 2024).

From Data Output to Admissible Knowledge. The distinction between *data*, *information*, and *knowledge* becomes legally and operationally critical. Explainable AI and knowledge graphs enable the transformation of machine outputs into structured, traceable, and evidentiary knowledge artifacts (Hermosilla et al., 2025; Iyengar et al., 2024). This evolution supports judicial standards of transparency and reproducibility under the EU AI Act (2024).

From Human Oversight to Human–Machine Synergy. Human involvement shifts from reactive oversight to proactive co-creation of knowledge. Human-in-the-loop and team-centered AI frameworks (Wu et al., 2022; Hagemann et al., 2023) demonstrate that when human experts guide data interpretation and contextualization, algorithmic accuracy and trustworthiness increase substantially. In policing, this manifests as analyst–AI collaboration where investigators validate, annotate, and recontextualize system outputs within institutional KM systems.

The AI-Enabled KM Cycle

To visualize the integration between KM and AI within law enforcement workflows, the study proposes the conceptual model *"AI-Enabled KM Cycle for Criminal Investigation"* (Figure 2).

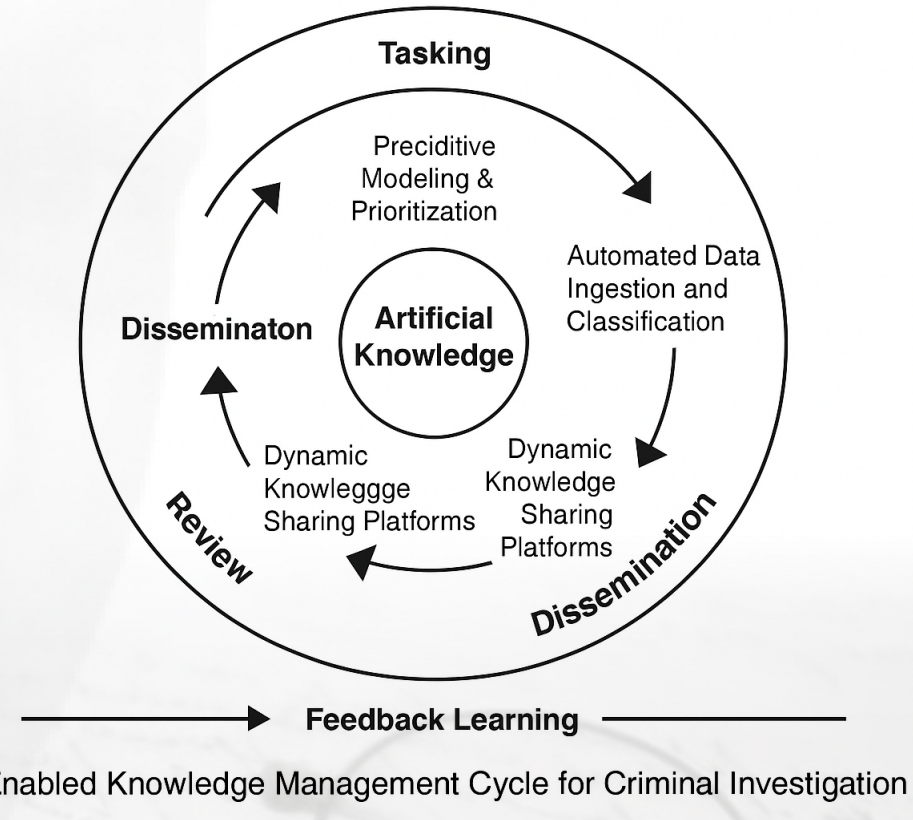

Figure 2: *AI-Enabled KM Cycle for Criminal Investigation* (Source: Author's processing)

The model is represented as a cyclic, five-phase framework reflecting continuous learning and feedback between human and machine actors.

The outer cycle mirrors the *intelligence-led policing* structure (Tasking → Collection → Analysis → Dissemination → Review).

The inner cycle embeds AI-driven processes that augment each stage:

- *Tasking* → predictive modeling & prioritization (AI analytics support resource allocation).

- *Collection* → automated data ingestion and classification (AI assists in capturing and structuring knowledge).
- *Analysis* → hybrid reasoning (human + AI co-analysis via knowledge graphs and XAI tools).
- *Dissemination* → dynamic knowledge sharing platforms (KM systems updated with validated insights).
- *Review* → feedback learning (results fed back into AI models for retraining and into KM systems for organizational learning).

A feedback arrow connects *Review* to *Tasking*, symbolizing the learning loop and the emergence of AK — the shared, validated, and evolving knowledge space that fuses human judgment and AI insight.

