(IJIASE) 2023, Vol. No. 9, Jan-Dec **e-ISSN: 2454-9258, p-ISSN: 2454-809X**

A Comprehensive Analysis of the Prospects and Scope of Qualitative Legal Assistance to Maintain the Cybersecurity Safeguard to Effectively Link AI Technology Tools and Techniques

Suchit Lamba
NIIT University, Neemrana, Rajasthan, India

[1]*Received: 10 January 2023; Accepted: 24 July 2023; Published: 12 August 2023*

ABSTRACT

In the contemporary era, ensuring cybersecurity has emerged as a paramount obligation for modern states, integrated within their security framework. Recently enacted normative legal measures grounded in technical regulations and standards address this imperative. These regulations encompass laws and strategic directives concerning cybersecurity, cyber threats, and the mitigation of information warfare. The essential need to enact comprehensive legal provisions governing cybersecurity, including using artificial intelligence methodologies, is underscored by the escalating array of challenges and threats within the information domain. This paper delves into the legal underpinnings of cybersecurity in Russia within artificial intelligence technology applications.

INTRODUCTION

The rapid expansion of modern digital technologies necessitates the establishment of novel legal frameworks. Presently, legal systems must engage with other regulatory entities. Using emerging digital technologies for self-development across various levels is a primary objective for legal regulators. Artificial intelligence (AI) represents one such technology. Economically advanced nations recognize the development of AI as a crucial strategy for enhancing national competitiveness globally and ensuring national security. AI methods have widespread applications in diverse fields, such as education, personalized medicine, and environmental protection. These methods possess the capability to anticipate and issue warnings. Consequently, using AI methods emerges as a pivotal factor in the evolution of any nation's digital economy. However, potential threats stemming from the application of AI methods necessitate the establishment of legal safeguards to ensure the secure functioning of AI systems.

ARTIFICIAL INTELLIGENCE DEFINITION

Artificial intelligence (AI) encompasses a technology that brings forth several challenges, including shifts in employment structures, alterations in legal and ethical regulations, and concerns regarding the privacy of individuals' lives. The development of AI promises to revolutionize education, science, and society as a whole. AI technologies are advancing rapidly, necessitating a thorough examination of potential cybersecurity risks and threats. Controlled development of AI emerges as imperative.

The widespread adoption of AI technologies has prompted the creation of numerous legal documents essential for implementing regulatory frameworks governing relationships arising from AI utilization.

In the Russian Federation, the concept of artificial intelligence must be officially defined. AI is closely associated with the primary cross-cutting digital technology utilized in various public domains. According to the Information Society Development Strategy, AI is the primary direction in developing Russian information and communication technologies. The strategic priorities for scientific and technological development in the next decade to fifteen years underscore the emphasis on creating intelligent transport and telecommunication systems. The Transport

[1] *How to cite the article:* Lamba S. (2023); A Comprehensive Analysis of the Prospects and Scope of Qualitative Legal Assistance to Maintain the Cybersecurity Safeguard to Effectively Link AI Technology Tools and Techniques; *International Journal of Innovations in Applied Sciences and Engineering*; Vol 8, 14-18

(IJIASE) 2023, Vol. No. 9, Jan-Dec **e-ISSN: 2454-9258, p-ISSN: 2454-809X**

Strategy of the Russian Federation outlines plans to introduce next-generation on-board security systems incorporating computer technologies with AI elements.

The term "artificial intelligence" pertains to computer science, which focuses on creating technical systems capable of collecting data and making decisions or solving problems. It represents a developing field aimed at constructing "thinking machines," which are general-purpose systems possessing intelligence comparable to human intelligence, also known as vital artificial intelligence. Bernard Marr notes that the definitions of AI are evolving based on the goals sought through AI systems. Typically, investment in AI development aligns with one of three objectives: creating systems that emulate human thinking precisely (strong AI), developing systems that function without understanding human thought processes (weak AI) or utilizing human thinking as a model without necessarily aiming for identical replication.

