



CADERNOS DE DEREITO ACTUAL

www.cadernosdedereitoactual.es

© **Cadernos de Direito Actual** Nº 33. Núm. Ordinario (2026), pp. 558-591

·ISSN 2340-860X - ·ISSNe 2386-5229

Automated cybercrime monitoring systems in view of legal restrictions

Ivo Svoboda¹

Academy of the Police Force in Bratislava

Serhii Hermanov²

Donetsk State University of Internal Affairs

Olesia Urlapova³

Interregional Academy of Personnel Management

Ihor Fedchak^{4,*}

Lviv State University of Internal Affairs

Oleh Zachek⁵

Lviv State University of Internal Affairs

Summary: 1. Introduction. 2. Literature review. 2.1 Technical and conceptual directions of AI-based cybercrime detection. 2.2 Technical architectures for AI-based detection. 2.3 Research in AI governance and regulatory compliance. 2.4 Legislative and cross-system restrictions. 2.5 Architectural and legal mechanistic models. 2.6. A systematic comparison of existing approaches. 2.7 Identified research shortcomings and determination of the study contribution. 3. Methods. 3.1 Research design. 3.2 Sampling. 3.3 Research methods. 3.4 Built-in compliance checking method

¹ Guarantor of the Security Management Studies, AMBIS, a.s. Vyská škola, Prague, Czech Republic; Academy of the Police Force in Bratislava, Bratislava, Slovak Republic. ORCID: 0000-0002-0941-4686; Email: svobodaivo232@gmail.com

² Vice-Rector of Donetsk State University of Internal Affairs, Kropyvnytskyi, Ukraine. ORCID: 0000-0002-0151-7680; Email: serhihermanov@gmail.com

³ PhD Student of Interregional Academy of Personnel Management, Kyiv, Ukraine. ORCID: 0009-0003-5839-5383; Email: lesiaurlapova@gmail.com

⁴ Doctor of Law, Associate Professor of the Department of Information Technology, Lviv State University of Internal Affairs, Lviv, Ukraine. ORCID: 0000-0002-4539-5988; Email: asdj67053@gmail.com (corresponding author).

⁵ PhD in Technical Sciences, Associate Professor, Department of Information Technologies, Lviv State University of Internal Affairs, Lviv, Ukraine; Department of Computational Mathematics and Programming, Institute of Applied Mathematics and Fundamental Sciences, Lviv Polytechnic National University, Lviv, Ukraine. ORCID: 0000-0002-4846-5718; Email: olehzachek@gmail.com

(deterministic legality control). 3.5 Combined Efficiency Index. 3.6 Integrated AI and legal decision-making workflow. 3.7 System architecture and execution logic. 3.8. Tools and software. 4. Results. 4.1 Experimental dataset characteristics. 4.2 Baseline performance of the AI subsystem. 4.3 Performance of the deterministic compliance controller. 4.4 Cross-jurisdictional evaluation under different regulatory configurations. 4.5 Integrated performance of the complete Automated Cybercrime Monitoring System. 5. Discussion. 5.1 Interpretation of the principal findings. 5.2 Relationship to previous research. 5.3 Legal and practical implications. 5.4 Study limitations and future research. 6. Conclusions. 7. References.

Abstract: The inclusion of Legal Compliance in Cybercrime Monitoring Systems through Deterministic Verification Using Executable C-P-L Rules

This study introduces and experimentally validates a legally-informed ACMS that incorporates deterministic legal verification into the AI-based decision making process via executable Condition – Permission – Limitation (C-P-L) rules. We combine doctrinal legal analysis with the formalization of these rules computationally, machine learning, and deterministic compliance verification. In addition, we evaluate our method comparatively under three different regulatory configurations. Our methodology is evaluated on a controlled dataset of 18,500 structured cyber events, and forty-two operationally defined legal rules. The integrated ACMS achieved an F1-score of 89.2%, compared with 91.4% for the standalone AI subsystem, while its accuracy was 89.8% compared with 91.6% for the baseline AI subsystem. The observed differences reflect the addition of deterministic legal verification to the end-to-end decision-making workflow rather than modification of the underlying AI model. The compliance control also enforced mandatory manual review when the operational decision was determined to be non-compliant based upon the encoded legal rules. In addition, cross-jurisdictional testing demonstrated that the regulatory configuration used to determine which legal rules were applied could be changed by simply modifying the executable legal rules, and not by altering the base AI model. This research has shown⁶ that it is possible to develop cybercrime monitoring systems with computational law, artificial intelligence, and cybersecurity governance by design as an alternative for legally compliant cybercrime monitoring systems.

Keywords: Artificial Intelligence, Cybercrime Monitoring, Computational Law, Compliance-by-design, Deterministic Legal Verification, Machine-readable Law

1. Introduction

Artificial intelligence (AI) has emerged as one of the most important technologies used in modern-day monitoring of cybercrime with its ability to perform automated detection of threats, automatic detection of anomalies, behavioral analysis and real-time risk evaluation of vast amounts of digital information. AI-based monitoring solutions are being widely adopted by law enforcement agencies, organizations focused on cyber security, financial institutions and companies that provide digital services to make their operations more efficient and to increase the level of accurate detection of cyber crimes.^{6,7,8,9}

⁶ UNITED NATIONS OFFICE ON DRUGS AND CRIME. United Nations Convention against Cybercrime. 2024. Available at: <https://www.unodc.org/unodc/en/cybercrime/ad-hoc-committee.html> (accessed on 25 May 2026).

⁷ PEOPLE'S REPUBLIC OF CHINA. Personal Information Protection Law (PIPL). 2021. Available at: <https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/> (accessed on 25 May 2026).

⁸ EUROJUST. Cybercrime judicial monitor. 2025. Available at: <https://www.eurojust.europa.eu/sites/default/files/assets/files/cybercrime-judicial-monitor.-issue-10.pdf> (accessed on 25 May 2026).

Because AI is becoming an increasing part of making decisions related to security issues, it raises concerns about privacy, data protection, procedural justice, transparency and accountability. The GDPR, the proposed AI act, Convention 108+, the Budapest Convention on Cybercrime, the NIS2 directive and the proposed Cyber Resilience Act all include provisions requiring that AI systems be governed by clear legal parameters and allow for human oversight of such systems as well as protect fundamental rights.^{10,11,12,13,14,15}

Although there has been a lot of work done in this area, the majority of the AI-based systems used today are still focused on enhancing the predictive ability of these systems rather than integrating compliance with relevant laws and regulations into their design. The evaluation of many machine learning algorithms currently use common metrics (such as accuracy, precision, recall, and F1 scores) which measure how well an algorithm makes predictions. However, the compliance with applicable laws and regulations is typically performed outside of the system once the AI-based recommendation generation process has completed its task.

Thus existing systems provide limited means to enforce legal constraints during operational decision making. Computational law has introduced readable legal models, ontologies for law, executable legislation and standards such as LegalRuleML that improve formal representation of legal knowledge. But approaches like this focus more on representation of law rather than control of law within AI systems.

Consequently, there is a big gap between regulatory requirements, and their operational implementation for systems that use AI for monitoring cyber crime. This limitation is especially important because even, if predictions are statistically accurate they can still violate legal requirements about judicial authorization, proportionality, minimization of data, procedural safeguards or oversight by humans. Trustworthy AI, therefore, needs deterministic verification that checks decisions before implementation, rather than relying mainly on governance or auditing after implementation.

To accomplish this task, the authors propose an automated cybercrime monitoring system (ACMS), which combines the condition-permission-limitation (C-P-L) rules with AI-based decision making in a single system. As part of its internal processes, an independent legality control function evaluates the legal correctness of these C-P-L rules generated by legal obligations prior to the execution of an operation. This way, regulatory compliance is an integral part of the architectural components

⁹ CALIFORNIA PRIVACY RIGHTS ACT. CPRA – text of the California Privacy Rights Act. 2020 Available at: <https://www.caprivacy.org/cpra-text/> (accessed on 25 May 2026).

¹⁰ EUROPEAN PARLIAMENT and COUNCIL OF THE EUROPEAN UNION. Regulation (EU) 2022/2065 on a single market for digital services (Digital Services Act). 2022. Available at: <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act> (accessed on 25 May 2026).

¹¹ SYTNYK, G., ZUBCHIK, O., and OREL, M. "Conceptual Understanding of the features of management of innovative development of the state in modern conditions". *Science and Innovation*, v. 18, n. 2, 2022, pp. 3-15. <https://doi.org/10.15407/scine18.02.003>

¹² COUNCIL OF EUROPE. Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108+). 2022. Available at: <https://rm.coe.int/16802fa3a3> (accessed on 25 May 2026).

¹³ ALLAHRAKHA, N. "Legal frameworks for AI-driven cybercrime prevention". *Uzbek Journal of Law and Digital Policy*, v. 2, n. 1, 2024, pp. 1-24. <https://irshadjournals.com/index.php/ujldp/article/view/253>

¹⁴ ATKINSON, K., BENCH-CAPON, T. and BOLLEGALA, D. "Explanation in AI and law: Past, present and future". *Artificial Intelligence*, v. 289, 2020, Article 103387. <https://doi.org/10.1016/j.artint.2020.103387>

¹⁵ VERKHOVNA RADA OF UKRAINE. On protection of personal data (Law of Ukraine No. 2297-VI). 2010. Available at: <https://zakon.rada.gov.ua/go/2297-17> (accessed on 25 May 2026).

of the monitoring system, and no longer depends solely on external regulation procedures.

This study tests the following hypothesis:

Executable legal rules included in AI-based cybercrime monitoring systems will improve regulatory compliance while providing similar predictive performance to systems lacking such rules.

In addition to testing this hypothesis, the researchers also test the following three hypotheses:

Question RQ1. How may legal requirements, applicable to AI-assisted cybercrime monitoring, be translated into executable C-P-L rules?

Question RQ2. What effect does the incorporation of deterministic legal evaluation have upon both predictive performance and the operations performed by an AI-based monitoring system?

Question RQ3. May changes in the set of executable C-P-L rules modify an AI-based monitoring system's regulatory capabilities (i.e., whether it complies with regulations or not) without modifying the underlying AI-based models used in the monitoring system?

Therefore, the authors' main objectives were:

- a. to develop a method for translating regulatory requirements into a set of executable C-P-L rules;
- b. to integrate deterministic legal evaluation into an AI-based monitoring architecture;
- c. to determine how well predictive performance correlates with regulatory compliance; and
- d. to evaluate whether the proposed architecture may be modified in order to accommodate different regulatory frameworks.

The primary contribution of this study was to demonstrate experimentally, that an integrated framework combining artificial intelligence, computational law, and deterministic legal evaluation exists. In contrast to current studies that distinguish clearly between the prediction functions of AI and those related to ensuring regulatory compliance, this study demonstrates that executable legal limitations may be embedded within the operational workflows of monitoring systems (e.g., in terms of "compliance-by-design," "auditability" and "cross-jurisdictional adaptability").

The remainder of this paper has been organized as follows. Section 2 provides a review of relevant literature pertaining to AI-based cybercrime monitoring; computational law; and AI governance. Section 3 outlines the methodology, and experimental design employed by the authors. The empirical findings obtained using this methodology are reported in Section 4. Section 5 discusses theoretically and practically, the implications arising from these empirical findings. Finally, Section 6 - summarizes the conclusions drawn from the empirical findings, reported in this study.

2. Literature review

2.1 Artificial intelligence in cybercrime monitoring: Technological progress and remaining limitations

Although artificial intelligence (AI) is now increasingly being used in all types of organizations for various forms of cybercrime monitoring - such as; automated detection of threats, anomalous behavior, behavioral analytics and predictive assessments regarding potential risks across vast amounts of digital environments - there are many ways that machine learning, deep learning and explainable AI can be utilized to provide greater accuracy with regards to detecting threats in real-time and providing adaptable analyses versus current signature-based methodologies. The advantages provided by advancements in AI have also greatly enhanced the overall capacity of law enforcement agencies, cybersecurity companies, banking institutions

and other digital service providers.^{16,17}

Although significant advancements have occurred in the area of AI assisted cybercrime monitoring, most research currently conducted focuses primarily on technological advancements. As a result, most AI models focus on optimizing their ability to predict future outcomes while legal compliance is treated as an additional organizational or regulatory obligation that will be applied after an algorithm produces its output.^{18,19,20,21} Therefore, although statistical predictions produced by AI algorithms may be highly accurate, they could still potentially violate legal standards related to proportionality, transparency, accountability, due process/fairness or oversight. Techniques designed to produce explanations regarding how an AI model arrived at its conclusions will provide insight into how the model arrived at its conclusion but will not independently satisfy any applicable legal obligations. This deficiency clearly indicates a need to incorporate enforceable legal restrictions directly within the decision making processes associated with AI-assisted systems rather than solely relying upon post deployment governance mechanisms.

