Data protection challenges in the era of AI: Case study of Macedonia

Marjana PLANOJEVIKJ,
LL.M., Maj Pizza DOOEL - Slice Macedonia, Skopje, Republic of North Macedonia
marjanaplanojevicllm@gmail.com

Mimoza Bogdanoska JOVANOVSKA,
PhD, University St. Kliment Ohridski, Bitola, Republic of North Macedonia
mimoza.jovanovska@uklo.edu.mk

Abstract
In recent years artificial intelligence (AI) technologies have experienced exponential growth. This technology is associated with the collection and processing of a vast amounts of data, so there is complex challenges related to the way that the data are collected, processed and used; and the data privacy, primarily personal data. The researches related to the data protection faces with the challenges of balancing the need for large-scale data processing with the imperative to safeguard personal data. Ethical principles, codes and rules in AI implies undertaking a large number of activities, from in-depth analysis of the current state of play and prediction of negative consequences, to thorough development and definition of them. Very often public debates about these tools and systems are the next steps that need to be taken before approaching the process of creating legal standards as part of public policies for their design, development and use. Despite the enormous efforts to act quickly in the field of protection when using AI, there is an evident gap in monitoring and analyzing the evolution of personal data protection in the context of AI which has not been completed. The efforts are mainly focused on creating strategies and legal regulation for AI, and legal reforms in almost all areas where AI is used. However, some countries lag behind in the basic steps related to the regulation of AI and especially data processing and personal data protection. This paper presents the current state of play in the RN Macedonia related to the data protection regulation in the field of AI. As a method of research are used on-desk document and web page analysis. This paper will shed light on the problems faced by developing countries in which novelties always occur with a delay, and especially their regulation.

Keywords: artificial intelligence, data protection regulation, legal regulation.

1. Introduction
The rapid progress of digital technologies, especially artificial intelligence, has reshaped the world, so nowadays an artificial intelligence (AI) is already considered a new industrial revolution [1]. The development of machine learning and neural networks, as well as the digitalization of everyday activities that generate an abundance of data, have created the conditions and opportunity for using AI for analysis and decision-making. As a technology that solves complex problems based on learns from data, AI grown at an exceptionally fast pace altering and changing the methods of data collection, analysis, that led to complex concerns about privacy, clarity, and accountability, as well as an intricate issues related to data protection [2].

Similar to other technological innovations, AI carries not only positive outcomes but also possible adverse effects on people and society. One of recognized risks among others, is the risk related to data, especially two of them: (1) its concentration in a few companies that would become a monopoly, which would create the possibility of filtering the content and information that will be offered to them, thus compromising the freedom of choice of the individual, as well as the ability to self-determination; and (2) the need to protect that

data, especially those that relate to an identified or recognizable natural (living) person, including names, dates of birth, photographs, video recordings, e-mail addresses and telephone numbers, as well as IP addresses and the content of communications in order to ensure their fair processing (collection, use, storage) [3].

As technology becomes widely available, AI applications have enabled continuous monitoring of the human needs because only on that way can be analyze users' interests and objectives, so the tools powered by AI can learn to better meet their needs. Yet, the extensive use of AI to enhance user services has triggered legal concerns regarding privacy and security due to its reliance on personal data [4]. Moreover, AI can deliver predictive machine learning models, help minimize human bias, and support decision-making by applying probabilistic reasoning and data analysis [5]. Because AI systems have the ability to access, utilize, and learn from personal data, a strong regulatory framework is required to prevent potential misuse [6]. To make the governance of generative AI models more manageable, the principle of purpose limitation should be applied, ensuring that each model's intended use is clearly defined. Without narrowing its purpose, challenges may emerge, such as difficulties in justifying the collection of specific personal data. While AI is poised to drive positive global change, the creation of new AI tools and services must align with established data protection and regulatory standards to safeguard user information.

So, AI and data protection are interconnected concepts since AI uses data sets to make decisions and perform activities. So, ethical questions about personal data use and potential bias in AI had a high level actual. The need to regulate specific issues related to the use of data, especially personal data, within AI requires the adoption of new, specific legal principles, whereby the protection of human dignity and the protection of human rights and fundamental freedoms, in particular the right to the protection of personal data, is of essential importance. Consequently, in today's fast-paced technological landscape, ensuring data security has become a critical concern for individuals, organizations, and states alike. To protect data, companies and institutions must not only implement internal security measures but also adhere to laws regulating AI use. Therefore, government bodies likewise need to establish data protection policies, as AI applications are widely used by public agencies as well.