Hence, artificial intelligence comprises a blend of technologies, including information and digital technologies, to solve cognitive problems primarily associated with human intelligence. Defining "artificial intelligence" from a legal perspective proves challenging and is traditionally considered through related categories such as robots, robotic agents, robotic systems, and cyber-physical systems integrated with AI.

REGULATION OF ARTIFICIAL INTELLIGENCE

Efforts to regulate the utilization of artificial intelligence (AI) and robotics involve various initiatives aimed at identifying potential societal and legal challenges. With the rapid advancement of cyber-physical systems, it is imperative to consolidate fundamental regulations governing AI usage, outlining potential solutions for current and anticipated issues. Currently, all categories of robots, regardless of their purpose, danger level, mobility, or autonomy, are encompassed within the scope of robotics objects. This classification extends to cyber-physical systems integrated with AI. Thus, robots encompass both robotic mechanisms and cyber-physical systems equipped with AI [8].

A robot is defined as a programmable drive mechanism capable of movement along two or more axes, possessing a certain degree of autonomy to perform tasks within its operational environment. This definition is outlined in the national standard of the Russian Federation titled "Robots and Robotic Devices: Terms and Definitions" [9].

The terminological standard titled "Artificial Intelligence: Concepts and Terminology" serves as the cornerstone for all international regulatory frameworks concerning AI. Consequently, a decision was made to develop a Russian standard alongside the primary English version. This document comprises:

1. Artificial intelligence basic principles

2. AI terminology.

3. AI definitions.

4. AI approaches.

5. Principles for constructing systems incorporating AI elements.

6. Regulations for AI encompass both normative and technical aspects [9].

Building upon the Russian Venture Company (RBC), a Technical Committee (TC) for AI standardization was established to address legal and technical regulations governing AI technology applications. Furthermore, a draft of the National Strategy for AI Development in Russia has been formulated.

Presently, the principle of mandatory human oversight over AI algorithm outputs is enshrined. Issues pertaining to AI and robotics utilization across various sectors of public life necessitate mandatory regulation to ensure the security of individuals, society, and the state against potential AI-related threats. The Russian legislation increasingly reflects foreseeable risks and threats arising from AI technology usage [10].

The main challenges encountered in the adoption of AI technologies revolve around legislative inadequacies and a shortage of qualified professionals with interdisciplinary expertise, encompassing fields such as information law and network security. Consequently, specialized education combining IT and legal disciplines is essential for such professionals.

Self-regulation emerges as a crucial mechanism for governing relationships within the AI domain. It entails leveraging self-regulatory mechanisms to foster development in sectors heavily reliant on digital technologies.

(IJIASE) 2023, Vol. No. 9, Jan-Dec **e-ISSN: 2454-9258, p-ISSN: 2454-809X**

Digitalization efforts in education exemplify this, incorporating various information systems leveraging big data, blockchain technology, and AI. Notably, the student's digital portfolio serves as a comprehensive record of their academic achievements, facilitating university admissions and providing employers with a holistic overview of applicants, thereby enhancing the selection process.

REGULATING SYSTEMS FOR CYBERSECURITY WITH AI APPLICATIONS

In today's digital landscape, virtually every individual worldwide interacts with the Internet on a daily basis, engaging in online transactions, managing bank transfers, and accessing personal data across various services. These aspects of the digital realm hold immense significance for society. However, the deficiencies in information system security present significant risks. For example, banks are vulnerable to substantial losses in the event of system downtime, while individuals face the threat of financial loss or exposure to data breaches.

By the end of 2018, Kaspersky Lab reported a 13% decrease in the overall number of Distributed Denial of Service (DDoS) attacks compared to 2017 statistics. Nevertheless, experts noted an increase in the duration of mixed attacks and HTTP floods, suggesting a shift towards more sophisticated methodologies by attackers.

Recent data indicates a pressing need for clearer positive trends in the cybersecurity landscape. According to Kaspersky DDoS Protection, there was a decrease in activity during the second quarter of 2019 compared to the previous quarter. The number of attacks thwarted by Kaspersky Lab security systems decreased by 44 percentage points (pp), attributed to the customary decrease in cybercriminal activity during the summer period. Furthermore, compared to the second quarter of the previous year, the total number of attacks increased by 18 pp, indicating a resurgence in the DDoS market. This upward trend has persisted since the beginning of 2019.