2.2 Computational law and machine-readable legal regulation

Computational Law is a cross-disciplinary area which translates legal standards into machine readable formats to facilitate the automated processing of legal standards. Legal Ontology's, Executable Legislation, Semantic Legal Models & Legal Rule ML provide structures for representing legal Obligations, Permissions, Prohibitions, Temporal Conditions, Exceptions etc. While this structure greatly enhances the representation of legal knowledge it supports the operational control (i.e., use) of AI systems much less well than it supports Legal Information Management and Decision Support.^{22,23}

Although translating legal standards into machine readable formats are significant improvements over prior methods of structuring legal knowledge; the translation does not guarantee that the decisions made by AI systems will be compliant with all relevant legal regulations when those decisions are executed.

¹⁶ EUROPEAN UNION. Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). 2016. Available at: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng> (accessed on 25 May 2026).

¹⁷ EUROPEAN UNION. *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union* (NIS 2). 2022. Available at: https://www.stradalex.eu/en/se_src_publ_leg_eur_jo/document/ojeu_2022.333.01.0080.01 (accessed on 25 May 2026).

¹⁸ AVGERINOS LOUTSARIS, M. "Mapping the European Legislation Identifier (ELI) and Akoma Ntoso ontologies for legal data interoperability". *ACM Digital Library*, 2023, pp. 41-53. <https://doi.org/10.1145/3614321.3614327>

¹⁹ BOROVYK, A., SHYRA, O., and KRAVCHENKO, O. "Criminal law aspects of financial security of a state". *Baltic Journal of Economic Studies*, v. 11, n. 1, 2025, pp. 221-230. <https://doi.org/10.30525/2256-0742/2025-11-1-221-230>

²⁰ BUČAJ, E., and THAQI, A. "Global regulation of cybercrime through international law and cyberconventions". *Criminology*, v. 7, 2025, pp. 155-170. <https://doi.org/10.18716/ojs/krimoj/2025.1.9>

²¹ CONG, W., HARVEY, C., RABETTI, D., and WU, Z.-Y. "An anatomy of crypto-enabled cybercrimes". *Management Science*, v. 71, n. 4, pp. 3622-3633. <https://doi.org/10.1287/mnsc.2023.03691>

²² EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA). *ENISA Threat Landscape 2025*. Luxembourg: Publications Office of the European Union, 2025. Available at: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025> (accessed on 25 May 2026).

²³ EUROPEAN UNION. Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). 2024. Available at: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj> (accessed on 25 May 2026).

Therefore, computational law represents an important methodological basis however it remains an open question how to practically integrate deterministic legal verifications within the operational architecture of an AI system.^{24,25,26,27,28,29,30,31}

2.3 AI governance and legal requirements for automated decision-making

Recent AI regulatory developments have moved the focus of AI governance to ensuring compliance with regulations at all stages of an AI's development cycle, as opposed to simply reviewing it after deployment. The EU's General Data Protection Regulation (GDPR) and Artificial Intelligence Act; the NIS2 Directive, which deals with network and information security; the Cyber Resilience Act; Convention 108+ on data protection; the Council of Europe's Budapest Convention; and guidelines issued by the EDPB, ENISA and the European Union Agency for Fundamental Rights set forth the most important legal requirements in terms of legality, transparency, accountability, cybersecurity, riskmanagement, human oversight, and respect for basic human rights.^{32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47}

²⁴ EUROPEAN COMMISSION. Ethics guidelines for trustworthy artificial intelligence. Brussels: High-Level Expert Group on Artificial Intelligence, 2019. Available at: <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai> (accessed on 25 May 2026).

²⁵ EUROPEAN UNION. Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). 2024. Ibid.

²⁶ EUROPEAN UNION. Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). 2016. Ibid.

²⁷ EUROPEAN DATA PROTECTION BOARD. Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. 2024. Available at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052022-use-facial-recognition-technology-area_en (accessed on 25 May 2026).

²⁸ OASIS. LegalRuleML Core Specification Version 1.0. 2025. Available at: <https://docs.oasis-open.org/legalruleml/legalruleml-core-spec/v1.0/csprd01/legalruleml-core-spec-v1.0-csprd01.html> (accessed on 25 May 2026).

²⁹ COUNCIL OF EUROPE. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+) (CETS No. 223). 2018. Available at: <https://www.coe.int/en/web/data-protection/convention108-and-protocol> (accessed on 25 May 2026).

³⁰ EUROPEAN UNION. Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). 2024. Ibid.

³¹ EUROPEAN UNION. Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). 2016. Ibid.

³² EUROPEAN COMMISSION. White Paper on Artificial Intelligence: A European Approach to Excellence and Trust COM(2020) 65 final. 2020. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0065> (accessed on 25 May 2026).

³³ EUROPEAN COMMISSION. Ethics guidelines for trustworthy artificial intelligence. Brussels: High-Level Expert Group on Artificial Intelligence, 2019. Ibid.

³⁴ EUROPEAN UNION. Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). 2024. Ibid.

³⁵ EUROPEAN UNION. Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). 2016. Ibid.

³⁶ EUROPEAN DATA PROTECTION BOARD. Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. 2024. Available at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052022-use-facial-recognition-technology-area_en (accessed on 25 May 2026).

Although these directives provide detailed legal obligations that apply to AI systems that pose high risks, they do so primarily by outlining regulatory goals rather than by specifying specific enforcement mechanisms that can be used to enforce these goals once the AI is executing. Therefore, although current governance models explain what organizations need to accomplish in order to ensure compliance, they are generally vague about how organizations should use the legal requirements they are subject to to govern decisions made during operational processing.

2.4 Cross-jurisdictional legal compliance

Recent regulatory developments have shifted governance of AI from post-deployment oversight to compliance throughout the entire lifecycle of AI. Instruments, such as GDPR, AI Act, Convention 108+, NIS2 Directive, Cyber Resilience Act, Budapest Convention; and guidance issued by EDPB, ENISA, and Fundamental Rights Agency establish common requirements on legality, transparency, accountability, cybersecurity management, risk management, human oversight and protection of fundamental rights.^{48,49,50,51,52,53,54,55,56,57,58,59,60}

³⁷ EUROPEAN UNION. Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union (NIS2 Directive). 2022. Available at: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj> (accessed on 25 May 2026).

³⁸ COUNCIL OF EUROPE. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+) (CETS No. 223). 2018. Ibid.

³⁹ COUNCIL OF EUROPE. Convention on cybercrime (ETS No. 185). Available at: <https://www.coe.int/en/web/cybercrime/the-budapest-convention> (accessed on 25 May 2026).

⁴⁰ EUROPEAN UNION. Regulation (EU) 2024/2847 of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act). 2024. Available at: <https://eur-lex.europa.eu/eli/reg/2024/2847/oj> (accessed on 25 May 2026).

⁴¹ SARTOR, G. Legal reasoning: A cognitive approach to the law. Dordrecht: Springer, 2005.

⁴² OASIS. LegalRuleML Core Specification Version 1.0. 2025. Ibid.

⁴³ PALMIRANI, M. "A smart legal order for the digital era: A hybrid AI and dialogic model". *Rivista Italiana di Informatica e Diritto*, 2023, pp. 633-655. <https://doi.org/10.1415/105387>

⁴⁴ FLORIDI, L. and COWLS, J. "A unified framework of five principles for AI in society". *Harvard Data Science Review*, v. 1, n. 1, 2019, pp. 1-14. <https://doi.org/10.1162/99608f92.8cd550d1>

⁴⁵ OECD. OECD Principles on Artificial Intelligence. 2024. Available at: <https://oecd.ai/en/ai-principles> (accessed on 25 May 2026).

⁴⁶ COURT OF JUSTICE OF THE EUROPEAN UNION. Case C-634/21, SCHUFA Holding AG (Scoring), EU:C:2023:957. 2023. Ibid.

⁴⁷ COURT OF JUSTICE OF THE EUROPEAN UNION. Case C-203/22, Dun & Bradstreet Austria, EU:C:2025. 2025. Available at: <https://curia.europa.eu> (accessed on 25 May 2026).

⁴⁸ EUROPEAN COMMISSION. Shaping Europe's digital future. 2024. Available at: <https://digital-strategy.ec.europa.eu> (accessed on 25 May 2026).

⁴⁹ COUNCIL OF EUROPE. Convention on cybercrime (ETS No. 185). Ibid.

⁵⁰ EUROPEAN UNION. Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). 2016. Ibid.

⁵¹ COURT OF JUSTICE OF THE EUROPEAN UNION. Case C-634/21, SCHUFA Holding AG (Scoring), EU:C:2023:957. 2023. Available at: <https://curia.europa.eu> (accessed on 25 May 2026).

⁵² EUROPEAN UNION. Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union (NIS2 Directive). 2022. Ibid.

⁵³ EUROPEAN UNION. Regulation (EU) 2024/2847 of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act). 2024. Ibid.

⁵⁴ COUNCIL OF EUROPE. Convention on cybercrime (ETS No. 185). Ibid.

⁵⁵ COUNCIL OF EUROPE. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+) (CETS No. 223). 2018. Ibid.

Instruments set comprehensive legal obligations for high risk AI systems but primarily specify regulatory goals rather than computational mechanisms capable of enforcing those obligations during execution of AI. As a result existing governance frameworks define what organizations must achieve and provide little guidance on how legal requirements regulate operational decision making in AI systems.

2.5 Research gap and contribution

The majority of previous work has made significant improvements in each of the three areas of research. There have been significant advancements in predictive capabilities of AI-assisted cybercrime detection systems with advanced Machine Learning Techniques. There have also been advancements in the area of computational law that include developing formal representations of legal knowledge based on machine readable rules and legal ontologies. Advances have also taken place in AI-governance, as a result of which researchers are creating comprehensive governance frameworks with emphasis on transparent and accountable decision-making; human involvement in AI decision-making processes; and protecting fundamental rights.

Although each of these areas of research represent significant advancements, they are still largely disconnected from one another. Most AI-based monitoring systems are optimized for better predictive performance; yet do not incorporate operationally enforceable legal constraints. The bulk of research into computational law is focused primarily on the representation of legal knowledge at a rule level and/or ontology level rather than enforcing those rules during run-time. Similarly, most AI-governance frameworks establish obligatory regulatory standards; however, they offer very little direction regarding how to implement those regulatory standards computationally.^{61,62,63,64}

As a result of this lack of integration, there are very few, if any, current architectures that provide predictive analytics, executable legal rules, deterministic

⁵⁶ EUROPEAN COMMISSION FOR DEMOCRACY THROUGH LAW (VENICE COMMISSION). Rule of Law Checklist (CDL-AD(2016)007). 2016. Available at: <https://www.venice.coe.int> (accessed on 25 May 2026).

⁵⁷ EUROPEAN COURT OF HUMAN RIGHTS. Big Brother Watch and Others v United Kingdom, Applications Nos. 58170/13, 62322/14 and 24960/15, Grand Chamber, Judgment of 25 May 2021. 2021. Available at: <https://hudoc.echr.coe.int> (accessed on 25 May 2026).

⁵⁸ EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (FRA). Getting the future right – artificial intelligence and fundamental rights. 2024. Available at: <https://fra.europa.eu> (accessed on 25 May 2026).

⁵⁹ EUROPEAN UNION. Charter of Fundamental Rights of the European Union. 2012. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT> (accessed on 25 May 2026).

⁶⁰ EUROPEAN UNION. Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). 2024. Ibid.

