ISSN 2713-2749

Legal Issues in the DIGITAL AGE

Вопросы права в цифровую эпоху

1/2025

Volume 6

Legal Issues in the DIGITAL AGE

1/2025

ISSUED QUARTERLY VOLUME 6

Publisher

National Research
University Higher
School
of Economics

ISSN 2713-2749

The journal
is registered in the
Federal Service
of Supervision of
Communications,
Information Technology and Mass
Media. Certification
of registration
of mass media
серия
Эл № ФС77-83367

Address:
3 Bolshoy
Triohsviatitelsky Per.,
Moscow 109028,
Russia
Tel.:
+7 (495) 220-99-87
e-mail lida@hse.ru

Designer
Andrei Pavlov
Pre-press
Natalya Puzanova

ARTIFICIAL INTELLIGENCE AND LAW

COPYRIGHT LAW IN THE DIGITAL AGE

REVIEWS

Legal Issues in the **DIGITAL AGE**

EDITORIAL BOARD

Legal Issues in the **DIGITAL AGE**

ISSUED QUARTERLY

"Legal Issues in the Digital Age" Journal is an academic quarterly e-publication which provides a comprehensive analysis of law in the digital world. The Journal is international in scope, and its primary objective is to address the legal issues of the continually evolving nature of digital technological advances and the necessarily immediate responses to such developments.

The Digital Age represents an era of Information Technology and Information Communication Technology which is creating a reliable infrastructure to the society, taking the nations towards higher level through efficient production and communication using digital data. But the digital world exposes loopholes in the current law and calls for legal solutions.

"Legal Issues in the Digital Age" Journal is dedicated to providing a platform for the development of novel and analytical thinking among academics and legal practitioners. The Journal encourages the discussions on the topics of interdisciplinary nature, and it includes the intersection of law, technology, industry and policies involved in the field around the world.

"Legal Issues in the Digital Age" is a highly professional, double-blind refereed journal and an authoritative source of information in the field of IT, ICT, Cyber related policy and law.

Authors are invited to submit papers covering their state-of-the-art research addressing regulation issues in the digital environment. The editors encourage theoretical and comparative approaches, as well as accounts from the legal perspectives of different countries.

Publication in the journal is free of charge.

All materials are available for free download.

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

Research article
JEL: K00
UDC: 340
DOI:10.17323/2713-2749.2025.1.4.27

A Comparative Perspective on the Future of Law in a Time of Artificial Intelligence

Steve Cornelius

Professor, Faculty of Law, University of Pretoria, Lynnwood Road, Pretoria, 0002, Private Bag X20, Hatfield, Pretoria 0028, Republic of South Africa, steve.cornelius@up.ac.za https://orcid.org/0000-0003-1145-0392, Scopus ID: 39361195000

Abstract

The article explores the impact of AI on legal systems globally. It highlights how technology, particularly AI, disrupts social order and power dynamics, necessitating legal adaptations. The document categorizes global AI regulatory responses into four types: no response, reliance on existing tech regulations, fragmented solutions, and unified approaches. The European Union (EU) has adopted a unified approach with the Artificial Intelligence Act (AIA), aiming to harmonize AI rules, address risks, and stimulate AI development. The United States employs a piecemeal approach with the National Artificial Intelligence Act of 2020 and various state laws and executive orders. Australia lacks specific AI legislation, but it has an AI Action Plan focusing on economic benefits and talent development. South Africa's National AI Policy Framework emphasizes economic transformation and social equity. The African Union's Continental AI Strategy aims for socio-economic transformation while addressing AI risks. Canada has a Voluntary Code of Conduct and a proposed Artificial Intelligence and Data Act (AIDA). The document critiques current AI regulations for incomplete definitions and a lack of focus on the broader societal purpose of AI. It stresses the need for regulations to consider ethical dimensions and societal impacts. The document concludes that AI regulation must balance innovation with social order, human dignity, and safety, emphasizing the urgent need to address AI's energy and water consumption to prevent potential global instability.

Keywords

artificial intelligence; technologies; development; policy, regulation; ethical use.

For citation: Cornelius S. (2025) A Comparative Perspective on the Future of Law in a Time of Artificial Intelligence. *Legal Issues in the Digital Age*, vol. 6, no. 1, pp. 4–27. DOI:10.17323/2713-2749.2025.1.4.27

Introduction

Over the past 5,000 years, humans have created a world which is extremely rich in diversity. Often, though, events, places and things that appear completely unrelated, are deeply connected at a hidden level. We can truly ask, what do the Greek Empire, the Roman Empire, the Inca Empire, the British Empire, the Great Wall of China, paved roads, ships, the Greco-Persian wars, the Franco-Prussian War, the Anglo-Boer War, the First World War, the Second World War, telegraphs lines, railway lines, bicycles, aeroplanes, the Space Race, professional sports, celebrity weddings, celebrity sex scandals and stock exchanges have in common? Quite a lot actually. All of these relate to the value of information and the ability to make swift informed decisions based on the best available information.

When the Soviet Union has launched Sputnik, Lyndon B. Johnson, who was the Senate Majority Leader at the time and later President of the United States of America, remarked: "Whoever controls the high ground of space controls the world. The Roman Empire controlled the world because it could build roads. Later, the British Empire was dominant because they had ships. In the Air Stage, we were powerful because we had the airplane. And now the Soviet Union have established a foothold in outer space".[1]

While many people at that time were concerned that space could be used to deploy weapons, Johnson understood that the ability to launch satellites would have a profound effect on the way in which we communicate and on the way in which we gather, process and disseminate information. In less than two centuries, humans have moved from messages via dispatch runner, stage coach or mail ship, to instantaneous transmission of data via satellite link.

[1] Lyndon B. Johnson. AZQuotes.com. Available at: https://www.azquotes.com/quote/1059545 (accessed: 01.03.2025)

Throughout human history, technology has always been a big disruptor that has impacted on social order and the dynamics of power. Technology has always allowed some humans to work smarter and be more productive, giving them the competitive edge over those that are slow to adapt. But every new technology has also harboured the potential for unimaginable harm and destruction [Hopster J., 2021: 1 *et seq*].

Artificial Intelligence (AI) is no different. We currently live in the disruptive moment precipitated by AI as new technologies have suddenly become freely accessible by consumers across the globe. The law is primarily a reactive phenomenon which always tends to follow technological innovation and disruption. As a result, the disruptive moment constitutes a thesis in the Hegelian sense [Berenson F., 1982: 77 *et seq*], that introduces legal uncertainty, legal gaps, loopholes and obsolescence of laws. By necessity, this thesis highlights the disruptive nature of AI and spawns an antithesis of legal review and legal development that will eventually result in the synthesis of a revised legal and social order with new social and legal environment with revised social relationships, organisational structures, institutions, policies and laws [Hopster J., 2021: 2].

While technology has always been disruptive, the main difference that we face in this current disruptive moment precipitated by AI, is the explosive pace at which technology develops [Cloete F., 2024: 1]. While jurisdictions across the globe are scrambling to deal with the legal challenges posed by AI, the risk is that technology is now developing at such a pace that legal measures to deal with AI could be too vague, inadequate or obsolete before it has even been implemented.

Therefore, in this article, I will firstly consider and give a high-level overview of legal measures that have already been adopted or introduced in selected jurisdictions across the globe in an attempt to deal with the disruptive effect of AI. Secondly, I will consider the shortcomings of current legislative and policy initiatives in dealing with changing technology. And thirdly, I will consider whether the disruptive moment precipitated by AI truly poses new challenges to the law, or whether there are historical perspectives that can provide some guidance for the future of the law with AI.

1. AI Regulation across the Globe

The response to AI in various jurisdictions may be classified into four categories: jurisdictions that have not yet responded to AI and similar technologies, jurisdictions that have not responded to AI specifically, but rely on existing measures aimed at regulation of technology; jurisdictions that follow fragmented piecemeal solutions to different challenges posed by AI, and lastly jurisdictions that seek to introduce a unified approach to the regulation of AI.

1.1. European Union

The European Union (EU) seems to have opted for the unified approach and approved the Artificial Intelligence Act[2] (AIA) to create harmonised rules for AI in the EU market, seeks to address the potential risks associated with AI, prohibits or restricts the use of certain AI systems, provides transparency rules for certain AI systems and seeks to stimulate development of further AI technologies.

The complexity of the task to regulate AI in a comprehensive unified way, is reflected in the preamble to the AIA, which contains 180 recitals setting out the rationale, aims and objectives of the AIA. The preamble begins by explaining the need to lay down uniform rules for the internal market for the adoption and use of trustworthy AI systems while protecting health, safety, fundamental rights, including democracy, the rule of law and environmental protection.[3] Very importantly, the preamble recognises some member states of the EU had begun to explore regulation of AI and raises the concern that diverging national rules on AI may lead to fragmentation of the internal market and hamper the free circulation, innovation, deployment and uptake of AI systems within the common market. This fragmentation should be prevented by laying down uniform obligations for operators and guaranteeing the uniform protection of overriding reasons of public interest and of rights of persons throughout the internal market.[4] Despite the references to health, safety and protection of human rights, the *raison d'être* of the AIA is quite clearly the protection of the internal market and, by implication, the global competitiveness of the EU member states in the global economy.

Nonetheless, there is a significant focus on the potential risks that unregulated AI can pose for society. The European Parliament has distinguished between AI applications that pose unacceptable risks, AI sys-

[2] See: Artificial Intelligence Act, Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending. Regulations (EC) No 300/2008, (EU) No. 167/2013, (EU) No/ 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828.

[3] Para 1.

[4] Para 3.

tems that pose high risk and AI systems that pose low risk. The AIA therefore prohibits certain AI practises, such as subliminal manipulation or deception, systems that exploit vulnerabilities of certain groups due to their age, disability or economic situation, AI systems that evaluate or classify natural persons for detrimental or unfavourable treatment, AI systems that predict risks of persons committing criminal offences, as well as certain biometric AI systems and face and mood recognition systems.[5] In addition, the AIA refers to high-risk AI systems. These relate mostly to machinery, equipment and toys that incorporate AI, as well as applications used in education, employment, access to essential services, law enforcement, migration and border control, and administration of justice and democratic processes.[6]

The AIA also imposes transparency obligations to ensure that natural persons who interact with AI are informed of such interaction and that synthetic or manipulated audio, image, video and text content that are generated by AI can be identifiable as such.[7]

An important governance element of the AIA is the establishment of the European Artificial Intelligence Board which consists of one representative for each member state.[8] While it is a requirement that designated members should have "the relevant competences and powers in their Member States so as to contribute actively to the achievement of the Board's tasks", this requirement is, perhaps deliberately, vague and political considerations are bound to outweigh considerations of social responsibility, accountability and safety in the designation of board members by member states. This risk is to some extent offset by the establishment of an Advisory Forum of Stakeholders[9] and the establishment of a Scientific Panel of Independent Experts[10] to advise the Board and the European Commission on matters relating to AI.

1.2. United States of America

In stark contrast to the European Union, the United States has, even at a federal level, opted for a piecemeal approach, with various legisla-

[5] Art. 5.

[6] Art. 6, read with Annex I and Annex II.

[7] Art. 50.

[8] Art 65.

[9] Art 67.

[10] Art 68.

tive and policy measures, as well as executive orders that deal with various matters relating to AI. The primary legislative instrument is the National Artificial Intelligence Act of 2020 (hereinafter NAIIA).[11] In terms of this act, the President must establish the National Artificial Intelligence Initiative to ensure continued US leadership in AI research and development, lead the world in development and use of trustworthy AI systems, prepare the US workforce for integration of AI systems across all sectors of the economy and coordinate ongoing AI research and development of AI among US government agencies and departments.[12]

The NAIIA provides for the establishment of a National Artificial Intelligence Initiative Office[13] and an Interagency Committee[14] by the Office of Science and Technology Policy, while the Secretary of Commerce must establish a National Artificial Intelligence Advisory Committee.[15] Provision is further made for the National Science Foundation to establish a National AI Research Resource Task Force "to investigate the feasibility and advisability of establishing and sustaining a National Artificial Intelligence Research Resource".[16]

In addition to the NAIIA, there are also currently more than 50 bills before the US House of Representatives and Senate dealing with various matters, including maintenance of US dominance on AI research and development, intellectual property and publicity rights, transparency, healthcare, financial services and consumer protection.

Furthermore, both Presidents Trump and Biden have issued executive orders relating to AI. These include the Executive Order on Maintaining American Leadership in Artificial Intelligence[17] and Executive order on the Use of Trustworthy Artificial Intelligence in the Federal Government,[18] as well as the Executive Order on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence,[19] which was repealed by the Executive Order on Removing Barriers to Ameri-

[11] 15 U.S.C. 9401.

[12] § 9411.

[13] § 9412.

[14] § 9413.

[15] § 9414.

[16] § 9415.

[17] Executive Order 13859 of 11 Feb. 2019.

[18] Executive Order 13960 of 3 Dec. 2020.

[19] Executive Order 14110 of 30 Oct. 2023.

can Leadership in Artificial Intelligence.[20] The hands of powerful lobby groups driven by technology billionaires, who would be defined as oligarchs in any other context, are clearly evident in these executive orders as policies would promote an environment which is conducive to the interests of technology companies for the research, development and dissemination of AI and related technologies, while the risks associated with the unregulated and unrestricted development of AI seem to be glossed over.

Apart from Federal measures, various states have also enacted state legislations dealing with various matters, such as interdisciplinary collaboration to promote the design, development and use of AI,[21] protection from unsafe or ineffective systems,[22] data privacy,[23] transparency,[24] protection from discrimination[25] and accountability of those developing and deploying AI systems.[26]

1.3. Australia

While Australia has no specific legislation dealing with AI, the Australian government has released a policy framework titled *Australia's AI Action Plan* in June 2021.[27] The strategic vision calls for the broad adoption of AI and touts the potential benefits for the Australian economy in doing so. The action plan calls for the introduction of AI direct mea-

[20] Executive Order 14179 of 23 Jan. 2025.

[21] Illinois (HB 3563, 2023); New York (AB A4969, 2023, SB S3971B, 2019); Texas (HB 2060, 2023); Vermont (HB 378, 2018).

[22] California (AB 302, 2023); Connecticut (SB 1103, 2023); Louisiana (SCR 49, 2023); Vermont (HB 410, 2022).

[23] California (AB 375, 2018); Colorado (SB 21-190, 2021); Connecticut (SB 6, 2022); Delaware (HB 154, 2023): Indiana (SB 5, 2023); Iowa (SF 262, 2023); Montana (SB 384, 2023); Oregon (SB 619, 2023): Tennessee (HB 1181, 2023); Texas (HB 4, 2023); Virginia (SB 1392, 2021).

[24] California (SB 1001, 2023): Illinois (HB 2557, 2019); Maryland (HB 1202, 2020); New York City (2021/144, 2021).

[25] California (SB 36, 2019); Colorado (SB 21-169, 2021); Illinois (HB 0053, 2021).

[26] California (AB 375, 2018); Colorado (SB 21-190, 2021); Connecticut (SB 6, 2022); Delaware (HB 154, 2023); Indiana (SB 5, 2023); Iowa (SF 262, 2023); Montana (SB 384, 2023); Oregon (SB 619, 2023); Tennessee (HB 1181, 2023); Texas (HB 4, 2023); Virginia (SB 1392, 2021); Washington (SB 5092, 2021).

[27] Australia's AI Action Plan. Available at: https://wp.oecd.ai/app/uploads/2021/12/Australia_AI_Action_Plan_2021.pdf (accessed: 01.03.2025)

sures to unlock the potential of AI, establishment of programs and incentives that drive the growth of technology and digital skills, as well as adoption of policies that support business, innovation and the Australian economy, to drive the development of AI.

The action plan identifies four focus areas:

Focus one: Developing and adopting AI to transform Australian businesses.

Focus two: Creating an environment to grow and attract the world's best AI talent.

Focus three: Using cutting edge AI technologies to solve Australia's national challenges.

Focus four: Making Australia a global leader in responsible and inclusive AI.

Although the Minister's Foreword states that the "plan will ensure AI is used and developed to practically improve our lives, guided by appropriate security and ethical considerations",[28] the action plan is remarkably silent about the risks posed by unregulated and uncontrolled development and deployment of AI systems.

1.4. South Africa

The South African National Department of Communications and Digital Technologies published its *South Africa National Artificial Intelligence Policy Framework* in August 2024.[29] This policy document is unique in that it identifies present states of technological development, economic necessity, social demands and global trends in AI governance that are shaped by historical challenges relating to a digital divide, part inequities, institutional inertia and outdated regulatory frameworks, to set a future vision of economic transformation, social equity, sustainable development and global leadership through responsible adoption of AI.

The policy document identifies nine pillars on which future AI regulation and policies should be based: talent and capacity development; digital infrastructure; research, development and innovation; public

[28] Idem. P.1.

[29] South Africa National Artificial Intelligence Policy Framework. Available at: https://techcentral.co.za/wp-content/uploads/2024/08/South-Africa-National-AI-Policy-Framework.pdf (accessed: 01.03.2025)

sector implementation; ethical AI guidelines development; privacy and data protection; safety and security; transparency and explainability; fairness and mitigating bias.

1.5. African Union

The African Union has approved the *Continental Artificial Intelligence Strategy* in August 2024.[30] The strategy identifies the potential that AI holds for socio-economic transformation of Africa by creating jobs, improving service delivery, advancing agriculture, education and health, promoting access to information, protecting the environment and sustainable exploitation of natural resources. However, the strategy also warns that AI holds inherent risks relating to input/output bias, potential for discrimination against vulnerable groups, job displacement, the effect on indigenous knowledge, disinformation, data privacy, surveillance and copyright violations.

The strategy calls for five strategic objectives to be achieved:[31]

maximising the benefits of AI trough adoption by the public and private-sectors, with particular emphasis on an AI startup ecosystem;

building capabilities for AI through research and innovation and skills development;

minimising AI risk by setting AI safety and security standards and promoting inclusivity and diversity in AI;

promoting African private and public sector investment in AI;

regional and international cooperation and partnerships.

1.6. Canada

The Canadian government has introduced the *Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems* in September 2023.[32] This code requires devel-

[30] Continental Artificial Intelligence Strategy. Available at: https://au.int/sites/default/files/documents/44004-doc-EN-_Continental_AI_Strategy_July_2024.pdf (accessed: 01.03.2025)

[31] Idem. P. 18.

[32] Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems. Available at: https://ised-isde.canada.ca/site/ised/en/voluntary-code-conduct-responsible-development-and-management-advanced-generative-ai-systems (accessed: 01.03.2025)

opers and managers of advanced generative AI systems to achieve six outcomes:

accountability and appropriate risk management;

safety;

fairness and equity,

transparency;

human oversight and monitoring;

validity and robustness to ensure that systems operate as intended.

Canada has also introduced the proposed Artificial Intelligence and Data Act (AIDA) as a bill before the Canadian parliament. If passed, this measure would introduce requirements for businesses to ensure the safety and fairness of high-impact AI systems in the design, development and deployment stages.

2. Shortcomings of Current Regulation

2.1. Incomplete definitions

It is notoriously difficult to define AI in a clear, uniform and consistent way [Sheikh H. et al., 2023: 15]. The difficulties in clearly determining and defining the purpose of AI in the sense explained above, as well as the conceptual difficulties that arise from the category mistakes mentioned by Sanguinetti,[33] simply adds to the confusion. Most regulators have thus far opted for some form of task-based definition. In other words, AI systems are defined as systems that follow a certain process to achieve a particular result.

The EU AIA defines[34] "AI system" as "a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments".

In the United States, the NAIIA[35] provides that "'artificial intelligence' means a machine-based system that can, for a given set of hu-

[33] Supra.

[34] Art. 3(1).

[35] § 9401 (3).

man-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to

A. perceive real and virtual environments;

B. abstract such perceptions into models through analysis in an automated manner; and

C. use model inference to formulate options for information or action.

In terms of the California AI Transparency Act,[36] "'Artificial intelligence' or 'AI' means an engineered or machine-based system that varies in its level of autonomy and that can, for explicit or implicit objectives, infer from the input it receives how to generate outputs that can influence physical or virtual environments".[37]

The Colorado Artificial Intelligence Act[38] defines "artificial intelligence system" as "any machine-based system that, for any explicit or implicit objective, infers from the inputs the system receives how to generate outputs, including content, decisions, predictions, or recommendations, that can influence physical or virtual environments".[39]

The proposed Canadian AIDA defines[40] "artificial intelligence system" as "a technological system that, autonomously or partly autonomously, processes data related to human activities through the use of a genetic algorithm, a neural network, machine learning or another technique in order to generate content or make decisions, recommendations or predictions".

Australia's AI Action Plan[41] explains that "AI is a collection of interrelated technologies that can be used to solve problems autonomously and perform tasks to achieve defined objectives. In some cases, it can do this without explicit guidance from a human being ... AI is more than just the mathematical algorithms that enable a computer to learn from text, images or sounds. It is the ability for a computational system to sense

[36] SB-942.

[37] § 22757.1. See also AB-2013 Generative artificial intelligence: training data transparency, which contains exactly the same definition in § 3110.

[38] SB 24-205.

[39] § 6-1-1701.

[40] Sec 2.

[41] Supra p. 4.

its environment, learn, predict and take independent action to control virtual or physical infrastructure".

This is perhaps why the African Union *Continental Artificial Intelligence Strategy*[42] explains that there "is no universal definition of Artificial Intelligence. Within the framework of this Strategy, AI refers to computer systems that can simulate the processes of natural intelligence exhibited by humans where machines use technologies that enable them to learn and adapt, sense and interact, predict and recommend reason and plan, optimise procedures and parameters, operate autonomously, be creative and extract knowledge from large amounts of data to make decisions and recommendations for the purpose of achieving a set of objectives identified by humans".

What is most likely, is that definitions of AI will develop over time to account for more specific applications of AI and to ensure that such specific uses of AI are properly regulated. Having a comprehensive all-encompassing definition of AI at this time may be as helpful for future regulation of AI, as a proper definition of "internal combustion engine" may have been for the regulation of transportation and related industries in the 20th century.

2.2 The purpose of AI

If comprehensive definition of AI is not currently possible or feasible, the regulation of AI should be guided by another fundamental principle. The legislative, policy and framework instruments that have been developed to address the disruptive moment precipitated by AI, all seem to be derived primarily from an economic concern and the fear that failure to promote the adoption of AI, will leave a particular country or region at an economic disadvantage when compared to countries or regions that foster research, development and deployment of AI. There is an inherent risk that this economic focus "may spark a race among commercial and national superpowers to build the most powerful AI system. There is a legitimate fear that a "winner-takes-all" approach may result in a poverty of options for consumers and could lead to a concentration of power or even geopolitical unrest"[43] AI regulation should not focus only on governance of AI research, development and deployment, but must

[42] Supra p. 14.

