Baltic J. Modern Computing, Vol. 13 (2025), No. 1, 166-176
https://doi.org/10.22364/bjmc.2025.13.1.09

Advancing Cybersecurity through AI: Insights from EU and Candidate Nations

Blerta LEKA[1], Daniel LEKA[2]

[1] Department of Mathematics and Informatics, Faculty of Economy and Agrobusiness, Agricultural University of Tirana, St. Paisi Vodica 1025, Tiranë, Albania,
[2] Special Court of First Instance for Corruption and Organized Crime, St. Jordan Misja, 1057, Tiranë, Albania

bmocka@ubt.edu.al, lekadaniel@yahoo.com

ORCID 0009-0000-6734-8237, ORCID 0009-0003-6154-9996

Abstract. Artificial Intelligence technologies are changing many sectors, but they also bring difficult challenges, especially in cybersecurity and data protection. As the adoption of artificial intelligence increases, countries face growing threats from cybercrime and must implement frameworks strong data protection. This study examines the connections between artificial intelligence, cyber security and data protection in relation to Albania and North Macedonia's progress towards integration into the European Union. The challenges and progress that these countries are experiencing to reach EU standards are assessed, especially in relation to the General Data Protection Regulation (GDPR). Using qualitative methods, including policy analysis and case studies, will help determine the effectiveness of cybersecurity and data protection frameworks.

Keywords: Digital Transformation, AI Ethics, Regulatory Compliance, Information Security, Threat Mitigation and National Cybersecurity Strategy

1. Introduction

Artificial Intelligence (AI) is a dynamic field within computer science dedicated to creating systems that can learn, reason, and operate autonomously. Russell and Norvig (2009) define AI as a focus on agents that perceive their environment and take actions based on that perception. Rich et al. (2009) further emphasize that AI's aim is to enable machines to perform tasks typically requiring human intelligence. This broad field encompasses sub-domains like deep learning, natural language processing, robotics, and computer vision. According to Gartner (2024), although over 60% of Chief Information Officers (CIOs) believe AI is essential for driving innovation, less than half are prepared to manage the associated risks.

AI is revolutionizing various industries, from healthcare and finance to transportation and telecommunications, with significant applications in cybersecurity. AI systems are particularly important in automating threat detection and anomaly identification, crucial for mitigating risks. The 2024 Cyber Security Breaches Survey highlights that a substantial number of businesses (50%) and charities (32%) in the UK faced cyberattacks

over the past year (UK Government, 2024). While larger organizations tend to implement stronger security measures, smaller entities struggle with vulnerabilities. The European Cybersecurity Strategy stresses the necessity of industry collaboration to reinforce defenses, and initiatives like Horizon Europe focus on advancing AI-driven security measures.

The European Court of Auditors (2024) points to an urgent need for a coherent regulatory framework for AI within the EU, advocating for the integration of ethical considerations while fostering innovation. The General Data Protection Regulation (GDPR) serves as the cornerstone of EU data protection law, establishing compliance standards for AI systems processing personal data to safeguard individual privacy rights (European Union). Furthermore, the AI Act aims to enhance oversight concerning AI's role in data protection, underscoring the importance of privacy by design.

The EU has been proactive in regulating AI, as evidenced by the Proposal for an AI Act introduced in April 2021. This legislation categorizes AI systems based on their risk profiles, establishing regulatory measures for high-risk systems and prohibiting those deemed unacceptable. The EU's strategy emphasizes human oversight and data quality, ensuring AI systems operate ethically and reliably. Mandatory assessments facilitate risk identification, aligning AI use with privacy and human rights standards. These efforts are vital for building public trust in AI technologies while mitigating potential abuses of automated decision-making. Also, the European Data Protection Board (EDPB) provides important guidelines and recommendations to candidate countries, helping to implement data protection standards (EDPD, 2024). This is essential to building a cyber security culture that includes not only laws but also good practice.

