Legal Issues in the Digital Age. 2025. Vol. 6. No. 1.
Вопросы права в цифровую эпоху. 2025. Том 6. № 1.

Research article
JEL: K24
UDC: 340
DOI:10.17323/2713-2749.2025.1.28.52

Model Regulation of Artificial Intelligence and other Advanced Technologies

Ludmila K. Tereschenko

Institute of Legislation and Comparative Law under the Russian Federation Government, 34 Bolshaya Cheremushkinskaya Str., Moscow, Russia 117218, adm2@izak.ru, https://orcid.org/0000-0002-2170-5339

Alexander V. Tokolov

Financial University under the Russian Federation Government, 49/2 Leningradsky Prospekt, Moscow, Russia 125167,
Altok40@mail.ru, Istina Researcher ID (IRID): 229255925 РИНЦ (SPIN): 5479-0469

Abstract

The article provides a discussion of legal regulation of social relations by the Interparliamentary Assembly of the CIS Member States with regard to AI and other advanced information technologies, identifiable regulatory gaps, conceptual framework, analysis of possible use scenarios and related risks, as well as the range of problems to be addressed by regulation on a priority basis. It contains a brief overview of how AI-related social relations are regulated in the CIS member states. While all these countries admit the importance of such regulation, none has developed a clear understanding of a number of issues, only to stress the relevance of developing a draft model law on AI technologies. The authors demonstrate the following common problems of regulating these relations in the CIS member states: identifying the regulatory scope and the parties concerned and, importantly, addressing the issues of liability including what party (AI technology rights holder, developer, system operator etc.) and in what case will assume a particular type of liability (administrative, civil, financial, criminal). Another important aspect is also discussed — digitization and advanced digital technologies shaping "new" digital personal rights — with an analysis and brief overview being provided. The study purports to identify the trend and opportunities for public regulation of AI and other advanced digital applications. With this in mind, the authors discuss possible regulatory vectors in the given area

in light of the risks related to operational specifics of digital technologies, and identify groups of social relations to be adequately addressed by legal regulation. With digitization covering an ever wider range of social relations, the problems to be addressed by law include the protection of personal rights as well as prevention of non-discrimination of individuals and economic agents. The article employs a number of scientific methods of inquiry, general and special research methods including the formal law method. The general research methods include systemic, dialectic, structural systemic, analytical/synthetic, inductive and deductive methods, abstraction, simulation. The article concludes that, while the CIS countries are at different regulatory stages in the discussed area, there is no comprehensive regulation, with only individual provisions and regulations in place to govern specific aspects of AI use. A model law, once developed, will allow to lay the ground for comprehensive regulation of the discussed relations by the national legislation.

Keywords

artificial intelligence; human rights; discrimination; digital technologies; digital transformation; supranational regulation; legal person; legal personality; liability; model regulation.

For citation: Tereschenko L.K., Tokolov A.V. (2025) Model Regulation of Artificial Intelligence and other Advanced Technologies. *Legal Issues in the Digital Age,* vol. 6, no. 1, pp. 28–52. DOI:10.17323/ 2713-2749.2025.1.28.52

Background

The Interparliamentary Assembly of the Commonwealth of Independent States (IPA CIS) was established in the late 1991 after the collapse of the Soviet Union as a regional organization of former Soviet republics having as one of its principal tasks the development of (non-binding) model regulations to put in place similar (comparable) regulatory approaches to priority areas that currently include the relations associated with digitization of the economy, government and other domains of mutual interest.

The issue of legal regulation of AI uses is high on the agenda as digital technologies are increasingly applied to many aspects of modern life in a majority of countries including the CIS. While the legal framework is applicable to digital technologies to a varying extent, there is still no shared approach as to the need, feasibility, scope and extent of regulation. More researchers note the forthcoming or already ongoing transformation of law brought about by digital technologies. The prevailing opinion is that “the progress of digital information technologies in the

21st century has already revolutionized law (with the emergence of new things at law, forms of law, methods to exercise a right etc.)" [Amelin R.V., Channov S.E., 2023: 280]; [Khabrieva T.Ya., Chernogor N.N., 2018: 88]; [Khisamova Z.I., Begishev I.R., 2020: 100–103].

Moreover, it is also noted that "the digitization processes are taking place in a specific legal environment that can be described as slackening of the government's regulatory role manifested in the first place by an absolute regulatory slippage, with the legislator struggling to adapt to the rate of scientific and technological progress" [Khabrieva T.Ya., 2009: 14–24]; [Sharnina L.A., 2023: 22–27]. However, this does not mean that nothing is being done for legal support of digitization. On the contrary, many countries are actively involved in this work, with a special focus on AI-related issues. According to the Stanford University's 2023 AI Index Report, the number of regulations governing AI grew 37 times in the period from 2016 to 2022.[1]

As is rightly stated in the doctrine, "using AI becomes a major factor of digital economic development of any country" [Global AI Regulation Atlas. Ed. by V. Neznamov, 2023: 3]. While it is no longer debatable whether the emerging relations need to be regulated — of course they do — many countries including the CIS are taking steps in this direction.

Along with the drafting work done by the CIS countries, it is useful to study the experience of the European Union which has passed the wide-ranging Artificial Intelligence Act.[2] Thus, the EU AI Act has harmonized the rules for marketing, commissioning and using AI systems across the European Union; prohibited specific AI practices; put in place special requirements to high-risk AI systems and imposed obligations on their operators; as well as harmonized transparency rules for a number of AI systems; marketing rules for general purpose AI systems; market surveillance rules etc. Since not much time has elapsed since EU AI Act was made effective, it is hard to judge whether its provisions are adequate, but their underlying approaches will be undoubtedly useful to inform the drafting of the AI Model Law. From this perspective, it is important to compare the approaches to address the most crucial issues which should include, in our view, the scope of AI legislation,

[1] 2023 AI Index Report — Artificial Intelligence Index. Available at: URL: https://aiindex.stanford.edu/report/ (accessed: 19.02.2024)

[2] Artificial Intelligence Act passed by the European Parliament on 13 March 2024 and approved by the EU Council on 21 May 2024, with the first part came into force on 2 February 2025 // Cyberleleninka

conceptual framework, possibility of and the proportion of public and self-regulation, necessary conditions, limits and constraints of AI usage, as well as liability as one of the core issues.