[43] Dentons Global Team. The Future of Global AI Governance. In: IBA Annual Conference — 2023. Paris—Washington. P. 5.

also include governance of the AI systems themselves, as well as the networks, systems and devices on which they operate.[44] In short, current regulatory measures appear to emanate from very specific premises and may therefore prove to be inadequate to deal with challenges posed by AI in the medium to longer term as technology continues to develop.

While most of these instruments acknowledge the potential risks posed by unbridled adoption of AI, none of the measures introduced thus far, seem to consider the purpose of AI in the broader teleological sense of the word. Purpose in this sense is not restricted to the immediate aim which the developer of an AI system wishes to attain, but refers rather to broader societal values and norms and the way in which AI systems would impact on the fabric of society. A teleological approach is based on the individual's realisation of justice. Values beyond the legislative texts or policy documents therefore have an influence on the purpose of AI in this sense. As a result, purpose in the teleological sense has an ethical dimension which requires the consideration of moral issues and justice [Devenish G.E., 1992: 44–47]. Any attempt to regulate AI through legislation or policy should therefore be premised on the question of purpose.

This question should firstly be concerned with the expression "artificial intelligence" itself and whether it serves any useful or legitimate purpose. The expression has its roots in a proposal made in August 1955 to host a study of artificial intelligence during the summer of 1956 at Dartmouth College, New Hampshire. The proposal was based on the premise that every aspect of learning or any other feature of intelligence can in principle be so precisely described that a machine can be made to simulate it. The proposal was that a machine could be made to behave in ways that would be called intelligent if a human behaved in the same way. [McCarthey J. et al., 2006: 12]. In this regard, one has to agree with Floridi and Cowls when they state: "This is a counterfactual: were a human to behave in that way, that behaviour would be called intelligent. It does not mean that the machine is intelligent, or even thinking. The latter scenario is a fallacy, and smacks of superstition. Just because a dishwasher cleans the dishes as well as (or even better than) I do does not mean that it cleans them like I do, or needs any intelligence to achieve its task". In other words, the mere fact that a machine can perform tasks that would otherwise require human intelligence and intervention to be performed successfully, does not make the machine intelligent [Floridi L. and Cowls J., 2019: 4]. The term was coined by researchers who

[44] Idem. P. 6.

were looking for a catchy label that would attract funding,[45] and undoubtedly this motive in the use of the expression remain as valid today for both researchers and technology companies, as it was when it was first coined. The idea of creating machines that are more intelligent than mankind has appealed to humans since the earliest times and stories of "intelligent machines" have played on the imagination from ancient mythologies to modern science fiction.

Sanguinetti[46] refers to the expression "artificial intelligence" as a category mistake, much in the same as considering the physical campus, buildings and facilities to be a university is a category mistake. He explains that "'artificial intelligence' generates a category mistake of at least three kinds:

1. Discipline vs. entity: 'Artificial intelligence' is a discipline, a field of study, but the term is sometimes used with the indefinite article as if it were an individual, countable entity. For instance, phrases like 'An AI designs materials...' confuse a discipline with a tangible being, akin to saying 'a medicine cures a tumor'.

2. Aspiration vs. reality: The term originally described an aspiration, a goal to be achieved in the distant future. Today, it is often used as if such intelligence already existed, as an already accomplished task. In 1955, the name denoted a promise, not an achievement. This is still true today.

3. Tool vs agent: The term contributes to anthropomorphizing AI, confusing a tool with an agent, a piece of software with a being with its will, desires, and ideas. This is easy to see in the positioning of AI as the subject of the sentence, replacing the real agents of the action (humans who have used AI as a tool to do something), like in: 'AI discovers...'

The name 'artificial intelligence' also fosters a more subtle but equally powerful misconception. Namely, that AI systems not only do the same things as humans, but do them in the same way and according to the same internal mechanisms. This is not true. Airplanes fly, like birds, but by very different physical principles. If they were called "artificial birds", it would probably be easier to misconceive what they are and how they work. People would be more likely to discuss false, nonexistent problems in aeronautics and to relegate the real ones. The same

[45] Sanguinetti P. Why the Term 'Artificial Intelligence' Is Misleading. IE Insights. Available at https://www.ie.edu/insights/articles/why-the-term-artificial-intelligence-is-misleading/ (accessed: 01.03.2025)

[46] Idem.

can be said of AI. But the activity of thinking is less visible than that of flying, and the differences between what humans and machines do in this area are therefore harder to see."

Any regulation of AI that ignores these category mistakes may not only be inadequate to address current legal concerns relating to AI, but may in fact set dangerous precedents that future generations may have to contend with. Such regulation would be as appropriate for socio-legal and socio-economic development as transportation safety regulations based on the flight of birds. The purpose in the teleological sense must define the regulation and it must proceed from a correct understanding of what AI actually is and what AI certainly is not.

Purpose in this sense also requires reflection on the objective that technological advancement is supposed to achieve in society. The sad reality is that very few technologies can honestly be said to have significantly improved the life of most humans [Vernyuy A., 2024: 62]. The first industrial revolution with its mechanisation and second industrial revolution with its electrification, produced unimaginable pollution and was based to a significant extent on some of the most exploitative labour practices in history. It produced wars and genocide on an industrial scale that saw the demise of more people than all the wars and diseases in history combined. It also created super rich industrialists who profited from factories inhumane working conditions and the sale of arms and resources to belligerents. The nuclear age brought with it the risk of destruction at an unimaginable scale. Current generations grapple with problems of climate change and the risk of nuclear holocaust is ever present. These problems will certainly not be solved in our time and future generations will continue to face the consequences of past technological developments. The risk, if AI is not properly understood and regulated in a human-centred way to improve the lives and livelihoods of humans, is that it will become yet another burden on future generations to deal with.

The current disruptive moment precipitated by AI provides a unique opportunity to learn from past mistakes and address the development and deployment of AI in a structured regulated way that would benefit the majority of humans. Floridi and Cowls propose five principles on which any future regulation of AI should be based [Floridi L. and Cowls J., 2019: 5–8].

> Beneficence: The development and deployment of AI should be beneficial to humanity by promoting well-being, preserving dignity and sustaining the planet.

Non-maleficence: AI should not be misused or overused.

Autonomy: The autonomy of humans should be promoted and the autonomy of Ai systems should be restricted.

Justice: The deployment of AI should provide equal access to the benefits of technology while avoiding or at least acknowledging inherent bias in the datasets used to train AI systems.

Explicability: AI systems should be intelligible, in the sense that its processes can be understood, as well as transparent and accountable, in the sense that someone is responsible for the way in which a particular AI system works.

These five principles are certainly not unique to AI and should arguably inform the regulation of any human endeavour. While these principles should then indeed be fundamental principles on which future regulation of AI is based, it is also crucial that the category mistakes highlighted by Sanguinetti[47] should be avoided. This latter aspect may have the effect that a generalised approach to regulation of AI may prove to be inadequate in future in much the same way as a generalised regulatory approach to transportation would be inappropriate and inadequate. Sheikh et al compares the development of AI with the invention of the internal combustion engine in the 19th century [Sheikh H. et al., 2023: 333]. Neither the inventors and early developers of internal combustion engines, nor regulatory authorities at the time, could have foreseen how this invention would drastically alter all forms of transport, render existing technologies, such as horse-drawn carriages obsolete, and spawn a diverse range of industries. A single unified law on internal combustion engines would simply not have sufficed. In much the same way as regulators have had to provide policies for rail, road, air and marine infrastructure, as well as distinct regulatory measures for air, sea, rail and road transport, distinguish between passenger and freight transport, and distinguish between ordinary freight and hazardous freight, regulators may find that AI is too pervasive and the specific applications of particular AI systems are too unique to rely on a single regulatory framework. A general framework may set the initial stage for the introduction of some structure and control, but industry- or activity-specific regulation will soon be required. The use of AI as a tool in the judicial or administrative decision-making process, for instance, requires different measures from the use of AI to generate patentable designs, which in turn requires different measures from AI used to generate or process news reports.

[47] Supra.

2.3. Reflections from the past

The current disruptive moment precipitated by AI, revolves to a significant extent around the use of machines to serve the interests of humans and perform more and more tasks that humans find mundane, repetitive or difficult to do. In much the same way, the current consternation about AI and the discussions relating to the creation of "intelligent machines" are reminiscent of the ancient Roman obsession with slaves. Gaius distinguished between free men and slaves,[48] much in the same way that the debate today revolves around human intelligence and artificial intelligence.

Many people today live in fear of technology and of AI in particular. At the very least, there is a fear that AI systems will make many jobs redundant and that AI systems will be able to do many jobs that are currently reserved for humans,which will lead to increased unemployment. At the extreme, there is a fear that machines, particularly autonomous AI driven machines, will take over the world and lead to war with humans or the eventual extinction of the human race [Kim J., 2019: 9]. This fear is nothing new — the ancient Romans lived in constant fear of an uprising by slaves. This was to a significant extent the result of the high proportion of slaves per household, as well as in the overall population of Rome. As a result, many repressive measures were introduced to not only deal decisively with disobedience and uprisings when they occurred, but also to provide significant deterrence against any future contemplation of disobedience or uprising. However, the Romans also realised that that there was a close correlation between the maltreatment of slaves and the hostility of slaves towards their masters. As a result, measures were also introduced to protect slaves against maltreatment and abuse [Gamauf R., 2007: 159, 160].

In the Roman *Ius Civile* and Praetorian law, a slave was *pro nullo* — viewed not as a human with a separate identity, but as a mere possession in the same way that a horse or an ox would have been [Van den Bergh R., 2015: 361]. Cartwright[49] explains the status of slaves in Rome:

> To all intents and purposes they were merely the property of a particular owner, just like any other piece of property — a building, a chair or a vase — the only difference was that they could speak.

[48] Institutes. 1.9–11.

[49] Cartwright M. Slavery in the Roman world. 2013. Available at: https://www.worldhistory.org/article/629/slavery-in-the-roman-world/ (accessed: 18.03.2025)

This seems remarkably similar to AI systems today — they are merely the property of a particular owner, but they can “speak”. A slave was therefore a means to perform work which the slave owner considered as too menial. It was also not uncommon for slaves to have specialised skills, such as weaving or writing, which could be put to good use by the slave owner. As such, the slaves of the Roman times can in many ways be compared with the machines we employ today to perform menial or highly specialised tasks.

This means that we can take some guidance from the way in which the ancient Romans regulated matters relating to slaves to provide some guidance for the future in respect of AI systems. This would be very useful in a jurisdiction such as South Africa, where the law of contract is based on Roman-Dutch common law and reference is often still made to some of the old Roman sources [Hutchinson D. et al., 2022: 11]. This particularly in view of the lack of effective regulation in South Africa which deals with AI. But it can also be of value to other jurisdictions that struggle to adapt to the challenges posed by AI. The reason is simple:

> Roman law has a lot to tell us. It forms the basis for most private law systems in use today. It is an important source for the history of concepts and ideas in western civilisation [Schermaier W. et al., 2023: 1].

So what can Roman law tell us about AI?

2.3.1. Purpose

Slavery in ancient Rome had a purpose, just as the use of AI today has a purpose. Plautus[50] explained that “a good servant, [is one] who takes care of his master’s business, looks after it, arranges it, thinks about it, in the absence of his master diligently to attend to the affairs of his master, as much so as if he himself were present, or even better”. Bearing in mind the risk of anthropomorphising AI, in much the same way, we can define the purpose of AI today to take care of its master’s business, arrange it, think about it and attend to its master’s affairs. The only pressing question would be: Who is the master? Is it a multinational technology company? Is it the person who uses an AI application for a particular purpose or outcome? These are indeed vexed questions

[50] Menaechmi. Act V. Scene IV. Translation available at: https://archive.org/stream/comediesofplautu00plau_0/comediesofplautu00plau_0_djvu.txt (accessed: 01.03.2025).

that regulators will have to address in future regulation of AI technology. When a person operates a dishwasher or a motor car, it is fairly obvious that the machine is in service of the particular operator. But when a person uses an AI application, is the AI system designed to serve the particular user? Should it be designed to serve the particular user?

2.3.2. Agency

Humans today use machines, and AI systems in particular, as agents in the broad sense, to perform work more efficiently than humans themselves can do. AI also now poses the distinct possibility that AI can be used as agent in the more specific legal sense of the word, meaning that AI can be used in a representative capacity to create legal obligations on behalf of a principal [Scott T.J. et al, 2020: 282]. The possibility that machines which are connected to the internet, can order supplies required for their proper operation without intervention of the user or operator, is nothing new. Photocopiers and printers have for some time now had the ability to monitor the level of ink or toner in the machine and automatically place an order for replacement of an empty cartridge when this becomes necessary.[51] The user or the photocopier or printer merely signs up when they install the machine and the rest is up to the machine to manage. This function, which does not require any measure of AI, will certainly be improved and expanded upon with the introduction of AI. For instance, the current function places an order when the amount of ink left on the system reaches a certain minim level. The introduction of AI systems will make it possible for the machine to not only detect the level of ink left in the system, but also to make a much more refined decision, based on various other factors, such as historic use patterns around external events, to determine the most opportune moment to order more ink. It is not inconceivable that the printer can also eavesdrop and decide to order ink as a precaution when it “hears” that a user has a lengthy report which is due and will have to be printed. The same principle can now arguably apply in respect of equipment, such as fridges in household or industrial kitchens, as well as a vast number of other applications where AI can assist with or even take over the logistics around supplies and maintenance. The question then is, to what extent can the intervention of AI in these scenarios be compared with agency in the legal sense?

[51] See for instance HP Instant Ink. Available at: https://www.hp.com/us-en/printers/instant-ink.html (accessed: 17.03.2025)

Roman law did not know the concept of agency [Van den Bergh R., 2015: 359]. In ancient Rome, only the head of the household, or *paterfamilias,* had capacity to incur contractual liability [Thomas J.A.C., 1976: 414]. Roman law did not know the concept of agency, which means that it was, as a general rule, necessary for the *paterfamilias* to participate in the solemn legal acts that constituted the limited number of recognised contracts in early Roman law [Van den Bergh R., 2015: 359]. This was most likely due to the fact that only certain transactions, which relied on performance of ceremonial rituals in the presence of witnesses, were recognised as contracts in Roman law [Kaser M., 1975: 33.4.1].

As commerce developed from the 3rd century B.C. onwards, Roman law compensated for the lack of agency by allowing sons to conclude certain transactions on behalf of their fathers. More significantly, though, Roman law also began to recognise that slaves could in certain circumstances, conduct business on behalf of the *paterfamilias*. In this regard, the slave was not seen as acting on his own, but was rather viewed as the voice of the *paterfamilias*. The slave could not incur any rights or duties in terms of such transactions — the rights and, for the most part, the duties resulting from transactions concluded by slaves, vested in the *paterfamilias*.

> The capacity given a slave to represent his master in certain juristic acts — and thus to borrow, so to say, his master's personality so that the latter could acquire property or become a creditor — represents the first significant change to the view that a slave was a mere thing. In this respect, the slave was considered not merely as property, but as the instrument of a juristic act. However, the slave was allowed to act only in the interests of the owner, and by way of "involuntary" agency, and his capacity to do so was strictly limited. ... anything acquired by ... a slave immediately vested in his pater or dominus even if the latter had not consented to the acquisition [Van den Berg R., 2015: 362].

Using slaves as instruments of commerce in this way became commonplace in the Roman Republic and later in the Empire. The Romans later developed the figure of *peculium*, in terms of which a slave would be provided with a working capital which allowed them, at least *de facto*, if not *de jure*, to accumulate property. In this way, wealthy Romans could own and administer property or open businesses in different parts of the empire and appoint slaves to administer the property or business for the master. The slaves to whom a peculium was awarded, could then act with a significant measure of autonomy for the benefit of their masters without the constant supervision of their masters, while the obligations created in terms of any contracts concluded by such slaves, accrued to their masters and not to the slaves themselves [Silver M., 2016: 68].

This begs the question: What can we learn from the Roman law on slaves and *peculium* that can be of use for the foreseeable future in respect of AI? Firstly, Ulpian[52] explained that the "ownership of slaves should not be given greater consideration than the right of having authority over them" [Watson A., 1998: 415]. In other words, the question whether a master could incur liability for transactions concluded by a slave, depended on the control of the slave, rather than the ownership of the slave. A master who controlled the slaves that belonged to others, could therefore incur contractual liability for the transactions of those slaves, even though they were not the owners of the slaves. In much the same way, it may be proposed that it is not the ownership of an AI system which will determine liability for transactions conducted by that AI system. Rather, it is the ability to control the AI system at the time when the transaction is conducted, that should determine who incurs contractual liability for such transaction, even if the amount of control was minimal and amounted only to setting up or enabling the system to conduct the transaction autonomously. As Pomponius[53] explains, " the question to be considered is not what the slave, but what the master has done for the purpose of creating a peculium for the slave". In other words, when applied to transactions conducted by an AI system, the focus should not be on what the AI system had done, but rather on what the user had done to set up or enable the AI system to conduct the transaction. It should be on that basis that contractual liability should rest.

The same applies to the right to claim performance. Ulpian[54] explained that where "'anything is due to those who are under his control,' for no one doubts that this also is owing to the master" [Watson A., 1998: 416, 418]. The user who sets up or enables an AI system to conduct particular transactions, should therefore be entitled to claim the benefits that accrue from that transaction inasmuch as the user will be liable for the debts incurred. Ulpian[55] further explained:

[52] Digests. 15.1.1.6.

[53] Digests. 15.1.4.

[54] Digests. 15.1.9.3.

[55] Digests. 15.1.41.

> A slave cannot really owe or be owed anything, but we use the word loosely to indicate the facts rather than with reference to obligations at civil law.
>
> Thus, a master may sue third parties for what they owe the slave, and he may be sued for what the slave owes them up to the amount of the peculium, and for any benefit thereby accrue [Watson A., 1998: 431].

Similarly, AI cannot owe or be owed anything — the rights and duties in terms of a contract concluded through AI, even if it is done autonomously, should accrue to the user who sets up or enables an AI system to conduct particular transactions.

2.3.3. Taking care of AI

Just as the ancient Romans realised that the potential for disobedience and uprisings by slaves would be reduced if masters took care of their slaves, it will also be necessary to take care of AI.

What will AI demand from us in return for its services? Plautus[56] was of the view that food and drink were far more powerful tools than chains to bind a slave and secure his service: "He whom you wish to keep securely that he may not run away, with meat and with drink ought he to be chained ; do you bind down the mouth of a man to a full table. So long as you give him what to eat and what to drink at his own pleasure in abundance every day, i' faith he'll never run away, even if he has committed an offence that's capital; easily will you secure him so long as you shall bind him with such chains".

Similarly. AI will demand to be fed. Feeding AI begins by powering the specialised processing units that are typically housed in large data centres that also require vast amounts of water for cooling. This thirst for water has already brought technology companies in conflict with local farmers and native residents.[57] The potential that AI holds for "geopolitical unrest" that Denton's foresee, will almost certainly arise from the ever-increasing demands for energy and water to keep

[56] Menaechmi. Act I. Scene I. Translation available at: https://archive.org/stream/comediesofplautu00plau_0/comediesofplautu00plau_0_djvu.txt (accessed: 01.03.2025)

[57] Berreby D. As Use of A.I. Soars, So Does the Energy and Water It Requires. 2024. Available at: https://e360.yale.edu/features/artificial-intelligence-climate-energy-emissions (accessed: 01.03.2025)

the growing number of data centres operating.[58] If ever a conflict arose between humans and machines, it will most likely be the result of competition for water. If regulators wish to promote research, development and deployment of AI, particularly in a world already beset by climate change, they will have to address the energy and water consumption of data centres. As technology advance and more and more AI systems become decentralised, the heat generated by processing units running AI applications will pose further challenges for existing office buildings that are ill-equipped to handle high thermal loads. Effectively cooling such buildings may further increase the consumption of energy and water. More than any other aspect of AI, regulators will have to introduce policies and measures that not only compel developers of AI systems to develop and maintain renewable energy sources, but also to explore alternatives to water for cooling.

Conclusion

The sudden proliferation of AI systems precipitated a disruptive moment that requires careful analysis and timely legal intervention to ensure that the balance between research and development of AI systems on the one hand, and social order, human dignity and safety, on the other hand, is maintained. The law is primarily a reactive phenomenon which always tends to follow technological innovation and disruption. The rapid development of AI means that the law can no longer afford to be reactive, nor can regulators rely on a *liassez faire* mindset towards AI. The development of AI can no longer be ignored and the need to provide legal certainty and clarity is now more important than ever. Regulators and lawmakers must ensure that the benefits of AI are realised, while the risks relating to the deployment and use of AI is mitigated. In particular, the most pressing need for urgent action will be to address the consumption of energy and water by AI systems. Failing to do so raises various apocalyptic scenarios, ranging from a collapse of data centres, global instability, civil unrest and war.

References

1. Berenson F. (1982) Hegel on others and the self. *Philosophy,* vol. 57, no. 219, pp. 77–90.

2. Cloete F. (2024) Governing Artificial Intelligence (AI) and other Technologies in the Digital Era. *Administratio Publica,* vol. 32, issue 1, pp. 1–30.

[58] Dentons. P. 5.

3. Devenish G.E. (1992) Interpretation of Statutes. Cape Town: Juta & Co Ltd., 298 p.

4. Floridi L. and Cowls J. (2019) A Unified Framework of Five Principles for AI in Society. *Harvard Data Science Review,* vol. 1, issue 1, pp 1–14.

5. Gamauf R. (2007) *Cum aliter nulla domus tuta esse possit*… : Fear of slaves and Roman law. *Actes du Groupe de Recherches sur l'Esclavage depuis l'Antiquité*, vol. 29, pp. 145–164.

6. Hopster J. (2021) What are Socially Disruptive Technologies? *Technology in Society,* vol. 67, pp. 1–8.

7. Hutchinson D., Pretorius C.J. et al. (2022). The Law of Contract in South Africa 4 ed. Cape Town: Oxford University Press, 528 p.

8. Kaser M. (1975) Das Römische Privatrecht, 10 ed. München: CH Beck'sche Verlag sbuchshandlung, 634 p.

9. Kim J. (2019) Fear of artificial intelligence on people's attitudinal & behavioral attributes: An exploratory analysis of A.I. Phobia. *Global Scientific Journal*, vol. 7, issue 10, pp. 9–20.

10. McCarthy J., Minsky M. et al. (2006) A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, August 31, 1955. *AI Magazine,* vol. 27, issue 4, pp. 12–14.

11. Schermaier M. et al. (2023) The position of Roman slaves. Berlin: Walter de Gruyter GmbH, 296 p.

12. Scott T.J., Cornelius S.J. et al. (2020) The Law of Commerce in South Africa 3 ed. Cape Town: Oxford University Press, 638 p.