1.1. Global AI strategies and their impact

Globally, nations are advancing AI technologies with distinct strategies. The United States launched the American AI Initiative in 2019, aiming to maintain its leadership through increased research funding and promoting ethical AI. Meanwhile, China's New Generation AI Development Plan (2017) seeks to position the country as an AI leader by 2030, investing heavily in innovation centers to drive economic growth (Webster et al., 2017).

In Canada, the Pan-Canadian AI Strategy, initiated by CIFAR in 2017, promotes diversity in AI research and supports talent development. This initiative, backed by a $125 million commitment, also delves into the ethical, legal, and social implications of AI (CIFAR, 2017). Japan's Society 5.0 initiative integrates AI with the Internet of Things (IoT), focusing on sustainable development and addressing social challenges. Similarly, Europe's AI efforts are increasingly linked with regulatory and ethical frameworks.

The Stargate project, a $500 billion initiative led by OpenAI and SoftBank, aims to create shared AI computing infrastructure to meet rising demands. The project's first $100 billion phase focuses on facilities in Texas, involving partners like Oracle, Microsoft, and Nvidia. This initiative marks a shift toward shared resources across competitors, supported by the White House, to maintain U.S. AI leadership and address economic and security concerns. However, regulatory challenges regarding market competition may arise (Jackson, 2025). To tackle ethical concerns in AI, organizations should adopt best practices like regular audits, bias detection mechanisms, and a culture of ethical AI development. A clear

accountability framework is essential to address these concerns (Mensah & Sukah Selorm, 2023).

1.2. Regulatory Developments and Compliance in AI

The General Data Protection Regulation (GDPR) underpins EU data protection laws and serves as a model for AI governance in Albania and North Macedonia. Compliance with GDPR ensures AI systems operate ethically, promoting responsible deployment.
The AI Act, passed by the European Parliament, provides a comprehensive framework to regulate AI development, deployment, and use in the EU. It aims to ensure safety, transparency, and the protection of fundamental rights. The Act's risk-based approach categorizes AI systems based on their potential risks, imposing varying obligations depending on their classification. High-risk AI systems face stricter requirements, while general-purpose AI systems are subject to additional regulations to address systemic risks. The Act is expected to come into effect by the end of 2024, with organizations required to map AI systems, conduct risk assessments, and implement governance frameworks to comply with the legislation. In Figure 1 are shown the AI act risk-based approach by EU.

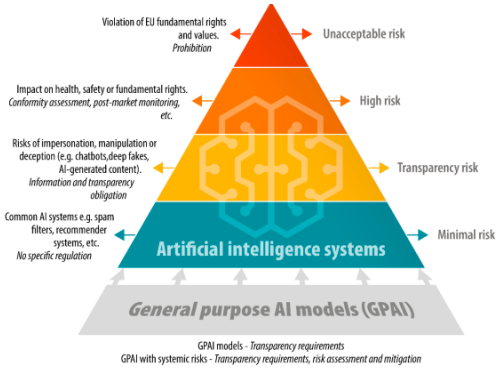

Figure 1. EU AI act risk-based approach (EU, 2024)

2. Current State of AI and Cybersecurity in Albania and North Macedonia

Both Albania and North Macedonia face significant cybersecurity challenges, including increasing cybercrime, outdated infrastructures, and limited enforcement of GDPR. These challenges are exacerbated by the rapid digitalization of government services, escalating threats from state-sponsored cyber activities, and a lack of local expertise in cybersecurity and AI-driven security solutions.

While both countries have made strides toward digital transformation, gaps remain in workforce readiness, regulatory frameworks, and technological capabilities. Key areas requiring urgent attention include:

- Cybercrime Trends: The frequency of cyberattacks targeting government institutions, businesses, and critical infrastructure has risen, revealing weaknesses in cybersecurity policies. Notably, the 2022 cyberattack on Albania's government systems, attributed to state-sponsored actors, disrupted public services and databases (Koloshi, 2022).
- Existing Policies: Both countries have national cybersecurity strategies, but enforcement remains inconsistent. Albania has adopted Laws No. 2/2017 "On Cybersecurity" and No. 9887 "On the Protection of Personal Data," aligning with EU standards. North Macedonia faces similar challenges in policy enforcement.
- Key Priorities: Strengthening regulatory enforcement, investing in AI-driven security measures, and improving cross-border collaboration with EU institutions are essential priorities for both nations.