This cyclical model illustrates the dual transformation identified in the findings: (1) AI enhances the operational intelligence cycle by automating data-intensive tasks, and (2) KM ensures that insights — human or machine — are institutionalized, ethically governed, and legally defensible.

Consolidated Interpretation

The integration of AI and KM in law enforcement represents not merely a technological modernization, but a paradigm shift from reactive data management to proactive knowledge creation. Key implications include:

Efficiency and Accuracy: AI-supported KM accelerates investigative processes while improving accuracy through automated data correlation and anomaly detection (Europol, 2024).

Transparency and Accountability: Embedding explainability and governance frameworks (HLEG, 2019; NIST, 2023) ensures that AI-generated insights can withstand judicial scrutiny.

Institutional Learning: Knowledge captured through ILP and KM systems fosters organizational memory, reducing repetition of past errors and enabling rapid adaptation in crisis situations (UN DPO, 2025).

Ethical Safeguards: Compliance with the EU AI Act (2024) and the Ethics Guidelines for Trustworthy AI protects against discriminatory practices, ensuring proportionality and respect for fundamental rights.

Human–Machine Synergy: The emergence of AK confirms that value is maximized not when AI replaces human expertise, but when it complements and extends it within an ethical, transparent KM ecosystem (Brătianu & Bejinaru, 2025).

The synthesis of qualitative evidence supports the argument that AI-enabled KM enhances both operational capability and evidentiary integrity in modern law enforcement. The transition from data-centric to knowledge-centric systems — governed by ethical frameworks and reinforced through human–AI collaboration — creates a resilient, transparent, and adaptive foundation for detecting and proving contemporary forms of crime.

ORIGINALITY/VALUE

This paper contributes a novel, integrative perspective on the intersection between KM and AI within the context of contemporary criminal investigation. Its originality lies in bridging conceptual, operational, and ethical dimensions that have traditionally been studied in isolation. By synthesizing insights from thirty-one open-access academic and institutional sources, the study constructs a coherent framework demonstrating how AI can transform KM from a repository-centered practice into a *dynamic, cognitive ecosystem* for law enforcement.

Unlike previous research that emphasized either technological innovation or organizational reform, this study positions AK — the emergent fusion of human expertise and machine intelligence — as a *third knowledge domain*. Within this paradigm, AI is not merely an analytical tool but an epistemic partner contributing to the creation, validation, and institutionalization of knowledge relevant to the detection and proof of crime.

The paper further advances scholarly discourse by translating theoretical constructs such as knowledge fields and knowledge dynamics (Brătianu & Bejinaru, 2020) into a law-enforcement setting, integrating them with explainable AI, human-in-the-loop frameworks, and the ethical governance structures defined by the EU AI Act (2024) and NIST AI RMF (2023). The resulting model — the *AI-Enabled KM Cycle for Criminal Investigation* — provides an actionable template for agencies seeking to balance efficiency, accountability, and human oversight.

Practically, the research offers policymakers and law-enforcement leaders a roadmap for responsibly embedding AI into investigative processes without compromising evidentiary integrity or legal proportionality. Academically, it enriches the limited literature connecting KM theory, forensic science, and AI ethics. Conceptually, it reframes crime detection as a process of *knowledge creation* governed by transparency, collaboration, and adaptive learning — a significant step toward operationalizing trustworthy, AI-augmented intelligence in the criminal justice domain.

REFERENCES

Brătianu, C. (2025). The challenge of artificial knowledge on knowledge management systems. In P. Gazzola & G. Dominici (Eds.), *Technology and society: Boon or bane?* (*BSLAB 2025, Springer Proceedings in Business and Economics*, pp. 3–18). Springer. https://doi.org/10.1007/978-3-032-07163-7_1

Brătianu, C., & Bejinaru, R. (2019). The theory of knowledge fields: A thermodynamics approach. *Systems, 7*(2), 20. https://doi.org/10.3390/systems7020020

Brătianu, C., & Bejinaru, R. (2020). Knowledge dynamics: A thermodynamics approach. *Kybernetes, 49*(1), 6–21. https://doi.org/10.1108/K-02-2019-0122

Brătianu, C., & Bejinaru, R. (2025). Integrating artificial intelligence and artificial knowledge in the knowledge management systems. *Proceedings of the 19th International Conference on Business Excellence 2025 (PICBE)*, 3171–3179. https://doi.org/10.2478/picbe-2025-0242

Brătianu, C., & Ioan, A. (2025). Challenges of artificial intelligence for knowledge management systems: A bibliometric analysis perspective. *Oradea Journal of Business and Economics, 10*(1), 108–120. https://doi.org/10.47535/1991ojbe183