13. Sheikh H., Prins C., Schrijvers E. (2023) Artificial Intelligence: Definition and Background. In: Mission AI. Research for Policy. The New System of Technology. Cham: Springer, 410 p.

14. Silver M. (2016) At the base of Rome's *peculium* economy. *Fundamina*, vol. 22, issue 1, pp. 67–93.

15. Thomas J.A.C. (1976) Textbook of Roman Law. Amsterdam: North-Holland Pub. Co., 592 p.

16. Van den Bergh R. (2015) 'He's one who minds the boss's business ...' *Fundamina*, vol. 21, issue 2, pp. 359–437.

17. Vernyuy A. (2024) Impact of Technological Advancements on Human Existence. *International Journal of Philosophy,* vol. 3, issue 2, pp. 54–66.

18. Watson A. (ed.) (1998) The Digest of Justinian, Vol. 4 (Revised). Philadelphia: University of Pennsylvania Press, 768 p.

Information about the author:

S.J. Cornelius — LLB, LLD, Professor.

The article was submitted to editorial office 03.03.2025; approved after reviewing 19.03.2025; accepted for publication 20.03.2025.

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

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

Research article
JEL: K3
UDC: 242
DOI:10.17323/2713-2749.2025.1.53.82

Legal Evolution of Human Rights Protection in Uzbekistan Amid Digital Transformation

Akmal Kholmatovich Saidov

Legislative Chamber of the Oliy Majlis of the Republic of Uzbekistan, Tashkent 100035, Bunyodkor Ave., Uzbekistan,
ncpch2@mail.ru, https://orcid.org/0000-0001-9990-0655

Abstract

The article is devoted to the development of legislation of Uzbekistan in the context of the transition to a digital economy. The article provides an overview of the norms introduced into the law taking into account the impact of digitalization on public relations. The author examines new provisions of the Constitution, codes, and other regulatory legal acts. Particular attention is paid to the review of concepts and strategies for the development of Uzbekistan until 2030 and their provisions regarding digital technologies. The author notes that the legislation of Uzbekistan is developing taking into account global trends, including such a factor as the intensive development of digital technologies. It is important to continue measures to improve legislation in the field of human rights taking into account the digitalization factor and to ensure reliable guarantees for the protection of human rights in the digital economy.

Keywords

digitalization; digital technologies; electronic legal proceedings; remote work; distance learning; right to information; information security.

For citation: Saidov A.Kh. (2025) Legal Evolution of Human Rights Protection in Uzbekistan Amid Digital Transformation. *Legal Issues in the Digital Age*, vol. 6, no. 1, pp. 53–82. DOI:10.17323/2713-2749.2025.1.53.82

Introduction

In today's global era, digitalisation is having a significant impact on virtually every aspect of social, political and economic life. Consequently, legal systems around the world are actively adapting to digital realities, especially in the area of human rights protection.

Digital technologies offer new opportunities, but also pose unprecedented challenges, requiring countries and international organisations to reassess and develop appropriate legal standards and practices. Notably, the United Nations (UN) has increasingly recognized the need to establish a comprehensive human rights framework that addresses the complexities posed by digital technologies. Ongoing UN initiatives include not only long-standing commitments to privacy under the International Covenant on Civil and Political Rights (ICCPR, 1966) but also emerging proposals such as the *Global Digital Compact*, which aims to outline shared principles for an *open, free, and secure digital future.*[1]

The international legal community has increasingly recognised the need to establish and improve a comprehensive human rights framework that takes into account the complexities posed by digital technologies. Such challenges include violations of privacy, algorithmic discrimination, digital exclusion and infringement of fundamental freedoms. Analysing international practice and experience provides vital insights into evolving legal standards and effective mechanisms for their implementation.

The introduction of digital platforms for communication, education, health care and judicial processes requires a strong and adaptive legal framework to ensure privacy, access to information and cybersecurity.

Uzbekistan is actively developing policies that incorporate human rights into digital governance, reflecting its commitment to international human rights obligations stemming from more than 70 treaties. An example of this approach is the national strategy 'Digital Uzbekistan 2030', which envisages the creation of a digital society in which technological innovation is harmoniously combined with the protection of individual rights. This strategic framework is supported by legislative reforms aimed at ensuring accessibility of digital technologies, strengthening cybersecurity and personal data protection. However, addressing

[1] United Nations. 2024. Global Digital Compact. Available at: https://www.un.org/en/summit-of-the-future/global-digital-compact (accessed: 25.02.2025)

challenges such as digital exclusion, misinformation and the regulation of new technologies such as artificial intelligence (AI) and big data analytics remains crucial.

A comparative analysis of the legislative frameworks of technologically advanced countries can further support Uzbekistan in improving legislation and strengthen the protection of human rights in the digital age.

This article examines Uzbekistan's legislative achievements aimed at protecting human rights in the context of digital transformation, as well as an in-depth study of international standards and global best practices. The hypothesis underlying this research suggests that Uzbekistan's evolving legal framework reflects broader international trends towards the integration of human rights in digital governance. The research methodology includes qualitative analyses of national legislation, policy documents, judicial practice, as well as comparative studies of international legal standards and foreign legislative models.

1. International Legal Standards in the Context of Digitalization

The rapid development of digital technologies has changed various aspects of society, necessitating the development of international legal standards to address human rights, privacy and ethical considerations.

In her book *Digital Empires: The Global Battle to Regulate Technology*, Anu Bradford explores the competing digital governance models of the United States, China, and the European Union (EU), highlighting how each seeks to expand its influence in the digital realm [Bradford A., 2023: 5–10].

Similarly, *The Law of Global Digitality*, edited by Matthias C. Kettemann and Alexander Peukert, examines how different areas of law, such as consumer contracts and data protection, have evolved in response to global digitalization, providing insights into the emerging legal frameworks governing digital spaces [Kettemann M.C., Peukert A., 2022: 15–20]. This analysis draws upon these works to examine the initiatives of organizations like the EU, the Organization for Economic Co-operation and Development (OECD), the UN, and the United Nations Educational, Scientific and Cultural Organization (UNESCO) in navigating the complexities of digitalization and contributing to digital governance.

K. Yeung critically explores 'algorithmic regulation' as a novel governance model, warning that increasing reliance on automated systems risks weakening transparency and democratic accountability in digital policy-making [Yeung K., 2018]. Z. Tufekci highlights that algorithmic systems can create opaque decision-making environments that extend beyond major platforms, affecting civic life, access to opportunities, and democratic participation [Tufekci Z., 2015: 211].

Significant international documents have contributed to shaping digital human rights standards. Notably, the **Universal Declaration of Human Rights (UDHR, 1948)** and the **International Covenant on Civil and Political Rights (ICCPR, 1966)** serve as foundational human rights instruments. Specifically, Article 17 of the ICCPR emphasizes the right to privacy and protection from unlawful interference, becoming increasingly relevant in digital contexts.

Recent developments at the United Nations underscore the applicability of traditional human rights offline as well as online. In particular, the UN Human Rights Council explicitly affirmed in its resolution on the "**Promotion, Protection and Enjoyment of Human Rights on the Internet**" (2018) that "the same rights that people have offline must also be protected online."[2]

In addition, the proposed **UN Global Digital Compact**, championed by the UN Secretary-General, sets forth principles for promoting an "*open, free, and secure digital future for all.*"[3]

Inter-parliamentary organizations have also taken the initiative. The Inter-Parliamentary Union (IPU) in particular, in October 2024, the city of Geneva, Switzerland, hosted the **149th Assembly of the Inter-Parliamentary Union (IPU)**,[4] a milestone event for global discussions on regulating artificial intelligence (AI) and its implications for democracy, human rights, and the rule of law. Parliamentarians from around the world convened to address pressing questions related to science, technology, and innovation, aiming to build a more peaceful and sustainable future. The main focus of the 149th IPU Assembly was leveraging achievements in science and technology to tackle global challenges, such as inequitable access to technology, the protection of human rights, and

[2] UN Human Rights Council Resolution 47/16 on the Promotion, Protection, and Enjoyment of Human Rights on the Internet, adopted on 26 July 2021 // UN Doc. A/HRC/RES/47/16.

[3] Global Digital Compact. Available at: https://www.un.org/digital-emerging-technologies/global-digital-compact (accessed: 10.03.2025).

[4] Inter-Parliamentary Union. 149th Assembly and related events. 2024. Available at: https://www.ipu.org/event/149th-ipu-assembly-and-related-meetings (accessed: 05.03.2025)

climate change mitigation. The Assembly marked an important step toward strengthening international cooperation and implementing ethical standards for emerging technologies, including AI.

Three major documents were adopted at the conclusion of the 149th IPU Assembly:

First. **The Geneva Declaration:** *Harnessing science, technology and innovation (STI) for a more peaceful and sustainable future* .[5] This Declaration reaffirms the IPU member states' commitment to harnessing the National Technology Initiative to achieve peace, sustainable development, and human rights protection. While acknowledging the rapid progress of new technologies, the Declaration stresses the need for responsible and ethical use that includes the interests of all segments of society. Particular attention is given to gender equality, inclusive participation of youth and vulnerable groups, respect for human rights, and digital security.

Second. **The Resolution on "The Impact of AI on Democracy, Human Rights, and the Rule of Law**".[6] This Resolution highlights that AI presents both opportunities and risks for contemporary society. Parliamentarians noted that AI can enhance transparency and accountability in government, improve access to information, and promote public engagement in political processes. Nonetheless, they voiced concerns that AI may also contribute to the spread of disinformation, discrimination, and heightened social inequality. The Resolution calls for establishing a legal framework that promotes responsible AI use, with transparency, accountability, and human rights protection as guiding principles. It further underscores the need for international cooperation to develop standards that regulate AI without stifling innovation, and for an inclusive approach to AI that takes into account gender considerations and the prevention of bias and discrimination.

Third. **The IPU Charter on Ethics of Science and Technology**.[7] This Charter is designed as guidance for parliaments on the ethical use of

[5] Inter-Parliamentary Union. Geneva Declaration: Harnessing science, technology and innovation (STI) for a more peaceful and sustainable future. 2024. Available at: https://www.ipu.org/file/20059/download (accessed: 05.03.2025)

[6] Inter-Parliamentary Union. The Impact of Artificial Intelligence on Democracy, Human Rights and the Rule of Law. Resolution unanimously adopted by the 149th IPU Assembly (Geneva, 17 October 2024). Available at: https://www.ipu.org/file/20059/download https://www.ipu.org/file/20061/download (accessed: 05.03.2025)

[7] Inter-Parliamentary Union. IPU Charter on Ethics of Science and Technology // Inter-Parliamentary Union, 149th Assembly, 13–17 October 2024. Available at: https://www.ipu.org/file/19917/download (accessed: 06.03.2025)

scientific and technological advances, including AI. It underscores the importance of an inclusive and responsible approach to the National Technology Initiative one aimed at fulfilling the goals of sustainable development and strengthening democratic institutions. The Charter sets forth principles that must guide the use of technology: respect for human rights, fairness, transparency, and the prevention of any form of discrimination. It supports initiatives to develop international standards for AI and related technologies, and calls for intensified inter-parliamentary cooperation. Parliaments worldwide pledged to promote these principles within their respective countries, facilitating ethical governance of the National Technology Initiative for a more inclusive and sustainable future.

The 149th IPU Assembly thus became a crucial milestone in shaping global approaches to governing scientific and technological breakthroughs. By adopting the Geneva Declaration, the Resolution on AI, and the IPU Charter, the international community demonstrated its commitment to inclusive and ethical technological development, particularly with respect to AI. The 149th IPU Assembly underscored that international collaboration and shared ethical standards are indispensable in ensuring that digital technologies serve humanity rather than pose new threats and barriers.

Similarly, the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+ of 2018)[8] represents one of the strongest international frameworks addressing data protection and digital privacy issues. Additionally, the Council of Europe has elaborated the Budapest Convention on Cybercrime (2001),[9] establishing international cooperation mechanisms for addressing cybercrime and protecting citizens from digital abuses.

The most important and influential model of digital human rights protection is the European Union (EU). The EU's **General Data Protection Regulation** (GDPR, 2016)[10] has had a significant impact on glob-

[8] Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108, 28.01.1981); Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+). Strasbourg, 10.10.2018 // Council of Europe Treaty Series, No. 223.

[9] Convention on Cybercrime (Budapest Convention). Budapest, 23.11.2001 // Council of Europe Treaty Series, No.185.

[10] Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union. L 119/1. 27 April 2016.

al digital human rights protection practices, emphasizing strong data protection, privacy standards and strict corporate responsibility. The GDPR emphasizes informed consent, transparency in data handling, users' rights to access and delete personal data, and penalties for violations, setting global precedents. In addition, the EU **Digital Services Act** (DSA, 2022)[11] establishes broad obligations for online platforms, focusing on accountability, transparency of algorithmic decisions, and prevention of digital discrimination. These comprehensive measures represent significant progress in protecting human rights against algorithmic bias and digital misinformation.

The EU has been a leader in digital regulation through its ambitious **AI Act**, which was adopted by the European Parliament on March 13, 2024, and later approved by the Council of the European Union on May 21, 2024.[12] The AI Act introduces a risk-based classification system, distinguishing AI applications into prohibited, high-risk, limited-risk, and minimal-risk categories. High-risk AI applications, such as biometric surveillance and AI-driven healthcare decisions, are subjected to stringent transparency and accountability measures. The EU's approach aims to balance technological innovation with fundamental rights protection, ensuring that AI developments do not compromise privacy, freedom of expression, or non-discrimination principles.

Furthermore, in September 2024, the EU, along with the United States and the United Kingdom, has signed the **Framework Convention on Artificial Intelligence**, a legally binding treaty developed by the Council of Europe. This treaty aims to ensure that AI is used in ways that align with **human rights**, **democracy**, and the **rule of law**, mandating the protection of user data, adherence to legal standards, and transparency in AI practices.

The OECD has developed its own regulatory framework for AI, known as the **OECD AI Principles**.[13] These principles, endorsed by 38 member countries, including Brazil and Russia, advocate for transparent, ac-

[11] Regulation (EU) 2022/2065 on a Single Market for Digital Services (Digital Services Act). Official Journal of the European Union. L 277/1. 19 October 2022.

[12] European Union. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L 277, pp. 1–78. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689 (accessed: 13.03.2025)

[13] Organization for Economic Cooperation and Development. AI Principles overview. Available at: https://oecd.ai/en/ai-principles (accessed: 16.03.2025)

countable, and fair AI systems. The OECD approach is unique in that it emphasizes AI's role in promoting inclusive economic growth while ensuring that AI applications do not contribute to discrimination or social inequalities. Unlike the legally binding EU AI Act or the Council of Europe's AI Convention, the OECD AI Principles function as policy guidelines, offering best practices that governments and industries can adopt voluntarily.[14]

The OECD has addressed the implications of digital transformation on human rights through various initiatives. In its report "Rights in the Digital Age: Challenges and Ways Forward," the OECD examines how digitalization affects internationally recognized human rights and proposes strategies to address these challenges. The report emphasizes the need for policies that protect privacy, prevent discrimination, and ensure equitable access to digital technologies.[15]

Furthermore, the OECD's "Shaping a Rights-Oriented Digital Transformation" report highlights the importance of integrating human rights considerations into digital policies. It advocates for a human-centric approach to digitalization, ensuring that technological advancements do not infringe upon fundamental rights and freedoms.[16]

The United Nations has been at the forefront of promoting global ethical standards for AI and digital governance. In 2021, UNESCO has released the **Recommendation on the Ethics of Artificial Intelligence**,[17] which became a landmark international standard emphasizing the protection of human rights, fostering sustainable development, and ensuring transparency in AI applications.[18] This recommendation calls for AI governance frameworks that respect human dignity and promote inclusive access to AI benefits. UNESCO's approach aligns with the UN's broader goal of leveraging AI for the Sustainable Development Goals

[14] Ibid.

[15] OECD. Rights in the digital age. Paris, 2022. Available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/12/rights-in-the-digital-age_d3a850de/deb707a8-en.pdf (accessed: 16.03.2025)

[16] OECD. 2024. Shaping a rights-oriented digital transformation // OECD Digital Economy Papers. No. 368. Available at: https://doi.org/10.1787/86ee84e2-en (accessed: 16.03.2025)

[17] UNESCO Recommendation on the Ethics of Artificial Intelligence. Paris, 2021. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000380455 (accessed: 01.03.2025)

[18] Ibid.

(SDGs), particularly in areas such as reducing inequalities, improving healthcare, and enhancing educational access.[19]

UN Secretary-General António Guterres has consistently stressed the need for an internationally coordinated AI regulatory framework. Speaking at the AI Safety Summit in London on November 2, 2023, he asserted that **"The principles for AI governance should be based on the United Nations Charter and the Universal Declaration of Human Rights"**.[20] This statement reinforces the UN's commitment to ensuring that AI advancements do not undermine fundamental freedoms but rather contribute to global peace and security.

The Council of Europe (CoE) has also taken an active stance on AI regulation, emphasizing human rights compliance in digital governance. In 2024, the CoE adopted **the Framework Convention on Artificial Intelligence**, **Human Rights, Democracy, and the Rule of Law**,[21] marking the first legally binding treaty on AI ethics. The convention mandates that all member states integrate AI regulatory policies that respect democracy and human dignity. Unlike other voluntary guidelines, this treaty imposes legal obligations on states, making it a robust mechanism for AI governance. It has gained support from **57 countries**, including non-CoE members such as the United States and Japan, demonstrating a global commitment to ethical AI use.

An analysis of international frameworks for AI governance and digital regulation reveals several key similarities and differences among the UNESCO AI Ethics Recommendation, Council of Europe AI Convention, EU AI Act, and OECD AI Principles. Each of these frameworks aims to balance technological innovation with human rights protection, democratic values, and regulatory efficiency, but they differ in terms of legal enforceability, risk assessment, and global adoption.

[19] UNESCO. 2022. Leveraging innovative AI solutions to address SDGs. Available at: https://www.unesco.org/en/articles/leveraging-innovative-ai-solutions-address-sdgs (accessed: 03.03.2025)

[20] Guterres A. Secretary-General's statement at the UK AI Safety Summit. United Nations Secretary-General, 2023. 2 November. Available at: https://www.un.org/sg/en/content/sg/statement/2023-11-02/secretary-generals-statement-the-uk-ai-safety-summit (accessed: 19.03.2025)

[21] Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law // CETS No. 225. 2024. Available at: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=225 (accessed: 09.03.2025)

First, all frameworks place a strong emphasis on human rights, privacy, and transparency in AI governance. The UNESCO AI Ethics Recommendation, Council of Europe AI Convention, and EU AI Act explicitly integrate human rights safeguards into their regulatory frameworks. They ensure that AI technologies comply with fundamental rights obligations such as freedom of expression, data privacy, and non-discrimination. The OECD AI Principles also promote responsible AI development, though they focus more on economic growth and technological advancement rather than explicitly prioritizing human rights concerns. The UN has further reinforced the human rights-centered approach through initiatives that promote the ethical use of AI in achieving Sustainable Development Goals (SDGs), particularly in areas such as education, healthcare, and social equality.

Second, there is a significant difference between legally binding regulations and voluntary standards. The EU AI Act and the Council of Europe AI Convention establish binding legal obligations, requiring member states to enact national regulations that align with these international frameworks. These laws impose strict compliance measures, enforceable through legal penalties for non-compliance. In contrast, the UNESCO AI Ethics Guidelines and OECD AI Principles function as soft law instruments, providing non-binding recommendations for governments and industries. While these guidelines influence policy development, they do not impose direct legal consequences for violations.

Third, the regulatory approaches vary in how they categorize and mitigate risks associated with AI applications. The EU AI Act follows a risk-based classification system, dividing AI applications into prohibited, high-risk, limited-risk, and minimal-risk categories. This tiered regulation ensures that AI applications used in critical sectors such as healthcare, law enforcement, and financial services meet rigorous transparency and accountability standards. The Council of Europe AI Convention also incorporates a risk-management approach, emphasizing the potential human rights implications of AI deployment. Conversely, the UNESCO AI Ethics Guidelines and OECD AI Principles adopt a broader ethical framework, focusing on guiding principles rather than establishing specific risk categories. As a result, the EU's AI Act provides stronger enforcement mechanisms, while the UNESCO and OECD frameworks leave risk assessments largely to individual stakeholders.

Fourth, the implementation mechanisms differ significantly. The Council of Europe AI Convention mandates that signatory states incorporate AI governance standards into national legislation, ensuring legal consistency across jurisdictions. The EU AI Act, as a direct regulation, requires immediate implementation across all EU member states, with specific provisions for AI developers and deployers. In contrast, the OECD AI Principles encourage self-regulation, allowing governments and industries to voluntarily adopt best practices. While this flexibility promotes innovation, it also raises concerns about inconsistent enforcement and corporate accountability.

Fifth, the degree of global adoption varies across these frameworks. The EU AI Act and Council of Europe AI Convention have been widely adopted in Europe and have influenced regulatory discussions in countries such as Canada, Australia, and Japan. The Council of Europe AI Convention is particularly notable because it has gained support from non-European nations, including the United States and Japan, demonstrating its broader international relevance. Meanwhile, the UNESCO AI Ethics Guidelines and OECD AI Principles enjoy wider global endorsement, particularly from Latin America, Africa, and Asia. This broader adoption is largely due to their voluntary nature, making them more accessible for developing nations that may lack the regulatory capacity to enforce strict AI laws [Mantelero A., 2018: 757].

L. Floridi and J. Cowls propose a unified ethical framework for AI that includes principles of beneficence, non-maleficence, autonomy, justice, and explicability principles increasingly referenced in international instruments [Floridi L. and Cowls J., 2019: 5–10].

Overall, while these international frameworks share a common goal of responsible AI governance, their differences in enforceability, risk assessment, and global adoption highlight the challenges of harmonizing digital regulations across jurisdictions. The EU's approach is characterized by strict legal enforcement, ensuring compliance through legally binding rules. The Council of Europe's AI Convention promotes intergovernmental cooperation, providing a structured legal framework for AI oversight. In contrast, UNESCO's ethical guidelines and OECD's policy principles prioritize flexibility and voluntary adoption, allowing nations and industries to adapt AI governance measures at their own pace.

As AI continues to evolve, the need for global cooperation and standardization becomes increasingly urgent. Future regulatory developments are likely to focus on enhancing transparency, strengthening enforcement mechanisms, and promotion international collaborations to address emerging AI challenges.

2. Foreign Experience in Digital Human Rights Protection

In the digital age, the protection of human rights — from privacy and freedom of expression to data protection — has become a pressing issue for states around the world. This part examines how different regions and governments are responding to these challenges by establishing legal frameworks and practices aimed at protecting digital human rights. Drawing on comparative analyses of experiences in Europe, North America, Asia and Latin America, both innovative approaches and the tensions between security imperatives and individual freedoms are discussed.