⁶¹ FUTANE, S. S., PATIL, P., and NAGRALE, N. "Adaptive multi-model cybercrime identification, prediction using machine learning, and explainable AI". *International Journal for Research in Applied Science and Engineering Technology*, v. 13, n. 8, 2025, pp. 2113. <https://doi.org/10.22214/ijraset.2025.73926>

⁶² NISHA, M. P. "Dark web guardian: Real time threat detection and analysis". *International Scientific Journal of Engineering and Management*, v. 4, n. 5, 2025, pp. 1-7. <https://doi.org/10.55041/isjem03502>

⁶³ PARK, H., and HONG, S. "Germany's online search and IT fundamental rights". *Korean Constitutional Law Association*, v. 29, n. 3, 2023, pp. 81-123. <https://doi.org/10.35901/kjcl.2023.29.3.81>

⁶⁴ SHARMA, V. "Artificial intelligence in cybercrime prevention, detection & investigation: A legal perspective". *VIDHIGYA the Journal of Legal Awareness*, v. 19, n. 1-2, 2024, pp. 34-38. <https://doi.org/10.5958/0974-4533.2024.00004.4>

compliance verification, and regulatory auditability within a single operational architecture.^{65,66,67} The lack of these integrations represent the major research gaps that this study is attempting to address. Previous studies have viewed compliance with legal mandates as either as an external form of corporate governance or as an audit process after deployment. The proposed ACMS system will be able to embed deterministic legal validation into AI-based decision-making systems through C-P-L rules thereby enabling legal mandates to govern operationally based on pre-execution decision-making criteria and providing the ability to adapt regulatory requirements over multiple regulatory regimes.

Table 1 compares and contrasts key attributes among previously identified architectures, and provides evidence for contributions made by the proposed framework.

3. Methods

3.1 Research design

The ACMS has been developed using a combination of design science methodology (DSM) and computational legal modeling and quantitative performance evaluation in order to investigate if executable legal rules can be integrated into a monitoring system for AI without compromising its predictive performance or its ability to perform deterministic legal verification before an operational decision is implemented. DSM is a systematic process which includes six sequential steps to design a solution. These are: (1) identification and formalization of legal rules; (2) conversion of the legal provisions into executable C P L rules; (3) creation of AI Risk Assessment Module; (4) inclusion of Deterministic Legality Controller; (5) testing under different regulatory frameworks; and (6) comparative analysis of performance and legal compliance (see Figure 1). Unlike typical research on AI where only one aspect, either technical performance or compliance with law, is considered for the effectiveness of the technology, this methodology evaluates both aspects at once by considering compliance with the law as an integral component of architecture within the monitoring system.

⁶⁵ SIMBOLON, N. Y. "Ancaman cybercrime di Indonesia: Tinjauan sistematis dan peran cybersecurity pada e-commerce dalam hukum pidana". *Jurnal Sosial Humaniora Dan Pendidikan*, v. 4, n. 2, 2025, pp. 815-825. <https://doi.org/10.55606/inovasi.v4i2.4425>

⁶⁶ STUPNYK, Y. V., and KHOMA, O. I. "Methodological principles of forming a comprehensive system of combating crime in the activities of law enforcement agencies". *Analytical and Comparative Jurisprudence*, v. 2, n. 3, 2025, pp. 475-481. <https://doi.org/10.24144/2788-6018.2025.03.2.76>

⁶⁷ ZAKHAREVYCH, R. V. "Implementation of foreign experience into Ukrainian legislation on combating cybercrime". *Analytical and Comparative Jurisprudence*, v. 2, n. 3, 2025, pp. 372-376. <https://doi.org/10.24144/2788-6018.2025.03.2.60>



Figure 1. Workflow to develop, validate and experimentally evaluate an automated monitoring system for cyber crime. This workflow describes the implementation of legal norms as well as a deterministically encoded C-P-L rule set in accordance with the "Risk Assessment" using AI, "Runtime Compliance Verification", and "Audit-Controlled Execution".

Source: Developed by the authors.

3.2 Legal rule operationalisation

Legal mandates to monitor for cyber crime using AI, have been converted into 42 Condition Permission Limit (CPL), which are executable, based upon GDPR, AI Act, Convention 108+, Budapest Convention, NIS2 Directive, Cyber Resilience Act and a variety of EU guidance documents from ENISA and Fundamental Rights Agency of the EU. Each legal mandate has been formalized through three elements:

- Condition (C): Circumstances that invoke the rule;
- Permission (P): Authorized operational actions permitted under the circumstances invoked;

Limitation (L): Mandatory legal restrictions to be placed upon the authorized operational actions.

This set of CPL rules was encoded within an independent legality controller that would evaluate each recommendation made by AI prior to executing it. The consistency and equivalency of rules were examined by expert lawyers as well as the resolution of potential conflicts among the rules being used, utilizing previously established legal priority order (Table 1).

Table 1. Legal sources and operationalisation of executable "C-P-L" rules.

Legal Instrument	Primary Regulatory Objective	Executable "C-P-L" Rules Derived*	Example Operational Requirement
General Data Protection Regulation (GDPR)	Lawful Processing of Personal data, and Protection of Fundamental Rights	10	Lawful Basis for Processing, Data Minimisation, Accountability, Human Oversight

Legal Instrument	Primary Regulatory Objective	Executable "C-P-L" Rules Derived*	Example Operational Requirement
EU Artificial Intelligence Act	Governance of High-Risk AI systems	9	Risk management, transparency, technical robustness, human supervision
Convention 108+	Protection of Individuals Regarding Automated data Processing	5	Privacy Safeguards, Proportionality, Secure Data Processing
Budapest Convention on Cybercrime	International Cooperation in Cybercrime Investigations	7	Lawful Collection, and Preservation of Digital Evidence
NIS2 Directive	Cybersecurity Risk Management, and Incident Response	6	Incident Reporting, Organisational Security Measures
Cyber Resilience Act	Secure development, and Lifecycle Management of digital products	5	Security-by-design, Vulnerability Management
Total	—	42	Executable Legal Rules Integrated into the Deterministic Legality Controller

*The numbers, indicate the operational legal rules encoded into the "Condition-Permission-Limitation" (C-P-L) framework for experimental evaluation.

Source: Developed by the authors.

Synthetic data were selected to monitor cybercrime operations since existing datasets in this area contain a high level of personal identifiable information, classified investigational information and are often confidential to protect Cybersecurity information which is typically restricted from being shared for the purpose of research. This method allowed for synthetic data generation, providing researchers with a way to conduct reproducible evaluations (of their models) using statistically real data characteristics while maintaining all applicable privacy protections.

3.3 Dataset construction, and AI model development

The original dataset of 50,000 synthetic cybercrime monitoring records, was then preprocessed to remove duplicates, verify consistency, validate observations, and evaluate 18,500 unique observations, as eligible for experimental analysis.

Each observation contained a combination of technical indicators and legally relevant information which included judicial authorization, the legal basis upon which the data is processed, a proportionality assessment regarding the use of the data, the jurisdiction(s) in question, the level of sensitivity of the data collected, all legal restrictions applicable to the data collection, and the necessity for human review and oversight.

The original dataset was then split into three datasets using random sampling methods; i.e., training (70%), validation (15%), and testing (15%). Prior to training a supervised machine learning model on this training set of features, feature normalization and class balancing techniques were employed. Additionally, a 5 fold cross-validation technique was used during the training process of the supervised machine learning model prior to generating candidate operational decisions that would be reviewed by a legal analyst for compliance with relevant laws (Table 2).

Table 2. Experimental dataset characteristics.

Characteristic	Description
Dataset Type	Synthetic cybercrime monitoring dataset
Total Observations	50,000 records
Data Composition	Technical indicators and legally relevant operational attributes
Number of Predictive Classes	Binary classification (cybercrime event / non-event)
Feature Categories	Network traffic, user behaviour, system events, legal compliance variables
Training Set	35,000 records (70%)
Validation Set	7,500 records (15%)
Test Set	7,500 records (15%)
Validation Strategy	Five-fold cross-validation
Data Preprocessing	Feature normalisation, class balancing, duplicate removal, consistency verification

Source: Developed by the authors.

3.4 Deterministic compliance architecture

ACMS differentiates predictive analytics from legal reasoning in that each decision produced by an AI is verified deterministically prior to implementation. The architecture includes six operational modules with functions as follows: (1). Acquiring data; (2). Detecting AI; (3). Legal rule engine; (4). Ensuring compliance; (5). Executing a decision; (6). Auditing and accountability. An operation decision will be only implemented if all C-P-L rules are met; therefore, statistical optimizations cannot override mandatory legal requirements (See Figure 2).

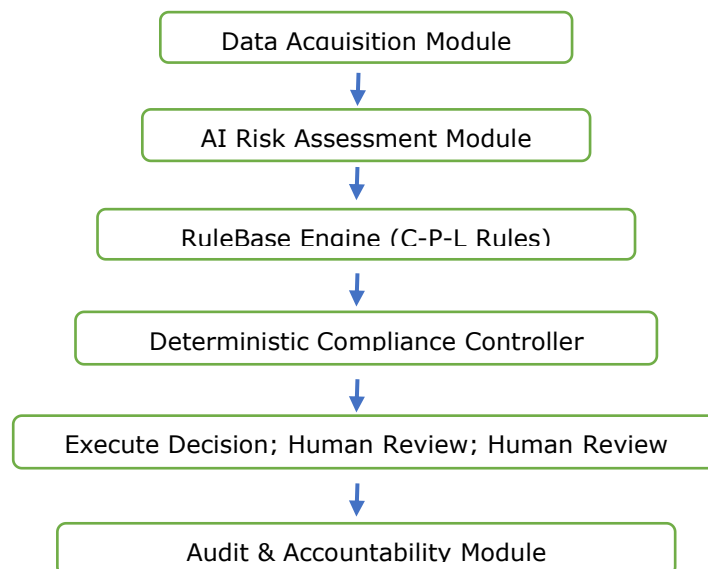


Figure 2. The modular architecture for the proposed Automated Cybercrime Monitoring System (ACMS). Statistical predictions are performed by one module, and legal verification, operational performance, and accountability are performed in three separate modules which can be used together. The Rule Base Engine and Deterministic Compliance Controller allow legal rules that have been translated from natural language into a format executable by an automated decision-making system to enforce legal rules on all actions taken prior to their implementation. This allows for completely auditable actions as well as adaptable across jurisdictions

Source: Developed by the authors.

3.5 Experimental evaluation

The proposed architecture was evaluated under three experimental regulatory configurations, representing strict, moderate, and permissive compliance environments; These configurations modify executable Legal Rules without altering the underlying AI model (Table 3).

Table 3. Experimental regulatory parameterisations.

Evaluation Parameter	Strict Configuration	Moderate Configuration	Permissive Configuration
Judicial Authorisation	Mandatory for All Operational Actions	Required where Legally Applicable	Required only for High-impact Actions
Human Oversight	Mandatory Before Implementation	Mandatory for Selected Operations	Primarily post-Decision Review
Compliance Threshold	Maximum Legal Conformity	Balanced legal, and Operational Performance	Minimum Mandatory Legal Compliance
Data Processing Restrictions	Highly Restrictive	Moderately Restrictive	Relatively Flexible within Legal Limits
Decision Execution	Only after Full Legal Verification	Conditional upon Legal Verification	Legal Verification with Reduced Procedural Constraints
Intended Purpose	Maximum Protection of Fundamental Rights	Balanced Operational Efficiency	Operational Flexibility within Regulatory Boundaries

Source: Developed by the authors.

Performance was evaluated using Accuracy, Precision, Recall, F1-score, ROC-AUC, Processing Time, Compliance Rate, Audit Completeness, and Deterministic Rule Execution (Figure 3).