Addressing these challenges will enhance digital infrastructure protection, foster innovation, and improve trust in AI-driven cybersecurity solutions.

2.1. Development of Artificial Intelligence in Albania and North Macedonia

Both Albania and North Macedonia are advancing AI integration, though challenges remain in aligning with EU standards for data protection and cybersecurity.

Albania has initiated projects to integrate AI into public administration and align with EU legislation. The National Agency for Information Society (AKSHI) is leading an NLP-based project to automate the transposition of EU laws (AKSHI, 2024). Additionally, Albania's National Cybersecurity Agency (NCERT), within the National Agency for Electronic Certification and Cybersecurity (NAECCS), coordinates cybersecurity efforts (NAECCS, 2023). Albania has ratified the Budapest Convention on Cybercrime and enacted laws aligned with international standards to enhance cybersecurity resilience. Notable AI initiatives in Albania include:

- AI for Youth Program: A partnership between the Albanian-American Development Foundation (AADF) and Intel introduces AI education in 30 high schools, aiming to reach 2,000 students by 2026 (AADF, 2021).
- EU Digital Justice Project: This initiative modernizes Albania's justice system through digital transformation, improving efficiency and transparency (En, 2025).
- AI in Public Procurement: The Albanian government has proposed using AI to enhance public procurement transparency, aiming to reduce corruption (Balkaninsight, 2024).
- Memorandum of Understanding with Italy: Albania and Italy have signed a memorandum to strengthen bilateral cooperation in cybersecurity. This agreement focuses on enhancing capabilities to defend against cyber-attacks, sharing information on emerging threats, and adopting best practices in cybersecurity(Caffo, 2024).

Despite these efforts, local businesses in Albania are slow to adopt AI and machine learning, remaining in early stages of AI implementation (Kaso & Xhindi, 2023). To

address this, AKSK has implemented additional training programs for employment, business, and education. Recently, the LAIA project has been introduced to further enhance AI education and align with EU standards (LAIA, 2023).

Similarly, North Macedonia is integrating AI in public administration, digital infrastructure, and services. AI is also increasingly applied in sectors like manufacturing and healthcare. However, challenges remain in raising public awareness and strengthening cybersecurity resilience, especially against geopolitical cyber threats (Poposka, 2023).

A major cybersecurity incident in North Macedonia in 2020 exposed personal data of millions of citizens, highlighting significant gaps in preparedness for large-scale cyber threats. The government's response involved collaboration with law enforcement and private sector cybersecurity firms, along with public transparency efforts. Additionally, both Albania and North Macedonia benefit from IPA (Instrument for Pre-Accession Assistance) II and IPA III funding, which continues to support cybersecurity capacity-building efforts and alignment with EU directives (CILC, 2025).

2.2. Estonia's and Slovenia's Experiences

The integration of emerging technologies such as Artificial Intelligence (AI) with robust cybersecurity frameworks is critical for countries seeking EU membership. As EU members, Estonia and Slovenia provide valuable case studies for Albania and North Macedonia, illustrating how these technologies can be harmonized with national policies to address both digital innovation and cybersecurity challenges.

Estonia stands out for its advanced AI strategy and the 2020 AI Act, which prioritizes AI ethics and data protection. Similarly, Slovenia has aligned its data protection legislation with the GDPR, establishing a strong foundation for both AI development and cybersecurity. The experiences of both countries demonstrate the importance of integrating AI into national policies while simultaneously addressing cybersecurity concerns.