The rapid advancement of AI has raised profound legal and ethical concerns regarding data protection and privacy, particularly in developing nations. The rapid integration of artificial intelligence (AI) technologies in developing nations presents both opportunities for progress and significant challenges, particularly in the realms of data protection and privacy. Those countries mostly face with complex legal and institutional obstacles in regulating AI: lack of comprehensive data governance frameworks, weak enforcement mechanisms, and technological dependence on foreign-developed systems. Resent findings reveal that developing nations often lack the institutional capacity and normative clarity required to regulate AI effectively, which exacerbates risks of surveillance, discrimination, and rights violations [7].

The focus of this paper is to explore the broader relationship between the development of AI and data protection, by examining the current regulatory frameworks. The paper emphasizing legal reform the pressing necessity for well-structured AI governance strategies that safeguard human dignity and digital rights in the Republic of North Macedonia (RNM) by creating law framework rooted in human rights and tailored to specific contexts. It advocates for a multi-layered legal reform strategy designed to fit the capabilities and requirements of developing countries. Thus, the second part of the paper reviews the key areas that are intertwined in the focus. Then, the methodology used in the research is given at the third part. The fourth part focuses on the existing legal regulation worldwide and specifically in the RNM. The fifth part deals with ways to mitigate privacy risks in the era of AI, while the last part covers conclusions and suggestions for future research.

2. Research methodology

This paper has exploratory nature, employs a qualitative methodology approach to investigate the challenges of regulating AI and ensuring data protection in developing countries with focus on RNM as a case study. The study relies on a combination of document on-desk, web source analysis. The primary sources included: national laws, international regulations, and reports from international organizations. The secondary sources included: recent academic articles, policy papers, and institutional reports. The focus is identifying and analyzing existing legal frameworks and the gaps in AI regulation in RNM. The snowballing method was applied to identify the most relevant academic papers. A descriptive approach was employed to elaborate the collected materials, along with a comparative analysis and the presentation of a case study from RNM.

3. An Overview

3.1. Artificial intelligence (AI)

Artificial Intelligence (AI) is not a novel or futuristic concept but a long-integrated tool in everyday life and decision-making. It dates back to the middle of the last century and broadly refers to systems performing tasks that typically require human intelligence, such as perception, speech recognition, translation, and decision-making. AI includes technologies like machine learning, deep learning, and neural networks. It enables machines to mimic human problem-solving abilities and act autonomously. AI systems learn from vast datasets, recognizing patterns in text, speech, and images. Their power lies in analyzing data and adapting to complex challenges [8]. AI is defined as a technology that enables computers and machines to impersonate human intelligence and problem-solving abilities [9]. The most useful and popular AI uses are all based on learning patterns from data that has learned textual patterns from a huge amount of books, transcripts, and scraped content, all distilled in its deep neural network [10].

3.2. Privacy and data protection

Respect for privacy and data protection is a core value in democratic societies, shaped by standards from the United Nations [11], the Council of Europe [12] and the European Commission [13], and reflected in both international and national laws. While often linked, privacy and data protection are recognized as distinct rights, especially in Europe, where they are seen as vital for democratic sustainability. Privacy supports human dignity,

granting individuals autonomy and control over their personal information. It is both a personal right and a broader social value. Globally, privacy is widely acknowledged in constitutions or legal frameworks, unlike data protection, which is not yet universally recognized. Data protection focuses on the fair and secure handling of personal information like names, emails, or IP addresses, ensuring transparency and accountability. As AI becomes increasingly involved in decision-making, protecting personal data and upholding human rights and dignity remain crucial. Data protection has precise aims to ensure the fair processing (collection, use, storage) of personal data by both the public and private sectors [14]. The protection of human dignity and safeguarding of human rights and fundamental freedoms, in particular the right to the protection of personal data, are essential when developing and adopting AI applications that may have consequences on individuals and society. This is especially important when AI applications are used in decision-making processes [15].

3.3. Security of personal data processing

The concept of information security in data protection context refers to the security of personal data processing and is a part that complements and functions as part of the personal data protection system established by the organization in accordance with the personal data protection regulations.