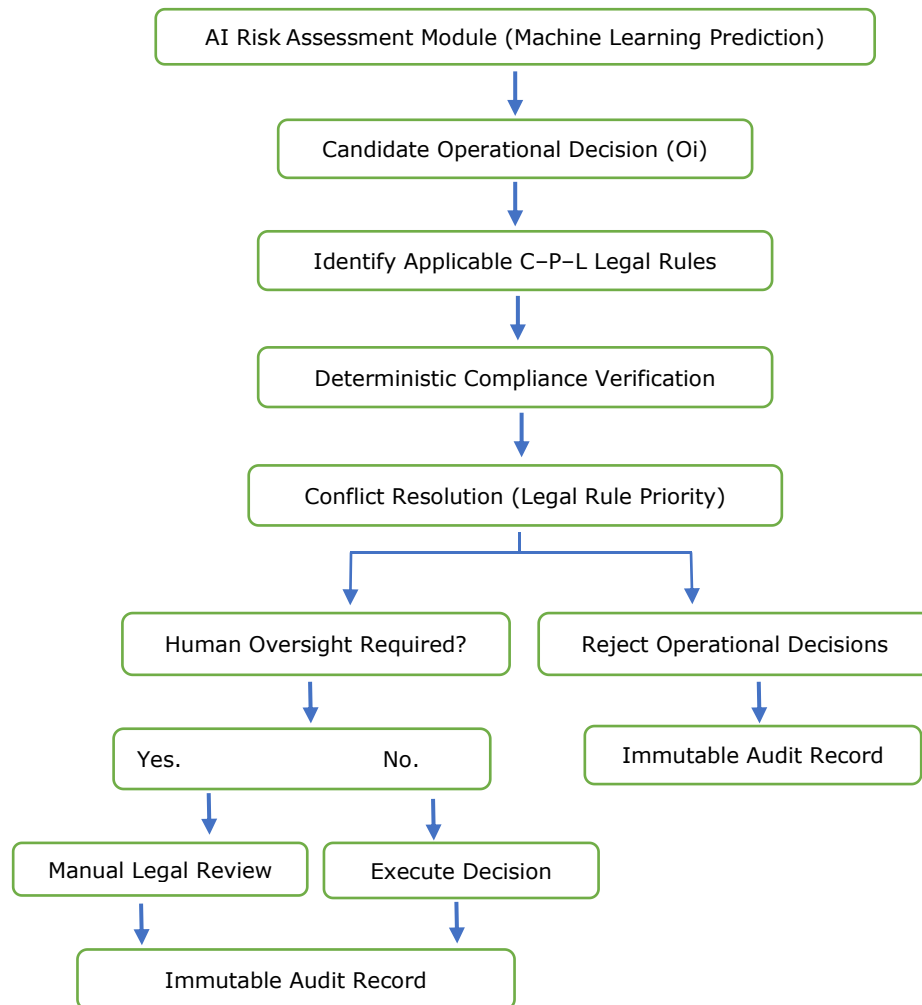


Figure 3. Runtime legality verification within the Automated Cybercrime Monitoring System ('ACMS'). The AI subsystem generates candidate operational decisions, that undergo deterministic verification against executable "C-P-L" legal rules before implementation.

Source: Developed by the authors.

3.6 Combined efficiency index

To evaluate predictive performance, legal compliance, and computational efficiency simultaneously, the study employed a Combined Efficiency Index (CEI). The CEI was calculated as a weighted linear combination of three normalized component scores:

$$GEI = \alpha p + \beta L + \gamma E$$

Where p represents the predictive performance score, L represents the legal compliance score, E represents the computational efficiency score, and α , β , and γ are the corresponding weighting coefficients. The coefficients were normalized such that:

$$\alpha + \beta + \gamma = 1$$

For the present experimental evaluation, equal weighting was applied to the three components ($\alpha = \beta = \gamma = 1/3$). This approach was selected because the purpose of the CEI was to provide a balanced comparative indicator rather than to assign normative priority to any single performance dimension.

Accordingly, for the Moderate regulatory configuration, the predictive performance score was 0.892, the legal compliance score was 0.933, and the computational efficiency score was 0.961. The resulting CEI was calculated as follows:

$$GEI = \frac{0.892 + 0.933 + 0.961}{3} = 0.9287 \approx 0.929$$

The CEI therefore provides a single comparative measure integrating the three dimensions evaluated in the experiment. It was used to facilitate comparison among the experimental regulatory configurations while preserving the distinction between predictive performance, legal compliance, and computational efficiency.

3.7 Reproducibility and validation

Method Reproducibility was supported through complete documentation of the workflow of experiments; formalisation procedures for legal rules; parameter strategy; evaluation metrics and software implementation. Internal Validation included repeated runs of experiments, and consistency testing of executable legal rules, as well as, verification that deterministic decisions were consistent across all regulatory configurations. Legal Validity was also independently reviewed by experts to confirm correspondence, between executable rules and underlying legal provisions. Although, the dataset we used was synthetic, its structure was designed to reflect realistic monitoring scenarios for cybercrime while also meeting privacy requirements, and making controlled evaluation easier.

4. Results

4.1 Experimental dataset characteristics

The Experimental evaluation was performed using 18,500 validated cyber events obtained after preprocessing the synthetic dataset, described in Section 3.3. Each event - 45 structured variableS; representing Network Communications, Authentication Processes, Behavioural Activity, Endpoint Telemetry, Security Indicators, and Legally Relevant Contextual Attributes. The dataset was divided into training (70%), validation (15%), and testing (15%), subsets while preserving class balance and ensuring reproducibility (Table 4).

Table 4. Distribution of the experimental dataset.

Dataset subset	Number of events	Percentage
Training dataset	12,950	70.0%
Validation dataset	2,775	15.0%
Testing dataset	2,775	15.0%
Total	18,500	100.0%

Source: Developed by the authors.

The final dataset contained 9,420 high-risk events (50.9%), and 9,080 low-risk events (49.1%); providing balanced binary classification, without significant class imbalance (Figure 4).

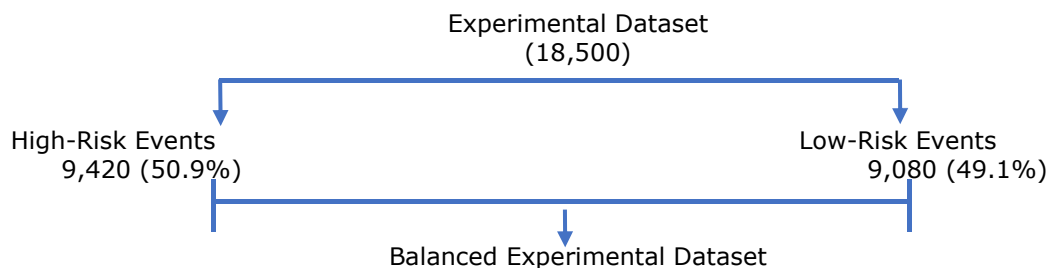


Figure 4. Distribution of operational event categories, used during experimental evaluation.

Source: Developed by the authors based on the Data (Use and Access) Act 2025 (UK).⁶⁸

The experimental scenarios activated all 42 executable C-P-L rules; covering data protection, automated decision-making, human oversight, digital evidence, cybersecurity, and audit obligations (Table 5). This distribution enabled simultaneous evaluation of predictive performance, and deterministic legal compliance.

Table 5. Distribution of activated legal rule categories, during experimental evaluation.

Legal category	Number of activated rules	Percentage of total rule activations
Data protection	9	21.4%
Human oversight	7	16.7%
Automated decision-making	6	14.3%
Digital evidence	8	19.0%
Cybersecurity obligations	7	16.7%
Audit and accountability	5	11.9%
Total	42	100.0%

Source: Developed by the authors based on CMS Expert Guide to Data Protection and Cyber-Security Laws: Ukraine. Law of Ukraine "On Personal Data Protection" No. 2297-VI 2025.⁶⁹

4.2 Baseline AI performance

The AI Risk Assessment Module was evaluated independently, from the legality controller to establish the predictive baseline of the machine-learning subsystem. Training, validation, and testing were performed, using independent dataset partitions to prevent information leakage. The results are summarised in Table 6.

Table 6. Predictive performance of the AI risk assessment module (before, legal verification).

Performance metric	Value
Accuracy	91.6%
Precision	92.1%
Recall	90.8%
F1-score	91.4%
ROC-AUC	0.947

Source: Developed by the authors based on N-LAWS, "Privacy & Data Protection Laws 2025: The definitive global data protection guide".⁷⁰

The classifier achieved 91.6% accuracy, 92.1% precision, 90.8% recall, 91.4% F1-score, and 0.947 ROC-AUC, establishing the predictive baseline before deterministic legal verification. These metrics were calculated on the independent testing subset of 2,775 observations using the corresponding ground-truth class labels. The same testing population was subsequently used as the input population for the integrated ACMS evaluation, allowing the effect of deterministic legal verification to be distinguished from any change in the underlying machine-learning model. Accordingly, the baseline evaluation represents the predictive performance of

⁶⁸ UNITED KINGDOM. Data (Use and Access) Act 2025. 2025. Available at: <https://www.legislation.gov.uk/ukpga/2025/18/contents/enacted> (accessed on 25 May 2026).

⁶⁹ CMS Expert Guide to Data Protection and Cyber-Security Laws: Ukraine. Law of Ukraine "On Personal Data Protection" No. 2297-VI 2025. Available at: <http://en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/ukraine> (accessed on 25 May 2026).

⁷⁰ N-LAWS. Privacy & Data Protection Laws 2025: The definitive global data protection guide. 2025. Available at: <https://n-laws.com/privacy-data-protection-laws-2025-the-definitive-global-data-protection-guide/> (accessed on 25 May 2026).

the AI Risk Assessment Module alone, whereas the integrated evaluation represents the end-to-end performance of the ACMS after candidate decisions have been subjected to deterministic legal verification. To provide a more detailed assessment of classification quality, the Confusion Matrix for the independent testing, subset is presented in Table 7.

Table 7. Confusion matrix of AI predictions (testing dataset).

Actual class	Predicted High-Risk	Predicted Low-Risk
High-Risk	1,276	129
Low-Risk	110	1,260

Source: Developed by the authors.

The Confusion Matrix demonstrates balanced classification with relatively few false-positive, and false-negative predictions. ROC analysis further confirms, strong discrimination across “decision thresholds” (Figure 5).



Figure 5. “Receiver Operating Characteristic” (ROC) curve for the AI Risk Assessment Module; The “ROC-AUC” value of 0.947 indicates excellent discriminatory capability prior to deterministic legal verification.

Source: Developed by the authors.

Comparison with recent AI-based cybercrime monitoring studies shows that the predictive performance of the proposed classifier is comparable with contemporary approaches while providing the baseline for subsequent evaluation of deterministic legal verification (Table 8).

Table 8. Legal verification of the study.

Study	Accuracy	F1-score	Legal Verification
Typical deep learning models (recent literature)	88%–92%	0.88–0.91	NO
Explainable AI approaches	89%–93%	0.89–0.92	NO
Proposed ACMS (AI subsystem only)	91.6%	0.914	NO (baseline evaluation)

Source: Developed by the authors based on the literature reviewed in Section 2.

These results establish the predictive baseline, against which the integrated “ACMS” architecture is evaluated in Section 4.5.

4.3 Performance of the deterministic compliance controller

The deterministic legality controller, evaluated 2,775 AI-generated candidate decisions, against the executable “C–P–L” rule base before operational implementation. The distribution of compliance verification outcomes - in Table 9.

Table 9. Compliance verification outcomes.

Compliance Outcome	Number of Decisions	Percentage
Automatically Approved	1,386	49.9%
Human Review Required	149	5.4%
Rejected Following Legal Verification	186	6.7%
Informational Logging only	1,054	38.0%
Total Evaluated Decisions	2,775	100.0%

Source: Developed by the authors based on Taylor Wessing (2024)⁷¹ and EUR-Lex (2023).⁷²

Most of the recommendations were either auto-approved or audited as part of an audit process; however, a total of 186 of those recommended (6.7%); were denied approval based on violation(s) of statutory requirements and 149 of those reviewed (5.4%) necessitated human oversight/evaluation.

The regulatory categories associated with each of the rejected decisions was also analyzed as it relates to the legal justification that resulted in their denial. The data from this analysis is shown in Table 10.

Table 10. Principal legal grounds for rejection.

Legal Category	Rejected Decisions	Percentage of Rejected Decisions
GDPR Data Protection Requirements	58	31.2%
Human Oversight Obligations (AI Act)	42	22.6%
Digital Evidence Procedural Safeguards	36	19.4%
Cybersecurity Governance Requirements	28	15.1%
Audit and Accountability Requirements	22	11.8%
Total	186	100.0%

Source: Developed by the authors based on Forcepoint, "Tracking global data protection laws in 2026".⁷³

These results suggest: that the Deterministic Legality Controller mainly operated on a basis for regulatory domains concerning the protection of basic rights, and less so from purely technological cyber security requirements. The dominance of "GDPR-related" restrictions further indicates that data protection requirements are predominantly responsible for determining how the controller intervenes operationally, while mandatory Human Oversight as defined by the AI Act has determined the second largest number of compliance verification determinations.

