YANGI O‘ZBEKISTON, YANGI TADQIQOTLAR JURNALI
Volume 5 Issue 1 June 2026
https://phoenixpublication.net/ Online ISSN: 3030-3494

LEGAL RISKS OF USING NEURAL NETWORKS IN BUSINESS

Javohirbek Umarov
Master of Law, Independent Researcher

Abstract:
This article examines the key legal risks arising from the use of neural network technologies in business activities. The study analyzes issues related to personal data protection, intellectual property, liability for artificial intelligence decisions, compliance with digital legislation, and cybersecurity. Special attention is given to the legal aspects of generative artificial intelligence, automated data processing, and the commercial use of neural network systems. The research shows that the rapid implementation of AI technologies outpaces the development of legal regulation, creating significant legal uncertainty for businesses. The paper proposes recommendations for minimizing legal risks and establishing a legal compliance system for the use of neural networks in commercial activities.

Keywords: *artificial intelligence, neural networks, digital law, legal risks, personal data, intellectual property, AI compliance, cybersecurity, digital economy, business automation.*

Introduction

The modern digital economy is characterized by the active implementation of artificial intelligence technologies and neural network systems across all areas of business activity.

Neural networks are used in banking, e-commerce, healthcare, marketing, logistics, education, manufacturing, and human resource management.

Generative AI models enable the automation of data processing, creation of textual and visual content, analysis of large datasets, and support for managerial decision-making.

The growing popularity of neural networks is driven by their high efficiency, ability to reduce business costs, and acceleration of decision-making processes. Companies actively integrate AI technologies into business processes to enhance competitiveness and optimize operations.

However, alongside technological advantages, significant legal risks arise in connection with the use of artificial intelligence.

One of the key issues is the lack of unified international regulation of AI systems. The legislation of most countries does not keep pace with the rapid development of technology, creating legal uncertainty regarding liability, data protection, and intellectual property regulation. This issue is particularly complex in the field of generative AI, where outputs may infringe copyright, spread misinformation, or use personal data without consent.

Another important issue is liability for decisions made by neural network algorithms. In the event of an AI error, the question arises as to who bears legal responsibility: the software developer, the business owner, the system operator, or the user. This issue is especially critical in healthcare, finance, and transportation, where errors may result in serious damage or harm to human life and health.

The issue of personal data protection is also highly significant. Training neural network models requires vast amounts of data, including biometric information, user queries, and digital footprints. Failure to comply with data protection laws may result in substantial fines, lawsuits, and reputational damage.

The relevance of this study is обусловлена (NOTE: исправлено) → **determined by** the need for a comprehensive analysis of legal risks associated with neural networks in the context of digital transformation.

The purpose of this study is to identify the main legal risks of using neural network technologies in business, analyze existing legal challenges, and develop recommendations for minimizing legal threats when implementing AI in entrepreneurial activity.

Main Part

Neural networks are a type of artificial intelligence technology based on modeling the functioning of the human nervous system. Modern AI systems are capable of learning from large datasets, identifying patterns, generating content, and performing analytical tasks.

In business, neural networks are used for:

- document workflow automation;
- processing customer requests;
- forecasting market trends;
- generating texts, images, and software code;
- analyzing consumer behavior;
- financial modeling;
- logistics and personnel management.

Despite their high efficiency, AI technologies involve a number of legal risks that may affect business stability.

One of the most significant risks is the violation of personal data protection laws. Neural networks require large volumes of data, including:

- user names;
- contact details;
- biometric information;
- search histories;
- behavioral data.

In many cases, users are unaware that their data is being used for machine learning, which creates a risk of violating data privacy regulations.

Strict requirements are established under:

- GDPR in the European Union;
- CCPA in the United States;
- national data protection laws.

Violations may lead to:

- substantial administrative fines;
- lawsuits;
- blocking of digital services;
- reputational damage.

To minimize risks, businesses must implement AI compliance systems, ensure transparency in data processing, and obtain user consent.