In Europe, the European Union has emerged as a frontrunner by adopting a comprehensive regulatory framework that sets high standards for data protection. The **General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)**[22] has become a global benchmark by enforcing stringent obligations on the processing of personal data and empowering citizens with robust rights over their digital information. This framework is complemented by the Charter of Fundamental Rights of the European Union,[23] as well as longstanding instruments such as the European Convention on Human Rights (ECHR)[24] and the International Covenant on Civil and Political Rights (ICCPR),[25] which together create a solid foundation for protecting privacy and other digital rights.

Across the Atlantic, the United States offers a contrasting approach. Rooted in constitutional traditions that emphasize free speech and civil liberties, the U.S. legal landscape faces the challenge of balancing national security with individual rights. Landmark judicial decisions most notably in *Carpenter v. United States*[26] illustrate the evolving nature of digital surveillance under the U.S. Constitution's Fourth Amendment. Complementing these decisions are legislative measures such as the

[22] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L 119, 2016.

[23] Charter of Fundamental Rights of the European Union. Official Journal of the European Union, C 364/01, 2000.

[24] European Convention on Human Rights. Council of Europe, 1950.

[25] International Covenant on Civil and Political Rights (ICCPR). United Nations, 1966.

[26] Carpenter v. United States, 138 S. Ct. 2206 (2018).

USA PATRIOT Act,[27] as well as foundational statutes like the Electronic Communications Privacy Act (ECPA)[28] and the Computer Fraud and Abuse Act[29] (CFAA), which together frame the nation's efforts to address digital privacy and cybersecurity.

In Asia, diverse national contexts have led to markedly different regulatory responses. Japan's Act on the Protection of Personal Information[30] (APPI) and South Korea's Personal Information Protection Act[31] (PIPA) exemplify legal frameworks designed to foster secure digital environments without unduly limiting individual freedoms. These statutes reflect a commitment to adapting privacy protections in step with technological change. Conversely, in China, the Cybersecurity Law of the People's Republic of China[32] establishes a framework that prioritizes state control and social stability over the broad spectrum of digital rights found in democratic societies. This divergence within the region highlights the importance of cultural, political, and historical factors in shaping digital rights policies.

Latin America also plays a significant role in the global mosaic of digital human rights protection. In Brazil, the Lei Geral de Proteção de Dados[33] (LGPD) inspired in part by the European GDPR model marks a milestone in the modernization of data protection law. This legislative reform, driven by both domestic pressures and international trends, underscores the role of grassroots advocacy and progressive legal change in protecting citizens' digital rights in an era of rapid technological evolution.

The Russian Federation has actively developed its legal framework to address the challenges and opportunities presented by digital transformation. A cornerstone of this effort is the national program "Digital Economy of the Russian Federation," approved by Government Order No. 1632-r on July 28, 2017.[34] This program aims to create conditions for

[27] USA PATRIOT Act of 2001, Pub. L. 107–156, 115 Stat. 272 (2001).

[28] Electronic Communications Privacy Act (ECPA) of 1986, United States.

[29] Computer Fraud and Abuse Act (CFAA), United States, 1986.

[30] Act on the Protection of Personal Information (APPI), Japan, Act No. 57 of 2003.

[31] Personal Information Protection Act (PIPA), South Korea, enacted 2011 (with subsequent amendments).

[32] Cybersecurity Law of the People's Republic of China, effective 1 June 2017.

[33] Lei Geral de Proteção de Dados (LGPD), Law No. 13,709, 14 August 2018 (Brazil).

[34] Government Order No. 1632-r of July 28, 2017. Digital Economy of the Russian Federation.

the development of digital technologies, enhance economic competitiveness, and ensure national security. A significant legislative milestone was the adoption of Federal Law No. 34-FZ on March 18, 2019, which has introduced the concept of "digital rights" into Russian civil law.[35] These rights are defined as obligations and other rights, the content and conditions of which are determined in accordance with the rules of an information system. This legal recognition provides a foundation for regulating relationships arising in the digital environment. Academician Taliya Khabrieva emphasizes that digitalization profoundly influences constitutional modernization. According to her analysis, the proliferation of information and communication technologies has reshaped social and economic realities, compelling legal institutions to evolve correspondingly. She notes the necessity for a comprehensive modernization of constitutional norms to ensure effective regulation in this new digital age. Digital transformation requires adjusting traditional legal tools to address newly emerging issues, such as data privacy, digital identities, and cybersecurity, thus safeguarding fundamental human rights and freedoms in digital environments [Khabrieva T.Ya., 2019].

Ilya Rassolov highlights the complexities introduced by Internet law, advocating for a specialized legal framework addressing the nuanced dynamics of digital interactions. Rassolov identifies critical areas such as digital property, network contracts (smart contracts), and digital traces, emphasizing the importance of clear legal definitions and standards to enhance cybersecurity and data protection. He argues for international cooperation to effectively manage jurisdictional challenges arising from the borderless nature of cyberspace [Rassolov I., 2022].

Additionally, Russia has been proactive in developing legislation on cybersecurity and personal data protection. Federal Law No. FZ-152 "On Personal Data" and Federal Law No. FZ-149 "On Information, Information Technologies, and Information Protection"[36] establish the foundation for safeguarding citizens' privacy amid the widespread use of information systems and the internet.

Despite distinct political, cultural, and legal contexts, states worldwide face similar digital-era dilemmas: (1) bridging legislative gaps to

[35] Federal Law No. FZ-34 of March 18, 2019 On Amendments to Parts One, Two and Article 1124 of Part Three of the Civil Code of the Russian Federation // SPS Consultant Plus.

[36] Federal Law No. 152-FZ "On Personal Data" and Federal Law No. 149-FZ "On Information, Information Technologies, and Information Protection" // SPS Consultant Plus.

keep pace with rapid tech innovation; (2) reconciling national security imperatives with civil liberties; and (3) ensuring that citizens can exercise their rights in a global, networked environment. The need for agile, forward-looking policies is evident in both democratic and more centralized systems, as evidenced by debates in the United States and Europe alike.

Moreover, balancing national security imperatives with individual rights remains an enduring struggle. Effective oversight of digital surveillance and data collection is crucial to prevent the erosion of civil liberties. International legal instruments, such as the Budapest Convention on Cybercrime and various EU directives,[37] serve as important tools for fostering cross-border cooperation and ensuring that security measures do not undermine human rights [De Gregorio G., 2021: 44–46].

In conclusion, protecting digital human rights is a multifaceted challenge that requires coordinated and dynamic responses at both national and international levels. Experience in Europe, North America, Asia and Latin America suggests that while no single model can solve all complex problems, each provides valuable insights into creating an effective legal framework for the digital age.

3. Legal Framework for Digital Human Rights Protection in Uzbekistan

On November 18, 2024, in Tashkent, the first post-election session of the Legislative Chamber of the Oliy Majlis of the Republic of Uzbekistan (Parliament) was held with the participation of President Shavkat Mirziyoyev. In his address, the President emphasized that legislative initiatives should primarily address pressing societal issues and proposed a range of reforms. His proposals included constructing modern residential buildings to replace outdated housing, guaranteeing the protection of citizens' funds allocated for housing construction, and supporting investors in the private education and electric power sectors. He also underlined the need to implement compulsory health insurance and to establish legal frameworks for the application of **emerging technologies**

[37] Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995; Directive (EU) 2016/1148 on the security of network and information systems (NIS Directive), European Parliament and Council, 2016.

such as artificial intelligence, as well as for the regulation of franchising, the capital market, and startups. This forward-looking agenda signals that, in the near future, Uzbekistan will develop specific legislation to integrate artificial intelligence more broadly across sectors including the economy, healthcare, and education, reinforcing the nation's commitment to an innovative and technologically advanced economy.[38]

These legislative proposals come at a time when Uzbekistan is actively reforming its legal framework to safeguard digital human rights and support digital transformation.

A legal framework for digital transformation is currently being formed. **The Strategy "Digital Uzbekistan — 2030" has been adopted**.[39] Moreover, the President of Uzbekistan Shavkat Mirziyoyev has repeatedly emphasized that Uzbekistan needs to be transformed into a regional IT center.

At the same time, the country's digitalization processes, according to international standards, should be based on a human rights approach. All concepts in other areas also pay special attention to the introduction and widespread use of digital technologies.

The Ministry of Health of Uzbekistan has developed a Strategy for the Digitalization of the Healthcare System for 2021–2025 (E-Health-2025).[40] **The concept of development of higher education in Uzbekistan until 2030 provides** for measures to introduce digital technologies into the educational process.[41]

It is important to note that the **Constitution of the New Uzbekistan** has enshrined new trends in the field of ensuring and protecting human rights in the digital age. Article 33 of the updated Constitution of the Republic of Uzbekistan states that "The state creates conditions for ensuring access to the global information network Internet." In addition,

[38] President of the Republic of Uzbekistan. President participates in the session of the Legislative Chamber. Official Website of the President of Uzbekistan, 18 November 2024. Available at: https://president.uz/en/lists/view/7711 (accessed: 18.03.2025)

[39] Strategy "Digital Uzbekistan–2030." Available (in Uzbek/Russian) at: https://lex.uz/docs/5031048 (accessed: 18.03.2025)

[40] Strategy for the Digitalization of the Healthcare System for 2021–2025 (E-Health-2025). Available at: https://lex.uz/ru/docs/5434367 (accessed: 17.03.2025)

[41] The text of the document is available at: https://lex.uz/ru/docs/4545887 (accessed: 15.03.2025)

Article 53 of the Constitution stipulates that "Everyone is guaranteed freedom of scientific, technical and artistic creativity, the right to use cultural achievements."[42]

Particular attention is paid to the implementation of information and communication tools in the **National Strategy of the Republic of Uzbekistan on Human Rights**.[43] Thus, the Strategy provides for provisions regarding the development of a draft Information Code of the Republic of Uzbekistan in order to systematize access to information as one of the most important factors in the development of civil and information society, ensuring the protection of human rights in the information space, cybersecurity, compliance with media culture and online hygiene. The Law of the Republic of Uzbekistan dated 15.04.2022 No. ZRU-764 "On Cybersecurity" was adopted.[44] The laws "On guarantees and freedom of access to information", "On the protection of personal data", "On the protection of children from information harmful to health" and others have been adopted. The law "On appeals of individuals and legal entities" has been adopted in a new edition, which enshrines the concept of "electronic appeal". The law enshrines the right to appeal in electronic form, which can facilitate the appeal procedure. An important step was the adoption of the Law of the Republic of Uzbekistan "On personal data" in 2019.[45] According to the Law, the state guarantees the protection of personal data. The owner and (or) operator, as well as a third party, take legal, organizational and technical measures to protect personal data, ensuring:

implementation of the subject's right to protection from interference in his private life;

integrity and safety of personal data;

compliance with the confidentiality of personal data;

prevention of illegal processing of personal data.

According to this law, the confidentiality of personal data is a mandatory requirement for the owner and (or) operator or other person who has gained access to personal data on the inadmissibility of their disclo-

[42] The text of the document is available at: https://lex.uz/docs/6445147 (accessed: 17.03.2025)

[43] The text of the document is available at: https://lex.uz/ru/docs/4872357 (accessed: 17.03.2025)

[44] The text of the document is available at: https://lex.uz/ru/docs/5960609 (accessed: 19.03.2025)

[45] The text of the document is available at: https://lex.uz/docs/4396428 (accessed: 19.03.2025)

sure and distribution without the consent of the subject or the presence of other legal grounds. The owner and (or) operator and other persons who have gained access to personal data are obliged not to disclose or distribute personal data without the consent of the subject.

The adoption of the **Law of the Republic of Uzbekistan "On the Protection of Children from Information Harmful to Their Health"** is of particular importance in modern realities.[46] According to this law, the main directions of state policy in the field of protecting children from information harmful to their health are:

creation of legal, socio-economic, organizational and technical conditions that ensure the protection of children from information harmful to their health, as well as the development of scientific and applied research in this area;

prevention of illegal information and psychological influence on the consciousness of children, manipulation of them, distribution of information products that provoke children to antisocial actions, as well as prevention of offenses in this area;

support for the activities of self-government bodies of citizens, non-governmental non-profit organizations, other institutions of civil society, individuals and legal entities in the field of protecting children from information harmful to their health;

development and improvement of criteria, mechanisms and methods for classifying information harmful to children's health, the introduction of hardware, software and technical means to ensure information security for children.

It is important to develop legislation on protection from cyber violence. The first steps in this direction have already been taken. Thus, in particular, in the field of protecting women from violence**. The Law of the Republic of Uzbekistan "On the Protection of Women from Harassment and Violence"** stipulates that "stalking is an action committed against the will of the victim, despite two or more of her resistance or warnings, expressed in searching for the victim, communicating with her orally, through telecommunications networks, including through the Internet, or by using other methods, visiting her place of work, study and (or) residence, and causing the victim to fear for her safety.[47]

[46] The text of the document is available at: https://lex.uz/docs/3333805 (accessed: 17.03.2025)

[47] The text of the document is available at: https://lex.uz/docs/4494712 (accessed: 18.03.2025)

The Code of the Republic of Uzbekistan on Administrative Responsibility contains Article 462 (Violation of legislation on personal data).[48] According to the article, illegal collection, systematization, storage, modification, addition, use, provision, distribution, transfer, depersonalization and destruction of personal data, as well as failure to comply with the requirements for the collection, systematization and storage of personal data on technical means physically located on the territory of the Republic of Uzbekistan, and in personal data bases registered in the established manner in the State Register of Personal Data Bases, when processing personal data of citizens of the Republic of Uzbekistan using information technologies, including the Internet, shall entail a fine for citizens in the amount of seven, and for officials — fifty basic calculation units.

Also, Article 202^{2} (Dissemination of false information) is enshrined in this code. According to the article, "Dissemination of false information, including in the media, telecommunications networks or the Internet, leading to humiliation of the dignity of the individual or discrediting the individual, shall entail a fine in the amount of fifty basic calculation units."

Amendments have also been made to **the Criminal Code of the Republic of Uzbekistan**.[49] Thus, according to Article 139, "Slander in printed or otherwise reproduced form, including that posted in the media, telecommunications networks or the Internet, is punishable by a fine of two hundred to four hundred basic calculation units or compulsory community service from three hundred to three hundred sixty hours or correctional labor from two to three years or restriction of freedom for up to one year." Article 1412 of the Criminal Code establishes liability for violating legislation on personal data. According to the article, "illegal collection, systematization, storage, modification, addition, use, provision, distribution, transfer, depersonalization and destruction of personal data, as well as failure to comply with the requirements for the collection, systematization and storage of personal data on technical means physically located on the territory of the Republic of Uzbekistan and in personal data bases registered in the established manner in the State Register of Personal Data Bases, committed after the application

[48] The text of the document is available at: https://lex.uz/acts/97661 (accessed: 18.03.2025)

[49] The text of the document is available at: https://www.lex.uz/acts/111457 (accessed: 16.03.2025)

of an administrative penalty for the same actions, shall be punishable by a fine of one hundred to one hundred and fifty basic calculation units or deprivation of a certain right for up to three years or correctional labor for up to two years." Article 1413 provides for liability for disclosure of information that infringes the honor and dignity of an individual and reflects the intimate aspects of a person's life. According to the article, dissemination of information containing photos and (or) video images of a naked body and (or) genitals of a person without his consent, including dissemination in the media, telecommunications networks or the World Wide Web, or the threat of dissemination of such information shall be punishable by a fine of four hundred to six hundred basic calculation units or compulsory community service for up to three hundred sixty hours or correctional labor for up to three years. The same actions committed repeatedly or by a dangerous recidivist; by prior conspiracy by a group of persons; in relation to a person who the perpetrator clearly knows has not reached the age of eighteen, shall be punishable by compulsory community service from three hundred sixty to four hundred eighty hours or restriction of liberty from one year to three years or imprisonment for up to three years. According to Article 246 of the Criminal Code of The Russian Federation (Dissemination of False Information), dissemination of false information, including in the media, telecommunications networks or the Internet, which results in the humiliation of personal dignity or discrediting of a person, committed after the application of an administrative penalty for the same actions, shall be punishable by a fine of up to one hundred and fifty basic calculation units or mandatory community service for up to two hundred and forty hours or correctional labor for up to two years or restriction of freedom for up to two years. Dissemination of false information, including in the media, telecommunications networks, the Internet, which contains a threat to public order or security, in the absence of elements of a crime provided for in Article 2441 of this Code, committed after the application of an administrative penalty for the same actions, shall be punishable by a fine of up to two hundred basic calculation units or mandatory community service for up to three hundred hours or correctional labor for up to two years or restriction of freedom for up to two years. Changes in connection with digitalization have also been made to the Labor Code of the Republic of Uzbekistan.[50] Thus, Articles 452-464 of the Labor Code are devoted to the specifics of regulating remote work. According to Article

[50] The text of the document is available at: https://lex.uz/ru/docs/6257291?ONDATE2=30.04.2023&action=compare (accessed: 18.03.2025)

452, remote work is the performance of a labor function specified in the employment contract outside the location of the employer, a separate division of the organization (including those located in another locality), outside a stationary workplace, territory or facility directly or indirectly under the control of the employer, provided that information and telecommunications networks, including the World Wide Web, are used to perform this labor function and to interact between the employer and the employee on issues related to its performance. According to Article 456, in addition to the conditions, the following conditions are also included in the employment contract with a remote employee:

remote work schedule — the number and frequency of providing working days and working hours to the employee in the remote work mode;

methods of exchanging information between the parties on production tasks and their implementation;

periods of work at a stationary workplace and remote work, as well as the procedure for alternating them when a combined remote work mode is established;

the procedure for providing a remote worker with equipment and (or) office equipment, if the remote worker needs the appropriate equipment and (or) office equipment to perform his/her work function, except for cases when the parties have agreed that the remote worker can use the equipment and (or) office equipment that he/she owns or leases;

employer's obligations to repair the equipment and (or) office equipment transferred to the remote worker for him/her to perform the work function stipulated by the employment contract;

providing the employee with the necessary means of communication for regular interaction with the employer, including access to the World Wide Web;

conditions for compensation by the employee for damage caused to the employer through his/her fault, related to damage to the equipment and (or) office equipment transferred by the employer to the remote worker;

the procedure for conducting an inventory of the equipment, office equipment, software and hardware, communication tools, information security tools and other tools transferred for use to the remote worker;

the procedure and conditions for reimbursement of expenses to a remote worker in the event of the use of his/her own equipment and (or) office equipment to perform work duties;

the procedure and conditions for reimbursement of expenses to a remote worker in connection with the use of communication facilities to perform work duties;

the procedure for interaction between a remote worker and an employer through the exchange of electronic documents;

obligation of a remote worker to notify the employer in the event of the impossibility of performing the work stipulated by the production assignment within the timeframes established by the employment contract, indicating the reason preventing its timely completion;

obligations of the employer and the remote worker to comply with the necessary rules for safety and working conditions.

According to Article 462 of the **Labor Code**, the duration of the annual labor leave of a remote worker may not be less than twenty-one calendar days, unless he/she, in accordance with labor legislation, other legal acts on labor or an employment contract, has the right to an annual labor leave of a longer duration. The procedure for granting a remote worker an annual leave and other types of leave shall be determined by the employment contract for remote work in accordance with this Code and other legal acts on labor.

The remote worker shall be paid for the time actually worked under the time-based remuneration system, and for the actual volume of work performed under the piecework remuneration system. Output standards and piecework rates shall be established by agreement of the parties to the employment contract based on the normal working hours established in accordance with labor legislation for the performance of work. The amount of remuneration for the remote worker shall be comparable with the terms of remuneration for workers employed at the employer's production facility. The remuneration for the remote worker may not be lower than the minimum wage established by law, provided that he or she fulfills labor standards and labor duties, and is not limited by any maximum amount. If a regional coefficient for wages has been established in the area where the remote worker carries out his or her work, the remuneration for the remote worker shall be made taking into account this coefficient.

Changes have also been made to the legislation on education. Thus, Article 16 of the Law of the Republic of Uzbekistan establishes the concept of distance education. According to this article, distance education is aimed at providing students with the necessary knowledge, skills and abilities in accordance with curricula and educational programs at a distance using information and communication technologies and the

Internet. The law also provides for an article regarding the openness and transparency of the activities of educational organizations. According to Article 27 of the Law, the openness and transparency of the activities of educational organizations are ensured by open information resources about the activities of educational organizations, posted on their official websites on the Internet.

Particular attention is paid to digitalization issues in the judicial and legal sphere. The Resolution of the President of the Republic of Uzbekistan "On measures to digitalize the activities of judicial authorities" dated September 3, 2020 is also important in defining long-term tasks to improve the efficiency of the judicial system, ensure openness and transparency of the court for the population. Digitalization of the judicial system should ensure even more effective protection of human rights. The widespread introduction of modern information and communication technologies in the activities of courts, along with the expansion of the scale of interactive services provided to the population and business entities, increases both the efficiency of office work and the mobility of consideration of court cases.[51]

Digitalization allows courts to automate many processes related to the consideration of cases. Now judges can send subpoenas and documents electronically, which significantly saves time and effort. Electronic queues for the consideration of cases have also been introduced, which allows for a more even distribution of the workload among judges. One of the main advantages of digitalization is the ability to hold online court hearings. Now participants in the process can attend the hearing, being in different cities or even countries. This significantly simplifies access to justice and makes the judicial system more open and transparent. In addition, digitalization allows courts to more effectively monitor the execution of court decisions. The system automatically tracks the status of the execution of decisions and reminds about the need to implement them. This helps prevent abuses and increases trust in the judicial system. In general, the digitalization of the judicial system of Uzbekistan is an important step in the development of the legal sphere of the country. It allows for an increase in the efficiency of the courts, a faster and fairer consideration of cases, and a more accessible and transparent judicial system for citizens.[52]

[51] The text of the document is available at: https://lex.uz/ru/docs/4979899 (accessed: 18.03.2025)

[52] Каюмов Б. Будущее цифровой судебной системы Узбекистана: новые вызовы и перспективы. 04.07.2023 // https://uztrend.uz/wordpress/archives/3661 (accessed: 20.03.2025)

In the context of digitalization, the role of legislation in the field of information, informatization and media is increasing. **The Law of the Republic of Uzbekistan "On the principles and guarantees of freedom of information" enshrines the concept of "information security"**.[53] According to the law, information security is the state of protection of the interests of the individual, society and the state in the information sphere. According to this law, state authorities and administration bodies, citizens' self-government bodies, public associations and other non-governmental non-profit organizations and officials are obliged, in the manner prescribed by law, to provide everyone with the opportunity to familiarize themselves with information affecting their rights, freedoms and legitimate interests, create accessible information resources, carry out mass information support for users on issues of the rights, freedoms and obligations of citizens, their security and other issues of public interest. Article 12 of the Law stipulates that the state policy in the field of ensuring information security is aimed at regulating public relations in the information sphere and defines the main tasks and areas of activity of state authorities and administration, as well as the place and role of self-governing bodies of citizens, public associations and other non-governmental non-profit organizations, citizens in the field of ensuring information security of the individual, society and the state. Of particular importance is Article 13, according to which "Information security of the individual is ensured by creating the necessary conditions and guarantees of free access to information, protecting privacy, and protecting against illegal information and psychological influences. Information about the personal data of individuals is classified as confidential information." The Law stipulates that the collection, storage, processing, distribution and use of information about private life, as well as information that violates the privacy of private life, the secrecy of correspondence, telephone conversations, postal, telegraph and other messages of an individual without his consent, except in cases established by law, is not allowed. It is prohibited to use information about individuals for the purpose of causing them material and moral damage, as well as obstructing the exercise of their rights, freedoms and legitimate interests. Legal entities and individuals who receive, own and use information about citizens bear liability under the law for violating the procedure for using this information. Mass media do not have the right to disclose the source of information or the author who signed with a pseudonym

[53] The text of the document is available at: https://lex.uz/docs/52709 (accessed: 15.03.2025)

without their consent. The source of information or the name of the author may be disclosed only by a court decision. These provisions of the law are important for the protection of personal data.