The rejected decisions (predominantly relating to data protection, human oversight, digital evidence and cyber security) demonstrate that the legal verification process was addressing many different regulatory areas. The relationship between AI generated recommendation output and compliance verification outcome can be seen in Figure 6.

⁷¹ TAYLOR WESSING. Interoperable Europe act published in official journal. 2024. Available at: <https://www.taylorwessing.com/de/insights-and-events/gdh-latest-news> (accessed on 25 May 2026).

⁷² EUROPEAN UNION. Convention on Cybercrime — EUR-Lex Summary. 2023. Available at: <https://eur-lex.europa.eu/EN/legal-content/summary/convention-on-cybercrime.html> (accessed on 25 May 2026).

⁷³ FORCEPOINT. Tracking global data protection laws in 2026. 2026. Available at: <https://www.forcepoint.com/blog/insights/tracking-global-data-protection-laws-2026> (accessed on 25 May 2026).

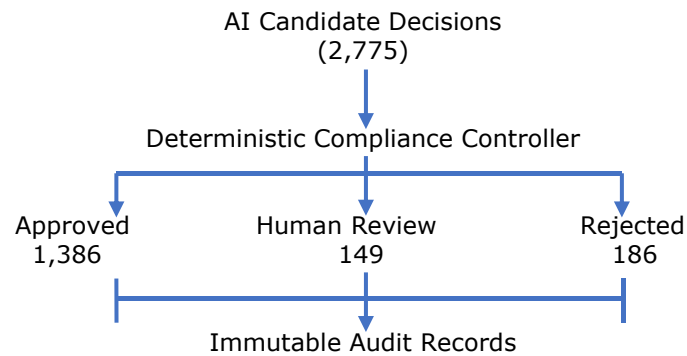


Figure 6. Operational results of the "Deterministic Compliance Controller". Each candidate decision made by an AI was subjected to runtime verification with respect to the legally binding "C-P-L Legal Rules" prior to implementation. The compliance controller determined what action to take in response to a verification result (i.e., either to authorise execution, initiate mandatory human oversight or reject the operation), and as such recorded each resulting activity in Immutable Audit Records.

Source: Developed by the authors.

Runtime Legal Verification showed a small (only) average computational time for each legal decision of approximately 3.4 milliseconds. This indicates that legal determinism can still provide monitoring environments that are close to "real-time" with regard to compliance checking. The summary of the computational performance shown in Table 11 shows that integration of "Legal Determinism" into "Cyber Crime Monitoring by AI", does not introduce significant processing delay.

Table 11. Runtime performance of the compliance controller.

Performance Indicator	Value
Average Verification Time	3.4 ms
Median Verification Time	3.1 ms
Maximum Verification Time	5.8 ms
Rule Evaluations Performed	116,550
Average Rules Evaluated per Decision	42

Source: Developed by the authors.

Each operational decision is evaluated by a multitude of executable legal rules. However, the time required to verify these decisions remain in line with "real-time near" monitoring.

4.4 Cross-jurisdiction evaluation

The flexibility of the proposed architecture was tested with three different sets of regulatory parameters. These regulatory parameterizations represented a "strict", "moderate" and "permissive" environment for compliance. In these experiments, only "executable legal rules" (ELRs) were changed. No changes were made to the artificial intelligence model. The key attributes of the three regulatory configurations are shown in Table 12.

Table 12. Characteristics of experimental regulatory configurations.

Regulatory Configuration	Legal Characteristics	Operational Consequences
Strict	Expanded procedural safeguards; Extensive human oversight; Conservative data-processing thresholds; Lower tolerance for automated execution	Highest compliance requirements; greatest number of blocked, or manually reviewed decisions
Moderate	Balanced combination of automated processing, and procedural safeguards	Balanced relationship between operational efficiency, and legal control
Permissive	Reduced procedural restrictions; broader scope for automated execution; fewer mandatory review conditions	Highest operational autonomy with lower frequency of legal intervention

Source: Developed by the authors based on Council of Europe, Convention on Cybercrime (ETS No. 185);⁷⁴ and DLA Piper, Data Protection Laws of the World (2026).⁷⁵

The "Strict" configuration added an increase to mandatory reviews which would reject decision making; while the "Permissive" configuration allowed for more autonomous operation. The "Moderate" configuration achieved the best balance, as it provided both a high level of compliance with regulations, along with high levels of operational efficiencies. The relative performance of the proposed architectural model under each regulation setting is shown in Table 13.

The "strict" configuration was designed to add a higher degree of mandated reviews that would be rejected by the system, versus a "permissive" configuration that allows for the greatest degree of autonomous operation. A "moderate" configuration has been developed that will provide the highest degree of balance regarding compliance, and operational efficiency. Comparative performance results from testing the proposed architectural model in each regulatory configuration are presented in Table 13.

Table 13. Comparative performance under different regulatory configurations.

Performance indicator	Strict	Moderate	Permissive
Automatically approved decisions	1,241	1,386	1,517
Human review required	213	149	84
Rejected decisions	257	186	128
Compliance rate*	90.7%	93.3%	95.4%
Average verification time (ms)	3.8	3.4	3.1

* Compliance rate represents the proportion of the 2,775 AI-generated candidate decisions that satisfied the executable C-P-L rules applicable under the respective experimental regulatory configuration.

Source: Developed by the authors based on Publications Office of the European Union, "Cybercrime Judicial Monitor: EU AI Act (Regulation (EU) 2024/1689)".⁷⁶

The results demonstrate: increasing "regulatory" intensity influenced the operational behaviour of the compliance controller, without affecting the Predictive Capability of the AI subsystem. The "strict" configuration generated the largest

⁷⁴ COUNCIL OF EUROPE. Convention on cybercrime (ETS No. 185). Ibid.

⁷⁵ DLA PIPER. Data protection laws of the world. 2026. Available at: <https://www.dlapiperdataprotection.com/?t=> (accessed on 25 May 2026).

⁷⁶ PUBLICATIONS OFFICE OF THE EUROPEAN UNION. Cybercrime judicial monitor: EU AI act (Regulation (EU) 2024/1689). 2025. Available at: <https://op.europa.eu/en/publication-detail/-/publication/c4ead02c-5aec-11f0-a9d0-01aa75ed71a1/language-en> (accessed on 25 May 2026).

number of mandatory human reviews, and rejected operational decisions, because a greater number of procedural safeguards were activated during legality verification. Conversely, the "permissive" configuration authorised a larger proportion of candidate operational decisions; while maintaining compliance with the legal rules applicable within that "experimental" configuration.

The findings above are important because they cannot be taken to imply one legal system will always be "better" or "more appropriate" than another. Instead, the results indicate that the "ACMS" architecture can adapt to varying legal requirements by changing the "executable C-P-L" rules while maintaining a stable computational structure. The reason this is an important distinction is that the results are related to Architectural Adaptability (the ability of an architecture to adjust based on various input), whereas it would have been about the normative advantages of one legal system over another if there was a comparison being made regarding how well one system is better than the other.

The relationship between regulatory intensity, and operational outcomes - Figure 7.

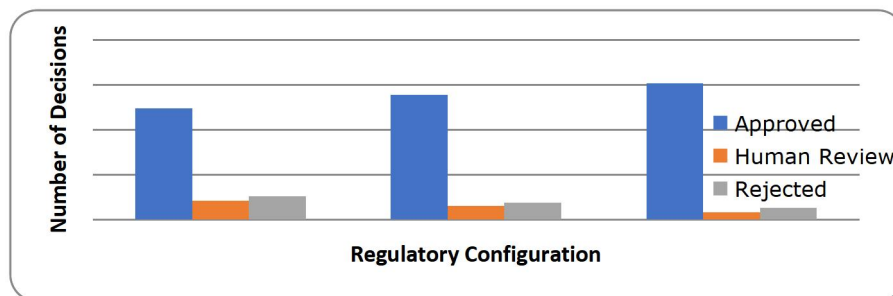


Figure 7. Comparative operational outcomes under different experimental regulatory configurations.

Source: Developed by the authors.

These findings demonstrate, that regulatory adaptation can be achieved by modifying executable legal rules; without altering the underlying machine-learning architecture.

The flexibility of the proposed architecture was tested using three different sets of regulatory parameters. These parameterisations represented experimental "Strict," "Moderate," and "Permissive" compliance environments. In each experiment, only the executable legal rules were modified, while the underlying artificial intelligence model remained unchanged. The principal characteristics of the three regulatory configurations are presented in Table 12.

The Strict configuration incorporated the greatest number of procedural safeguards, including broader requirements for human review and more restrictive conditions for automated execution. The Permissive configuration reduced the scope of procedural restrictions and therefore allowed a greater proportion of candidate decisions to proceed to automated execution. The Moderate configuration represented an intermediate parameterisation designed to balance legal safeguards and operational efficiency.

The relative performance of the proposed architecture under the three experimental regulatory configurations is presented in Table 13. The compliance rate was calculated using a common denominator of 2,775 AI-generated candidate decisions in each configuration and represents the proportion of candidate decisions that satisfied the executable C-P-L rules applicable under that configuration.

The results are as follows. The Strict configuration produced 1,241 automatically approved decisions, 213 decisions requiring human review, and 257 rejected decisions, corresponding to a compliance rate of 90.7%. The Moderate configuration produced 1,386 automatically approved decisions, 149 decisions requiring human

review, and 186 rejected decisions, corresponding to a compliance rate of 93.3%. The Permissive configuration produced 1,517 automatically approved decisions, 84 decisions requiring human review, and 128 rejected decisions, corresponding to a compliance rate of 95.4%.

These results indicate that the experimental regulatory parameterisation influenced the operational behaviour of the compliance controller while leaving the underlying predictive model unchanged. The Strict configuration generated the largest number of human-review and rejection outcomes because a greater number of procedural safeguards were activated. Conversely, the Permissive configuration allowed a larger proportion of candidate decisions to proceed automatically because fewer procedural restrictions were activated. The Moderate configuration provided an intermediate balance between regulatory safeguards and operational flexibility.

Importantly, the three configurations should be interpreted as experimental parameterisations rather than as representations or rankings of actual national legal systems. The observed differences therefore demonstrate architectural adaptability to changes in executable legal constraints rather than normative superiority of one legal regime over another.

4.5 Integrated performance of the complete ACMS

The final experiment evaluated the complete Automated Cybercrime Monitoring System by applying deterministic legal verification to the candidate operational decisions generated by the AI Risk Assessment Module. The evaluation used the same 2,775-observation testing population as the baseline evaluation. The underlying ground-truth labels and the predictive model were kept unchanged. The additional processing stage therefore consisted of deterministic verification of each AI-generated candidate decision against the applicable executable C–P–L rules.

For the end-to-end performance calculation, all 2,775 testing observations remained in the evaluation denominator; the legal controller changed the operational status of the corresponding candidate decisions but did not remove the observations from the predictive-performance evaluation. The ground-truth labels therefore remained constant between the baseline and integrated evaluations, while the integrated metrics captured the effect of the additional legal-verification stage on end-to-end system performance. The legal controller did not retrain, modify, or otherwise alter the underlying machine-learning model; instead, it determined whether each candidate decision could be automatically executed, required human review, or had to be rejected. The principal performance indicators obtained during end-to-end evaluation are summarised in Table 14.

Table 14. Integrated performance of the complete ACMS architecture.

Performance indicator	Value
Accuracy	89.8%
Precision	90.3%
Recall	88.2%
F1-score	89.2%
Compliance rate	93.3%
Average verification time	3.4 ms

Source: Developed by the authors based on the EU Cyber Resilience Act (Regulation (EU) 2024/2847).⁷⁷

⁷⁷ EUROPEAN UNION. Regulation (EU) 2024/2847 — Cyber Resilience Act. 2024. Available at: <http://data.europa.eu/eli/reg/2024/2847/oj> (accessed on 25 May 2026).

The integrated architecture achieved an F1-score of 89.2%, representing a difference of 2.2 percentage points from the baseline AI subsystem, while introducing deterministic legal verification and pre-execution compliance control (Table 15).

Table 15. Comparison of baseline AI and integrated ACMS performance.