Information Security refers to the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure confidentiality, integrity, and availability [16]**.** While information security focuses on assets, material or immaterial values of an organisation, data protection places the data subject in the center of all security related work. The concept of information security in data protection context refers to the security of personal data processing and is a part that complements and functions as part of the personal data protection system established by the organization in accordance with the personal data protection regulations [17]**.**

3.4. AI development and personal data

As AI rapidly advances, it raises important ethical concerns about the protection of users' personal data. Developers and users of AI systems must ensure transparency by informing individuals if and how their data is collected and processed. An issue of paramount importance when it comes to the connection between artificial intelligence and the protection of personal data is the issue of automated decision-making [18]. Users should clearly understand the purpose of data collection and be given the option to give or withhold consent. Under the GDPR, people have the right not to be subjected to such decisions, including profiling that involves analysing personal data to predict aspects like behaviour, preferences, or health. Ethical AI development requires clear regulations and accountability in algorithmic processes. A balanced approach is needed to support both innovation and the protection of personal data. This helps individuals and organizations navigate the challenges of AI while maintaining privacy and trust.

3.5. Key legal framework of data protection

The processing of personal data is subject to a complex interplay of different legal standards globally. The General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) are landmark data privacy regulations that impact organizations worldwide.

The General Data Protection Regulation (GDPR) is one of the most comprehensive data protection laws in the world and provides an overarching framework for the processing of personal data of individuals in the European Union (EU) and beyond, influencing global data privacy practices.

The GDPR sets out seven key principles such as: lawfulness, lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality (security) and accountability. It sets strict rules for processing personal data, including rights to access, correct, delete data, and requires user consent for data use.

GDPR enforces high standards and obliges organizations to take proper measures to ensure compliance.

In the United States of America, the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), represents a significant shift in the U.S. privacy and data security landscape. The CCPA introduced rights for consumers and obligations for businesses regarding the collection, sale, and handling of personal information.The CPRA, known as CCPA 2.0, amends CCPA by expanding consumer rights, heightening privacy protections, and establishing an enforcement agency to protect consumers.

Tibebu [19] points out that "the General Data Protection Regulation (GDPR) by the European Union and the California Consumer Privacy Act (CCPA) serve as benchmarks in legislative efforts to safeguard personal data". The paper highlights that these regulations underscore a global shift towards strengthening individual rights and imposing stricter obligations on data handlers.

According to Kotov [20] global data protection is also supported by international data security standards such as ISO/IEC 27001, which guide organizations in managing information security and preventing unauthorized access. These standards include policies and controls to reduce data protection risks. National laws also vary across countries, so organizations must adjust their data protection strategies to meet local regulations. Legal diversity makes it important to understand regional differences when handling personal data.

Ensuring privacy and security is critical condition for the free flow of personal data across borders. The EU-U.S. Data Privacy Framework [21] is a mechanism designed to facilitate the cross-border transfer of personal data between the EU and the U.S. while ensuring compliance with EU data protection standards. This framework replaces the previous Privacy Shield and provides a set of principles and commitments that U.S. organizations must adhere to, ensuring that personal data transferred from the EU to these organizations is adequately protected.

4. Literature review

The comprehensive and fast integration of AI technologies for developing nations causes significant challenges especially in the domain of privacy and personal data protection. Many author in the last period research different aspects of this area, at different countries, as follows. In 2019, Mazurek and Malagocka [22] discuss various approaches to artificial intelligence, highlighting how differing interpretations of privacy, rising consumer concerns, and data protection regulations—aligned with official administrative policies—shape these approaches. Their work examines how the adoption of AI affects the relationship between businesses and their customers, particularly when viewed through the lens of regulatory frameworks and individuals' perceptions of privacy. Almeida et al. [23] introduce the "AIR framework," a conceptual tool designed to help societies collectively consider and make informed policy choices about what aspects of AI should be regulated, as well as when and how such regulations should be implemented. The article outlines a comprehensive framework for AI regulation that spans all stages of public policy-making—from foundational steps to sustainable governance. Drawing on an extensive systematic review of literature on Artificial Intelligence Regulation (AIR) published between 2010 and 2020, the authors organize and clarify a previously fragmented body of knowledge focused on the "framework" concept. The resulting model integrates 21 existing representations of the policy-making process, with the goal of advancing key societal principles such as fairness, freedom, and long-term sustainability.