Notably, the seasonal decline in activity had minimal impact on the organization and thwarting of technically advanced attacks: their frequency decreased by only four percentage points compared to the previous quarter. However, the difference compared to the same period last year is significant, indicating an upward trend—intelligent attacks increased by 32 percentage points in Q2 2019. The proportion of such attacks, among all others, continues to rise steadily, showing an increase compared to both the previous quarter (by 9 points) and Q2 2018 (by 15 points). Moreover, the duration of DDoS sessions continues to increase steadily in both absolute and relative terms, with the most extended reflected attacks lasting up to 75 minutes, a substantial duration considering that most attacks are filtered in their early stages. Much of this growth can be attributed to the prolonged duration of technically complex attacks, as both their average and maximum durations have increased compared to the last quarter and overall compared to the previous year [12].

Given this less-than-optimistic trend, new approaches to combating network attacks could significantly enhance information system security. One strategy involves leveraging machine learning algorithms, such as neural networks, which significantly improve attack detection. Neural networks exhibit adaptability, the capability to analyze incomplete or distorted data, and high-speed data processing, contributing to enhanced detection capabilities [13].

Intrusion detection systems utilizing neural network technology address existing challenges within such systems. The key advantages of employing neural network approaches include flexibility, the ability to detect unknown or lesser-known attack types, and the identification of low-intensity attacks distributed over time, all while maintaining high-speed data analysis. However, these systems also present several drawbacks, including the need for extensive neural network training, the opacity of processes within complex neural networks, and the direct dependence of analysis quality on training data [14-15].

Although machine learning algorithms have existed for many years, their regulatory framework lacks semantic value. However, their application in specific tasks and systems warrants regulation. For instance, cybersecurity systems leveraging machine learning algorithms are currently in use. Numerous articles have been published outlining the application of artificial intelligence methods in cybersecurity [16].

For instance, recent advancements in machine learning techniques have provided cybercriminals with new tools for cybercrime, leading to large-scale and complex attacks. The primary defence against these attacks lies in network intrusion detection systems, which learn patterns of network activity to detect potential or actual threats. One such framework, SynGAN, generates attacks using a generative network to enhance attack detection capabilities. While these frameworks are promising, ethical considerations and regulations surrounding their publication and use remain paramount.

Currently, there exists a series of documents that govern the inclusion of scientific materials (articles, monographs, etc.) in dual-use technologies. For instance, the Decree of the President of the Russian Federation outlines a list

of dual-use goods and technologies subject to export control. Technologies related to artificial intelligence systems fall under this purview. However, the legality of research in this area is currently ambiguous, as the development of artificial intelligence algorithms for generating malicious traffic has dual purposes—posing challenges to scientific development and cybersecurity. Therefore, the establishment of ethical standards for scientific research and publications, as well as regulations governing the use of artificial intelligence algorithms in software, is imperative to address these concerns.

CONCLUSION

National regulations are examined, revealing a relatively narrow scope of relationships subject to legal oversight, predominantly within the transport sector, education, medicine, public safety, industry, and public administration. However, there is a discernible trend towards expanding and encompassing new domains wherein the utilization of artificial intelligence is governed. The active deployment of organizational norms, ethical standards, self-regulation, and co-regulation, along with the development of supranational norms, indicates concerted efforts to address the complex challenge of regulating relationships using cyber-physical systems and artificial intelligence.