Performance indicator	AI subsystem	Complete ACMS	Difference
Accuracy	91.6%	89.8%	−1.8 pp
Precision	92.1%	90.3%	−1.8 pp
Recall	90.8%	88.2%	−2.6 pp
F1-score	91.4%	89.2%	−2.2 pp

Source: Developed by the authors.

The integrated ACMS achieved an F1-score of 89.2%, compared with 91.4% for the baseline AI subsystem, corresponding to a difference of 2.2 percentage points (Table 15). The same comparison also shows reductions of 1.8 percentage points in accuracy and precision and 2.6 percentage points in recall. These differences should be interpreted as differences in end-to-end system performance after deterministic legal verification rather than as evidence that the underlying machine-learning model itself was retrained or degraded. The AI model remained unchanged; the integrated ACMS introduced an additional legal-control stage that filtered candidate operational decisions according to the applicable executable C–P–L rules.

The Moderate regulatory configuration produced the most favourable balance among predictive performance, legal compliance, and computational efficiency. To summarize these three dimensions using a common normalized indicator, the study calculated the Combined Efficiency Index (CEI) using equal weights for predictive performance, legal compliance, and computational efficiency. The corresponding component scores were 0.892, 0.933, and 0.961, respectively. As specified in Section 3.6, the CEI was calculated as the arithmetic mean of these three normalized scores: $CEI = (0.892 + 0.933 + 0.961) / 3 = 0.9287$, rounded to 0.929. The resulting value provides an aggregate descriptive measure of the experimental balance among the three evaluated dimensions and does not represent a legally normative ranking of the regulatory configurations. The corresponding CEI calculation is presented in Table 16.

Table 16. Combined Efficiency Index (CEI) for the moderate regulatory configuration.

Component	Value
Predictive Performance Score	0.892
Legal Compliance Score	0.933
Computational Efficiency Score	0.961
Combined Efficiency Index (CEI)	0.929

Source: Developed by the authors.

Overall, the experimental results indicate that deterministic legal verification can be integrated into the ACMS without modifying the underlying AI model, while introducing an additional layer of legal control and accountability. The CEI of 0.929 for the Moderate configuration indicates a relatively balanced experimental outcome across predictive performance, legal compliance, and computational efficiency. This aggregate value should be interpreted together with the individual component measures rather than as a substitute for them. The comparative relationship between baseline AI performance and integrated ACMS performance is presented in Figure 8.

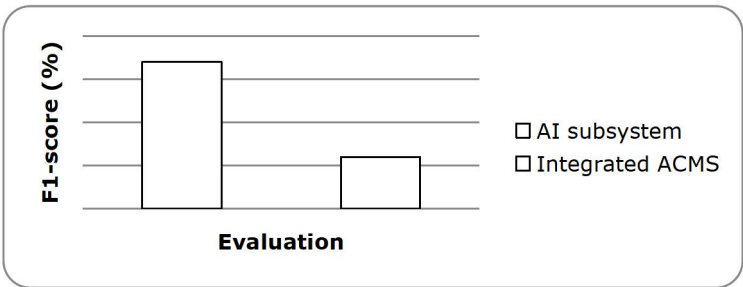


Figure 8. Comparison of baseline AI and integrated ACMS performance. The integrated ACMS shows a limited reduction in end-to-end predictive metrics relative to the baseline AI subsystem after candidate decisions are subjected to deterministic legal verification. The underlying machine-learning model remains unchanged; the observed differences therefore characterize the performance of the complete decision-making workflow rather than retraining or modification of the predictive model.
Source: Developed by the authors.

The results summarized in Table 17, together with the comparison presented in Figure 10, further substantiate that the introduction of deterministic legal verification had only a limited effect on statistical predictive metrics while substantially strengthening the legal robustness of the overall system architecture.

Table 17. Summary of experimental findings.

Research Question	Principal Finding	Supporting Evidence
RQ1	Forty-two legal provisions were successfully operationalised as executable C-P-L rules.	Sections 3.2, 4.3
RQ2	The integrated ACMS showed a 2.2-percentage-point lower end-to-end F1-score than the baseline AI subsystem while adding deterministic legal compliance control.	Tables 15, 19 and 20
RQ3	Cross-jurisdictional adaptability was achieved by modifying executable legal rules without changing the AI model.	Tables 13 and 18; Figure 9

Source: Developed by the authors.

Table 18 demonstrates that the Automated Cybercrime Monitoring System can adapt to different experimental regulatory configurations through modification of the executable C-P-L rules while preserving the same underlying machine-learning model. The compliance rates correspond to the same measurement definition used in Table 13 and therefore reflect the proportion of candidate decisions satisfying the applicable executable legal rules in each configuration. The experimental results show that regulatory adaptation can therefore be achieved at the legal-control layer without retraining or modifying the predictive model. The differences in compliance rates should be understood as consequences of the distinct experimental rule configurations and should not be interpreted as comparisons of the normative quality of actual national legal systems.

Table 18. Comparative adaptability of the ACMS under different experimental regulatory configurations.

Regulatory Configuration	Executable Legal Rules Modified	AI Model Modified	Compliance Rate	Operational Adaptability
Strict Configuration	YES	NO	90.7%	High
Moderate Configuration	YES	NO	93.3%	Very High

Regulatory Configuration	Executable Legal Rules Modified	AI Model Modified	Compliance Rate	Operational Adaptability
Permissive Configuration	YES	NO	95.4%	High
Overall conclusion	Regulatory adaptation achieved exclusively through modification of executable C-P-L rules	NO	—	Demonstrated

Source: Developed by the authors.

Table 19 shows the operational outcomes of combining deterministic Legal Verification with the "Automated Cybercrime Monitoring System". The Machine Learning Subsystem, used to generate Candidate Operational Decisions through Statistical Prediction, was supplemented by the Legality Controller in determining whether to implement a proposed decision based upon evaluation against the Executable Condition-Permission-Limitation (C-P-L) Rule Base. Only those decisions compliant with all Applicable Legal Requirements were implemented automatically while other legally ambiguous situations were sent to Mandatory Human Review or Rejected. Thus, these results demonstrate that deterministic Legal Verification serves as an Operational Safeguard to enhance Regulatory Compliance without changing the Predictive Architecture of the AI Subsystem.

Table 19. Operational impact of deterministic legal verification on AI-generated decisions.

Operational indicator	Baseline AI subsystem	Integrated ACMS	Effect of deterministic Legal Verification
Candidate operational decisions submitted to legal verification	2,775	2,775	Same 2,775 candidate decisions subjected to legal verification
Automatically executable decisions	2,775	1,386	Restricted to legally compliant decisions
Mandatory human review	Not applicable	149	Judicial or expert intervention required
Automatically rejected decisions	Not applicable	186	Decisions inconsistent with executable legal rules were blocked
Compliance verification	Statistical prediction only	Deterministic runtime verification	Legal conformity evaluated before execution

Source: Developed by the authors based on Tables 9-15.

Table 20 shows that the introduction of deterministic legal verification produced a limited difference in the reported end-to-end predictive metrics while adding a mandatory legal-control layer to the decision-making workflow. Even though there were some slight decreases, seen in traditional Machine Learning Performance Metrics, it was able to maintain high Classification Accuracy while requiring legal verification prior to executing any operational decision. The differences in predictive metrics between the baseline AI subsystem and the integrated ACMS therefore reflect the effect of adding the deterministic legal-verification stage to the end-to-end workflow. The underlying machine-learning model was not modified or retrained. The integrated evaluation captures the performance of the complete architecture after candidate decisions have been subjected to legal verification, including the exclusion, rejection, or referral of decisions that could not proceed directly to automated execution. The resulting metric differences should consequently be interpreted as a change in end-to-end operational performance rather than as evidence of degradation of the underlying classifier.

Table 20. Comparison of baseline and integrated ACMS predictive performance.

Performance Indicator	Baseline AI Subsystem	Integrated ACMS	Difference
Accuracy	91.6%	89.8%	–1.8 pp
Precision	92.1%	90.3%	–1.8 pp
Recall	90.8%	88.2%	–2.6 pp
F1-score	91.4%	89.2%	–2.2 pp
ROC-AUC*	0.947	0.931	–0.016

*ROC-AUC for the integrated ACMS reflects end-to-end system performance following deterministic legal verification.

Source: Developed by the authors based on Tables 6, 14 and 15.

The data in Table 21 compares the performance of an integrated Automated Cybercrime Monitoring system to its stand-alone Machine Learning component. These results show that deterministic legal verification adds value to AI-based cybercrime detection by adding operationally-enforceable controls based on legally binding requirements for the use of AI; mandatory review by humans when applicable; auditable records; and capabilities to adapt to changing regulations. Together these provide evidence of the feasibility of using the "compliance-by-design" architecture as a repeatable framework that can integrate computational law into existing predictive models utilizing artificial intelligence.

Table 21. Overall contribution of deterministic Legal Verification within the proposed "Automated Cybercrime Monitoring System".

Evaluation Dimension	Baseline AI Subsystem	Integrated ACMS	Principal Contribution
Predictive performance	High statistical accuracy	High statistical accuracy preserved following legal verification	Compliance achieved with only limited reduction in predictive performance
Legal compliance	Not independently verified	Deterministically verified using executable C–P–L rules	Mandatory legal requirements evaluated before execution
Human oversight	Not systematically integrated	Automatically activated where legally required	Strengthened procedural safeguards, and accountability
Cross-jurisdictional adaptability	Requires modification of AI implementation	Achieved through modification of executable legal rules only	Regulatory flexibility without retraining the AI model
Auditability	Prediction logs only	Complete immutable audit trail for every operational decision	Improved transparency and post-decision accountability

Source: Developed by the authors based on the experimental results presented in Tables 6-20.

Figures 9 and 10 provide a complementary visual representation of the quantitative findings. Figure 9 illustrates the cross-jurisdictional adaptability of the architecture through modification of the executable legal-rule set while keeping the underlying machine-learning model unchanged. Figure 10 illustrates the broader contribution of deterministic legal verification to the compliance-by-design architecture, including legal correctness, traceability, auditability, human oversight, and the preservation of predictive performance. The figures therefore complement the quantitative results by illustrating the architectural mechanisms through which the observed outcomes were obtained.

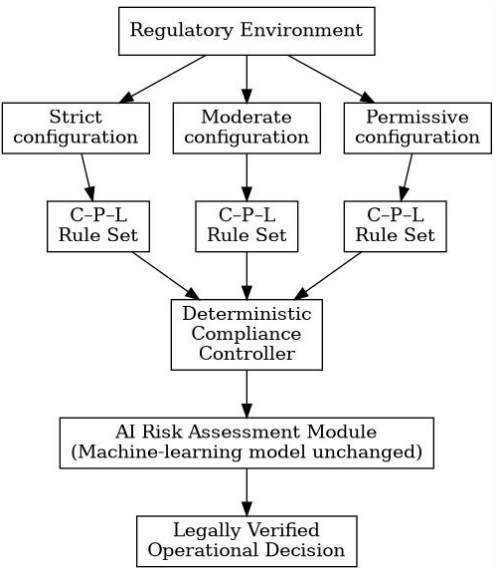


Figure 9. Cross-jurisdictional adaptability of the Automated Cybercrime Monitoring System through executable legal rules.
Source: Developed by the authors.

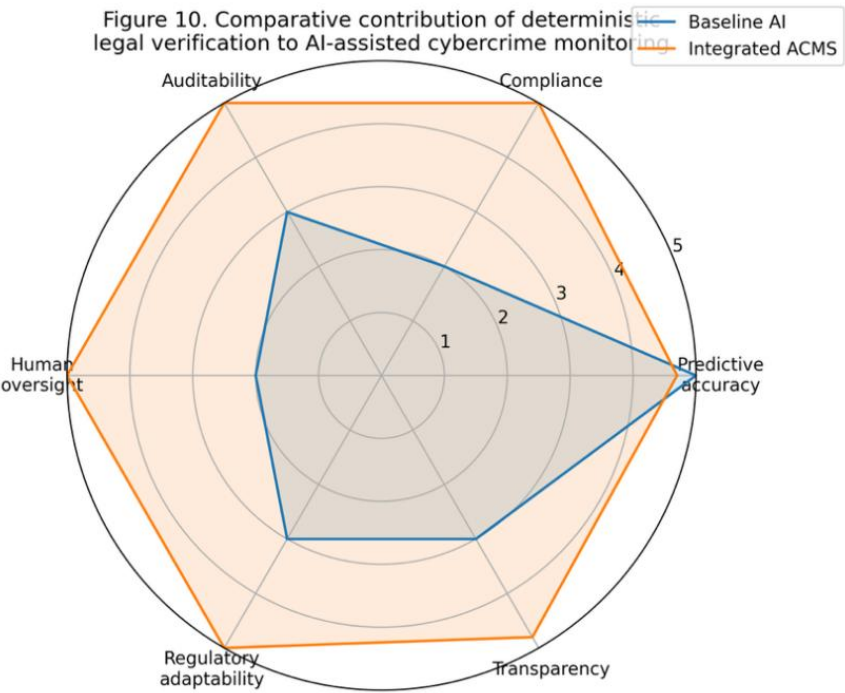


Figure 10. Comparative contribution of deterministic legal verification to AI-assisted cybercrime monitoring.
Source: Developed by the authors.