According to Malik et al. [24] developing nations face complex legal and institutional hurdles in regulating AI. The study emphasizes "the lack of comprehensive data governance frameworks, weak enforcement mechanisms, and technological dependence on foreign-developed systems." Its primary goal is to "critically assess the regulatory structures in these countries, identify shortcomings in existing data protection laws, and analyze the challenges posed by AI adoption in low-capacity environments." Based on an examination of Pakistan, Nigeria, Brazil, and Kenya, the research concludes that limited institutional capacity and a lack of clear regulatory norms often prevent effective AI governance, increasing the likelihood of surveillance, discrimination, and rights violations. Hasan [25] conducts a comparative analysis of the regulatory frameworks governing artificial intelligence in South Asian countries, contrasting them with those of selected nations and international organizations, while considering the unique challenges the region faces in AI regulation. The study highlights that South Asian nations exhibit a substantial and ongoing legal gap compared to other parts of the world—a disparity that is both unintentional and unequal. The paper advocates for the establishment of AI regulations and provides recommendations to help South Asian countries implement effective governance mechanisms despite constraints related to technological design and economic resources.

Mohebbi and Amiri [26] examine the legal and ethical issues associated with implementing AI in Iran's administrative justice system. Their research highlights challenges that demand broad and multidimensional solutions, such as creating legal and ethical frameworks, enhancing system transparency, and ensuring continuous human oversight. Sharma and Sharma [27] conduct a comparative analysis of privacy and data protection risks linked to the adoption of artificial intelligence (AI) applications across the BRICS nations—Brazil, Russia, India, China, and South Africa. Their study critically examines the data protection

legislations of these countries, assessing how effectively they address privacy concerns arising from AI technologies. By exploring each nation's legal frameworks and policy strategies, the research identifies both similarities and differences in managing AI-related privacy issues. A key aspect under investigation is the definition and scope of personal data. The findings emphasize the continuously evolving nature of privacy and data protection regulations within the rapidly advancing AI landscape. Alazam and Aldrou [28] argue that the fast-paced development of artificial intelligence (AI) technologies has made data privacy a central issue within international trade law. Their research explores the intricate relationship between AI innovation and data protection regulations in global commerce. It seeks to determine how international privacy legislation influences AI-related activities in trade and how technological progress in AI affects compliance with these laws and shapes public trust in international markets. The study particularly examines the links between AI research and development investments, trade-oriented regulatory frameworks, data privacy compliance standards, public perception, and the financial implications of adhering to such regulations.

At the other hand, there are comparative research conduct also in developed countries. The privacy is also field of research by on different angle. Ishii [29] undertakes a comparative legal study to analyse the challenges of privacy and personal data protection posed by AI embedded in Robots, and to offer policy suggestions. He analyse legal frameworks and relevant discussions in the EU, USA, Canada, and Japan, and further consider the efforts of Privacy by Design ("PbD") originating in Ontario, Canada. Ijaiya and Odumuwagun [30] perform a comparative analysis of the data privacy regulatory frameworks of the European Union (EU) and the United States (US) in the face of emerging cyber threats. Their research highlights the need for international collaboration to address AI-related privacy challenges and suggests practical measures to enhance regulatory effectiveness, resilience, and accountability.

5. The Macedonian case study

The state of AI in Southeast Europe, especially in Republic of North Macedonia [31] shows a moderate level of development with significant challenges, but also potential for progress. In Macedonia development of projects using AI dates back to 2012, whereby the first complete speech synthesizer in the Macedonian language TTS-MK, which has been used as an aid in the National Union of the Blind of the Republic of North Macedonia and for the needs of the State School for Rehabilitation of Children and Youth with Visual Impairment "Dimitar Vlahov" - Skopje, an interface for enabling a printer for Braille. Therefore, were introduced Mila - Artificial Intelligence Tutor for Smarter Learning, Fire Alarm System , [31] p.17] and the first Macedonian AI-based digital public administration assistant - "ADA" intended to provide information to citizens and interested potential foreign investors about investment opportunities is no longer in operation. Other AI projects were introduced in the:

- IT sector: Smart Monument, Cybersecurity Management Center, Automated Painting System - Michelangelo, AI-based Vehicle License Plate Recognition System for Automated Parking Management, Digital Transformation Platform, Speech Transcription.

- Healthcare sector: digital dentistry for analysis, planning and prediction of dental treatment outcomes in implantology and prosthetics, 3D visualization of peripheral nerves, personalized heart monitoring device as a life-saving cardiac monitor, live heart and glucose level monitoring and receiving medical care, diagnostics and treatments of eye convergence deficiency.
- Agricultural sector: drone for sowing, fertilization and protection, non-invasive and portable food analysis and quality control, disease forecasting model software and mobile application that represent an upgrade of an agro-meteorological station, multifunctional controller for precise irrigation and nutrition management of different types of crops.