European Commission—High-Level Expert Group on AI. (2019). *Ethics guidelines for trustworthy AI*. Publications Office. https://doi.org/10.2759/346720

European Commission—Publications Office. (2025). *AI and policing—Main report landing page.* https://www.europol.europa.eu/publication-events/main-reports/ai-and-policing

European Parliament & Council. (2024). *Regulation (EU) 2024/1689—Artificial Intelligence Act.* Official Journal of the European Union. https://data.europa.eu/eli/reg/2024/1689/oj

Eurojust & eu-LISA. (2022). *Artificial intelligence supporting cross-border cooperation in criminal justice.* https://www.eurojust.europa.eu/sites/default/files/assets/artificial-intelligence-cross-border-cooperation-criminal-justice-report.pdf

Europol Innovation Lab. (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

Griffiths, K., Birdi, K., Alsina, V., Andrei, D., Baban, A., Bayerl, P. S.,Vonas, G. (2016). Knowledge sharing practices and issues in policing contexts: A systematic review of the literature. *European Journal of Policing Studies, 3*(3), 267–291. Open-access VoR. https://shura.shu.ac.uk/13586/

Hagemann, V., Kluge, A., & Zohren, S. (2023). Human–AI teams: Challenges for a team-centered AI at work. *Frontiers in Artificial Intelligence, 6*, 1252897. https://doi.org/10.3389/frai.2023.1252897

Hermosilla, P., Díaz, M., Berríos, S., & Allende-Cid, H. (2025). Use of explainable artificial intelligence for analyzing and explaining intrusion detection systems. *Computers, 14*(5), 160. https://www.mdpi.com/2073-431X/14/5/160

INTERPOL & UNICRI. (2023). *Toolkit for responsible AI innovation in law enforcement.* https://www.interpol.int/en/How-we-work/Innovation/Artificial-Intelligence-Toolkit

INTERPOL/UNICRI. (2025). *Introduction to responsible AI innovation (companion resource).* https://unicri.org/sites/default/files/2025-03/Intro_Resp_AI_Innovation_Mar25.pdf

Iyengar, S. S., et al. (2024). Advancing forensic science: AI and knowledge graphs unlock new insights. *Journal of Forensic Research, 15*(3), 615. https://doi.org/10.37421/2157-7145.2024.15.615

Nakash, M., & Bolisani, E. (2024). Knowledge management meets artificial intelligence: A systematic review and future research agenda. In *Proceedings of the 25th European Conference on Knowledge Management* (pp. 544–552). Academic Conferences International. https://doi.org/10.34190/eckm.25.1.2443

National Institute of Standards and Technology (NIST). (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0).* https://doi.org/10.6028/NIST.AI.100-1

OSCE. (2017). *Guidebook on intelligence-led policing.* https://www.osce.org/files/f/documents/d/3/327476.pdf

Pendleton, M. R., Chavez, T. D., Jr., & Bueerman, J. (2001). *Knowledge management in policing.* U.S. DOJ, COPS Office. Open-access PDF. https://sandbox:/mnt/data/GOVPUB-J36-PURL-gpo8361.pdf

Rigano, C. (2019). Using artificial intelligence to address criminal justice needs. *NIJ Journal, 280.* National Institute of Justice. https://nij.ojp.gov/topics/articles/using-artificial-intelligence-address-criminal-justice-needs

U.S. Department of Justice. (2024). *Artificial intelligence and criminal justice: Final report (pursuant to Executive Order 14110).* https://sandbox:/mnt/data/AI EO Report (2024.12.03) - final.pdf

UN Department of Peace Operations (UN DPO). (2025). *Manual on intelligence-led policing (2025.14).* https://resourcehub01.blob.core.windows.net/%24web/Policy%20and%20Guidance/corepeacekeepingguidance/Thematic%20Operational%20Activities/Police%20and%20Law%20Enforcement/2025.14%20Manual%20on%20Intelligence-Led%20Policing.pdf

United Nations Peacekeeping Resource Hub. (2025). *Policy and guidance: UN police—Manuals and guidance (index).* https://peacekeepingresourcehub.un.org/en/policy

Wang, H., Guo, Z., & Chen, H. (2022). Human-in-the-loop machine learning: A macro–micro perspective. *arXiv preprint* arXiv:2202.10564. https://arxiv.org/abs/2202.10564

Wu, T., Lin, C., Zhang, W., & Yu, P. S. (2022). A survey of human-in-the-loop for machine learning. *arXiv preprint* arXiv:2108.00941 (v3, 2022). https://arxiv.org/abs/2108.00941