Among the measures taken, the following measures can also be mentioned:

creation of websites of all government agencies and departments, which expands access to information;

creation of the www.regulation.gov.uz platform, where draft regulatory legal acts are posted, on which the public can express its opinion;

creation of the "Mening fikrim" website, where citizens can put forward their initiatives to improve legislation or public policy;

creation of an electronic justice system (E-sud) for appeals to courts, which helps save time and financial costs for citizens in the event of the need to go to court to protect their rights; — expansion of the system of providing free legal assistance to the population, the capabilities of the legal information system "Advice.uz", as well as support for the non-governmental non-profit organization "Madad", which provides citizens with free legal advice.

Particular attention is paid to training and developing digital skills. The above measures contribute to the promotion and protection of human rights in the country. In addition to measures to overcome the digital divide at the global level, it is important to take measures to bridge the gap at the national level. As the former UN High Commissioner for Human Rights Michelle Bachelet noted, "we need to work together — human rights lawyers, computer scientists and engineers, representatives of businesses and governmental and inter-governmental bodies — to develop human rights impact assessment methodologies, and other systems for analysis and guidance, which can address the specific requirements of digital systems.... Above all, the duty to protect human rights need to be an explicit priority for all stakeholders — States, developers, scientists, investors, business and civil society."[54]

Uzbekistan's legislative approach to digitalization includes human rights considerations at all stages, and the human rights legal framework also recognises the impact and potential of new digital technologies. In line with global trends, Uzbekistan is modernising its legislation to take

[54] Speech at the University of Geneva by UN High Commissioner for Human Rights Michelle Bachelet. November 14, 2018. Available at: https://www.ohchr.org/en/statements/2018/11/human-rights-new-era (accessed: 08.03.2025)

account of the rapid development of digital tools, paying particular attention to the protection of fundamental rights in the digital economy. Ensuring solid legal safeguards remains crucial, especially in the context of the rapid development of AI in sectors such as health, education and finance. To combat algorithmic bias, data misuse, and associated risks while promoting innovation, a draft Law on AI is being developed to reaffirm Uzbekistan's commitment to the responsible use of AI.

Conclusion

Uzbekistan's digital transformation legal reforms are at the intersection of global efforts to protect and advance human rights in an increasingly interconnected world. As technological advances driven by artificial intelligence, big data analytics, telecommuting platforms and digital health solutions accelerate, governments around the world are having to find a delicate balance between innovation and the protection of individual freedoms [Gasser U. et al. 2017: 59]. In this regard, Uzbekistan's legislative path, as reflected in the new Constitution, sectoral policies and revised codes, demonstrates a growing desire to integrate digital rights into the broader landscape of national governance.

A key facet of this evolution lies in ensuring that recognized human rights standards apply equally in online and offline contexts. International law has long upheld such equivalences, notably through the International Covenant on Civil and Political Rights and, in the regional context, through instruments like the European Convention on Human Rights. Yet, digital technologies introduce novel dimensions of potential harm ranging from large-scale data harvesting to algorithmic discrimination that often require states to refine existing statutes [Binns R., 2017: 3]. Over the past decade, global institutions such as the United Nations Human Rights Council, the Organization for Economic Co-operation and Development (OECD), and UNESCO have increasingly devoted attention to these emerging risks. In its most recent reports, for instance, UNESCO underscores the necessity of equipping policymakers with robust ethical guidelines for AI deployment, warning that unchecked technological innovation can exacerbate social inequalities and infringe on citizens' rights to privacy and information.

As artificial intelligence continues to evolve, the urgency of shaping regulatory frameworks that anticipate ethical, legal, and societal impacts becomes increasingly apparent. R. Calo emphasizes that society is uniquely positioned at a moment when policy responses can still influence the trajectory of AI in a human-centered direction [Calo R., 2017: 435].

Uzbekistan's "Digital Uzbekistan 2030" agenda seeks to address these challenges by advancing IT infrastructure, e-government programs, and digital literacy initiatives that support both economic modernization and human rights protection. This dual objective mirrors global best practices, where economic growth is pursued alongside principles of transparency, accountability, and inclusivity. Comparative experiences from the European Union particularly regarding data protection regulation and AI oversight illustrate how comprehensive legal frameworks can foster innovation without sacrificing fundamental rights. The EU's General Data Protection Regulation (GDPR) remains a leading example, emphasizing clear consent, user control over personal data, and substantial penalties for infractions. Although Uzbekistan's data protection laws are still in formative stages, the recent adoption of the Law "On Personal Data" and the Law "On Cybersecurity" demonstrates a strong push toward establishing protective mechanisms. These laws codify core safeguards against unlawful data processing, emphasize confidentiality, and impose penalties on parties failing to meet set standards reflecting Uzbekistan's willingness to learn from transnational precedents.

However, passing secure legislation is only part of the solution.

First. Successful digital rights protection depends as much on rigorous enforcement as it does on normative clarity. Scholars have emphasized that progressive laws can fail to curb rights violations if institutional capacity, judicial independence, and public awareness remain insufficient. In this light, Uzbekistan's initiatives to automate court procedures, enable online hearings, and strengthen digital forensic capabilities represent an attempt to ensure that legal protections migrate from theory to practice. This approach aligns with recommendations from the *World Development Report 2021: Data for Better Lives*,[55] which outlines how digital governance reforms must be matched with practical implementation measures, particularly in the judiciary and law enforcement arenas.

Likewise, *UNESCO's AI and Education: Guidance for Policy-makers highlights the importance of digital literacy and ethical standards*, especially in the areas of artificial intelligence and distance learning two fronts on which Uzbekistan is already moving forward through initia-

[55] World Bank World Development Report 2021: Data for Better Lives. Washington: World Bank, 2021.

tives like E-Health-2025 and the expansion of e-government services all integrate references to inclusivity by targeting digital infrastructure improvements in rural and remote regions. These policies draw inspiration from successful global models. South Korea's longstanding emphasis on universal broadband, for example, has helped bridge the digital divide, while Estonia's e-residency initiative highlights the value of secure digital identities that encourage economic participation and entrepreneurial growth.

Second. Further underscoring Uzbekistan's progress is the updating of the Criminal Code and the Code of Administrative Responsibility to criminalize specific forms of cybercrimes, harassment, and dissemination of false information. These reforms reflect a broader alignment with international norms, such as the Budapest Convention on Cybercrime, which fosters cross-border cooperation against emerging threats in the digital sphere [Svantesson D., 2017: 123–150]. As the Internet transcends territorial boundaries, questions arise about jurisdiction, extradition, and evidence-gathering. Uzbekistan's new legal provisions, especially those dealing with cyberstalking and illegal data collection, represent a response to these transnational dilemmas. This move parallels legislative trends in nations like Japan, where the Act on the Protection of Personal Information (APPI) requires entities handling personal data to maintain strict safeguards, and in Brazil, where the Lei Geral de Proteção de Dados (LGPD) modernized the country's data protection landscape, illustrating a convergence of national strategies in tackling digital rights issues.

Third. Despite the promise of these developments, certain challenges remain. The first is the perennial problem of ensuring that technology does not outpace the law. Artificial intelligence applications, facial recognition systems, and large-scale data analytics are evolving so quickly that even the most forward-looking statutes risk obsolescence within a few years.

A second challenge is the cultivation of specialized expertise within governmental bodies, which is essential for drafting regulations, adjudicating complex digital disputes, and overseeing compliance in rapidly evolving domains. Building up a cadre of well-trained cybersecurity experts, AI ethicists, and data-protection officers will be indispensable for translating legislative texts into lived protections. Finally, there is the question of public trust. While Uzbekistan has made advancements in expanding e-governance portals and online judicial services, their long-term effectiveness depends on citizens' confidence in both technology and government agencies. As the former UN High Commissioner for Human Rights Michelle Bachelet emphasized, the ultimate measure of digital policy success lies in how well it fosters human dignity and democratic engagement.[56] If citizens fear digital surveillance or worry that their data might be misused, they are less likely to embrace remote learning platforms, telemedicine, or online dispute resolution procedures, thereby undermining the potential societal gains [Zuboff S., 2019].

Overall, Uzbekistan's digital transformation journey demonstrates how a carefully calibrated approach to legislation can contribute to economic growth, simplify government and protect basic human rights. While the way forward will undoubtedly involve improving legal standards to keep pace with new technologies, building institutional capacity and bridging the digital divide, Uzbekistan has already set a promising precedent by synchronizing national priorities with recognized global norms. **If these efforts continue, the country is well positioned to sustain progress and ensure an equitable, inclusive and human dignity-based digital future.**

Lessons confirm that digital innovation, if done responsibly, can not only improve the quality of public services, but also protect the dignity and freedoms of every individual. By continuing to adopt international best practices, investing in legal and technological infrastructure, and putting the public interest at the centre of policy decisions, Uzbekistan stands a good chance of maintaining this constructive momentum and firmly anchoring human rights in its digital future.

References

1. Binns R. (2017) Fairness in Machine Learning: Lessons from Political Philosophy. Conference on Fairness, Accountability, and Transparency. *Proceedings of Machine Learning Research*, vol. 81, pp. 1–11. Available at: SSRN: https://ssrn.com/abstract=3086546.

2. Bradford A. (2023) *Digital Empires: The Global Battle to Regulate Technology*. Oxford: University Press, 599 p.

[56] Human rights in the digital age — Can they make a difference? Keynote speech by Michelle Bachelet, UN High Commissioner for Human Rights Japan Society, New York, 17 October 2019. OHCHR Speeches. Available at: https://www.ohchr.org/en/speeches/2019/10/human-rights-digital-age (accessed: 08.03.2025)

3. Calo R. (2017) Artificial Intelligence Policy: A Primer and Roadmap. *University of California Davis Law Review,* no. 51(2), pp. 399–435. https://ssrn.com/abstract=3015350

4. De Gregorio G. (2021) The Rise of Digital Constitutionalism in the European Union. *International Journal of Constitutional Law*, vol. 19, issue 1, pp. 41–70. https://doi.org/10.1093/icon/moab001

5. Floridi L. and Cowls J. (2019) A Unified Framework of Five Principles for AI in Society. Available at SSRN: https://ssrn.com/abstract=3831321 or http://dx.doi.org/10.2139/ssrn.3831321

6. Gasser U., Almeida V.A. (2017) A *Layered Model for AI Governance*. IEEE Internet Computing, no. 21(6), pp. 58–62. doi: 10.1109/MIC.2017.4180835.

7. Kayumov B. (2023) The Future of the Digital Judicial System of Uzbekistan: New Challenges and Prospects. 4 July. Available at: https://uztrend.uz/wordpress/archives/3661(in Russ.)

8. Kettemann M.C., Peukert A. et al. (2022) *The Law of Global Digitality*. London: Routledge, 255 p.

9. Khabrieva T.Yu. (2019) Constitutional Development in the Context of Modern Challenges and Global Social Transformations. *Gosudarstvennaya sluzhba*=State Service, no.1, pp. 17–25 (in Russ.)

10. Mantelero A. (2018) AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment. *Computer Law & Security Review,* no. 4, pp. 754–772. Available at: SSRN: https://ssrn.com/abstract=3225749

11. Rassolov I.M. (2022) *Law and the Internet: Theoretical Issues*. Moscow: Norma, 304 p. (in Russ.)

12. Svantesson D.J.B. (2017) *Solving the Internet Jurisdiction Puzzle*. Oxford: University Press, 254 p.

13. Tufekci Z. (2015) Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency. *Colorado Technology Law Journal,* no. 13, pp. 203–218.

14. Yeung K. (2018) Algorithmic Regulation: A Critical Interrogation. *Regulation* & *Governance*, no. 12, pp. 505–523. https://doi.org/10.1111/rego.12158

15. Zuboff S. (2019) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Public Affairs, 691 p.

Information about the author:

A.Kh. Saidov — Deputy of the Legislative Chamber of the Oliy Majlis of the Republic of Uzbekistan, Director of the National Center of the Republic of Uzbekistan for Human Rights, Member of the United Nations Human Rights Committee, Academician of the Academy of Sciences of the Republic of Uzbekistan, Doctor of Sciences (Law), Professor

The article was submitted 21.03.2025; approved after reviewing 25.03.2025; accepted for publication 25.03.2025

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

Research article
JEL: K14
UDC: 343
DOI:10.17323/2713-2749.2025.1.83.104

The Application of Artificial Intelligence in China's Criminal Justice System

Zhiyuan Guo[1], Jiajia Yang[2]

[1, 2] China University of Political Science and Law, School of Criminal Justice, 25 Xitucheng Road, Haidian District, Beijing, China 100088,

[1] guozhiyuan@hotmail.com, https://orcid.org/0000-0003-4329-5825

[2] jiajia1023@outlook.com, https://orcid.org/0009-0009-4120-2622
Corresponding Author: Zhiyuan Guo

Abstract

Influenced by the advanced technologies, in recent years, Chinese criminal justice system has begun integrating artificial intelligence (AI) to assist judicial decision-making. AI has entered into various areas such as criminal investigations, prosecution assistance, and sentencing support. However, Chinese legal system has not comprehensively addressed the regulation of judicial AI technology yet. This paper aims to explore the application of AI in Chinese criminal justice system and propose a systematic regulatory framework for its future development. Part I provides an overview of the specific application scenarios of AI in Chinese criminal justice system. Part II analyzes the general characteristics of judicial AI and the benefits it brings to the justice system. Part III examines the challenges limiting the further development of judicial AI and the potential risks associated with its application. Part IV proposes an inclusive regulatory framework to balance the intension and potential conflicts between judicial fairness and technological advancement. This research seeks to enhance the understanding of AI application in Chinese criminal justice system and to identify and prevent potential judicial risks arising from AI application.

Keywords

artificial intelligence; application of judicial AI; Chinese criminal justice; criminal procedure law; algorithm; data.

For citation: Guo Zh., Yang J. (2025) The Application of Artificial Intelligence in China's Criminal Justice System. *Legal Issues in the Digital Age*, vol. 6, no.1, pp. 83–104. DOI:10.17323/2713-2749. 2025.1.83.104

Introduction

Human society is currently at the center of an information revolution storm. At the beginning of the 21st century, the pace of technological innovation has accelerated continuously. Advanced technologies such as artificial intelligence, big data, blockchain, and cloud computing have emerged one after another. China does not intend to miss this unprecedented technological revolution. As early as 1982, the Chinese leadership incorporated artificial intelligence research into the **Sixth Five-Year Plan for National Economic and Social Development of the People's Republic of China (1981–1985)**.[1]

Subsequently, the 13th Five-Year Plan for National Economic and Social Development of the People's Republic of China,[2] released in 2016, emphasized the need to overcome key technological challenges related to artificial intelligence. These challenges included breakthroughs in big data and cloud computing technologies, independently controllable operating systems, high-end industrial and large-scale management software. Building upon the 13th Five-Year Plan, China successively introduced several national strategies, including the National Informatization Plan, the National Science and Technology Innovation Plan, and the National Strategic Emerging Industries Development Plan. These policies highlighted the importance of emerging technologies such as the Internet of Things, deep machine learning, blockchain, and bio-genetic engineering. Additionally, they called for strengthening technological development in cutting-edge fields such as quantum communication, future networks, brain-inspired computing, virtual reality, and big data analytics. These efforts aim to promote the intelligentization process of various sectors and lay the groundwork for building a "Digital China."

On July 8, 2017, the State Council released the New Generation Artificial Intelligence Development Plan,[3] which explicitly called for the de-

[1] Available at: https://www.ndrc.gov.cn/fggz/fzzlgh/gjfzgh/200709/P020191029595670483752.pdf (accessed: 03.05.2025)

[2] Available at: https://www.gov.cn/xinwen/2016-03/17/content_5054992.htm (accessed: 03.05.2025)

[3] Available at: https://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm (accessed: 03.05.2025)

velopment of judicial AI, the establishment of smart courts and the judicial data platforms to achieve court digitalization. Driven by national policies, courts and procuratorates across China began developing their own AI-powered judicial platforms. This marked a nationwide "judicial intelligence movement" gradually unfolding across the country.

In Beijing, the Beijing Internet Court developed the "Mobile Micro Court" platform and an "AI Virtual Judge." The former is embedded within WeChat, allowing users to access online litigation services simply by opening the corresponding program. The latter, created by using speech and image synthesis technology, can assist judges by handling repetitive front-end tasks such as litigation reception.[4] In Shanghai, the Shanghai Higher People's Court developed the "Intelligent Criminal Case Assistance System," which consists of three components: the Shanghai criminal case big data resource, an intelligent case-handling software, and an intelligent case-handling system network platform.[5] Additionally, in the procuratorial system, the Zhejiang People's Procuratorate partnered with Alibaba Cloud to build a big data platform. This platform enables the visualization of case data, presenting it dynamically, intuitively, and in chart form to assist judicial decision-making. Meanwhile, the Beijing People's Procuratorate developed a big data decision-making platform, which integrates information from all litigation stages, allowing case handlers to quickly access legal documents.[6] Besides, other provinces such as Guizhou, Hainan, Yunnan, Jiangsu, and Guangdong are also progressively building their own AI-powered judicial case-handling systems. Overall, the application of AI is widespread in Chinese criminal justice system, covering the vast majority of regions in China.

In the future, as AI technology continues to develop in China, its impact on the judicial system will also deepen. As a variable factor intervening in the criminal justice system, AI is bound to increase the risks and uncertainties in current criminal legal framework. To address potential issues and threats, this paper examines the specific application scenarios of AI in Chinese criminal justice system, revealing its operational mode and characteristics. Furthermore, exploring the advantages, challenges,

[4] Available at: https://tech.chinadaily.com.cn/a/201906/28/WS5d156c9ca3108375f8f2cfc9.html (accessed: 03.05.2025)

[5] Available at: https://www.chinacourt.org/article/detail/2019/01/id/ 3713361.shtml (accessed: 03.05.2025)

[6] Available at: https://www.spp.gov.cn/xwfbh/wsfbt/201706/t20170612_192863_2.shtml (accessed: 03.05.2025)

and potential risks AI may bring to the system. Finally, the paper seeks to propose a possible regulatory framework for the application of AI in criminal justice system.

1. The Application Scenarios of AI in Chinese Criminal Justice System

1.1. Crime prediction

In 2015, the General Office of the Communist Party of China Central Committee and the General Office of the State Council jointly issued the Opinions on Strengthening the Construction of the Social Security Prevention and Control System,[7] which stated: "Strengthen the deep integration and application of information resources, fully utilize modern information technology, and enhance the ability to proactively prevent and combat crime." Following this direction, various regions across China have started to strengthen predictive policing efforts.

Predictive policing operates based on two modes: (1) crime trend analysis and forecasting. Chinese polices utilize vast amounts of previously accumulated crime data to build big data platforms. By analyzing crime patterns, frequencies, and high-incidence areas, these platforms can predict future crime trends and help to deploy officers in advance for crime prevention. In sector of routine policing and crime prevention, crime alert prediction systems allow real-time tracking and dynamic monitoring of potential criminal activities. These systems provide valuable insights for daily patrol planning while enhancing proactivity of crime prevention. For example, the crime prediction system used by the police in Suzhou, Jiangsu Province, contains over 13 million records of crime-related data spanning the past decade, along with 780 million records related to entertainment venues, commercial establishments, and other relevant locations. The system's predictive model analyzes 382 variables, including population data, geographic information of specific groups, weather conditions, sunset times, etc. Based on the analysis results, it will send patrol alerts to frontline officers. At the Weitang Police Station in Suzhou, within the first three months of implementing this system, crime-related police reports dropped by 54% compared to the previous period. (2) real-time crime monitoring. Polices integrate existing video surveillance systems across various public areas in cities into a

[7] Available at: https://www.gov.cn/xinwen/2015-04/13/content_2846013.htm (accessed: 03.05.2025)

centralized, internet-connected monitoring platform. This platform is accessible via a mobile app, allowing users to view real-time footage of public areas and detect suspicious activities. If a crime occurs, users can report it immediately through the app. For instance, Sichuan Province's "Xueliang Project" utilizes this approach for real-time crime monitoring, enhancing public security.[8]

The Guiding Opinions of the State Council on Strengthening Digital Government Construction, issued in 2022, explicitly emphasized the need to enhance the construction of public security big data platforms to improve the ability to predict, warn, and prevent various risks.[9] It is foreseeable that Chinese predictive policing will continuingly develop in the future. The frequency of police using big data and AI technologies for early crime detection is expected to increase as well, reinforcing the trend toward the normalization of predictive policing [Wang L., 2024: 55–88].

1.2. Criminal investigation

In China, the development of AI technology has provided new support for criminal investigations. The main roles of AI in criminal investigations include: collecting and analyzing crime clues; rapidly accessing and securing criminal evidence; and accurately identifying criminal suspects.

In terms of collecting and analyzing crime clues, if the police obtain personal identity information such as name, identification number, real-time location, movement trajectory, and biometric data, AI technology can be used to analyze this information or compare it with specific data to uncover criminal clues. For example, the National DNA Database System developed in China in the early 21st century stores a large amount of personal DNA information. Police can compare the DNA of potential suspects with the database to accurately identify the criminal suspects or determine whether they were at crime scene when the crime happened. Similarly, by analyzing movement trajectory and real-time location information, specific crime areas can be identified, enabling police to quickly locate criminal tools or the hiding places of suspects.

In terms of collecting criminal evidence, police can use AI systems to gather and preserve evidence. In crimes involving cyberattacks, illegal

[8] Available at: https://www.gov.cn/xinwen/2015-04/13/content_2846013.htm (accessed: 03.05.2025)

[9] Available at: https://www.gov.cn/zhengce/content/2022-06/23/content_5697299.htm (accessed: 03.05.2025)

fundraising, financial fraud, police can utilize network and data collection technologies to quickly secure relevant evidence.