Even the number of AI projects in Republic of North Macedonia is significant, the current situation is lacks AI-specific regulations (laws and by-laws) and lagging behind neighboring countries, as well as limited availability of open data, poor coordination with international bodies which track countries' progress in digital transformation and AI and low institutional readiness represent serious obstacles to the development of AI in the country. An adequate control mechanism and coordination of activities between the competent bodies in the country for the protection of personal data during the implementation of projects using artificial intelligence has not been established [31]. So, the personal data in physical environment is protected by a comprehensive legal system that includes several key acts for individual privacy and personal data security (the Constitution of RNM, Law on Personal Data Protection, Law on the ratification of the Protocol to amend the Convention for the Protection of Persons with regard to automatic processing of personal data, Law on the ratification of the Additional Protocol to the Convention for the Protection of Individuals with regard to the automatic processing of personal data, in relation to supervisory bodies and cross-border transfer, Law on the ratification of the Convention for the Protection of Persons with regard to automatic data processing and by-laws for the protection of personal data), but personal data protection in digital environment is not full regulated. Today, the situation has been significantly improved through adoption of the Law on Security of Network and Information Systems [32] and strategies [33] [34] [35] that integrate personal data security with broader network governance. The key Law on Security of Network and Information Systems represents the first comprehensive legal framework in Macedonia for regulating cybersecurity. This law is aligned with the European NIS2 Directive [36] and aims to establish a high and common level of protection of network and information systems, both in the public and private sectors. Notably, the primary AI challenge to data protection will be implementation of the recommendation of the State Audit Office about strengthening cooperation between Ministry of Digital Transformation and Personal Data Protection Agency in risk analysis during the development and implementation of each AI project through an assessment of the impact on the protection of personal data and coordination and involvement in the preparation and adoption of legal regulations from the perspective of personal data protection.

6. Conclusion

As physical–digital environments continue to evolve, it is essential to prioritize security, privacy, and confidentiality to create a secure and trustworthy virtual world for everyone. By taking a proactive approach to security and data protection, it suppose that it is possible to ensure physical–digital environments remain safe and inclusive spaces for all [37]. This

virtual world involves complying with data protection regulations, and being vigilant against emerging threats.

This article provides an overview of the legal issues and challenges related to AI in RNM. Although the legal framework for the data protection is in place and aligned with European legislation, continuous monitoring of personal data protection is required throughout the full implementation of projects using AI. In the absence of appropriate national legislation on AI aligned with the Law on Personal Data Protection, the protection of citizens' personal data cannot be guaranteed.

In the current globalized world, the government also has the responsibility to ensure strong compliance to AI data protection principles and international standards. So, on EU path Macedonia will have to align with EU AI regulations - Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law and transposition the EU AI Act into national legislation. Additionally, AI Strategy that fully focuses on the use of AI in the public sector of the Republic of North Macedonia need to be prepared and adopted. The path forward requires not only innovative legal reasoning but also a willingness to challenge and adapt traditional legal doctrines to meet the unique challenges posed by AI technologies. By applying the knowledge, tools, and data protection principles outlined in this paper, will help to shape the future of ethical, secure and trustworthy AI.

References

[1] A. Vlachos, "Artificial Intelligence Challenges to Data Protection," 2024.

[2] Belgian Data Protection Authority, General Secretariat, "Artificial Intelligence Systems and GDPR from a," 2024.

[3] E. Glerean , "Fundamentals of Secure AI Systems with Personal Data," p. 9, 2025.

[4] C. Meurisch and M. Muhlhauser, "Data Protection in AI Services: A Survey," *ACM Computing Surveys,* vol. 54, no. 2, pp. 1-38, 2021.

[5] "Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) ‘Artificial Intelligence-Proof’?," *SSRN Electronic Journal,* 2018.

[6] R. Almarzoqi and M. Albakjaji, "The Patentability of AI Invention: The Case of the Kingdom of Saudi Arabia Law," *International Journal of Service,* vol. 13, no. 1, pp. 1-22, 2022.

[7] W. Malik, S. Gul and G. M. Qureshi, "Regulating Artificial Intelligence: Challenges for Data Protection and Privacy in Developing Nations," *Journal of Social Signs Review ,* vol. 3, no. 5, 2025.

[8] E. Chikhaoui, A. Alajmi and S. Larabi-Marie-Sante, "Artificial Intelligence Applications in Healthcare Sector: Ethical and Legal Challenges," *Emerging Science Journal,* vol. 6, no. 4, pp. 717-738, 2022.