1. Regulatory approaches

So far AI has been primarily regulated at the level of supranational organizations although different nuanced approaches (risk-oriented approach, targeted regulation, non-binding approach etc.) are actively applied at the regional and national levels.

Based on analysis of international experience, A.V. Neznamov notes that "the importance of building a balanced regulatory system for this industry is discussed in almost every national AI strategy. Regulation should protect personal rights and liberties through safe implementation of innovations while providing for unobstructed technological development" [Global AI Regulation Atlas. Ed. by V. Neznamov, 2023: 3].

It is obvious from the specific nature of the emerging relations that AI systems should be subject to comprehensive regulation to include both public and private law provisions. This is true because AI can be (and is already) used across a vast majority of areas of economy, government and social life.

A.V. Minbaleev rightly notes a need for "a combination of various mechanisms for social regulation of AI uses (legal, ethical, technical, local and other regulatory, self-regulatory and co-regulatory mechanisms including their synthesis)" [Minbaleev A.V., 2023: 82–87].

The nature and diversity of the emerging relations require to tackle the question of not only regulatory approaches but also the extent of public regulation of artificial intelligence. The answer to this question will have a significant impact on AI development since tough restrictive policies will hold it back while inadequate regulation will jeopardize human rights and liberties. The best option is a combination of regulation and self-regulation which will both protect individual rights and support business initiatives.

So far one of the most controversial issues across many jurisdictions has been whether AI could be regarded as a legal person [Khisamova Z.I., Begishev I.R., 2020: 100–103]. It should be noted that theoretical solution to the problem of AI's legal personality is key to providing adequate legal regulation.

It is noteworthy that the idea of independent legal standing of AI has penetrated the studies of Russian researchers due to the impact of a number of international research projects including the concepts related to "non-personalized" legal entities and the creation of artificial legal persons [Klochkova E.N., Pimenova O.V., 2024: 43–52]; [Golovanov N.M., 2022: 24–25].

The question whether AI is a legal person is often a matter of discussion and has no clear answer. Unfortunately, the line of argument in support of this idea is not always there. In fact, where only two options are proposed — acknowledging AI as a person at law equal either to man or another legal entity — no justification of the choice between these alternatives is given [Ivliev G.P., Egorova M.A., 2022: 32–46].

It is also worth listening to the opinion of those who argue that acknowledging AI as a legal person is primarily hindered by the fact that AI is devoid of a will [Golovanov N.M., 2022: 24–25]. It should be borne in mind that AI can be theoretically made into a person even today but its main parameters will depend on the intentions of its creator (or "tutor") whose law obedience is hard to judge.

The existence of these problems is partly due to a lack (inadequacy, weak development) of AI-related legal and ethical framework. There are certain solutions in a majority of countries (for example, in the European Union) that prioritize AI problems. However, the need to regulate the emerging relations is no longer debatable.

As follows already from the draft law's title, whether AI can be considered a legal person is not an issue since no technology could be a person at law. Meanwhile, there are active doctrinal discussions of this question [Novikov D.A., 2024: 19–22], with the attempts to identify the conditions whereby AI can be regarded as a legal person.

With regard to the development and use of AI, both public regulation and self-regulation are feasible. In fact, the underlying problems could be partly addressed by self-regulation. Such documents are already available in a number of countries including Russia where a Code of Good Conduct for AI ("Code of Conduct") was drafted.[3] The parties to the relations to develop and use AI systems will voluntarily undertake to abide by the ethical principles and standards of conduct established by the Code.

[3] Available at: kodeks-etiki-v-sfere-iskusstvennogo-intellekta.pdf // SPS Consultant Plus.

The Code of Conduct applies to the relations associated with ethical aspects of introducing and using AI technologies across all stages of their lifecycle not governed by federal law and/or technical regulations. This serves to avoid a conflict between the provisions of the effective and newly adopted AI legislation, on the one hand, and the ethical principles and rules of conduct enshrined in the Code, on the other hand.

Of special interest are the priorities established by the Code including, in particular:

human-centered humanistic approach;

respect for human autonomy and free will;

non-discrimination;

risk-oriented approach;

maximum transparency and credibility of information on the progress of AI technologies, their potential and risks.

Almost all of the said priorities serve to protect the interests of individuals involved in the use of AI. These requirements, rather than being newly formulated, have been already enshrined in the Constitution and federal law and are only reproduced in the Code of Conduct with regard to AI-related relations. As was stated in the 2024 Guidelines for Further Regulation of the Relations Involving AI Technologies and Robotics,[4] the development of AI technologies should be based on fundamental legal provisions. Ethical standards will normally predate legal provisions. They are validated for specific relations and become legal provisions, once their adequacy and value have been demonstrated.

Legal liability associated with AI use is one of the most difficult issues. It would be useful to focus on the established approaches to regulate liability. As a document for self-regulation, the Code of Conduct cannot address the issues to be handled by public authorities, but self-regulated entities can take a stance with regard to liability. A fundamental position on this issue is that the authority for responsible moral choices cannot be delegated to AI; AI cannot be held liable for the decisions it makes: any liability resulting from AI operations should be always assumed by man (natural or legal person recognized as a liable party under the effective legislation of the Russian Federation).[5] The liable party should

[4] See Government order No. 2129-r "On Approving the 2024 Guidelines for Further Regulations of the Relations Involving AI Technologies and Robotics" of 19 August of 2020 // Collected Laws of Russia. 2020. No. 35. Art. 5593.