In contrast, Albania and North Macedonia face challenges in modernizing their cybersecurity laws and developing national AI strategies. Albania's cybersecurity framework remains outdated, and North Macedonia's AI development frameworks are still limited. These gaps inhibit their ability to fully capitalize on the potential of AI and secure digital environments for their citizens.

Furthermore, Slovenia's commitment to cybersecurity education—through the establishment of specialized cybersecurity schools and a national coordination center—highlights the importance of building a skilled workforce to address emerging threats. Slovenia is also addressing 5G cybersecurity risks through the implementation of the 5G Cybersecurity Toolbox, further strengthening its digital transformation efforts (Digital Decade Report, 2024).

To overcome these challenges, Albania and North Macedonia should prioritize developing comprehensive AI frameworks that align with EU standards. Strengthening public-private collaboration in cybersecurity will also be essential to enhancing their digital resilience. By drawing lessons from Estonia and Slovenia's approaches, both countries can take significant steps toward securing their digital futures and meeting EU integration criteria.

3. Cybersecurity

Cybersecurity remains a critical concern for both Albania and North Macedonia, especially in light of growing digital threats. Albania, for instance, experienced significant cyberattacks in 2022, notably targeting government institutions. In response, Albania has established key entities such as the National Computer Incident Response Team (AL-CIRT) and the National Authority for Electronic Certification and Cybersecurity (NAECCS) to lead national efforts in mitigating cyber risks. The Albanian National Agency for Information Society (AKSHI) has been taking steps to bolster cybersecurity capabilities, although challenges related to expertise and resources persist. Notably, incidents like the cyberattack on the TIMS (Albanian Immigration System), which compromised sensitive immigration data, and another targeting the e-Albania portal, which disrupted public services, underscored the vulnerabilities in government digital platforms.

In North Macedonia, the National Cybersecurity Strategy (NAECCS) has been instrumental in improving the country's cybersecurity infrastructure and raising awareness about digital risks. The NAECCS closely aligns with EU standards, providing services such as secure online transactions and digital signature verification. Cooperation with both the EU and NATO plays a vital role in enhancing cybersecurity in North Macedonia and Albania.

A comparative analysis of the cybersecurity landscapes in Albania, North Macedonia, Estonia, and Slovenia, as presented in the Global Cybersecurity Index (2024), offers valuable insights into the countries' cybersecurity measures across various domains (Figure 2):

- Legal Measures
- Technical Measures
- Organizational Measures
- Capacity Development

In Figure 2 a), Albania and Estonia show strong legal frameworks in line with international standards, providing a solid foundation for safeguarding data and ensuring cybersecurity. Slovenia also maintains a robust legal structure, reflecting its commitment to effective cybersecurity governance. Albania exhibits relatively strong technical capabilities in cybersecurity, whereas North Macedonia faces considerable challenges in this domain (Figure 2 b), necessitating improvements in technical infrastructure and cybersecurity tools. Both Albania and North Macedonia share comparable organizational measures, reflecting their efforts to establish structured cybersecurity frameworks (Figure 2 c). Estonia’s perfect score for organizational measures exemplifies best practices and serves as a model. However, Albania and North Macedonia lag in capacity development, as highlighted in Figure 2 d), with both countries needing to invest in enhancing their cybersecurity workforce skills. Estonia and Slovenia, in contrast, have made significant investments in workforce development.

Cooperation measures are vital for building resilient cybersecurity frameworks. While Albania has shown notable progress, North Macedonia's lower score underscores the need for stronger international partnerships. Estonia and Slovenia lead by example, demonstrating the importance of collaborative cybersecurity efforts.