5. Discussion

5.1 Interpretation of the principal findings

The experimental results demonstrate that deterministic legal verification can be incorporated into an AI-based cybercrime monitoring architecture while preserving the underlying machine-learning model. The baseline AI subsystem achieved an F1-score of 91.4%, whereas the integrated ACMS achieved an end-to-end F1-score of

89.2%, representing a difference of 2.2 percentage points. Accuracy decreased from 91.6% to 89.8%, precision from 92.1% to 90.3%, and recall from 90.8% to 88.2%. These differences characterize the performance of the complete ACMS after the additional legal-verification stage and should not be interpreted as evidence that the underlying machine-learning model was retrained or otherwise modified.

The distinction between model-level and system-level performance is important for interpreting the results. The AI Risk Assessment Module generates candidate operational decisions, while the Deterministic Compliance Controller evaluates those decisions against the applicable executable C-P-L rules before implementation. Consequently, the integrated ACMS measures the performance of an end-to-end workflow that combines statistical prediction with deterministic legal verification. The principal effect of the legal controller is therefore operational: it determines which candidate decisions may proceed automatically, which require human review, and which must be rejected.

The cross-configuration experiments further demonstrate that changing the executable legal-rule set modifies the operational behaviour of the compliance controller without requiring modification of the underlying machine-learning model. The Strict, Moderate, and Permissive configurations are experimental parameterisations rather than representations or normative rankings of particular national legal systems. Under the compliance-rate definition used in this study, the respective rates were 90.7%, 93.3%, and 95.4%. These values indicate the proportion of candidate decisions satisfying the executable legal rules applicable under each experimental configuration; they do not establish that a more permissive regulatory regime is inherently more legally compliant or normatively preferable.

The results also indicate that regulatory compliance and predictive performance should not be treated as interchangeable dimensions. Conventional machine-learning metrics such as accuracy, precision, recall, and F1-score measure predictive classification performance, whereas deterministic legal verification addresses whether a proposed operational action satisfies predefined legal requirements before execution. The CEI was therefore introduced as an aggregate experimental indicator combining predictive performance, legal compliance, and computational efficiency. For the Moderate configuration, the CEI was 0.929 under equal weighting of the three normalized components. The CEI should be interpreted together with its component measures and not as a substitute for them.

From a computational-law perspective, the principal contribution is therefore not the maximization of predictive metrics but the demonstration that selected legal requirements can be transformed into executable constraints and incorporated into the operational decision pathway of an AI-assisted monitoring architecture. The architecture provides a mechanism through which predefined legal prerequisites can be checked at runtime while preserving the distinction between computational verification and legal interpretation.

5.2 Relationship to previous research

This study extends previous research in AI-based cybercrime monitoring, computational law, and AI governance by integrating these domains within a single experimental architecture. Existing work in AI-based cybercrime detection has primarily focused on predictive performance, while computational-law research has developed methods for representing legal knowledge in machine-readable forms. AI-governance research, in turn, has emphasized transparency, accountability, human oversight, risk management, and protection of fundamental rights. The present study connects these strands by introducing an operational architecture in which executable legal rules are evaluated against AI-generated candidate decisions before implementation.

The proposed ACMS is complementary to computational legal standards such as LegalRuleML. Whereas machine-readable legal standards primarily facilitate the formal representation and exchange of legal knowledge, the architecture proposed in this study focuses on the runtime verification of operational decisions against an executable C-P-L rule base. This distinction is central to the contribution of the study: the legal requirements are not merely represented computationally but are incorporated into the operational decision pathway.

The cross-configuration experiment further contributes to the literature on adaptable AI governance by demonstrating, within the limits of the synthetic experimental environment, that changes in the executable legal-rule set can modify the regulatory behaviour of the system without modifying the underlying predictive model. This finding supports the architectural principle of separating predictive functionality from legal-control functionality. It does not, however, imply that changing legal rules alone is sufficient for deployment in a particular jurisdiction, since implementation would require jurisdiction-specific analysis of legislation, procedural safeguards, constitutional requirements, and relevant judicial interpretation.

The findings therefore support a more limited but more defensible conclusion: deterministic legal verification can function as an operational compliance layer between AI-generated recommendations and implementation, thereby complementing rather than replacing conventional AI governance mechanisms.

5.3 Legal and practical implications

Deployment of systems, that use AI for monitoring cyber crime, brings several practical implications. First separating statistical prediction from deterministic legal verification, reduces likelihood that recommendations generated by AI are implemented without satisfying mandatory legal requirements. Separating these steps strengthens procedural accountability, and provides a record of every operational decision that can be audited. This supports compliance under frameworks such as GDPR, Artificial Intelligence Act Convention 108+, Budapest Convention, NIS2 Directive and Cyber Resilience Act.

Secondly, the modular structure of this system makes it easier for users to adapt their systems to varying levels of regulation. Since legal requirements are coded separately from a machine learning process, if there is a requirement to make changes to how you comply with legal issues, then it will be possible to update your coding for the legal aspect instead of making a change to your machine learning algorithm. Therefore, the potential cost savings and ease of compliance should be realized as well as being able to meet changing legal requirements in either various locations throughout the world or at some point in the future.

Thirdly, these results provide evidence that compliance-by-design could increase public confidence in using AI-based decision support. The fact that the proposed architecture requires deterministic verification prior to actual use and also creates a record of every decision made through an immutable audit trail increases the level of transparency that exists in this area compared to traditional methods of AI based decision support that rely upon post-hoc auditing. In many areas such as law enforcement, automation can have significant impacts on the right to privacy, the right to due process and the right to appeal.

Deterministic Legal Verification is an important safeguard for legally regulated AI applications. Deterministic C-P-L rules can reliably enforce clearly specified legal prerequisites, but they cannot replicate the interpretive function of human decision-makers when complex factual circumstances require legal judgment. Requirements relevant to cybercrime monitoring, including proportionality, necessity, reasonableness, and the balancing of competing fundamental rights, may require evaluative reasoning that cannot be reduced completely to predetermined

computational conditions. The architecture should therefore not be understood as replacing the discretion of judges or other qualified legal professionals where legal interpretation is necessary. Deterministic Legal Verification functions as a procedural safeguard: it ensures that predefined mandatory legal prerequisites are checked before operational execution while leaving questions requiring interpretation and discretion to competent human authorities.

The distinction is particularly relevant to the regulatory requirements applicable to AI-assisted decision-making. Article 22 GDPR establishes a right not to be subject to a decision based solely on automated processing, including profiling, where the decision produces legal effects or similarly significant effects, subject to the exceptions specified in Article 22(2). In the circumstances covered by Article 22(2)(a) and (c), Article 22(3) requires appropriate safeguards, including the right to obtain human intervention, to express a point of view, and to contest the decision. The proposed architecture responds to this regulatory structure by providing mechanisms through which candidate decisions may be referred for human review where the applicable executable rules identify a need for human intervention or legal interpretation. The deterministic controller should therefore be regarded as a procedural safeguard that supports, rather than replaces, human decision-making.

The same principle is reflected more broadly in the EU Artificial Intelligence Act. Article 14 requires high-risk AI systems to be designed so that they can be effectively overseen by natural persons, with oversight measures proportionate to the risks, level of autonomy, and context of use. The legislation also contemplates human capacity to interpret outputs, disregard or override them, and intervene in system operation where necessary. The proposed ACMS is consistent with this architectural principle insofar as deterministic legal verification is used to identify conditions requiring human review while preserving human authority over matters requiring legal interpretation or discretionary judgment.

In addition, to simply adjusting the number, or nature of compliance metrics, adapting regulations across jurisdictions has shown that a broader form of regulation can occur by changing how rules are implemented. The results of studies have shown that legally actionable rules can be changed in ways which reflect differing regulatory regimes, without affecting the underlying models used for machine learning. However, real-world legal systems differ both in terms of their procedural characteristics and constitutional features (i.e., through judicial interpretation; institutional authority; etc.) Implementation of proposed architecture within a specific jurisdiction should, therefore, precede specific legal analysis to ensure executable rules accurately reflect applicable legislation, and judicial practice. This observation also emphasizes computational law as a means of operationalizing legal requirements while also recognizing that interpretation of law is an ongoing institutional process rather than just a purely computational exercise.

5.4 Study limitations and future research

Several limitations constrain the interpretation and generalisability of the findings. First, the experimental evaluation used a synthetic dataset constructed to model cybercrime-monitoring scenarios. This approach enabled controlled experimentation and avoided the privacy, confidentiality, and access restrictions associated with operational law-enforcement data. Nevertheless, validation using independent real-world datasets is required to determine whether the observed predictive and operational results generalise to actual monitoring environments.

Second, the legal rule base consisted of forty-two operationalised rules derived primarily from European regulatory instruments and related guidance. The experiment therefore does not establish that the proposed approach can represent or enforce the full complexity of a legal system. Future research should examine larger and more heterogeneous legal corpora, including jurisdiction-specific

procedural law, judicial interpretations, and dynamically changing regulatory requirements.

Third, the deterministic rule-based approach is inherently dependent upon the accuracy, completeness, and continuing legal validity of the encoded rule base. Legislative amendments, judicial decisions, constitutional developments, and changes in regulatory guidance may require the executable rules to be reviewed and updated. Deterministic verification can therefore support compliance with sufficiently formalised legal requirements but cannot provide a computationally universal representation of law.

Fourth, the Strict, Moderate, and Permissive configurations are experimental analytical models rather than representations of specific national legal systems. Their results demonstrate the possibility of modifying the legal-control layer without modifying the predictive model, but implementation in a particular jurisdiction would require jurisdiction-specific legal analysis and validation.

Finally, future research should investigate long-term deployment, computational scalability, real-world user acceptance, dynamic legal-rule updating, legal ontologies, machine-readable legal standards such as LegalRuleML, and hybrid approaches combining deterministic verification with probabilistic legal reasoning or argumentation. Such approaches may provide greater capacity to represent legal uncertainty while maintaining the transparency, auditability, and human oversight required in legally regulated AI environments.

6. Conclusions

This study examined whether deterministic legal verification can be integrated into an AI-assisted cybercrime monitoring architecture through executable Condition–Permission–Limitation (C–P–L) rules. The proposed Automated Cybercrime Monitoring System separates statistical risk assessment from legal verification and places the latter between AI-generated candidate decisions and operational execution.

The experimental results indicate that forty-two selected legal requirements can be operationalised as executable C–P–L rules and evaluated deterministically before implementation. The integrated ACMS achieved an F1-score of 89.2%, compared with 91.4% for the baseline AI subsystem, while its accuracy was 89.8%, compared with 91.6% for the baseline. These differences represent end-to-end performance after the addition of the legal-verification stage; the underlying machine-learning model was not modified or retrained. The architecture consequently demonstrates the feasibility of adding a legal-control layer without changing the predictive model.

The cross-configuration experiment further demonstrated that the operational behaviour of the compliance controller can be modified through changes to the executable legal-rule set while preserving the underlying machine-learning model. The Strict, Moderate, and Permissive configurations are experimental analytical models rather than representations of particular national legal systems. Under the compliance-rate definition adopted in this study, the configurations produced rates of 90.7%, 93.3%, and 95.4%, respectively. These results demonstrate architectural adaptability to changes in executable legal constraints rather than normative superiority of one regulatory regime over another.