[5] See the Code of Conduct.

be identified solely by public authorities, not by the Code of Conduct or another document of a self-regulated entity.

2. Brief Overview of National AI Regulations within the CIS

A vast majority of the CIS countries are actively promoting AI considered to be one of the main vectors of economic development. However, despite the adoption of regulations to govern AI development and use, only individual issues have been addressed so far. Thus, in Kazakhstan Government Resolution No. 25 "On Identifying the National AI Platform Operator" of 23 January 2024[6] defines the national AI platform as a digital platform for collection, storage and distribution of datasets and for provision of AI-related services. The national AI platform operator has a status of a joint-stock company. Thus, artificial intelligence is considered to be directly associated with the digital platform.

In Kyrgyzstan, Law No. 88 "On the Creative Industries Park" of 8 August 2022[7] provides in Article 4 that creative industries include the economic sectors such as programming, IT product development, robotics and artificial intelligence. In this case, artificial intelligence is regarded as an economic sector, creative industry.

Uzbekistan has taken major legal and organizational efforts to develop AI, with Presidential Resolution No. PP-358 of 14 October 2024 approving the 2030 Strategy for the Development of AI Technologies.[8] The Strategy identified the priorities for extensive AI development and use, as well as the conditions required to introduce AI technologies into social services and economic sectors.

The Strategy has a conceptual framework with the terms related to AI this way or another including the definition of AI itself considered to be "a set of technological solutions that allows to imitate human knowledge and skills (such as self-learning and search for solutions) to perform specific tasks with an outcome comparable to those of human intellectual activity". Along with this definition, the Strategy introduces the term "artificial intelligence technologies".

The Strategy envisages that a regulatory framework for the progress of AI technologies will be developed to include the development and

[6] Available at: https://base.spinform.ru/# (accessed: 20.05.2024)

[7] Ibid.

[8] Ibid.

improvement of national regulations based on the study of international experience; bringing the national standards in line with those internationally adopted; establishing links with international organizations and major international firms active in this area; enhancing the regional and international cooperation. In this context, the development of a Model AI Regulation appears quite timely.

An equally important step for the development of AI technologies at the national level in Uzbekistan is Presidential Resolution No. PP-4996 "On the Measures to Create an Environment for Accelerated Introduction of AI Technologies", 17 February 2021. This resolution introduced courses on AI applications for public governance at 15 higher education institutions, with aspiring AI students to be also referred to major universities abroad.

To implement this resolution, pilot projects for the introduction of AI technologies are underway in priority sectors such as agriculture, banking and finance, transportation, health care, pharmaceutics, energy, tax administration etc.

In Russia, AI is also an economic and governance priority. Despite a lack of federal level regulation of AI development and operation, AI is regulated this way or another by legislation and bylaws. The guidelines to be followed were identified in the Presidential Address to the Federal Assembly of 29 February 2024[9] which called for self-sufficiency in AI to "ensure economic and social breakthrough".

At the legislative level, AI is regulated by Federal Law No. 152-FZ "On Personal Data" of 27 July 2006 as amended on 6 February 2023[10] to reflect the changes associated with artificial intelligence. At the level of Presidential Decrees, AI is regulated primarily by Presidential Decree No. 490 "On the Development of artificial intelligence in Russia" of 10 October 2019.[11] Federal executive authorities also adopt regulations applicable to specific aspects of AI usage. Thus, the Rosstandart has issued over 50 executive orders to approve preliminary national standards and those concerning AI.

Of principal importance are documents such as the Federal Artificial Intelligence Project[12] and the 2030 National Artificial Intelligence

[9] SPS Consultant Plus.

[10] Collected Laws of Russia. 2006. No. 31 (part 1). Art. 3451.

[11] Collected Laws of Russia. 2019. No. 41. Art. 5700.

[12] SPS Consultant Plus.

Strategy[13] that provides a framework for addressing the tasks of developing domestic AI technologies. The Data Economy and Digital Government Transformation National Project[14] launched on 1 January 2025 as a continuation of the Digital Economy National Project[15] expired in 2024 is expected to last until 2030 and includes AI-related interventions. It is envisaged to introduce AI services across all economic sectors while ensuring support to developers and transition of all spheres of civil society to new operating principles.

The 2030 National Artificial Intelligence Strategy[16] was approved as early as in 2019, with Sberbank appointed to head AI development. In addition, the National AI Development Center was set up under the Federal Government primarily with the purpose of "providing expertise and analytical support for AI implementation and development across the economy and government, and coordination of efforts by public authorities, research institutions and business community".

This document defines AI systems as "a set of technological solutions that allows to imitate human knowledge and skills in performing specific tasks with an outcome comparable to or exceeding those of human intellectual activity".[17]

The work to address legal problems related to AI, its potential and constraints for the use in the economy and public governance is also underway elsewhere in the CIS. Essentially, all these countries pursue a common objective of establishing the basic principles of legal regulation of AI.

3. CIS Interparliamentary Assembly and the Status of Model Regulations

The importance of supranational regulation of information technologies stems from the fact that the said technologies (including AI) are international by their nature and transcend national borders, only

[13] Collected Laws of Russia. 2024. No. 8. Art. 1102.

[14] Available at: http://static.government.ru/media/files/Mfmc7JI8A90E7KVfowedDeshpshSGNYt.pdf.

[15] Official web portal of legal information. Available at: http://www.pravo.gov.ru, 03.08.2017. (accessed: 25.12.2024)

[16] Presidential Decree of 10 October 2019 .On the Development of Artificial Intelligence in Russia" // Collected Laws of Russia, 2019. No. 41. Art. 5700.

[17] Ibid.

to make national-level regulation less efficient compared to coordinated regulation at the supranational level.

Regulating AI is also at the focus of the CIS Interparliamentary Assembly[18] that considers drafting and building up a stock of model laws as one of its main objectives to harmonize national regulation in this area and national legislation as a whole.