REFERENCES

1. Minbaleev A.V., “Problems of regulation of artificial intelligence”, Bulletin of the South Ural State University. 82 Ser. Law. 2018, vol. 18, no. 4, pp. 82–87. (in Russian).
2. Passport of the national program “Digital Economy of the Russian Federation” (approved by the Presidium of the Presidential Council for Strategic Development and National Projects, Minutes No. 16 dated 12.24.2018) Available at: http://www.pravo.gov.ru (accessed 10 June 2020). (in Russian).
3. Strategy for the development of the information society in the Russian Federation for 2017 - 2030, approved. By presidential decree of May 9, 2017 No. 203 “On the Strategy for the Development of the Information Society in the Russian Federation for 2017 - 2030” Available at: http://www.pravo.gov.ru, 10.05.2017. (accessed 10 June 2020). (in Russian).
4. Decree of the President of the Russian Federation dated 01.12.2016 No. 642 “On the Strategy for the Scientific and Technological Development of the Russian Federation”. Meeting of the legislation of the Russian Federation. 2016. No. 49. Page 6887. (in Russian).
5. Order of the Government of the Russian Federation of November 22, 2008 No. 1734-r (as amended on May 12, 2018) “On the Transport Strategy of the Russian Federation”. (in Russian).
6. Artificial Intelligence. Available at: https://www.merriamwebster.com/dictionary/artificial%20intelligence (accessed 10 June 2020). (in Russian).
7. Marr B. The Key Definitions Of Artificial Intelligence (AI) That Explain Its Importance Available at: https://www.forbes.com/sites/bernardmarr/2018/02/14/the-keydefinitions- of-artificialintelligence-ai-that-explain-itsimportance/# 4da358124f5d (accessed 10 June 2020).
8. “Draft Model Convention on Robotics and Artificial Intelligence. Rules for creating and using robots and artificial intelligence”, Available at: http://robopravo.ru/modielnaia_konvientsiia (accessed 10 June 2020). (in Russian).
9. ISO 8373: 2012. “Robots and robotic devices. Terms and definitions ”// https://www.iso.org/standard/55890.html (last accessed date: 05/30/2019); GOST R ISO 8373-2014 “Robots and robotic devices. Terms and Definitions”. Available at: http://docs.cntd.ru/document/1200118297 (accessed 10 June 2020). (in Russian).
10. “2019: ISO / IEC experts supported the proposal to develop a standard in Russian”, Available at: http://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:%D0%98%D1%81%D0%BA%D1%83%D1%81%D1%81%D1%82%D0%B2%D0%B5%D0%BD%D0%BD%D1%8B%D0%B9_%D0%B8%D0%BD%D1%82%D0%B5%D0%BB%D0%BB%D0%B5%D0%BA%D1%82_(%D0%98%D0%98,_Artificial_intelligence,_AI) (accessed 10 June 2020). (in Russian).
11. Decree of the Government of the Russian Federation of August 25, 2017 No. 996 (as amended on May 6, 2019) “On the approval of the Federal Scientific and Technical Program for the Development of Agriculture for 2017 - 2025”. Available at: http://www.pravo.gov.ru, 30.08.2017. (accessed 10 June 2020). (in Russian).
12. DDoS-2019: observations and trends. Available at: http://cybersafety. ru/2019/02/ddos-2019-nablyudeniya-i-tendentsii/ (accessed 10 June 2020). (in Russian).
13. “DDoS attacks in the second quarter of 2019”, Available at: https://securelist.ru/ddos-report-q2-2019/94452/ (accessed 10 June 2020). (in Russian).

14. Nazarenko E., Varkentin V., Polyakova T., “Features of Application of Machine Learning Methods for Classification of Network Traffic (Features, Advantages, Disadvantages)”, IEEE International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon) Vladivostok, Russia, 1-4 Oct. 2019.
15. Boyko A., Varkentin V., Polyakova T., “Advantages and Disadvantages of the Data Collection's Method Using SNMP”, IEEE International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon) Vladivostok, Russia, 1-4 Oct. 2019.
16. Jeremy Charlier, Aman Singh, Gaston Ormazabal, Radu State, and Henning Schulzrinne, “SynGAN: Towards Generating Synthetic Network Attacks using GANs”, Available at: https://arxiv.org/pdf/1908.09899.pdf (accessed 10 June 2020).
17. “Degang Sun, Kun Yang, Zhixin Shi, Chao Chen. A New Mimicking Attack by LSGAN”, Available at: https://ieeexplore.ieee.org/document/8371977 (accessed 10 June 2020).