When it comes to identifying criminal suspects, AI technologies such as facial recognition, tagged profiling, and vehicle information comparison can help police quickly confirm the appearance, body shape, and vehicle information of suspects, directly identifying the perpetrators of crime. Chinese Tianyan Surveillance System is equipped with powerful facial recognition technology that can accurately identify criminal suspects. With the assistance of this system, Chinese police have apprehended numerous suspects and fugitives, solving many criminal cases.

1.3. Detention and bail decisions

According to Article 81 of the Criminal Procedure Law of China, for criminal suspects or defendants who have evidence proving the commission of a crime and may be sentenced to imprisonment or a more severe punishment, if bail is insufficient to prevent the following social dangers, they should be arrested: (1) the possibility of committing new crimes; (2) a real danger to national security, public safety, or social order; (3) the possibility of destroying or falsifying evidence, interfering with witness testimony, or colluding with others; (4) the possibility of retaliating against the victim, whistleblower, or accuser; (5) the risk of suicide or flight. In judicial practice, when making detention decisions, judicial officers need to consider three conditions: (1) whether there is evidence proving the defendant's criminal conduct; (2) whether the defendant is likely to be sentenced to a fixed-term imprisonment or above according to relevant laws; (3) the social danger posed by the defendant. The first two conditions are relatively easier to evaluate, but the concept of "social danger" is more subjective and may be interpreted differently by various judicial officers. Although criminal procedure law lists five specific risks, it still does not fully guide judicial officers in making detention decisions. Therefore, to ensure the fairness and rationality of the detention decision, some procuratorates and courts have started exploring the use of AI decision models to quantify the social danger factor.

A typical example is the social danger quantification evaluation system developed by the People's Procuratorate of Yuncheng City, Shanxi Province. This system identifies 60 variables that influence the assessment of social danger, categorized into three sectors: the nature of the crime, behavior after committing the crime, and the physical and mental condition of the criminal suspect. These 60 indicators are divided into five risk levels: high risk, medium-high risk, medium risk, medium-low risk, and low risk. Each risk level is assigned a corresponding score, and based on these scores, prosecutors make decisions regarding detention.[10] In addition, the quantification evaluation system developed by the Shanghai Higher People's Court includes 32 evaluation indicators, while the system in Nansha District, Guangzhou is based on 43 indicators, mainly considering personal danger, social harm, and litigation controllability. Although the number of variables used by these systems varies, the content of the variables consistently involves the suspect's criminal situation and litigation conditions. The working rationale of these quantification evaluation systems is similar: based on the information input by judicial officers, the AI model assigns scores and identifies risk levels according to the corresponding algorithm. Judicial officers then make the final detention decision based on the results.

1.4. Prosecutorial discretion

In China, the Procuratorate plays a critical role in initiating public prosecutions for criminal activities and protecting the legal rights of citizens. In most criminal cases, prosecutors are required to thoroughly understand the situation of the criminal suspect and the facts of the crime, and based on this, file public prosecutions to court. This procedure is similar to many countries around the world. However, in China, prosecutors are also required to present sentencing recommendations to the judges. The use of AI systems to assist with prosecutorial discretion not only enhances the efficiency of case handling but also improves the accuracy of sentencing recommendations, ensuring they align more closely with the judge's final sentencing decision. In 2018, the Supreme People's Procuratorate issued the National Smart Prosecution Action Guide (2018–2020), which outlined improving the infrastructure of procuratorate's big data center, accelerating the development of prosecution data resource system, and promoting the development of intelligent case-handling systems, in order to build a comprehensive smart prosecution ecosystem centered around case handling.[11] Since then, AI has increasingly been used in prosecutorial discretion tasks across China.

A typical example is the Jiangsu province's smart prosecution assistance system. This system helps prosecutors automatically filter out mat-

[10] Available at: https://m.faanw.com/anlizhengji/19686.html (accessed: 03.05.2025)

[11] Available at: https://www.spp.gov.cn/spp/xwfbh/wsfbt/201807/t20180720_385543.shtml (accessed: 03.05.2025)

ters that need legal procedure review, evidence review, case facts review, and criminal behavior information items. This makes the criminal cases review process more intuitive and clearer. Additionally, the system can automatically generate interrogation outlines, supplementary investigation outlines, case review reports, indictments, sentencing recommendations. This can help to save prosecutors' time, allowing them to focus more on evaluating evidence in complex cases. Furthermore, the system can track the number and quality of cases handled by each prosecutor, automatically generating prosecutor's performance results, which can be used for evaluating prosecutors' promotions, and rewards. In essence, this system integrates prosecutorial assistance, case fact review, and evidence review guidance, helping prosecutors efficiently process cases.[12]

Another example is the Guizhou province's prosecution big data application system, which serves three main functions: (1) establishing crime models based on the elements of various criminal behaviors and using these models to create unified legal standards for application; (2) providing precise data analysis for each case, relying on vast amounts of data to assist in constructing criminal facts, sentencing references, etc. The system can also analyze similar cases, identifying crime characteristics such as the time and location of certain crimes; (3) analyzing overall internal data of procuratorate system, monitoring the quality of prosecutorial work, and evaluating development trends to help the leadership make more scientific and reasonable plans for prosecutorial work.[13]

The two examples above emphasize different aspects. The first highlights the supportive role of AI in case processing, positioning AI as an assistant to the prosecutor. It helps with transactional and repetitive tasks, thus leaving prosecutors with more space for discretion. The second example emphasizes the guiding role of AI, positioning it as a leader in assisting prosecutors to evaluate criminal facts and may potentially influence prosecutors' judgement towards case facts.

1.5. Sentencing assistance

In the 1980s, scholars in China had already raised the issue of using AI for sentencing, and by 1993, the development of an AI-assisted sen-

[12] Available at: https://www.spp.gov.cn/spp/dfjcdt/201803/t20180304_368729.shtml (accessed: 03.05.2025)

[13] Available at: https://www.spp.gov.cn/xwfbh/wsfbt/201706/t20170612_192863_2.shtml (accessed: 03.05.2025)

tencing system was completed. In 2006, the People’s Court of Zichuan District in Zibo City, Shandong Province, collaborated with technology companies to develop computer sentencing software. In 2017, the Supreme People’s Court released the Opinions on Accelerating the Construction of Smart Courts,[14] which emphasized the use of big data and AI technology to assist case handlers in reducing the burden of non-judicial tasks and to provide intelligent litigation services to the public. Since then, smart court systems have been progressively established across China. For example, the Beijing Higher People’s Court built the “Smart Judge” system; Guiyang, Guizhou Province, developed the Guiyang Political and Legal Big Data Case Handling System, which integrates investigation, prosecution, and court functions; the Hainan Province Higher People’s Court built the “Sentencing Standardization Intelligent Assistance System”; the Higher People’s Court of Yunnan Province established the “Drug Case Big Data Analysis Platform” and the “Yunnan Political and Legal Big Data Case Handling Platform”; and the Guangzhou Internet Court built the “Online Evidence Exchange Platform” and the “Similar Case Intelligent Reference System”, etc.

These AI judicial systems typically possess the following functionalities: litigation service reception, case file transfer, pre-trial meetings, trial recording, evidence rule guidance, evidence verification, evidence exclusion, full-case evidence review guidance, similar case reference, sentencing reference, knowledge searching, litigation document generation, case procedure supervision, and case evaluation [Sun D., 2023: 112–116].

Overall, the use of AI technology in criminal trials is the most widespread. AI is positioned as an assistant in various stages of the trial process, primarily because: First, the number of criminal cases in China is enormous, and courts are constantly under pressure due to the shortage of personnel. In order to address the backlog of cases, courts urgently need to introduce AI technology. Second, the trial process involves a significant number of repetitive tasks, many of which are simple and procedural. Using AI to handle these tasks can ease the burden and improve efficiency.

1.6. Execution of punishment

In China, AI is also utilized in the execution of criminal punishment, particularly for supervising incarcerated individuals. For instance, Ji-

[14] Available at: http://gongbao.court.gov.cn/Details/5dec527431cdc22b72163b49fc0284.html (accessed: 03.05.2025)

angxi province established Chinese first special population big data platform to address the challenges of managing inmates, released prisoners, and individuals under community correction. This platform has recorded information on 470,000 individuals, allowing authorities to access real-time data on supervised individuals and monitor their likelihood of reoffending.[15]

Additionally, AI is used in commutation and parole decisions, operating similarly to the social dangerousness quantitative assessment system used for detention decisions. However, the key distinction is that the AI system for commutation and parole focuses on evaluating remorseful behavior and risk of recidivism. It conducts a comprehensive quantitative assessment based on variables such as an inmate's rehabilitation progress, fulfillment of obligations, mental health, criminal history, and family background etc. Based on these evaluations, the system assists in determining whether a prisoner qualifies for commutation or parole.

2. AI Applications in Chinese Criminal Justice System: Characteristics and Advantages

2.1. Characteristics of AI Applications in Chinese Criminal Justice System

2.1.1. Diverse AI Models with a Lack of Unified evaluation Standards

Chinese AI judicial system is being applied across a wide range of fields and is experiencing rapid development. However, different regions have established various types of AI models to address specific judicial issues, leading to a lack of unified evaluation standards for AI model.

On one hand, this is due to Chinese vast territory and regional cultural differences, which result in varying judicial challenges. To address these localized issues, judicial authorities have developed different AI models. For example, in the southwestern province of Yunnan, which borders the Golden Triangle and has a high incidence of drug-related crimes, an AI platform specifically for drug crime has been established. In contrast, such issues are not prevalent in eastern regions, where similar platforms are unnecessary. On the other hand, differences in the goals, functions, human resources, and financial investments in AI model development

[15] Available at: https://www.chinanews.com.cn/gn/2016/10-13/8030437.shtml (accessed: 03.05.2025)

across regions have also contributed to the disparity. Some areas have built integrated large-scale AI models that serve the needs of investigation, prosecution, and trials, or integrate the functions of document assistance, case handling support, and case monitoring. In contrast, part of regions has only developed single-purpose models with limited functions, such as sentencing assistance or similar-case recommendations.

Due to these factors, China has yet to establish a unified large-scale AI model in criminal justice system, and most regions remain in the pilot phase. Thus, a standardized evaluation system for AI applications is lacking. In the future, as regional disparities in AI judicial models diminish, a unified evaluation framework can be developed to guide AI-driven judicial system construction. Preliminary considerations for this framework may include aspects such as data collection, data analysis, algorithm interpretability, and transparency.

2.1.2. Focused on Handling Administrative Tasks with a Low Level of AI Integration

From the perspective of the functions of AI models, AI in Chinese criminal justice system generally serves five main functions: crime trend prediction, information comparison, information resource integration, non-decision-making administrative task handling, and judicial decision support and assistance. The systems used by investigators mainly focus on the first two functions: crime trend prediction and crime information comparison. On the other hand, the systems used by smart courts and smart procuratorates have similar functions, primarily focusing on information resource integration, non-decision-making administrative task handling, and judicial decision support and assistance.

In China, although prosecutors and courts have different functions, prosecutors handle public prosecutions, while courts are responsible for case rulings and sentencing. They still make decisions on the same aspects of the same case during different stages of the criminal process. For example, decisions on the detention of criminal suspects and sentencing decisions for cases where the facts of the crime are clear. The judicial decision-making process for both entities is similar, involving three main steps: analyzing the case facts and evidence (minor premise), applying and reviewing rules of evidence law, substantive law, and procedural law (major premise), and deciding guilt and the sentencing outcome (conclusion). This decision-making process aligns with the classic structure of syllogism. To assist judicial personnel in completing this three-step argumentation, the AI model's information resource integration function can capture most legal norms, the judicial decision support function can collect case evidence and factual information, and after judicial personnel make decisions, the system's administrative functions such as document generation can help create the judgment documents.

Based on this, Chinese prosecution discretion support systems and trial assistance systems include modules for online transfer of criminal case files, document generation, evidence standard guidance, legal application prompts, and similar case recommendations. These tasks are essentially preparatory work for judicial decision-making, characterized by simplicity, tediousness, and repetition. The use of AI technology to process these tasks only serves as a procedural aid and does not possess the characteristics of human-like reasoning. Chinese practical use of AI in judicial decision-making, to some extent, can be seen as a "weak-form" application of AI [Zuo W., 2021:7].

2.1.3. Aimed at Decision Support Rather than Replacing the Judicial Decision-Makers

In terms of how AI participates in judicial decision-making, three modes can be identified: (1) judicial AI decision support mode: in this mode, AI analyzes and learns from data to generate potential decision options, but the actual decision-making authority remains with judicial personnel. Judges can confirm or generate new decisions; (2) judicial AI supervisory decision mode: here, AI generates decision options, which are then confirmed by judicial decision-makers before directly generating documents. In this process, judicial personnel play a supervisory role in decision-making and can change the decision if necessary; (3) judicial AI autonomous decision mode: in this mode, AI is integrated into a closed-loop decision-making process, completely removing judicial personnel from control. AI has the authority for independent decision-making, the entire court system will be the central body controlling judicial decisions.

Currently, Chinese criminal justice AI systems incorporate the first two modes: the judicial AI decision support mode and the judicial AI supervisory decision mode. For instance, the intelligent case assistance system used in Shanghai adopts the first mode, providing sentencing references to judges while still retaining their final decision-making authority. AI serves as a technical tool to assist judges in making decisions.

This mode is advantageous in integrating sentencing information but has limitations in quickly processing cases and improving judicial efficiency. In contrast, the system used by Suzhou courts adopts the second mode, where it automatically extracts information from clear and simple cases and generates judgment documents based on existing legal rules, requiring only confirmation from the judge. This mode is more efficient than the first one but partially undermines the judge's autonomy in decision-making [Sun Q., 2022: 164–65].

Overall, China does not have a fully autonomous AI decision-making model yet. Whether using the judicial AI decision support mode or the judicial AI supervisory decision mode, AI has not completely replaced the judge's comprehensive judgment based on experience, logic, and perception. The difference lies only in the extent of technical assistance provided between those two modes.

2.2. Advantages of AI Applications in Chinese Criminal Justice System

2.2.1. Optimizing the Utilization of Judicial Resources

The structure of criminal cases in China follows a clear "80/20 rule," where complex cases account for a small proportion of overall crimes. However, in judicial practice, uncovering the truth of these cases, reviewing evidence, and applying the law can be quite challenging. Without sufficient investment in judicial resources, these cases may turn into long-unresolved, suspenseful cases. For the majority of simple cases with clear criminal facts, courts and procuratorates must handle many repetitive, procedural tasks. The application of judicial AI can quickly complete tasks such as providing litigation service guidance, searching for legal norms, and generating documents. This allows the remaining judicial resources to be more effectively dedicated to handling difficult cases. In this way, judicial resources in Chinese criminal justice system can be utilized more efficiently.

2.2.2. Conducive to Crime Prevention and Investigation

With the growth of emerging technologies, new forms of crime have been continuously emerging. These crimes often involve the use of technologies such as the internet and AI, making them difficult to detect and prevent due to characteristics like remote control and sophisticated methods. Without leveraging emerging technologies for crime prevention and control, a country's criminal prevention system could face significant challenges. However, the use of AI in crime investigation also carries negative effects. Without strict legal regulations, it could infringe upon citizens' legitimate rights and interests [Shi P., 2024: 17–18]. If AI technology is applied in a reasonable manner, it can indeed effectively prevent serious crimes and assist in criminal investigations.

3. AI Applications in Chinese Criminal Justice System: Challenges and Risks

3.1. Challenges of AI Applications in Chinese Criminal Justice System

3.1.1. Challenges of Discourse System Integration

The underlying architecture of AI technology consists of three elements: datasets, algorithms, and computing power. The core of AI lies in the operation process of algorithm models, which is governed by a code-based discourse system. AI's technical language system is precise and concise. However, many legal issues do not have standard answers. Legal interpretation and analysis are fundamentally based on complex trade-offs, value judgments, and consideration of social factors. When AI attempts to engage with the legal system, a fundamental difference between their underlying discourse systems becomes apparent.

If legal language is converted into mere logical judgments and internalized into algorithms and code framework, it will lose its original essence, and the algorithmic decisions may become biased or even lead to incorrect decisions. Therefore, with the increasing use of AI in the judicial field, a divide has emerged between traditional discourse and emerging technological discourse [Wang L., 2018: 140]. The accuracy of algorithmic decisions depends on the accuracy of language translation. However, the fundamental mismatch between the fuzzy logic of human language of and code poses a significant challenge. Future development of AI in the judicial field must address this issue.

3.1.2. Challenges of Judicial Decision-Making Reasoning

The human decision-making process is a long and complex journey, based on the intricate experience system of human society, and premised on human consciousness and agency. Factors such as emotions, feelings, and wisdom can all influence decision-making. If these factors are incorporated into the AI modeling system, the decision-making framework shifts from being open to closed, narrowing the decision elements. For instance, in evidence reasoning, if AI models are used to uncover the truth of a case, a massive and complex model system need to be established. Even then, it would be impossible to fully guarantee the accuracy of the factual determination. The human brain’s decision-making process is akin to a “black box”; simulating this process has no predetermined answer and is, in essence, another black box. Moreover, the conclusions of evidence reasoning are the result of the interaction between the shared knowledge base of society and the judge’s own knowledge base. An AI judicial system cannot fully encompass this knowledge, which leads to potential risks in the evidence reasoning process. Currently Chinese judicial AI is still in the weak AI stage, if “strong AI” is applied in the criminal justice system in the future, it will inevitably need to address the challenges of AI judicial decision-making reasoning.

3.2. Risks of AI applications in Chinese Criminal Justice System

3.2.1. Justifiability Risks

The data used by AI systems in the judicial context contains a large amount of personal information, which may infringe upon citizens’ privacy rights during its application. If citizens are not informed in advance and do not give consent during data collection or the application of AI technologies, the use of AI will lack legitimacy and potentially violate citizens’ constitutional rights. However, due to the vast amount of data involved, it is difficult to trace the data sources or identify the data owners, thus, it’s hard for the entities applying AI in the judicial system to obtain consent from data owners, and even when citizens’ rights are infringed, it becomes difficult to identify the responsible party, making it challenging for citizens to reasonably defend their rights. In a rule-of-law country, the principle is to protect citizens’ legitimate rights and interests, and if these rights are violated, there should be appropriate remedies. The difficulty lies in the legal status of AI decision-making models has not yet been clearly defined. Additionally, identifying the causality between algorithmic technology and the harm results is complex. These potential issues hinder the further expansion of AI applications in the criminal justice system.

3.2.2. Legitimacy Risks

Currently, there is no well-established legal framework in China to regulate the use of AI in crime prediction, leaving many legal gray areas [Xie Y., 2024: 85–86]. In criminal investigations, the traditional framework of criminal procedural norms struggles to regulate the use of various new investigative technologies by the police. The legitimacy of evidence collected by police is often challenged, and the judicial review system for these AI-based investigative techniques has yet to be established. The use of AI in crime prediction has led to an advancement of time point for initiating investigations, which is in conflict with the traditional presumption of innocence principle. Due to the rapid pace of technological innovation, the law lags behind social development, and as a result, AI-driven investigation and predictive policing increasingly face challenges regarding their legality.

3.2.3. Judicial Fairness Dangers

The traditional criminal litigation structure in China has historically been characterized by an imbalance of power between the prosecution and defense. The introduction of AI systems in the judicial process, has further exacerbated this inequality. The prosecution now holds a significant advantage over the defense in areas such as evidence collection, legal application, and case comparison, making it difficult for the defense to compete with conventional defense strategies. As a result, the defense finds it hard to challenge or undermine the prosecution's criminal accuses. In recent years, China has introduced a sentencing negotiation system, which is based on the premise that the defense has enough leverage to negotiate sentencing with the prosecution. However, the use of AI in criminal justice could intensify the inequality of bargaining power between the prosecution and defense, undermining the fairness of the sentencing negotiation process. The application of AI in the judicial system may challenge the traditional principle of equal arms between the prosecution and defense. Moreover, the initial intention of AI systems in judicial processes was to promote the uniform and equal application of the law, addressing issues such as sentencing unfairness and inequality. However, in practice, the use of AI may not necessarily alleviate sentencing disparities and could potentially exacerbate them.

3.2.4. Decision Accuracy Risks

There is no data that clearly shows that the evaluation accuracy of AI systems in judicial decisions such as detention, commutation, or parole exceeds the accuracy of judicial officers' evaluations [Xiong Q., 2022: 111]. Therefore, it is difficult to assess the urgency of using AI in the criminal justice system. On one hand, AI relies on past data to assess current outcomes, and the predictions made by AI models may be incorrect, leading to issues such as improper sentencing. On the other hand, AI judicial decision-making systems are closed systems and do not allow for the entire decision-making process to be traced, compared, or evaluated for its accuracy. Additionally, while AI models have scientific characteristics, it cannot guarantee that the decisions it generates will always be rational and accurate.

3.2.5. Data Risks

Data issues are a fundamental challenge hindering the development of judicial AI. Although China has established numerous big data platforms, problems such as data silos, data barriers, data gaps, data flaws, data monopolies, and data asymmetry still exist [Li X., 2021: 47–48]. Firstly, most courts and procuratorates in China have not achieved seamless data communication and flow. A single data platform can create data silos, and judicial decisions based on these isolated data sources may lack synergy, affecting the accuracy of the decisions. Secondly, the data used by AI may be incomplete. It might only cover data from specific periods or under specific conditions, and the data itself may be inaccurate or miss information. This leads to challenges in ensuring data quality, and judicial decisions based on flawed data may lack of reliability. Furthermore, high-tech companies that control the data and algorithms necessary for development gain the access to judicial AI systems. Over time, this can lead to data monopolies, creating an information asymmetry between the prosecution and defense, as well as between the public and tech giants.

3.2.6. Algorithm Risks

Algorithms are created by programmers, and the algorithmic code can be influenced by the programmers' preferences, personalities, and other subjective factors. Therefore, algorithms inherently carry human attributes, making issues such as algorithmic discrimination and bias unavoidable. Additionally, the "black box" nature of algorithms is a significant risk. Even if the technical controllers disclose the source code, the decision-making process of the algorithm is often complex and difficult to explain. Algorithmic bias and the black box problem can lead to a lack of transparency, fairness, and the undetectable risks in reviewing the accuracy of the decision-making process and outcomes.