In 2023, the IPA CIS has passed "The guidelines on AI normative regulation including ethical standards for research and development"[19] ("Guidelines"), in which a low level of legal certainty was noted with regard to AI systems. In particular, they highlighted a need to promote "a shared systemic approach to the integration of legal and ethical standards into public AI policies". As a mandatory condition, the Guidelines referred to a need "to promote a responsible, open and safe approach to the process of introduction and use of AI systems across the CIS".[20]

While not containing standards or decisions, the said Guidelines establish the principles to uphold legal regulation and a range of issues to be addressed by a shared conceptual approach, in particular:

risk minimization, application of the risk-oriented approach;

ensuring a balance of interests;

explainability of AI operating principles including the criteria for automated decision-making;

non-discrimination of individuals, avoiding any manipulation of human behavior.

An analysis of other countries' regulatory provisions allows to identify equally important principles to inform the legislation of the CIS member states:

reporting;

security;

fairness and equity;

transparency;

human control and monitoring;

stability and reliability.

[18] The IPA CIS is an interstate body authorized, in particular, to draft and approve model laws on matters of mutual interest.

[19] IPA CIS Resolution No. 55-23 (passed in Saint Petersburg on 14.04.2023) // SPS Consultant Plus.

[20] Ibid.

A comparison of these principles and those previously mentioned allows to conventionally identify the following groups of principles:

those aimed at protecting the rights and interests of individuals;

those pertaining to security and control.

The list of legal problems brought about by the use of AI technologies is quite extensive. In this regard, one of the crucial high priority objectives is the development of a shared conceptual framework. The Guidelines note that a lack of common understanding of the terms holds back the building of a systemic approach to regulation of any sector including AI. As part of this work, it is recommended to make up a glossary of AI terms that will establish a shared approach between the CIS states. It is worth noting that AI is defined differently across the CIS countries.

Globally, AI regulation purports both to create optimal conditions for AI use and to protect human rights and liberties related to such use. Drafters will have to find shared solutions in order to facilitate further development of the national AI legislation in the CIS countries.

4. Coverage of Artificial Intelligence by other Model Laws

Since digitalization is beset by numerous and various legal issues not solvable by any single Model Law, a range of such laws concerning different aspects of digitization and digital change have been drafted and adopted. Thus, the IPA CIS has passed at its 55th plenary meeting the Model Law "On Digital Transformation of Industrial Sectors in the CIS Member States"[21] ("Model Law on Digital Transformation") laying the basis for improving the national legislation on digitization and digital change involving the introduction and implementation of digital technologies in the area of sectoral governance.

With provisions applying to different digital technologies, the law contains two provisions that explicitly govern the relations involving AI. One provides that a public authority in charge of a branch of industry is empowered, in particular, to "exercise general control of security" of AI systems used in the given branch.[22] Thus, by virtue of this provision the Model Law on Digital Transformation provides for a duty of public control[23] over any industrial use of AI.

[21] Resolution No. 55-9 of 14 April 2023 // SPS Consultant Plus.

[22] Ibid. Art. 10.

[23] Control can be exercised depending on specific national legislation.

AI is also mentioned in Article 16 on national technical, technological and occupational standards for digital transformation of industries that assumes standardization of AI technologies. The Model Law on Digital Transformation provides for possible use of binding or non-binding technical (technological) specifications and/or nationwide (national) standards of digitization and digital change including those applicable to AI.

This provision echoes those of the draft Model Law "On AI Technologies" whereby, with regard to standardization, public regulation of AI-related relations is ensured, in particular, by the drafting of relevant rules, standards and principles. As follows from the discussed approaches to the regulation of AI technologies, there is a need to identify the "required standards" such as:

standard for assessing and classifying AI technologies;

standard for identifying the lifecycle processes of AI-based systems;

standard for managing the risks involved in AI-based systems;

standard for identifying bias in AI-based systems;

standard for identifying the implications from the use of such systems;

standard for AI-based system governance.

The relations associated with standardization are regulated in Russia by Federal Law No. 162-FZ "On Standardization" of 29 June 2015[24] ("Law No. 162-FZ") that provides for non-binding use of standardization documents (under the general rule, Article 4). In accordance with the definition provided in Article 2 of Law No. 162-FZ, a national standard is "a general-purpose standardization document" that describes the parameters of a given standardization item, as well as the applicable rules and overall principles. The non-binding principle allows interested parties to be actively involved in the development and adoption of standards.

Russia is now active in developing national standards, preliminary national standards and other documents to regulate the operation and use of advanced digital technologies including AI.

Since 2018 the national standardization programs have envisaged a list of core standards applicable to digital technologies: "Information technologies. Internet of Things. Compatibility requirements to platforms and devices for the Industrial Internet", "Information technolo-

[24] Collected Laws of Russia, 2015. No. 27. Art. 3953.

gies. Cloud computing. Structure of Service Level Agreement (SLA)", "Cloud computing. Service Level Agreement. Structure and technology. Part 1. Metrics", "Digital industry. Format of data exchange on production sites. General provisions" etc.

With more than 100 standards currently available,[25] these documents concern the ways AI is used in different spheres. For instance, "GOST R 71562-2024. National standard of the Russian Federation. AI-based measuring tools. Metrological support. General requirements"[26] contains the main requirements to the composition, structure and applications of AI-based measuring tools.

Part 3, Article 16 of the Model Law on Digital Transformation contains a provision unusual for the Russian legislation whereby "digital clones of control objects and other digital clones will be introduced based on the technological standard, prototype or similar thing effective in this or other country" for digital transformation of the national industries or other related activity "before binding or non-binding technical/technological specification and/or nationwide/national standards are formally adopted".