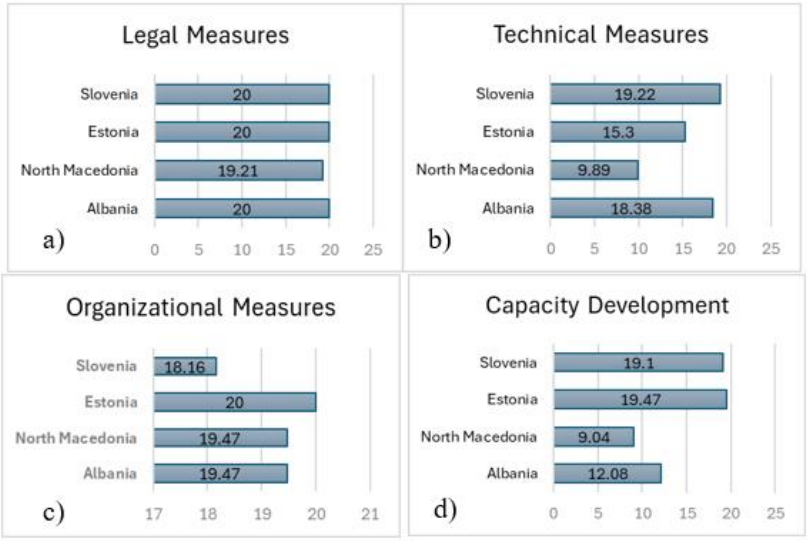

Figure 2. The cybersecurity landscape among Albania, North Macedonia, Estonia, and Slovenia (ITU, 2024)

Estonia and Slovenia, ranked in Tier 1, exhibit the most advanced cybersecurity capabilities, scoring highly across all five pillars: legal, technical, organizational, capacity development, and cooperation. Estonia stands out with technical measures (15.3), organizational measures (20), and cooperation measures (20), while Slovenia achieves similar success in these domains, with technical (19.22), organizational (18.16), and cooperation measures (20).

Albania, in Tier 2, has made significant progress, especially in legal and organizational measures, scoring 20 and 19.47, respectively. However, there is room for improvement in technical capabilities (18.38) and capacity development (12.08), as reflected in its rise of 23 positions in the Global Cybersecurity Index. North Macedonia, placed in Tier 3, faces considerable challenges, especially in technical (8.89) and capacity development (9.04) measures. Though it performs well in legal (19.21) and organizational measures (19.47), further investment and reforms are necessary to raise its cybersecurity standards.

4. Challenges and Recommendations for the Future

Both Albania and North Macedonia face challenges in complying with the General Data Protection Regulation (GDPR). Albania has enacted Law No. 9887 on the Protection of Personal Data, ensuring robust protection measures, but its enforcement is still a work in progress. North Macedonia has similarly introduced data protection regulations, but effective implementation remains a challenge.

Despite their progress, Albania and North Macedonia must continue aligning their regulations with EU standards. Both countries benefit from programs such as Horizon

Europe and Erasmus+, which help improve technological and digital capacities. International cooperation with the EU and NATO is critical for strengthening cybersecurity and data protection frameworks.

Albania is actively advancing its capabilities in artificial intelligence (AI) and cybersecurity. Recent initiatives, such as using Natural Language Processing (NLP) to facilitate EU regulation transposition and deploying a virtual assistant within public administration, underscore Albania's commitment to leveraging AI for governance and regulatory compliance (European Commission, 2023). Moreover, the establishment of AL-CIRT reflects Albania's proactive approach to cybersecurity, aiming to address vulnerabilities and safeguard critical infrastructure. However, challenges such as inadequate data infrastructure and ethical concerns surrounding AI deployment persist.

Both countries must invest in digital infrastructure and professional training to meet EU standards and accelerate their integration process. Strengthening enforcement mechanisms for data protection and cybersecurity regulations is key, as is fostering international collaborations to enhance technological capacities. Currently, AI regulatory frameworks in Southeast Europe are underdeveloped, and harmonization with EU standards is essential to ensure ethical AI use, stakeholder engagement, and adaptive policies that can keep pace with technological advancements (Kovacev et al., 2024).

The OECD highlights the importance of governance principles for AI, focusing on transparency, accountability, and public trust to mitigate AI-related risks (OECD, 2023). Adopting these principles can enhance Albania and North Macedonia's cybersecurity measures and align them with EU standards, addressing the pressing need for effective data protection strategies.