[9] C. Stryker and E. Kavlakoglu, "What is artificial intelligence (AI)?," *IBM ,* 2024.

[10] M. Almanda , "Law & Compliance in AI Security," *Support Pool Of Experts Programme, Training curriculum on AI and data protection,* 2024.

[11] United Nations, "Universal Declaration of Human Rights," 1948.

[12] Council of Europe, "European Convention on human rights," 1950.

[13] EUR-Lex, "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data," 1995.

[14] European Data Protection Supervisor, "Data Protection," *Data Protection.*

[15] Council of Europe, "Artificial Intelligence and Data Protection," 2019.

[16] "Cybersecurity strategy 2025–2028.".

[17] "Rulebook On Personal Data Processing Security 266/24".

[18] Metamorphosis , "Research on the Impact of New Technologies, With a Particular Focus on Artificial Intelligence, on Human Rights Online, and the Development of Ethical Standards for Protecting Human Rights on the Internet in the Context of Automated Decision-Making," 2024.

[19] H. Tibebu, "Framework for Data Protection, Security, and Privacy in AI," 2024.

[20] D. Kotov, "Data Security and Privacy in the Age of Artificial Intelligence.," *Universum Technical Science Journal*, vol. 6, no. 123, 2024.

[21] EUR-Lex, "Commission Implementing Decision EU 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework (notified under do," 2023.

[22] G. Mazurek and K. Małagocka, "Perception of privacy and data protection in the context of the development of artificial intelligence," *Journal Of Management Analytics*, vol. 6, no. 4, pp. 344-364, 2019.

[23] P. G. Rgo de Almeida, C. Denner dos Santos Jr and J. S. Farias, "Artificial Intelligence Regulation: a framework for governance," *Ethics and Information Technology*, vol. 23, no. 3, pp. 505-525, 2021.

[24] W. Malik, S. Gul and G. Qureshi, "Regulating Artificial Intelligence: Challenges for Data Protection and Privacy in Developing Nations," *Journal of Social Signs Review*, vol. 3, no. 5, 2025.

[25] M. Hasan, "Regulating Artificial Intelligence: A Study in the Comparison between South Asia and Other Countries," *Legal Issues in the Digital Age*, vol. 5, no. 1, pp. 122-149, 2024.

[26] D. Mohebbi and A. Amiri, "Legal and Ethical Challenges Related to the Use of Artificial Intelligence in the Administrative Justice System," *Legal Studies in Digital Age*, vol. 4, no. 1, 2025.

[27] A. Sharma and R. Sharma, "Comparative Analysis of Data Protection Laws and ai Privacy Risks in brics Nations: A Comprehensive Examination.," *Global Journal of Comparative Law*, vol. 13, no. 1, pp. 56-85, 2024.

[28] F. A. F. Alazzam and K. Abed, "Artificial intelligence and data privacy in international trade law," *Multidisciplinary Science Journal*, vol. 7, no. 8, 2025.

[29] K. Ishii, "Comparative legal study on privacy and personal data protection for robots equipped with artificial intelligence: looking at functional and technological aspects," *AI&SOCIETY*, vol. 34, pp. 509-533, 2019.

[30] H. Ijaiya and O. O. Odumuwagun, "Advancing Artificial Intelligence and Safeguarding Data Privacy: A Comparative Study of EU and US Regulatory Frameworks Amid Emerging Cyber Threats.," *International Journal of Research PublicationandReviews*, vol. 5, no. 12, pp. 3357-3375, 2024.

[31] State Audit Office, "Final Report of IT Audit as a performance audit opportunity for the use of Artificial Intelligence in the public sector.," 2025.

[32] Pepeljugoski, "New Law on Electronic Communications adopted," *Law Office & Intellectual Property Bureau* , 2025 .

[33] Ministry of Digital Transformation, "Cybersecurity Strategy 2025–2028 of the Republic of North Macedonia," 2024.

[34] Westren Balkans Info Hub , "Smart Specialisation Strategy of the Republic of North Macedonia S3-MK 2024-2027," 2023.

[35] "Strategy for the implementation of the Right to Personal Data Protection for the Republic of North Macedonia 2025-2030," 2025.

[36] EUR-Lex, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive".

[37] C. Pereira and e. al, "Security and Privacy in Physical–Digital Environments: Trends and Opportunities," *Future Internet*, vol. 17, no. 2, 2025.