---

[25] GOST R 70885-2023. National standard of the Russian Federation. Means of monitoring human behavior and forecasting intentions. AI algorithms for recognition of driver state and actions by analyzing static/dynamic images generated by photo and video surveillance systems for monitoring wheeled vehicle drivers. Methodology for assessment of functional correctness" (approved and made effective by Rosstandart Order No. 748-st of 29.08.2023),

"PNST 843-2023 (ISO/MEK 38507:2022). Preliminary national standard of the Russian Federation. Information technologies. Strategic governance of information technologies. Implications of strategic governance resulting from the use of artificial intelligence by entities" (approved and made effective by Rosstandart Order No. 58-pnst of 15.11.2023).

"GOST R 59278-2020. National standard of the Russian Federation. Information support of product lifecycles. Online technical guidance based on AI and AR technologies. General requirements" (approved and made effective by Rosstandart Order No. 1 of 23.12.2020).

"PNST 872-2023. Preliminary national standard of the Russian Federation. AI-based systems for support of medical decisions. Clinical testing methods" (approved and made effective by Rosstandart Order No. 64-pnst of 20.11.2023).

"PNST 842-2023 (ISO/MEK 25059:2023). Preliminary national standard of the Russian Federation. Software engineering. Requirements to and evaluation of system and software quality (SQuaRE). Quality model for AI systems" (approved and made effective by Rosstandart Order No. 50-pnst of 07.11.2023).

[26] Approved and made effective by Rosstandart Order No. 1526-st of 28.10.2024 // Consultant Plus.

It is worth noting that technical regulation in the EEU countries has been elevated from the national to supranational level. Supranational rules of procedure effective in these countries set up binding requirements to products. Provisions drafted by the Eurasian Economic Union will thus take precedence for the EEU member states including Russia.

On 14 April of 2023, the IPA CIS also has approved at the 55th plenary meeting[27] a Model Law on Digital Financial Assets to regulate finance as its title suggests. Its adoption allowed to identify shared approaches to the issuance and circulation of digital financial assets, accounting and title certification, methods to legitimize their holders and protect the rights of the parties to the digital financial asset market.

Characteristically, this law mentions another interstate organization, the EEU. In particular, it is provided that "regulation of the relations involved in the issuance and circulation of digital financial assets shall be exercised with a view to the purposes and objectives of digital economic development within the EEU and CIS". While such approach is not typical of model regulation, the countries making up the EEU are also members of the CIS. Moreover, it is crucial to enforce the established rules across both the EEU and CIS. This is reflected in the rule that the nationals of a CIS state enjoy in the digital financial asset market elsewhere in the CIS the same rights and obligations as locals (Article 5 of the Model Law).

The crucial question is the range of relations within the scope of the Model Law. The draft Model Law "On AI Technologies" purports to cover a wide range of social relations associated with AI technologies throughout their lifecycle such as research, development, design, evaluation and testing for compliance with certification requirements, marketing, use (including service and maintenance), monitoring and control, recycling, risk and liability insurance. It excludes only AI technologies and the underlying systems for military and defense.

The range of social relations to be regulated in connection with AI technologies is probably too wide, something that is confirmed by an almost total lack of provisions to regulate the said specific stages of AI lifecycle. Let us take the example of research that predates all other stages and shows the available opportunities and implementation options. Works will sometimes stop at this stage for lack of promise or otherwise. This stage typical of any scientific activity is regulated in detail by civil law provisions throughout the CIS countries. No peculiarities that would call for more requirements to AI research have been discovered yet. Thus, civil

[27] Resolution No. 55-11, 55th plenary meeting of the Interparliamentary Assembly of the CIS Member States // SPS Consultant Plus.

law provisions applicable to research as well as technical regulations largely suffice for the time being. The same is true for AI design and development. It would be reasonable only to prohibit the design and development of AI technologies that are incompatible with security requirements, are prone to high risk when used, and fail to uphold human rights and liberties etc., with legal instruments to reflect theses constraints.

It is also useful to consider the European Union's approach to identifying the scope of AI provisions. While not concerning itself with research and development, the EU AI Act covers the marketing of finished AI-based products, that is, the stage where AI can be viewed as commodity. Thus, the EU AI Act does not vest the persons such as AI producers and developers with any new rights and duties since the main requirements fall on suppliers that bring AI systems to market, as well as those that use them in their professional activities.

An important place is given to provisions that make it possible and feasible to incorporate into the AI Model Law specific regulation of stages such as evaluating and testing AI systems for compliance with certification requirements. In this regard, one should be careful not to ignore a number of decisions already made at the international level including within the framework of the Eurasian Economic Union. With a different and higher level of integration at the EEU, decisions are normally binding (depending on the status) on member states while legal regulation of social relations in specific spheres has been elevated, as was stated above, to the supranational level.

These spheres include, among other things, technical regulation that covers the questions of compliance, types and terms of certification (both binding and non-binding). These issues are regulated at the national level in the absence of supranational regulation. It is also worth noting the following general rule: only technical regulations establish mandatory security requirements. At the same time, it is possible and useful to build up a stock of legal solutions applicable to AI technologies by engaging, as was mentioned above, the standardization mechanisms.

5. Artificial Intelligence in Health Care

A few words about the Model Law on Digital Health Care, another one of those adopted by the Interparliamentary Assembly.[28] While its

[28] Passed at the 55th plenary meeting of the Interparliamentary Assembly of the CIS member states in Saint Petersburg on 14.04.2023, Resolution No. 55-22 // SPS Consultant Plus.

subject matter is evident from its title, it contains a definition of artificial intelligence close to the one mentioned above.

This law offers a number of provisions that can inform the development of AI legislation. It is provided that an authorized public body will monitor the security of AI systems, in particular, by logging any undesired system responses, as well as facts and circumstances that put at risk the life and health of individuals and medical workers. The same body will define a procedure for the clinical use of AI systems.

The services established for health institutions include, in particular:

AI-assisted medical decision-making;

telemedicine and AI-assisted diagnostic research management.