3.2.7. Ethical Risks

The application of AI in the criminal justice system raises an ethical issue: whether AI will eventually replace human judges in decision-making. Currently, AI in Chinese criminal justice system is still at the "weak AI" stage and has not fundamentally replaced judges. For example, AI cannot replace the judge's discretion of facts evaluation. However, as AI continues to develop, its influence on judges' decision-making may deepen, potentially eroding the space for judicial discretion and reinforcing the tendency towards strict evidentialism [Xiong Q., 2020: 88]. Once AI technology permeates the criminal justice system, a unique phenomenon will arise, where dual decision-making entities exist simultaneously in the system. How to adjust the relationship between these dual entities and whether to grant AI independent decision-making status will be a critical issue that the criminal justice system will soon face.

4. Regulatory Framework for the AI Applications in Chinese Criminal Justice System

Chinese basic policy of vigorously promoting technological development determines that the regulation of AI in criminal justice needs to both allow space for its future development and prevent the abuse of AI, which could infringe upon citizens' legal rights and lead to various social issues. This regulation method is regarded as "inclusive regulation model," which essentially balances the need for technological development and the value of judicial fairness. Under this model, the regulatory framework for AI in the criminal justice system includes three aspects: technological regulation, legal regulation, and ethical regulation.

In the technological regulation scheme, the quality and quantity of data used in judicial AI need to be improved, and the transparency of algorithms should be enhanced. First, to address issues such as incomplete judicial data and data silos, a unified cross-regional and provincial data information platform can be established to enable the communication and cross-utilization of data resources. Second, the substantial content beneath the data's surface must not be ignored. Given the mismatch in knowledge backgrounds between judicial personnel and technical staff, developers should focus on data related to judicial substance issues, enhance data identification capabilities, and make full use of high-quality data resources. Lastly, the transparency and openness of algorithms should be improved by requiring software companies to disclose the AI system's code, and organizing experts from various disciplines such as sociology, computer science, and law to supervise and evaluate the algorithms.

In the legal regulation scheme, the digital rights of the accused need to be constructed. The digital rights of the accused are a comprehensive right protected by a series of technology-related legal procedures. This represents a new challenge to the traditional "rights-power" dual balance framework in the information age [Pei W., 2021: 93–99]. Specifically, the procedural rights of the accused include: the right to procedural information, the right to dispose of the procedure, the right to system access, the right to algorithmic explanation, and the right to obtain professional assistance. The right to procedural information means the accused has the right to know when public authorities use judicial AI and understand the data and algorithms underlying AI tools [Zheng X., 2023: 48]. The right to dispose of the procedure means the accused has the freedom to decide on the initiation, modification, or termination of the AI application procedure [Zheng X., 2024: 161]. The right to system access means the accused has the right to access the data and algorithms used by AI tools. The right to algorithmic explanation means the accused can request an explanation of the algorithm from public authorities or seek remedies when algorithmic decisions are unfavorable to them [Wang Z., 2024: 257–259]. The right to obtain professional assistance is essentially the expansion and extension of the traditional right to legal defense in the digital space, emphasizing that the accused has the right to obtain professional help related to AI in judicial matters. In the field of AI in criminal justice, the power imbalance between the prosecution and defense is further widened, and Chinese criminal procedure law should emphasize the principle of equality between prosecution and defense [Zheng X., 2025: 59].

In the ethical regulation scheme, the development of AI in Chinese criminal justice should adhere to the principle of making judicial personnel the main decision subject, while also clearly addressing the ethical responsibilities of developers, users, and legislators. The former is the ethical baseline and principle for developing AI in criminal justice system. If this principle is breached, the development of AI could fall into disorder and chaos, and potentially trigger a crisis of public trust towards judicial branch. The latter concerns the distribution of interests among various parties and the incentives for technological development. If responsibility is not equally distributed, it could hinder the steady development of AI technology. Since Chinese AI is still in the flourishing stage and lacks many practical cases and experience in handling similar situations, this issue may have an answer once the conditions mature in the future.

Conclusions

By analyzing the application status of AI in Chinese criminal justice system, the following conclusions can be drawn.

In recent years, driven by top-down national policies, China is undergoing a judicial intelligence movement. Police, procuratorates, and courts across provinces all participating in this judicial reform movement.

In Chinese criminal justice system, AI technology is mainly applied in scenarios such as crime prediction, criminal investigation, pre-trial detention and bail decisions, prosecutorial discretion assistance, judicial decision support for judges, inmate supervision, commutation and parole decisions.

The current application of AI in Chinese criminal justice system exhibits three main characteristics: (1) the types of AI systems are diverse, and there is a lack of unified evaluation standards; (2) AI is mainly focused on handling routine judicial tasks and is still in the stage of weak AI; (3) AI is positioned as a tool to assist decision-making, rather than replacing human judges or prosecutors in making judgment based on experience and perception.

The application of AI in Chinese criminal justice system contributes to strengthening crime control, improving judicial efficiency, and rationally allocating judicial resources.

The further development of AI technology in Chinese criminal justice system is constrained by two factors: the difficulty in integrating the technical discourse system with the legal discourse system, and the challenge of replicating judicial decision-making reasoning process based on experience.

The application of AI in Chinese criminal justice system faces numerous risks, including justifiability risks, legality risks, judicial fairness danger, decision accuracy risks, data and algorithmic risks and ethical issues.

In the future, the regulatory framework for AI in Chinese criminal justice system should include three aspects: technological regulation, legal regulation focusing on protecting the data rights of the accused, and ethical responsibility regulation.

References

1. Li X. (2021) Inclusive Regulation of Artificial Intelligence in Criminal Justice. 中国社会科学=Social Sciences in China, no. 2, pp. 47–48 (in Chinese)

2. Pei W. (2021) *Digital Due Process: Criminal Proceedings in the Cyber Era*. Beijing: China Legal Publishing House, pp. 93–99. (in Chinese)

3. Shi P. (2024) On the Big Data Investigation: Mainline of the Right to Information Autonomy. 法治研究=Research on Rule of Law, no. 6, pp. 17–18 (in Chinese)

4. Sun D. (2023) AI-Assisting Sentencing: Going Back to Practice and Theoretical Supplement. 学术界=Academics, no. 3, pp. 112–116 (in Chinese)

5. Sun Q. (2022) *Research into the Application of Artificial Intelligence in Judicial Decision-Making*. Beijing: China Social Sciences Press, pp. 164–165 (in Chinese)

6. Wang L. (2018) Discourse Conflict in the Practice of Judicial Big data and Artificial Intelligence. 法学论坛=Legal Forum, vol. 33, no. 5, p. 140 (in Chinese)

7. Wang L. (2024) On Predictive Justice. 中国社会科学=Social Sciences in China, no. 6, pp. 85–88 (in Chinese)

8. Wang Z. (2024) The Institutional Options for Algorithm Explanation in Criminal Justice. 中国政法大学学报=Journal of China University of Political Science and Law, no. 6, pp. 257–259 (in Chinese)

9. Xie Y. (2024) The Dual Missions of China's Criminal Justice Reform in the Age of Artificial Intelligence. 政法论丛=Zheng Fa Lun Cong, no. 5, pp. 85–86 (in Chinese)

10. Xiong Q. (2020) The Application of Artificial Intelligence in Criminal Proof. 当代法学=Contemporary Law Review, no. 3, p.88 (in Chinese)

11. Xiong Q. (2022) Exploring the Application of Artificial Intelligence in Criminal Justice. 上海政法学院学报=Journal of Shanghai University of Political Science and Law, no. 6, p. 111 (in Chinese)

12. Zheng X. (2023) Protection of the Accused's Rights in Context of Application of Judicial Artificial Intelligence. 厦门大学学报(哲学社会科学版)=Journal of Xiamen University (Arts & Social Sciences), no. 6, p. 48 (in Chinese)

13. Zheng X. (2024) Structural Optimization of Criminal Procedure Rights in the Context of Digitalization. 中国社会科学=Social Sciences in China, no. 7, p. 161 (in Chinese)

14. Zheng X. (2025) Regulation of Digital Justice Practices in the Revision of the Criminal Procedure Law. 法学家=The Jurist, no. 1, p. 59 (in Chinese)

15. Zuo W. (2021) Will the Era of AI Judges Come: Based on the Comparison and Outlook of Judicial Artificial Intelligence Between China and Foreign Countries. 政法论坛=Tribune of Political Science and Law, vol. 39, no. 5, p. 7 (in Chinese)

Information about the authors:

Zh. Guo — Professor of Law.

J. Yang — PhD Candidate in Law.

The article was submitted to editorial office 10.03.2025; approved after reviewing 12.03.2025; accepted for publication 17.03.2025.

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

Copyright Law in the Digital Age

Research article
JEL: K15
UDC: 347
DOI:10.17323/2713-2749.2025.1.105.123

Digital Technologies and Forensic Examination of Copyright Works

N.V. Buzova

Russian State University of Justice, Address: 69 Novocheremushkinskaya Str., Moscow 117418, Russian Federation,
nbuzova@yandex.ru, ip_laboratory@mail.ru, https://orcid.org
0000-0003-2268-0345

Abstract

With the ability to enable remote trial sessions and promptly find and forward documents, digital technologies are increasingly used in judicial proceedings worldwide including Russia. However, in view of possible risks artificial intelligence is used at court only in the test mode, including for forensic examination of copyright works as a likely option. The article contains a discussion of the benefits and risks of AI when used for forensic examination. It is argued that AI can only serve as a tool for forensic examination, with shared approaches applicable to all copyright works to be developed and made available to judges, as well as expert opinion templates.

Keywords

copyright; works; artificial intelligence; related rights; forensic examination; digital technologies.

For citation: Buzova N.V. (2025) Digital Technologies and Forensic Examination of Copyright Works. *Legal Issues in the Digital Age,* vol. 6, no. 1, pp. 105–123. DOI:10.17323/2713-2749.2025.1.105.123

Background

Russia has embraced digitization like many other advanced countries as stated in the 2017–2030 Information Society Development Strategy for Russia approved by Presidential Decree No. 203 of 9 May 2017[1] which is focused on the development of digital economy and information society. While digital technologies permeate human activities across the board including public governance, justice is not left behind. As digital technologies are increasingly introduced into judicial proceedings worldwide to make justice more efficient and accessible, they allow to remotely file lawsuits and other documents, support videoconferencing of trial sessions, advise of the course of legal proceedings, find and forward trial documents. Federal Law No. FZ-440 of 30 December 2021[2] makes it legally possible to file e-documents, remotely participate in the trial and use e-documents in legal proceedings, a feature already implemented in court hearings across the country.

Expanded blockchain, chatbots and Artificial Intelligence (AI) could be considered as promising digital technologies for legal proceedings. While blockchain is essentially intended to assure unaltered storage of information to be used as evidence (to confirm facts), chatbots automatically provide information on specific issues (including legal), and support the completion of forms and other documents. Artificial Intelligence has multiple development prospects.[3] In view of potential risks, AI is introduced in the test mode, with an experiment of using AI to draft orders for the justice of peace held in the Belgorod Oblast in 2021 [Drobysheva A.V., 2022: 17–20]. In response to the Federal Tax Service claims, order templates were produced through an algorithmic process using the template designer made on the basis of standard forms developed by the Legal Department under the Supreme Court of the Russian Federation, to be further reviewed by the judge authorized to make the final decision [Momotov V.V., 2022: 2–9]. As a positive outcome, the time spent on drafting a court order was reduced by almost 80 percent [Kabatskaya E.A., 2023: 51–55].

[1] Presidential Decree No. 203 of 9 May 2017 "On the Information Society Development Strategy for Russia in 2017–2030" // Collected Laws of Russia, 2017, No. 20, Art. 2901.

[2] Federal Law No. FZ-440 "On Amending Specific Regulations of the Russian Federation" of 30 December 2021 // Collected Laws of Russia, 2022, No. 1 (Part I), Art. 9.

[3] Presidential Decree No. 490 "On the Development of Artificial Intelligence in Russia" of 10 October 2019 // Collected Laws of Russia, 2019, No. 41, Art. 5700.

The use of digital technologies (including AI) in legal proceedings is normally due to a substantial increase of cases and is intended to reduce the processing time. The studies of harnessing digital technologies for justice show that each country may adopt its own national approach. Technologies including AI can be used throughout the trial to perform all legal procedures across the board (as exemplified by Internet courts in China)[4] or only selectively (as follows from the use of AI in Brazil), see: [Valle V., Fuentes-i- Gasó J.R., Ajus A.M., 2023: 1–38].

China's Internet courts make a wide use of digital technologies ranging from e-filing with plaintiffs scanning documents for an e-case, synchronous transcription of the parties' explanations and evidence (speech-to-text conversion) up to AI-enabled decision-making based on the available and processed information on reported facts and legal provisions [Tahura U.S., Selvadurai N., 2022: 1]. In particular, these courts will handle IP-related disputes.

It is not accidental that intellectual property disputes were selected in China for digital decision-making as more IP-related lawsuits are brought each year worldwide, with intellectual property becoming economically more important by the advance of telecommunication networks capable of ensuring almost instant access to intellectual assets across vast territories.

Harnessing Digital Technologies to Examine Copyright Works

The progress of telecommunication networks has brought about widespread IP violations in the Internet, with not only content and design but also the structure of information resources being subject to unauthorized use to attract more attention and gain other advantages.

Consideration of disputes in respect of copyright and related rights involving the violation of personal non-property rights (as in the case of plagiarism) or exclusive rights (in particular, in case of unauthorized reproduction, remaking etc.) may require special knowledge that the judge might not possess, in particular, for comprehensive inquiry to prove the fact and extent of unauthorized use of an intellectual asset. Such cases may require the involvement of experts to provide an

[4] Online Operation Rules of the People's Courts. Available at: https://cicc.court.gov.cn/html/1/219/199/201/2212.html (accessed: 16.08. 2024)

opinion. As was noted in Supreme Arbitration Court of the Russian Federation Presidium Ruling No. 13765/10 of 9 March 2011, "forensic examination shall be commissioned by the court where legal issues cannot be resolved without reference to the facts that cannot be established without special knowledge".[5] Forensic examination can be carried out by special forensic agencies or individual forensic experts.

As part of the inquiry into violation of copyright and related rights, experts may be asked to:

establish whether the work in question is present in the given medium;

seek information on the creative product or other intellectual asset in the given physical medium (copyright holder's name, granted rights and entitled persons, terms of use etc.);

identify the parameters of a copyright work;

establish the identity, sameness, similarity and matches in the materials made available for analysis.

Moreover, different examinations — authorship, forensic photography, forensic examination of video and audio recordings, phonoscopic, artistic analysis, computer forensic examination — are envisaged in Russia depending on the work to be studied and the type of violation involved. Since 2023 the list of forensic examinations to be carried out at forensic agencies under the Ministry of Justice includes a new kind of examination, that of IP assets,[6] to examine these assets and visual identities.

Thus, a computer forensic expert will identify, depending on the assignment, if computer software, databases and other copyright works were installed in the digital form in a computer or other digital medium, examine actions performed in respect of the said items, identify the relevant information recorded to such devices and media, digital traces and dates these items were created and/or loaded to media, compare the works in question with those recorded to devices and media, and iden-

[5] Supreme Arbitration Court of the Russian Federation, Presidium Ruling No. 13765/10 of 9 March 2011. Available at: URL: https://arbitr.ru/materials/36169?path=%2Farxiv%2Fpost_pres%2F&ysclid=lypnls09bb282437776 (accessed: 17.07.2024)

[6] Ministry of Justice Order No. 72 "On Approving the List of Forensic Examinations at Federal Forensic Agencies of the Ministry of Justice, and the List of Forensic Positions Authorized to Perform Forensic Examinations at Federal Forensic Agencies of the Ministry of Justice" of 20 April 2023 (as amended). Available at: URL: https://base.garant.ru/406790301/ (accessed: 30.06 2024)

tify functional features of the works and other critical technical parameters [Marakhovskaya M.V., Pankevich L.L., Tushkanova O.V., 2015: 128–135].

For example, in case No. A40-90889/2021, a computer forensic expert was asked to establish the dates when the Module for generation of shift work orders for the shared instruction book and ALTAN were created, and to identify whether the source text/code for ALTAN is a reworked version of the Module.[7]

Forensic photography experts are asked to identify image framing, composite images, retouching, image date and time,[8] images from specific footage recorded to a medium (such as memory cards), prove whether the images in question are similar[9], establish technical parameters of the images and camera likely used to make them[10], and also to identify metadata containing the information on the work in question and possible author.[11] In addition, forensic photography serves to "establish the common origin" of images shot by the same camera, "identify the original image, the fact and methods of image alteration" [Moiseeva T.F., Maylis N.P., 2017:155].

Authorship forensic examination may serve to establish (prove) the authorship (still contestable after the examination), identify plagiarism, borrowed/reworded text, pastiches, imitations, specific features of the work in question, identical fragments in disputed copyright works (manuals and articles written by the plaintiff), analyze the work in question for matches with other works, specify non-copyrightable fragments ("principles, models, methods, methodologies, techniques, algorithms and problem solutions").[12]

[7] Moscow Arbitration Court Ruling, case No. A40-90889/2021 of 5 October 2023. Available at: URL: https://ras.arbitr.ru/ (accessed: 16.07.2024)

[8] Court for IP Rights Ruling, case No. A50-28924/2019 of 22 October 2021. Available at: URL: https://ras.arbitr.ru/ (accessed: 16.07.2024); Saint Petersburg City Court Appellate Ruling, No. 33-8361/18 of 17 May 2018 // SPS Consultant Plus.

[9] Saint Petersburg City Court Appellate Ruling No. 33-8361/18 of 17 May 2018 // SPS Consultant Plus.

[10] Moscow City Court Ruling No. 4g/8-7507 of 24 June 2019; Moscow City Court Appellate Ruling, case No. 33-881 of 28 January 2019 // SPS Consultant Plus.

[11] Third General Court of Cassation Ruling No. 88-19109/2020 of 9 December 2020 // SPS Consultant Plus.

[12] First General Court of Cassation Ruling No. 88-8658/2023 of 29 March 2023 // SPS Consultant Plus.

Since Russian Federation laws and other regulations do not define how much text or other material from a copyright work amounts to plagiarism, reproduction or citation, the involvement of a forensic expert may be required to analyze the use of a protected intellectual asset. In identifying matching or reworded text, the expert will confirm or dismiss part of claims or, more exactly, provide additional information on the work in question required for decision-making; describe the intellectual asset, identified information and manipulations with the asset, devices and media but will not qualify them. These facts and information will be evaluated by court with reference to the expert's opinion. The judge will qualify the defendant's actions in light of available evidence and conclude whether there was a violation.

Apart from plagiarism and borrowed/reworded text, experts are asked to identify "original text editing, whether the borrowed text (fragments thereof) is original/non-original or commonly used" [Galiashina E.I., 2006: 178].

Phonoscopic forensic examinations concern works subject to related rights such as performances and sound recordings. (It should be noted that while disputed sound recordings may be associated with the same pieces of music performed by the same artists, they can represent works covered by specific legal protection if the recordings were made, in particular, at different times or by different producers, or if one audio recording is a duplicate (copy) or derivative (cover version) of the other.

A phonoscopic examination requires technical expertise to identify any signs of arrangement, distortion, noise or modulation since alterations to the recorded sound can affect even the properties of digital files. The expert can perform an instrumental analysis in order to not only identify metadata associated with the recording and its parts, but also to compare the spectral features of specific sound fragments, identify alterations to the signal, phase spectrum of signal harmonics, background and noise induction, as well as phase differences, discontinuities or jumps.

Digital technologies can apparently help with the said tasks to some extent. N.S. Polevoy advocated the use of mathematical/cybernetic methods in forensic science and legal procedures in his book "Forensic Cybernetics" back in 1982 [Polevoy N.S., 1982]. The issues of using mathematical methods/models and computer technologies for forensic examinations were also raised by other Soviet and Russian researchers, in particular, T.V. Averianova [Averianova T.V., 2009]; R.S. Belkin [Belkin R.S., 1987]; N.V. Vitruk [Polevoy N.S., Vitruk N.V. et al., 1977]; N.A. Zamaraeva [Zamaraeva N.A., 2001]; D.I. Nemchin [Nemchin D.I., 2002]; E.V. Piskunova [Piskunova E.V., 2016]; T.V. Tolstukhina [Tolstukhina T.V., 1997]; [Tolstukhina T.V., 1998]; [Tolstukhina T.V., 1999], etc.

Forensic examinations are normally time-consuming (authorship examination in case No. A63-22578/2017 took more than one month[13]), only to protract the trial. In addition, the parties, doubtful of the expert's competence, may argue that conclusions are wrong and that the forensic examination procedure was grossly violated[14] and ask the court to resume or commission another examination (Article 87 of the Civil Procedural Code and Article 87 of APC), thus protracting the trial even further. Since digital technologies can store and rapidly process considerable amounts of information, the question is whether a technology (for instance, AI) can replace a human expert.

Harnessing technologies for forensic work will undoubtedly bring some benefits such as faster proceedings and avoidance of subjective bias since no technology will favor a party on the basis of personal, subjective factors.

According to E.V. Piskunova, mathematical methods will not only save time and improve the performance of forensic examinations but also make them objectifiable and even preserve the works to be studied. Mathematical research methods are now used in a majority of forensic examinations [Piskunova E.V., 2016: 34].

But will the technology always take precedence over man, and can it completely replace human expertise?

Digital services that can identify information contained in different devices and media and perform comparative analysis are already available and used, in particular, in forensic examinations to discover IP violations. *Transcribe*, for example, allows to identify a musical fragment in a recording, produce a transcript and also graphically represent sound intensity and other parameters[15] while *Shazam* helps identify musical

[13] Stavropol Regional Arbitration Court Ruling of 14 September 2018, case No. A63-22578/2017. Available at: URL: https://ras.arbitr.ru/ (accessed: 16.07.2024)

[14] Court for IP Rights Ruling, case No. A40-196910/2021 of 29 December 2022. Available at: URL: https://ras.arbitr.ru/ (accessed: 16.07.2024)

[15] Transcribe App and Online Editor. Available at: URL: https://transcribe.com/ (accessed: 16.07.2024)

pieces, audiovisual works etc. by a recorded fragment and retrieve information on metadata. The application makes a digital footprint of a musical piece which is then compared with music in databases. The output includes information on the piece such as its title, performing artist's name, lyrics etc.[16] *Acoust ID* will also identify music by an audio footprint helping to find the associated information (title, performer etc.) in databases using metadata.[17] Applications such as *Echoprint*, *Sound Hound* etc. also serve to create digital footprints and identify audio file contents.

Antiplagiat, Rukontekst and other systems are used by universities to identify borrowings in thesis and dissertation studies. Antiplagiat will identify whether the so-called target text (word string) matches the texts and other materials in the connected units (databases) to calculate the percentage of original text, citations, self-citations and matches. The output will contain references to sources of matches, citations and self-citations including matching fragments in the identified sources. Each university, publisher or another organization interested in text publication has its own criteria of originality and text matching tolerances.

Digital services can be apparently adapted as a digital tool for forensic study to expedite opinion drafting.