The study also demonstrates the potential value of treating legal compliance as an operational design property rather than solely as a post-deployment governance or auditing activity. Deterministic verification can enforce predefined and sufficiently formalised legal prerequisites, initiate mandatory human review where required, prevent specified non-compliant actions from being executed, and support auditability through recorded decision outcomes. At the same time, deterministic legal verification cannot reproduce the interpretive and discretionary functions of judges or other competent legal authorities. Questions involving proportionality,

necessity, reasonableness, competing fundamental rights, and complex factual interpretation therefore remain dependent upon appropriate human decision-making.

The principal contribution of the study is consequently architectural and methodological. It demonstrates how artificial intelligence, computational law, and compliance-by-design can be connected within an operational workflow in which legal constraints are evaluated before implementation. The findings support further research using real-world datasets, larger and dynamically maintained executable legal corpora, jurisdiction-specific validation, and hybrid computational-law approaches capable of addressing legal uncertainty while preserving transparency, auditability, and human oversight.

7. References

- ALLAHRAKHA, N. "Legal frameworks for AI-driven cybercrime prevention". *Uzbek Journal of Law and Digital Policy*, v. 2, n. 1, 2024, pp. 1-24. <https://irshadjournals.com/index.php/ujldp/article/view/253>
- ATKINSON, K., BENCH-CAPON, T. and BOLLEGALA, D. "Explanation in AI and law: Past, present and future". *Artificial Intelligence*, v. 289, 2020, Article 103387. <https://doi.org/10.1016/j.artint.2020.103387>
- AVGERINOS LOUTSARIS, M. "Mapping the European Legislation Identifier (ELI) and Akoma Ntoso ontologies for legal data interoperability". *ACM Digital Library*, 2023, pp. 41-53. <https://doi.org/10.1145/3614321.3614327>
- BOROVYK, A., SHYRA, O., and KRAVCHENKO, O. "Criminal law aspects of financial security of a state". *Baltic Journal of Economic Studies*, v. 11, n. 1, 2025, pp. 221-230. <https://doi.org/10.30525/2256-0742/2025-11-1-221-230>
- BUÇAJ, E., and THAQI, A. "Global regulation of cybercrime through international law and cyberconventions". *Criminology*, v. 7, 2025, pp. 155-170. <https://doi.org/10.18716/ojs/krimoj/2025.1.9>
- CALIFORNIA PRIVACY RIGHTS ACT. CPRA – text of the California Privacy Rights Act. 2020 Available at: <https://www.caprivacy.org/cpra-text/> (accessed on 25 May 2026).
- CMS Expert Guide to Data Protection and Cyber-Security Laws: Ukraine. Law of Ukraine "On Personal Data Protection" No. 2297-VI 2025. Available at: https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/ukraine?utm_source=chatgpt.com (accessed on 25 May 2026).
- CONG, W., HARVEY, C., RABETTI, D., and WU, Z-Y. "An anatomy of crypto-enabled cybercrimes". *Management Science*, v. 71, n. 4, pp. 3622-3633. <https://doi.org/10.1287/mnsc.2023.03691>
- COUNCIL OF EUROPE. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+) (CETS No. 223). 2018. Available at: <https://www.coe.int/en/web/data-protection/convention108-and-protocol> (accessed on 25 May 2026).
- COUNCIL OF EUROPE. Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108+). 2022. Available at: <https://rm.coe.int/16802fa3a3> (accessed on 25 May 2026).
- COUNCIL OF EUROPE. Convention on cybercrime (ETS No. 185). Available at: <https://www.coe.int/en/web/cybercrime/the-budapest-convention> (accessed on 25 May 2026).
- COURT OF JUSTICE OF THE EUROPEAN UNION. Case C-634/21, SCHUFA Holding AG (Scoring), EU:C:2023:957. 2023. Available at: <https://curia.europa.eu> (accessed on 25 May 2026).
- COURT OF JUSTICE OF THE EUROPEAN UNION. Case C-203/22, Dun & Bradstreet Austria, EU:C:2025. 2025. Available from: <https://curia.europa.eu> (accessed on 25 May 2026).
- DLA PIPER. Data protection laws of the world. 2026. Available at: <https://www.dlapiperdataprotection.com/?t=> (accessed on 25 May 2026).
- EUROJUST. Cybercrime judicial monitor. 2025. Available at: <https://www.eurojust.europa.eu/sites/default/files/assets/files/cybercrime-judicial-monitor-issue-10.pdf> (accessed on 25 May 2026).
- EUROPEAN COMMISSION. Ethics guidelines for trustworthy artificial intelligence. Brussels: High-Level Expert Group on Artificial Intelligence, 2019. Available at: [589](https://digital-</p>
</div>
<div data-bbox=)

- strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai (accessed on 25 May 2026).
- EUROPEAN COMMISSION. Shaping Europe's digital future. 2024. Available at: <https://digital-strategy.ec.europa.eu> (accessed on 25 May 2026).
- EUROPEAN COMMISSION. White Paper on Artificial Intelligence: A European Approach to Excellence and Trust COM(2020) 65 final. 2020. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0065> (accessed on 25 May 2026).
- EUROPEAN COMMISSION FOR DEMOCRACY THROUGH LAW (VENICE COMMISSION). Rule of Law Checklist (CDL-AD(2016)007). 2016. Available at: <https://www.venice.coe.int> (accessed on 25 May 2026).
- EUROPEAN COURT OF HUMAN RIGHTS. Big Brother Watch and Others v United Kingdom, Applications Nos. 58170/13, 62322/14 and 24960/15, Grand Chamber, Judgment of 25 May 2021. 2021. Available at: <https://hudoc.echr.coe.int> (accessed on 25 May 2026).
- EUROPEAN DATA PROTECTION BOARD. Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. 2024. Available at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052022-use-facial-recognition-technology-area_en (accessed on 25 May 2026).
- EUROPEAN PARLIAMENT and COUNCIL OF THE EUROPEAN UNION. Regulation (EU) 2022/2065 on a single market for digital services (Digital Services Act). 2022. Available at: <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act> (accessed on 25 May 2026).
- EUROPEAN UNION. Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). 2024. Available at: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj> (accessed on 25 May 2026).
- EUROPEAN UNION. Convention on Cybercrime — EUR-Lex Summary. 2023. Available at: <https://eur-lex.europa.eu/EN/legal-content/summary/convention-on-cybercrime.html> (accessed on 25 May 2026).
- EUROPEAN UNION. Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union (NIS2 Directive). 2022. Available at: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj> (accessed on 25 May 2026).
- EUROPEAN UNION. Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). 2016. Available at: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng> (accessed on 25 May 2026).
- EUROPEAN UNION. Regulation (EU) 2024/2847 of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act). 2024. Available at: <https://eur-lex.europa.eu/eli/reg/2024/2847/oj> (accessed on 25 May 2026).
- EUROPEAN UNION. Charter of Fundamental Rights of the European Union. 2012. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT> (accessed on 25 May 2026).
- EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA). ENISA Threat Landscape 2025. Luxembourg: Publications Office of the European Union, 2025. Available at: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025> (accessed on 25 May 2026).
- EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (FRA). Getting the future right – artificial intelligence and fundamental rights. 2024. Available at: <https://fra.europa.eu> (accessed on 25 May 2026).
- FLORIDI, L. and COWLS, J. "A unified framework of five principles for AI in society". *Harvard Data Science Review*, v. 1, n. 1, 2019, pp. 1-14. <https://doi.org/10.1162/99608f92.8cd550d1>
- FORCEPOINT. Tracking global data protection laws in 2026. 2026. Available at: <https://www.forcepoint.com/blog/insights/tracking-global-data-protection-laws-2026> (accessed on 25 May 2026).
- FUTANE, S. S., PATIL, P., and NAGRALE, N. "Adaptive multi-model cybercrime identification, prediction using machine learning, and explainable AI". *International Journal for Research in Applied Science and Engineering Technology*, v. 13, n. 8, 2025, pp. 2113. <https://doi.org/10.22214/ijraset.2025.73926>

- N-LAWS. Privacy & Data Protection Laws 2025: The definitive global data protection guide. 2025. Available at: <https://n-laws.com/privacy-data-protection-laws-2025-the-definitive-global-data-protection-guide/> (accessed on 25 May 2026).
- NISHA, M. P. "Dark web guardian: Real time threat detection and analysis". *International Scientific Journal of Engineering and Management*, v. 4, n. 5, 2025, pp. 1-7. <https://doi.org/10.55041/isjem03502>
- OASIS. LegalRuleML Core Specification Version 1.0. 2025. Available at: <https://docs.oasis-open.org/legalruleml/legalruleml-core-spec/v1.0/csprd01/legalruleml-core-spec-v1.0-csprd01.html> (accessed on 25 May 2026).
- OECD. OECD Principles on Artificial Intelligence. 2024. Available at: <https://oecd.ai/en/ai-principles> (accessed on 25 May 2026).
- PALMIRANI, M. "A smart legal order for the digital era: A hybrid AI and dialogic model". *Rivista Italiana di Informatica e Diritto*, 2023, pp. 633-655. <https://doi.org/10.1415/105387>
- PARK, H., and HONG, S. "Germany's online search and IT fundamental rights". *Korean Constitutional Law Association*, v. 29, n. 3, 2023, pp. 81-123. <https://doi.org/10.35901/kjcl.2023.29.3.81>
- PEOPLE'S REPUBLIC OF CHINA. Personal Information Protection Law (PIPL). 2021. Available from: <https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/> (accessed on 25 May 2026).
- PUBLICATIONS OFFICE OF THE EUROPEAN UNION. Cybercrime judicial monitor: EU AI act (Regulation (EU) 2024/1689). 2025. Available at: <https://op.europa.eu/en/publication-detail/-/publication/c4ead02c-5aec-11f0-a9d0-01aa75ed71a1/language-en> (accessed on 25 May 2026).
- SARTOR, G. *Legal reasoning: A cognitive approach to the law*. Dordrecht: Springer, 2005.
- SHARMA, V. "Artificial intelligence in cybercrime prevention, detection & investigation: A legal perspective". *VIDHIGYA the Journal of Legal Awareness*, v. 19, n. 1-2, 2024, pp. 34-38. <https://doi.org/10.5958/0974-4533.2024.00004.4>
- SIMBOLON, N. Y. "Ancaman cybercrime di Indonesia: Tinjauan sistematis dan peran cybersecurity pada e-commerce dalam hukum pidana". *Jurnal Sosial Humaniora Dan Pendidikan*, v. 4, n. 2, 2025, pp. 815-825. <https://doi.org/10.55606/inovasi.v4i2.4425>
- STUPNYK, Y. V., and KHOMA, O. I. "Methodological principles of forming a comprehensive system of combating crime in the activities of law enforcement agencies". *Analytical and Comparative Jurisprudence*, v. 2, n. 3, 2025, pp. 475-481. <https://doi.org/10.24144/2788-6018.2025.03.2.76>
- SYTNYK, G., ZUBCHIK, O., and OREL, M. "Conceptual Understanding of the features of management of innovative development of the state in modern conditions". *Science and Innovation*, v. 18, n. 2, 2022, pp. 3-15. <https://doi.org/10.15407/scine18.02.003>
- TAYLOR WESSING. Interoperable Europe act published in official journal. 2024. Available at: <https://www.taylorwessing.com/de/insights-and-events/gdh-latest-news> (accessed on 25 May 2026).
- UNITED KINGDOM. Data (Use and Access) Act 2025. 2025. Available at: <https://www.legislation.gov.uk/ukpga/2025/18/contents/enacted> (accessed on 25 May 2026).
- UNITED NATIONS OFFICE ON DRUGS AND CRIME. United Nations Convention against Cybercrime. 2024. Available at: <https://www.unodc.org/unodc/en/cybercrime/ad-hoc-committee.html> (accessed on 25 May 2026).
- VERKHOVNA RADA OF UKRAINE. On protection of personal data (Law of Ukraine No. 2297-VI). 2010. Available at: <https://zakon.rada.gov.ua/go/2297-17> (accessed on 25 May 2026).
- ZAKHAREVYCH, R. V. "Implementation of foreign experience into Ukrainian legislation on combating cybercrime". *Analytical and Comparative Jurisprudence*, v. 2, n. 3, 2025, pp. 372-376. <https://doi.org/10.24144/2788-6018.2025.03.2.60>