Article 22 of the Model Law deals specifically with AI uses. It is established that in digital health care AI technologies can be used on a standalone basis and integrated into another medical product, with the following core AI technologies being identified:

smart support of medical interventions for high-quality prevention, diagnostics, treatment and care;

digital assistant for appropriate treatment through ongoing monitoring to inform medical staff of the patient's condition;

machine learning for predicting pathologies by analyzing the data that affect the response to treatment;

predictive modeling to predict pathologic behavior and outcome, risks of complications, treatment adequacy and outcomes etc.

Evidently, digital health care allows to actively use AI by observing the duty of care to use only the clinically tested systems registered as a medical product in accordance with the national law.

6. Parties to Social Relations Involving AI

It is equally difficult to identify a range of the parties to social relations at different stages of AI development and operation. Meanwhile, the issues of liability should be addressed precisely in view of these parties' status and potential to affect AI parameters. The EU AI Act is focused primarily on the stages of marketing and further use of AI-based products, with the range of the parties limited to suppliers that market AI systems and entities that use them in their professional activities.[29] In

[29] As stated in European Parliament Resolution No. 2015/2103 (INL) Civil Law Rules on Robotics of 16 February 2017, these laws apply to AI system designers, producers and operators.

our view, it is no accident that the focus is on the liability of precisely these parties as the faults and errors of artificial intelligence become obvious at these stages, and human rights can be jeopardized.

In contrast to EU AI Act, the draft Model Law mentions a wide range of parties:

AI-based system operator: a party operating AI-based systems;

AI technology user: a party using AI technology to solve the assigned tasks or to perform certain functions;

AI technology producer: a party involved in the production of AI-based technologies and systems;

AI technology developer: a party designing AI-based technologies and systems;

AI technology owner: a party in whose name AI-based technologies are registered.

Given the terminology used in the intellectual property area, it would be more appropriate, in our view, to speak about an AI rights holder rather than owner since an AI-based system may be owned by someone else. In view of the provisions incorporated into the draft, it is practically impossible to separate the rights holder from the owner. Meanwhile, it is a party's status that will determine the amount of rights and duties, as well as liability.

The parties involved in the relations under discussion, their rights, obligations and potential to affect AI operations — all these things are crucial for solving the key problem of security and for identifying those responsible. The discussed relations may involve other parties in addition to those listed above. They include "researchers, developers, producers, persons funding AI-related R&D, owners, rights holders, operators, AI users and other persons collaborating in the area of AI technologies including authorized public bodies".

While the EU AI Act is largely focused in terms of requirements on suppliers marketing AI systems and on entities using them in their professional activities, the draft Model Law covers all parties involved in the emerging relations to whatever extent (at whatever stage), with their rights and obligations defined only generally and without specific association with a particular party.

It should be noted that the draft Model Law defines these rights and obligations simply by listing the parties to the emerging relations, with

no right or liability specifically assigned. But the said parties associated with the production and operation of AI systems have a different status and different potential to affect AI operation and to observe the established requirements. The rights, obligations and liabilities should thus be specifically defined for each group of the parties.

Here are some illustrative examples. The obligations imposed on AI researchers, producers, developers and funders (without specifying these parties) include those that only specific parties, not everyone across the board, can comply with. Thus, "persons funding AI-related R&D" are by virtue of their status unlikely to "ensure the maximum security of humans, society and state based on the rule of law and responsible development of AI technologies", and to "apply the systemic approach to risk management on ongoing basis at each stage of AI technology lifecycle with a view to the established standards in order to eliminate AI-related risks including confidentiality, digital security, robustness". Since by far not all parties can operate at each stage of lifecycle, the said persons will be equally unable to apply "systemic approach to risk management at each stage of AI technology lifecycle". In our view, a party subject to each requirement should be identified in each particular case.

This also applies to other obligations imposed on the parties to social relations associated with AI development and use. By far not all of the said parties can by virtue of their status and objective reasons "ensure transparency and traceability", "observe the requirements to robustness and security of AI technologies", "create a mechanism for assigning liability", "perform real-time analysis of AI technologies" etc. Obviously, only some of the said parties could perform specific listed actions, such as "registration and liability insurance". The implemented approach is causing confusion, only to complicate the solution to the paramount problem, that of establishing liability and identifying the liable party given that no party can be held liable for the action outside its competence and authority. We believe that a higher threat to human rights should call for tougher regulation.

7. Liability Problems in Social Relations Involving AI

In the relations under discussion, liability is one of the most challenging issues. While the available usage experience is not enough to address this issue in detail, it is nonetheless evident that liability should be equally assigned throughout the AI lifecycle (development, operation and recycling), with the types of liability and the parties subject thereto to be identified.

Depending on circumstances, the latter may include:

I system rights holder;

software developer;

I system operator.

It would be fair to assign liability throughout different stages of AI lifecycle (ranging from development to recycling). Each stage will therefore have a corresponding party (or parties) that could be held liable. As noted in the Code of Conduct, "as a result of multiple parties involved in AI-related activities (developers, data providers, designers, operators etc.), liability of artificial intelligence is hard to identify". It is in fact not always possible to detect the reason, identify the source of AI-related harm and find out where — at the development or production stage — the error or wishful misconduct comes from, only to adversely affect human rights and create a hazard.

Anyway, "the risks of harm to man or property should be minimized through requirements to the system design, software, information security..." [Ibraghimov R.S., Suragina E.D., Churilova D.Yu., 2021: 85–95]. An even more challenging issue is approval of technical standards that will also often affect AI quality and operational security. As L.A. Sharnina rightly observes, "regulators often hesitate to sanction technical standards, until they are tested internationally or as part of an experiment for limited use of digital technologies confined to a specific region or government agency" [Sharnina L.A., 2024: 22–27].

Mandatory civil liability insurance seems a viable option in light of the factors that affect the risk of harm. Moreover, such insurance can be required before an AI system is marketable.

The risk-oriented approach whereby AI systems are assigned to a risk category by assessing the resulting risk is equally promising.