The 2024 AI Index Report suggests several strategies for responsible AI deployment:

- Ethical Governance: Establish ethical frameworks that prioritize human rights and societal well-being.
- Data Privacy Regulations: Enforce robust data protection laws to build public trust in AI systems.
- Public-Private Partnerships: Foster collaborations between government and industry to drive innovation while maintaining accountability.
- Education and Workforce Development: Invest in AI training programs to enhance workforce capabilities and public AI literacy.
- Transparency and Accountability: Require AI systems to be explainable and accountable, with mechanisms for addressing biases.

These strategies will support the responsible adoption of AI, addressing societal challenges and ensuring the technology serves the broader public good (Stanford HAI, 2024).

5. Conclusion

Cybersecurity is a problem in every nation. North Macedonia and Albania Security regulations, knowledge, and procedures are being actively improved by groups like AL-CIRT and NAECCS. Significant strides have been made by both nations to improve their cyber security, particularly in the wake of the assaults. Cyberattacks targeting state institutions and critical infrastructure highlight the urgency of addressing these

vulnerabilities. Achieving EU standards requires continued efforts, international cooperation, and substantial investments in human and technological resources.

The Global Cybersecurity Index 2024 underscores the varied progress in cybersecurity among these countries. While Albania has made considerable progress in legal and organizational measures, it needs to focus on improving its technical capabilities. North Macedonia, while strong in legal and organizational aspects, requires investments in technical infrastructure and enhanced international cooperation. Estonia and Slovenia, ranked in Tier 1, serve as models in cybersecurity, setting benchmarks for Albania and North Macedonia.

Implementing GDPR regulations and adhering to EDPB guidelines will be crucial for both countries as they strive for EU integration. These frameworks will foster a culture of information security and facilitate the adoption of advanced technologies, such as AI, to enhance threat detection and response. A strong commitment to transparency and accountability will be essential for effective data protection and a safer digital environment for citizens. By improving data protection practices and frameworks, Albania and North Macedonia can lead by example and inspire other EU aspirants.

Furthermore, the European community is increasingly emphasizing the advancement of the Western Balkans. The institutions set up in both Albania and North Macedonia are growing their influence and impact. Efforts in training, legal framework implementation, investments, and raising awareness among citizens, businesses, and employees are improving. However, some ongoing challenges include insufficient human resources and outdated legal frameworks, and the focus is on improving these areas to meet EU standards. Strengthening regional cooperation and learning from one another will be essential for fostering a collaborative cybersecurity environment in the Western Balkans. By adopting a proactive and unified approach, Albania and North Macedonia can improve their cybersecurity posture and continue their path toward EU membership.

References

AADF (Albanian American Development Foundation) (2021). Memorandum of understanding paves way for AI empowerment among Albanian youth. Albanian American Development Foundation. https://www.aadf.org/memorandum-of-understanding-paves-way-for-ai-empowerment-among-albanian-youth

Balkan Insight (2024). Using AI in Albanian public procurements: No easy solution for corruption. https://balkaninsight.com/2024/10/28/using-ai-in-albanian-public-procurements-no-easy-solution-for-corruption

Caffo, A. (2024). Italy and Albania sign a memorandum for cooperation in cybersecurity. 4iMAG. https://4imag.com/italy-and-albania-sign-a-memorandum-for-cooperation-in-cybersecurity

Centre for International Legal Cooperation (CILC). EU support to Western Balkans cybersecurity capacity building. CILC. https://www.cilc.nl/projects/eu-support-to-western-balkans-cybersecurity-capacity-building/

EDPD-European Data Protection Board (2024). European Data Protection Board (EDPB). https://www.edpb.europa.eu/edpb_en

European Commission (2021). *Artificial Intelligence Act*.

European Commission (2023a). *Albania 2023 report: Accompanying the document communication from the commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: 2023 communication on EU enlargement policy (SWD(2023) 690 final).* Brussels.