A highly debated issue is the legal status of AI-generated content. Generative AI systems can produce:

- texts;
- images;
- musical works;
- software code;
- designs and visual objects.

This raises the question: who owns the rights to such outputs? Most legal systems do not yet provide a clear answer.

Key legal issues include:

- use of copyrighted materials in AI training;
- generation of content similar to existing works;
- lack of legal status of AI as a subject of law;
- difficulty in determining authorship.

A particularly serious issue is the training of models on copyrighted works without permission. Lawsuits against AI companies are currently being considered in multiple jurisdictions.

Businesses should therefore:

- verify AI tool licenses;
- analyze the origin of training data;
- monitor content originality;
- conduct legal audits of AI usage.

Neural networks are increasingly used for automated decision-making. However, algorithmic errors can cause significant harm.

High-risk sectors include:

- banking;
- healthcare;
- transportation;
- security systems;
- human resource management.

AI systems may:

- wrongly deny credit;
- introduce bias in hiring;
- produce incorrect medical diagnoses;
- generate inaccurate recommendations.

A major issue is that many AI systems function as a “black box,” meaning their decision-making processes are not transparent even to developers.

Legal questions include:

- who is liable for AI errors;
- how to establish causation;
- whether AI risks can be insured;
- whether human oversight is required.

Most jurisdictions currently assign responsibility to the system owner or operator.

The use of neural networks also increases cybersecurity risks. AI systems process large volumes of corporate data, making them attractive targets for cyberattacks.

Main threats include:

- hacking of AI platforms;
- data breaches;
- algorithm manipulation;
- injection of malicious data;
- deepfake technologies.

Deepfake systems pose a particularly serious threat, as they can create fake images, videos, and audio recordings, leading to fraud, misinformation, and reputational harm.

To protect businesses, it is necessary to:

- implement cybersecurity systems;
- regularly audit AI infrastructure;
- restrict data access;
- use encryption and multi-factor authentication.

Neural networks may also reproduce biases present in training data, leading to:

- gender discrimination;
- racial bias;
- social inequality;
- algorithmic unfairness.

For example, recruitment systems may disadvantage certain groups, potentially leading to legal claims and violations of anti-discrimination laws.

Businesses must therefore:

- audit algorithms;
- control training data quality;
- implement AI ethics principles;
- ensure transparency.

The analysis shows that while neural network technologies significantly improve efficiency, they also increase legal risks. The most problematic areas are data protection, intellectual property, and liability for automated decisions.

Many companies implement AI systems without prior legal risk assessment, resulting in regulatory violations, litigation, and financial losses.

Additionally, the lack of unified international AI regulation creates legal uncertainty for multinational businesses, requiring adaptation to different legal systems.

Conclusion

The use of neural network technologies is becoming an integral part of the digital economy. Artificial intelligence offers businesses significant opportunities for automation, efficiency, and cost reduction. However, legal risks increase alongside these benefits.

The study shows that the main risks include violations of data protection laws, intellectual property issues, algorithmic opacity, cybersecurity threats, and unclear liability frameworks.

To minimize risks, companies should:

- implement AI compliance systems;
- conduct legal audits of AI services;
- ensure transparency in data processing;
- control intellectual property usage;
- strengthen cybersecurity;
- adopt ethical AI principles.

In the context of rapid technological development, establishing effective legal regulation of AI is one of the key challenges of modern law. Businesses must not only innovate but also ensure legal security.

References

1. Turner, J. *Robot Rules: Regulating Artificial Intelligence.* Palgrave Macmillan, 2020.
2. Dubber, M., Pasquale, F., & Das, S. *The Oxford Handbook of Ethics of AI.* Oxford University Press, 2020.
3. Kosseff, J. *Cybersecurity Law.* 2nd ed. Wiley, 2022.
4. Witzleb, N., Paterson, M., & Richardson, M. *Big Data, Political Campaigning and the Law.* Routledge, 2021.
5. Murray, A. *Information Technology Law: The Law and Society.* Oxford University Press, 2022.