Supporting the necessary level of system security is crucial for introducing AI technologies. While the legislation of the CIS countries contains general requirements to safety of products and services, it is advisable in view of the progress of AI technologies to systematize and specify such requirements as applied to AI. Industry experts agree that legally binding requirements should be established throughout AI lifecycle [Minbaleev A.V., 2018: 82–87]. Moreover, it is noted that security of personal data of the CIS nationals and of related data is of special importance:

privacy (a cross-cutting concept for personal data);

risks of discrimination of individuals;

risks of manipulating human perception;

"black box" (non-transparency of technology).

The said risks have different causes. While discrimination is directly related to data quality, the "black box" problem (or non-transparency of technology) is related to the design stage[30] and privacy to the learning stage of artificial intelligence.

Another, equally important classification allows to rate AI systems depending on the extent of risk in order to make AI systems subject to requirements of variable strictness or prohibit them altogether. The said approach is used in a number of countries and unions including the European Union. The draft Model Law also assumes the risk-oriented approach that allows for evaluation of AI systems to assign the respective risk category.

It is proposed to identify a special group of prohibited AI systems to include those capable of creating inacceptable risk or fraught with clear security threats. As follows from the group title, such AI systems should not be allowed to market.

High-risk systems make up another group that includes: critical infrastructure that can put human life, health and rights at risk; biometric identification and categorization of individuals; education and vocational training; employment; access to core government services and benefits; police data; migration and border control data; judicial data.

The third group covers medium-risk AI systems, that is, AI technologies subject to special transparency requirements. The requirements for this group are largely focused on openness and transparency. Lastly, the fourth group includes low-risk (minimum risk) AI systems not subject to any specific requirements.

For lower risk, it is vital to identify the cause of threat that may result from the use of AI. In the doctrine [Klochkova E.N., Pimenova O.V., 2024: 43–52], two groups of threat are proposed:

those of imperfect system design;

those of unauthorized system use.

[30] The "black box" is normally defined as AI with decision-making processes absolutely non-transparent to man. The "black box" risk comes at the stage of design from built-in algorithms.

The first group includes multiple causes associated with errors such as poor model learning, non-transparent decision-making; likelihood of self-serving bias; information distortion, replacing true information with false; weak protection mechanisms; lack of development control on the part of designers; discrimination; lack of liability for AI system use etc. These causes are manifested to a varying extent in AI system learning and application processes.

The said causes testify to the challenge of identifying the liable party in each particular case since there is practically no telling at what stage the AI system becomes a threat. In our view, the second group of threats includes those associated with unauthorized AI use, something that comes around quite often.

It is worth considering the proposals for "corporate liability" to introduce the presumption of liability of businesses for the caused harm in specific cases and irrespective of the fault, as well as to make AI developers and operators subject to mandatory liability insurance.

In order to evaluate the operational quality of AI systems and check whether they pose any security threat, the Model Law proposes a regular quality assessment at the stage of development, production and operation of AI to achieve the necessary level of compliance with the established requirements.

Quality assessment allows to identify system parameters such as robustness, performance, functionality, compliance with the intended purpose, accuracy, reliability of output data.

The reliance of AI applications on general regulatory principles governing AI is expected to avoid violation of statutory rights of individuals, discrimination, negative environmental impact, manipulation, biometric categorization based on sensitive data, profiling with AI-based biometric identification methods, social scoring. AI technologies not complying with the said requirements should be prohibited at any stage of AI lifecycle.

For security reasons, there should be a comprehensive approach to AI covering technical, legal, ethical and social security. In other words, the regulatory approach should make sure that the established requirements are proportional to risk.

As the Model Law governs the relations, they are only emerging in a number of countries, the proposed regulatory approaches are crucial. They establish the types of digital financial assets, the terms of issuance,

mining and circulation of cryptocurrencies etc. Regulation in this area is essentially forward-looking to provide guidance for the development of national law in the wake of digitization processes.

Regarding the complicated issue of liability, the Model Law is specific only about liability of cryptocurrency market participants (Article 21). It is provided that cryptocurrency holders are liable for violation of the national legislation on cryptocurrency circulation throughout the CIS. The reference to the CIS is essential since liability is not restricted to the territory of the country where a crime was committed. It is explicitly provided that the established requirements apply to the CIS as a whole.

This is related to another important provision: "for performing transactions that violate the national legislation on legalization (laundering) of criminal proceeds, financing of terrorism and of the proliferation of weapons of mass destruction, as well as the principles of law and order and morals, buyers of cryptocurrencies shall be held liable irrespective of their domicile, location and registration". Here the focus is also made on extraterritoriality.

8. New Rights of Individuals in AI-related Relations

Using AI requires to understand the specifics of the emerging relations including by vesting users with the rights not typical of traditional relations (not involving AI). These should include the rights to:

know that they are dealing with AI;

require an explanation of AI decision;

contest AI decision;

require human intervention.

These rights partly allow to neutralize AI risks and threats. By their nature these rights are close to those already existing and essentially serve to make the available rights more specific as required by the underlying relations.

In fact, the right to seek and obtain information is a statutory right that in this case implies specific relations and relevant information that may be concealed from the individual (by virtue of the technology being used or intentionally).

Another right — that is, to require an explanation of AI decision-making — makes it possible to know and understand the ground for AI decisions. This possibility is crucial since AI decisions are often beyond

human reasoning and explanation. With automated decision-making on the rise, there is an urgent need to protect human rights and interests.

The Russian law already has a provision of close scope and meaning which is applicable to a certain range of relations. Found in Article 16, Federal Law 152-FZ "On Personal Data" of 27 July 2006,[31] it prohibits "to make decisions exclusively on the basis of automated processing of personal data that are legally binding on personal data subjects or otherwise affect their rights and legitimate interests...". In our view, restrictions of this kind should apply not only to relations associated with personal data but also to other areas of automated decision-making (including for public governance) identifiable primarily by the lack of human involvement.