European Commission (2023b). *EU AI Act: First regulation on artificial intelligence.* https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

European Commission (2024a). *European approach to artificial intelligence.* https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence

European Commission (2024b). *European AI office*. https://digital-strategy.ec.europa.eu/en/policies/ai-office

European Parliament (2023). *Cybersecurity strategy*.

European Union (2022). General Data Protection Regulation (GDPR). https://eur-lex.europa.eu/EN/legal-content/summary/general-data-protection-regulation-gdpr.html

Gartner (2024). *AI readiness.* https://www.gartner.com/en/information-technology/topics/ai-readiness

GDPR Info (2021). *General data protection regulation compliance guidelines.*

International Telecommunication Union (ITU) (2024). Global cybersecurity index 2024 (5th ed.). https://doi.org/10.1787/2476b1a4-en

Jackson, A. (2025). How the $500bn Stargate venture signals an AI strategy shift. Data Centre Magazine. https://datacentremagazine.com/technology-and-ai/how-500bn-stargate-venture-signals-ai-strategy-shift

Koloshi, E. (2022). Session I: Conducting criminal investigations of ransomware attacks. *International workshop on conducting criminal investigations of ransomware attacks*, The Hague, Netherlands. Council of Europe. https://rm.coe.int/session-i-edmond-koloshi-albania/1680a8cbe4

Kaso, E., Xhindi, T. (2023). The use of artificial intelligence and machine learning technology by companies in Albania. UMSH Press. https://www.umsh.edu.al/media/650d6a5695eea.pdf

Kovacev, A., Vujanović, P., Stanković, M. (2024). Regulatory frameworks for AI in Southeast Europe: Current state and future directions. *Journal of Regulation & Governance*, **22**(1), 22-34. https://www.eca.europa.eu/en/publications/SR-2024-08

LAIA (2023). *LAIA project: Developing AI education in Albania and Kosovo.* ERASMUS-EDU-2023-CBHE. https://laiaproject.eu/

Mensah, G. B., Sukah Selorm, J. M. (2023). Addressing ethical concerns in artificial intelligence: Tackling bias, promoting transparency and ensuring accountability. https://doi.org/10.13140/RG.2.2.20173.61925

National Agency for Electronic Certification and Cyber Security (NAECCS). (2023). *Annual report 2023*. https://aksk.gov.al/en/annual-report-2023/

National Agency for Information Society (AKSHI) (2024). *Report on the use of AI for transposing EU legislation*.

National Authority for Electronic Certification and Cyber Security (NAECCS) (2024). Law No. 25/2024 on Cybersecurity (in Albanian). https://aksk.gov.al/wp-content/uploads/2024/04/ligj-2024-03-21-25-5.pdf

OECD (2023). *AI governance: Implementing the OECD principles on artificial intelligence. OECD Artificial Intelligence Papers, No. 22.* https://doi.org/10.1787/2476b1a4-en

Poposka, V. (2023). Normative framework toward cyber crimes in North Macedonia. *International Scientific Journal Sui Generis*, **2.** 85-99. 10.55843/SG2321085p.

Rich, E., Knight, K., Nair, S. B. (2009). *Artificial intelligence (3rd ed.)*. Tata McGraw-Hill.

Russell, S., Norvig, P. (2010). *Artificial intelligence: A modern approach.* Prentice Hall.

Stanford University (2024). *2024 AI index report.* Stanford Human-Centered AI Institute. https://aiindex.stanford.edu/wp-content/uploads/2024/04/HAI_2024_AI-Index-Report.pdf

UK Government (2024). *Cyber security breaches survey 2024*. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024

Webster, G., Creemers, R., Kania, E., Triolo, P. (2017). *Full translation: China's 'New generation artificial intelligence development plan' (2017).* Stanford University. https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/

Received October 24, 2024, revised February 19, 2025, accepted February 19, 2025