The right to contest AI decisions equals the traditional right of appeal where the decision is made by AI rather than man. It is a crucial provision whereby AI decisions can be contested just like any other.

The right to require human intervention has emerged only against the backdrop of an ever wider AI usage and automated decision-making. It purports to protect human rights by allowing to seek another person's help. This right is close by its nature to a broader right considered to be universal — that is, to refuse digital technologies — which, although not yet adopted as a provision, is proposed for AI-related relations [Avdeev D.A., 2023: 18–20]; [Naumov V.B., 2024: 26–36]; [Fedotov M.A., Naumov V.B., 2024: 8–28].

Conclusion

While AI-related regulation is only emerging in Russia, it can be expected in light of the call for self-sufficiency in AI to "ensure economic and social breakthrough" formulated in the Presidential Address to the Federal Assembly on 29 February 2024[32] that the legal support will be actively developed, with the drafting of the Model Law to contribute to this process.

Model legislation will allow the CIS states to identify shared approaches to AI regulation, address crucial issues including of the extent of public regulation, ensure information security and identify liability, build up transformational legal institutions etc., something that will contribute to a shared and functional digital space within the CIS.

[31] SPS Consultant Plus.

[32] "Rossiyskaya Gazeta. No.46. 1 March 2024.

Law and digitization are in process of affecting each other: while law inevitably changes in the context of digitization, digitization processes are being integrated into the legal framework. A characteristic feature of the current development period of the Russian society and the CIS is the transition to digital economy as well as digitization of public governance and economic relations, something that requires legislative adaptation and reform. The progress of digital technologies is driving the evolution of law (emergence of new things at law, new rights and methods of exercise thereof, changes to the status of legal entities etc.).

With the digitization process largely in advance of legal regulation, there is yet no systemic solution to the discussed problems while AI regulation at the national level is fragmented. In this context, as follows from the example of a number of model laws, model regulation is playing a prominent and important role for the development of national legislation.

References

1. Amelin R.V., Chennov C.E. (2023) *The Evolution of Law under Influence of Digital Technologies.* Moscow: Norma, 280 p. (in Russ.)

2. Avdeev R.A. (2023) The Right to Abandon Using Digital Technologies in Private Life. *Grazhdanskoye obschestvo v Rossii i za rubezhom*=Civil Society in Russia and Abroad, no. 4, pp. 18–20 (in Russ.)

3. Fedotov M.A., Naumov V.B. et al. (2024) The Right to Refuse Technologies: the Results of Expert Poll. *Trudy po intellectualnoi sobstvennosti*=Works on Intellectual Property, vol. 48, no. 1, pp. 8–28 (in Russ.)

4. Global Atlas of Artificial Intelligence Regulation. Ed. by Neznamov V. (2023) Consultant Plus

5. Golovanov N.M. (2022) The Legal Personality of Artificial Intelligence. *Teoria prava i mezhgosudarstvennykh otnoshenyi*=Theory of Law and Interstate Relations, vol. 1, no. 9, pp. 24–25 (in Russ.)

6. Ibragimov R.S., Suragina E.D. et al. (2021) Ethics and Regulating Artificial Intelligence. *Zakon*=Statute, no. 8, pp. 85–95 (in Russ.)

7. Ivliev G.P., Egorova M.A. (2022) Legal Aspects of Status of Artificial Intelligence and Products Made with its Participation. *Zhurnal rossiyskogo prava*=Journal of the Russian Law, no. 6, pp. 32–46 (in Russ.)

8. Khabrieva T.Ya. (2009) The Legal Dimension of a Scientific Progress. *Zhurnal rossiyskogo prava*= Journal of the Russian Law, no. 8, pp. 14–24 (in Russ.)

9. Khabrieva T.Ya., Chernogor N.N. (2018) The Law in Conditions of the Digital Reality. *Zhurnal rossyiskogo prava*=Journal of the Russian Law, no.1, p. 88 (in Russ.)

10. Khisamova Z.I., Begishev I.R. (2020) The Substance of Artificial Intelligence and the Issue of its Legal Personality. *Vestnik Moskovskogo gosudarstvennogo oblastnogo universiteta. Yurisprudencia*=Bulletin of the Moscow Regional University. Juriprudence, no. 2, pp. 100–103 (in Russ.)

11. Klochkova T.N., Pimenova O.V. (2024) Artificial Intellect: Dangers and Security. *Bezopasnost biznesa*=Security of Business, no. 4, pp. 49–52 (in Russ.)

12. Minbaleev A.V. (2018) Issues of the Artificial Intelligence Regulation. *Vestnik Yuzhno-Uralskogo gosudarstvennogo universiteta*. Pravo=Bulletin of the Southern Ural State University. Law, no. 4, pp. 82–87 (in Russ.)

13. Naumov V.B. (2024) The Right for Abandoning Digital Technologies in the Sphere of Artificial Intelligence. *Vestnik gosudarsnvennogo yuridicheskogo universiteta Kutafina*=Bulletin of the Kutafin Law University, no. 10, pp. 26–36 (in Russ.)

14. Novikov D.A. (2024) Recognition of Legal Personality of Artificial Intelligence and Liability for its Decision-Making Abroad. *Trudovoe pravo v Rossii i za rubezhom*=Labor Law in Russia and Abroad, no. 2, pp. 19–22 (in Russ.)

15. Sharnina L.A. (2023) Normative Legal Regulation of Digitalization: Constitutional Dimension. *Konstitutcionnoe i municipalnoe pravo*=Constitutional and Municipal Law, no. 2, pp. 22–27 (in Russ.)

Information about the authors:

L.K. Tereschenko — Doctor of Sciences (Law), Senior Researcher, Honored Lawyer of Russia.

A.V. Tokolov — Candidate of Sciences (Law).

The article was submitted 17.02.2025; approved after reviewing 10.03.2025; accepted for publication 17.03.2025