Meanwhile, the currently available analytical systems have certain defects since matches are identified both within paragraphs and other parts of the text while what is counted as matches (paragraphs, sentences and word combinations) may be widely scattered and logically disconnected. Thus, Antiplagiat has certain inaccuracies, such as marking the text as a match rather than citation despite a reference to the source, and showing sources of matches irrelevant to the subject of study and not containing the target text. Some of the system's defects are discussed in more detail in Sergo's article "Antiplagiat and other ways to undermine the quality of research texts" [Sergo A.G., 2023: 40–45].

Further, the outcomes generated by both musical and literary services depend on the contents of connected databases used to check whether the data they contain are reliable. While an expert also relies on available data, he will need considerably more time to find and request information required for control than a web service would. However, if informa-

[16] Shazam. Available at: URL: https://www.shazam.com/ru-ru (accessed: 16.07.2024)

[17] Acoust ID. Available at: URL: https://acoustid.biz (accessed: 16.07.2024)

tion is not adequate or sufficient, the expert can keep searching while a digital service will confine itself to available resources.

In a comparative study, both the expert and the digital service will identify text fragment matches which may indicate that the authors (of the target text and similar text that the service refers to) has borrowed or used the same sources both copyright-protected or not (such as regulations, court rulings, information materials referred to in Article 1259 of the Civil Code) that do not require the copyright holder's consent. Matches can include, in particular, set phrases such as those used in copyright law that can be both found in regulations and doctrinally developed: violation of exclusive right, bypassing digital rights management, entity for collective rights management etc. As someone possessing special knowledge in the given field, the expert will normally know set phrases while digital services are yet to be refined in this regard.

The methodological guidelines for Antiplagiat provide for a possibility of such matches — for example, papers on jurisprudence can have fragments of court rulings, regulations, references to historical sources or archived documents [Belenkaya O.S., Strelkova I.B., Filippova O.A. et al., 2021: 13].

As follows from the methodological guidelines mentioned, Antiplagiat-checked texts will require a review: the system only serves as an aid to identify large unauthorized borrowings where the sources to be compared with the target text are loaded to the connected module.

In performing a comparative analysis of copyright works to identify available related information, experts will not only note exact matches but also characterize the items in question since courts in specific cases have to establish the protectability of disputed work where authorship or title is a matter of controversy. As observed in the opinion of a commission for examination of artworks in case No. 88-6869/2023, "the plaintiff's pictures... exhibit clear physiognomic, stylistic and proportional features of *Antoshka* and *Domovenok Kuzya* from the eponymous cartoons and the underlying animated (stop-motion) images. The plaintiff's pictures do not exhibit a well-thought composition or clearly constructed and original coloristic manner...".[18]

Depending on the assignment, experts can examine not only disputed artworks but also the author's whole creative output to identify

[18] Second General Court of Cassation Ruling of 27 April 2023, case No. 88-6869/2023 // SPS Consultant Plus.

speech patterns and style. In performing an authorship examination in case No. 2-24/2021 to recognize authorship and co-authorship of research papers, the expert observed a characteristic "diversity of introductory modal constructions, expressive syntax patterns in the form of author monologue segmented as questions and answers, parceled complex sentence patterns, active use of conjunctive constructions involving *that*, and other speech patterns not found in the disputed articles".[19]

Thus, forensic examination of copyright works is essentially exploratory rather than technical as noted by specialists including T.F. Moiseeva who pointed out that "it is research that makes forensic examination different from other forms of special knowledge" [Moiseeva T.F., 2024: 6]. Meanwhile, forensic examination of copyright works is not just research but creative research since the target works are themselves creations. A similar approach equally applies to works subject to related rights such as performances that are also treated as creations. In respect of these works, digital services can still play only auxiliary roles.

Can artificial intelligence be a better fit for forensic purpose?

This article does not purport to give a definition of artificial intelligence which is defined, in particular, by Federal Law No. FZ-123 "On the Experiment to Establish Special Regulation to Enable the Development and Introduction of AI Technologies in the Federal City of Moscow as a Constituent Territory of Russia, and on Amending Articles 6 and 10 of the Federal Law on Personal Data" of 24 April 2020. As follows from paragraph 2, Article 2 of this Law, a technology in order to be recognized as AI should "mimic human cognitive functions (including self-learning and searching for solution outside a preset algorithm) and handle specific assignments with an outcome at least comparable to that of human agents".[20] Similar definitions could be found in national standards such as GOST R 59277-2020 "Artificial Intelligence System. Classification of AI systems" (para. 3.18).[21] Specialists view artificial

[19] Seventh General Court of Cassation Ruling of 12 May 2022, case No. 88-6581/2022 // SPS Consultant Plus.

[20] Federal Law No. 123-FZ "On the Experiment to Establish Special Regulation to Enable the Development and Introduction of AI Technologies in the Federal City of Moscow as a Constituent Territory of Russia, and on Amending Articles 6 and 10 of the Federal Law on Personal Data" of 24 April 2020 // Collected Laws of Russia, 2020, No. 17. Art. 2701.

[21] National Standard of the Russian Federation GOST R 59277-2020 "Artificial Intelligence System. Classification of AI systems". Available at: URL: https://docs.cntd.ru/document/1200177292?ysclid=m1ujrmwo2e845963311 (accessed: 16.07.2024)

intelligence as a heuristic setup rather than data processing algorithm since heuristics is closer to human behavior by virtue of decision-making based on specific instructions, search rules and arguments [Piskunova E.V., 2016: 67].

Moreover, it is worth noting that AI, unlike many digital services today, does not boil down to a software connected to a database. According to researchers, "machine learning was actually inspired by neurobiological exploration of how information is processed by human brain". However, despite the advances in science including neurophysiology, technologies are yet unable to imitate human cognitive functions, including because it is not fully clear how information is transmitted and processed by human nervous system, something that affects behavior and decision-making and would allow to create technologies with similar capabilities. Researchers still do not know "how the brain encodes cognitive information and how the next AI generation could use it" [Medvedev Yu., 2020]. Meanwhile, other researchers have a different, albeit arguable, view that "advanced ML (Machine Learning) methods are no longer focused on biological models" [Anokhin K.V., Novoselov K.S., Smirnov S.K. et al., 2022: 98, 102].

The current AI technologies can be characterized as "weak" artificial intelligence perfect for searching and comparing information from an enormous body of data. Such technology is essentially an improved high-performance software. For AI to "learn" and later "self-learn" to perform forensic examination, the process has to be algorithmized but this is hampered by a lack of clear criteria in the Russian law, including the (terms) of protectability of copyright works.

The Civil Code of Russian Federation defines the "author" as "an individual whose work has resulted in a creation or other intellectual output" (Articles 1228 and 1257). As follows from Article 1257 and 1259 of the Civil Code, a creation shall be deemed protectable if embodied in an objective form. Such approach supported by specialists [Pavlova E.A., 2023:289] is also reflected in the Supreme Court of the Russian Federation explanations contained in paragraph 80 of Supreme Court Plenum Resolution No. 10 "On Applying the Civil Code of Russia, Part Four" of 23 April 2019.[22] This paragraph implicitly provides that novelty, uniqueness and/or originality can all be the qualifying cri-

[22] Supreme Court Plenum Resolution No. 10 "On Applying the Civil Code of Russia, Part Four" of 23 April 2019. Available at: URL: https://www.vsrf.ru/documents/own/27773/ (accessed: 30.06.2024)

teria of creative work. In particular, E.P. Gavrilov [Gavrilov E.P., 2020: 303–306] believed singularity, originality and uniqueness to be characteristic of creative work. He argued that while novelty was characteristic of works subject to patent law, those subject to copyright were characterized by originality. Meanwhile, according to A.P. Sergeev, novelty and originality are interchangeable [Sergeev A.P., 2001: 111]. However, as also follows from paragraph 80 of the Resolution, a failure to meet the above criteria (novelty, uniqueness and originality) does not imply that the author's work is not creative. Yet the Civil Code does not provide a definition of "creative work".

Thus, there are no clear criteria established by law for the expert to conclude that a product is the outcome of creative work. He can describe a work's characteristics as a proof of the author's creative efforts for the court to conclude whether someone's intellectual property is protectable, borrowed or used. In examining an artwork (floral design used as a print on various goods) and goods themselves, an expert has observed that the plaintiff's creative input was manifested "in the selection of floral items to create a design; in the development of a unique composition viewable from different angles and changeable depending on the viewer's perspective; in the development of individual principles to produce stylized floral designs as well as methods of artistic presentation (using stains, contours and colors to suggest a form)...".[23]

The notions of "creation" and "creative work" could be viewed as abstractions that present one of the most significant challenges for replacing human experts with technologies such as AI. A lack of clear criteria to define "creation" is a challenge for fully digital forensic examination as the accuracy of results produced by technology will increase with more clear-cut parameters to be checked and accounted for. The more abstract the criteria, the higher the likelihood of deviation, with more examples to be processed to identify common characteristics.

The question of qualifying criteria was raised back in the Soviet time including by V.Ya. Ionas [Ionas V.Ya., 1963]; V.I. Serebrovsky [Serebrovsky V.I., 1956]; B.S. Antimonov and E.A. Fleishits [Antimonov B.S., Fleishits E.A., 1957], who believed originality and novelty to be the criteria or, more precisely, features of creative work. Moreover, according to V.I. Serebrovsky, novelty "can be expressed in a new content, new form, or new idea, new scientific concept" [Serebrovsky V.I.,

[23] Second General Court of Cassation Ruling of 18 June 2020 // SPS Consultant Plus.

1956: 35]. B.S. Antimonov, E.A. Fleishis argued that novelty could find its expression in the work's underlying idea and imagery [Antimonov B.S., Fleishits E.A., 1957: 85, 120]. V.Ya. Ionas believed that novelty could be reflected in different features shared by all works of art such as objective form of the work's existence, language, imagery, ideas and emotional content, and in artistic form and storyline as additional features proper of literature and arts [Ionas V.Ya., 1963: 68]. While these researchers identified what is likely to prove the author's creative work, these qualifying features are not binding either for the Soviet or under the Russian law. These characteristics could only be taken into account by experts in providing an opinion on protectability and use of protected intellectual assets.

One must admit that technologies are able to identify similarities in the storyline or imagery. The works narrating a story (such as fiction, drama, audiovisuals) share a certain intrinsic structure, specific patterns including arranging and developing a plot as a certain sequence of events, and presence of some elements that make up a story. The number of possible storylines is believed to be limited. Where Georges Polti has identified 36 storylines common in 19th century[24] and Jorge Luis Borges just 4,[25] researchers now count over 1,000 ones. Undoubtedly, while numbers can differ depending on the preset criteria, one must agree that there are limits to storylines, especially for works of art, something that makes it possible to systematize and classify them.

Researchers believe today's neural networks to be able to collect a large number of facts and establish certain patterns. Moreover, AI can draw logical conclusions [Anokhin K.V., Novoselov K.S., Smirnov S.K.et al., 2022: 99]. The currently used AI technologies based on prompts — text queries describing the task for neural network — can generate the results relating to literature and arts. In learning from works that exist in an objective form, the technology will "memorize" schemas, samples, patterns of the studied works, with higher statistics of repetitions making the "idea" of these elements more "definite". In other words, the analysis and descriptions of works can be regarded as an opposite action to processing of prompts and generating a prompt-based outcome. Thus,

[24] Polti G. Les 36 situations dramatiques. Paris, 1895. Available at: https://www.gutenberg.org/cache/epub/72036/pg72036-images.html (accessed: 16.07.2024)

[25] Borges J.L. Los cuatro ciclos. Available at: https://www.babelmatrix.org/works/es/Borges%2C_Jorge_Luis-1899/Los_cuatro_ciclos (accessed: 16.07.2024)

the representation of characteristics of different works can be handled by technologies. A similar approach could apply to characters that can be copyright-protected in Russia (paragraph 7, Article 1259 of the Civil Code). Creating digital tools to identify similarities between storylines and characters would help experts identify derivative works, borrowings and remakes.

E.V. Piskunova in her article “Computer technologies and forensic work”, gives a number of examples of harnessing computer technologies to examine the works of art. In particular, she refers to the Polish writer Stanislaw Lem’s idea of decomposing the works of an author in a multidimensional coordinate system for spatial representation of critical features such as style, storyline, composition, structure, language etc. This will make a graphical cluster characterizing the author’s work where imitations will be outliers. This idea was implemented to some extent by Swedish researchers through analysis of each author’s language who concluded that individual features of each writer would help with identifying authorship. In addition, E.V. Piskunova refers to a mathematical method based on identifying critical “features of the artist’s personal style” implemented by researchers at the Cornwall University to identify whether artworks were authentic. In converting these features into numbers and formulas, they divided the work in question into calculable fragments to be compared with those of the original artist [Piskunova E.V., 2016: 107, 108].

Meanwhile, works subject to copyright and related rights are diverse, with each intellectual output being specific in terms of its structure, expressive means and other creative features. Thus, a storyline is not so critical for composite works, computer software and databases as it is for literary works; they are peculiar in the structural arrangement of textual or other materials while computer applications differ in their functions, and databases might not only have a specific structure but will differ in the way they process and systematize data including search engines etc. An analysis of current legal precedents in Russia with regard to copyright protection of photographs reveals a general trend where the author’s creative input plays only a minor role for copyright protection of photographs. According to Russian courts, creative work may manifest itself in specific light settings, choice of exposure, spatial arrangement of objects, etc.[26]

[26] Court for IP Rights Ruling of 3 February 2022, case No. A57-213/2021. Available at: URL: https://ras.arbitr.ru/ (accessed: 30.06.2024)

Moreover, works subject to related rights are not so homogeneous as the original creations. Whereas performances also share certain creative features such as artistic form inherent in artworks (it is not by accident that a proposal to qualify performance as derivative work was discussed in amending the Bern Convention for the Protection of Literary and Artistic Works), recordings and broadcasts lack the features proper of copyright works as they present other parameters of technical nature. For databases protected by related rights, critically important parameters will be both quantitative (such as the content in excess of 10,000 independent data units) and qualitative, in particular, financial costs to collect and maintain the information that makes up the database.

It should be also borne in mind that while digital technologies could process the items represented in digital form, intellectual outcomes may take a variety of forms. That is, technologies can apply to digital objects or objects converted to digital form beforehand. However, one should remember that conversion of certain works into digital form may result in a loss or distortion of specific parameters (nuances of color, light, sound) of paramount importance in certain cases. Thus, a change of material for a copyright work such as sculpture can affect the overall impression and perception by not only users but also specialists, only to undermine the final conclusion with regard to unauthorized use such as reproduction as well as reworking considered by Article 1270 of the Civil Code as independent use.

Using and borrowing copyright works to make other creations can be normally proved by matches identifiable by comparative analysis. Meanwhile, in order to use digital technologies for this purpose, all features common to the respective types of intellectual outputs should be taken into account. Thus, the diversity of items subject to copyright and related rights will require to develop either different tools for each intellectual outcome or (which appears more efficient) shared technology that would allow to account for the diversity of intellectual properties, their creative features and forms of expression.

With advances in AI technologies, the identification of works generated by AI becomes an increasingly challenging task. The expert can check the information that comes with the generated outcome (heading, description, comments and hashtags) for reference to AI, perform reverse image search, look for distortions. Analysis of text outcomes will focus on the absence of grammatical errors and certain discontinuity of individual fragments, lack of emotional coloring, professional jargon and non-typical abbreviations.

AI-generated items will sometimes have watermarks: for example, Open AI Dall-E 2 images will have five multicolor squares in the bottom right corner while Dall-E3 images — visible CR symbols in the upper left corner. Moreover, watermarks will be sometimes added to metadata.

However, it may well be that the said process will fail to achieve the objective of clearly identifying AI-generated outcomes. Even the increasingly used watermarks do not provide absolute protection and, since they could be deleted, may be of no help.

In this regard, harnessing digital technologies including AI to identify texts and other AI-generated outcomes holds a promise. It is worth noting the already available services able to identify works generated or edited by AI. For texts, these include *AI Detector* by text.ru, *Ai Busted*, *AI Content Detector*, *AI Text Classifier*, *Crossplag*, *GPT Zero*, *Contentat Scale*, *Copyleaks*, *Corrector*, *Sapling*, *Writer AI Content Detector*, *Writer*, *Zero GPT,* etc.; for images, *Hive Moderation*, *Optic AI or Not*, *AIArt Detector* etc. However, these services have limitations and are prone to error, with AI-generated outcomes sometimes attributed to man while those of human intellect attributed to AI.

Conclusion

Thus, digital technologies can be harnessed to perform forensic examination in disputes on violation of copyright and related rights. However, a number of steps will need to be taken before these technologies are fit for the purpose.

AI learns on a large number of valid examples. Where they are unavailable or deficient, the results may have defects while the technology will need to be validated in respect of those works that have a stock of expert opinions.

Overall, the development of shared approaches through standardization could be beneficial for forensic examination in the area of copyright and related rights as was repeatedly stressed by specialists, in particular, E.I. Galiashina [Galiashina E.I., 2020: 144–148]; [Galiashina E.I., Privodnova E.V., 2006: 761]; N.P. Maylis, T.F. Moiseeva [Maylis N.P., Moiseeva T.F., 2018: 219–224]. Before technologies could be used, it is needed to develop the relevant methodologies applicable to all copyright works to be accounted for in the examination algorithm (while such methodologies are available for examination of recordings and computer software [Galiashina E.I., 2006: 177], they are still emerging in respect of other copyright works). Unless there is a tried-and-tested methodology, using a digital technology including AI to perform forensic examination and make an opinion appears premature. The methodologies underlying the AI-enabled examination algorithms should be open and available to judges. But even with the shared methodologies, algorithms and machine learning templates for AI to make draft opinions, the technology would only provide a tool to expedite the examination and legal proceedings as a whole. It is the expert who will have the final word and confirm the (generated) draft opinion.

References

1. Anokhin K.V., Novoselov K.S., Smirnov S.K. et al. (2022) Scientific uses of artificial intelligence and a science of Artificial Intelligence. *Voprosy filosofii*=Issues of Philosophy, no. 3, pp. 93–105 (in Russ.)

2. Antimonov B.S., Fleishits E.A. (1957) *Copyright Law*. Moscow: Gosyurizdat, 278 p. (n Russ.)

3. Averianova T.V. (2009) Forensic Examination. A Course of General Theory. Moscow: Norma Publishers, 479 p. (in Russ.)

4. Belenkaya O.S., Strelkova I.B., Filippova O.A. et al. (2021) Methodological Guidelines for Forensic Examination of Dissertations for Original Content in the Antiplagiat System. Saint Petersburg: Lan Publishers, 92 p. (in Russ.)

5. Belkin R.S. (1987) *Forensic Science: Challenges, Trends, Prospects. General and Special Theory.* Moscow: Yuriduchrskaya literatura, 270 p. (in Russ.)

6. Drobysheva A.V. (2022) Prospects of Using AI in the Peace Justice Court System. *Mirovoy sudiya*=Peace Judge, no. 11, pp. 17–20 (in Russ.)

7. Galiashina E.I. (2006) Potential of Forensic Examination of Speech for IP Protection. *Yurislingvistika*=Legal Linguistics, no. 7, pp. 176–191 (in Russ.)

8. Galiashina E.I. (2020) Towards Higher Quality of Forensic Examination of Recordings through Standardization. *Vestnik ekonomicheskoy bezopasnosti*=Bulletin of Economic Security, no. 4, pp. 144–148 (in Russ.)

9. Galiashina E.I., Privodnova E.V. (2006) Authorship Examination in the Legal Proceedings in Russia**.** *Russkiy zakon*=Lex Russica, no. 4, pp. 755–761 (in Russ.)

10. Gavrilov E.P. (1984) *Soviet Copyright Law. Basic Concepts. Development Trends.* Moscow: Nauka, 222 p. (in Russ.)

11. Gavrilov E.P. (2020) *Intellectual Property Law. General Provisions. XXI Century.* Moscow: Yurservitum, 492 p. (in Russ.)

12. Ionas V.Ya. (1963) The Creative Work Criteria Work in Copyright Law and Case History. Moscow: Yuridicheskaya literatura, 138 p. (in Russ.)

13. Kabatskaya E.A. (2023) Harnessing Artificial Intelligence to expedite legal proceedings. *Rossiyskiy sudiya*=Russian Judge, no. 10, pp. 51–55 (in Russ.)

14. Maylis N.P., Moiseeva T.F. (2018) Standardization of forensic examination as a prerequisite of its progress. *Vestnik Nizhegorodskoy Akademii MVD Rossii*= Bulletin of Nizhniy Novgorod Academy of Internal Ministry, no. 2, pp. 219–224 (in Russ.)

15. Marakhovskaya M.V., Penkevich L.L., Tushkanova O.V. (2015) Public Law Copyright Protection Methods for Computer Software. Manual. Moscow: RGUP Press, 276 p. (in Russ.)

16. Medvedev Y. Academician Anokhin: AI today is a black box. *Rossiyskaya Gazeta*=Gazette of Russia, 20.10. (in Russ.)

17. Moiseeva T.F. (2024) Commissioning Forensic Examination: Methodological Guidelines. Moscow: RGUP Press, 40 p. (in Russ.)

18. Moiseeva T.F., Maylis N.P. (2017) Forensic Examination. Introductory Course. Manual. Moscow: RGUP Press, 224 p. (in Russ.)

19. Momotov V.V. (2022) Justice of the Peace: State, Challenges, Prospects. *Mirovoy sudiya*=Justice of the Peace, no. 3, pp. 2–9 (in Russ.)

20. Piskunova E.V. (2016) Computer Technologies and Forensic Work: Lectures. Moscow: RGUP Press, 152 p. (in Russ.)

21. Polevoy N.S. (1982) *Forensic Cybernetics*. Moscow: MGU University Press, 208 p. (in Russ.)

22. Polevoy N.S., Vitruk N.V. et al. (1977) The Principles of Applying Cybernetics to Legal Studies. Moscow: Yuridicheskaya literatura, 272 p. (in Russ.)

23. Serebrovsky V.I. (1956) *Copyright Law Issues in the Soviet Union.* Moscow: USSR Academy of Sciences, 283 p. (in Russ.)

24. Sergeev A.P. (2001) Intellectual Property Law in Russia. Textbook. Moscow: Prospekt, 752 p. (in Russ.)

25. Sergo A.G. (2023) Antiplagiat and other Ways and Means to Undermine the Quality of Research Texts. *Zhurnal po intellektualnym pravam*=Journal of Intellectual Rights, no. 4, pp. 40–45 (in Russ.)

26. Tahura S.U., Selvadurai N. (2022) The Use of Artificial Intelligence in Judicial Decision-making: the Example of China. *International* Journal *of Law*, *Ethics and Technology*, no. 3, pp. 1–20.

27. Tolstukhina T.V. (1998) Automation for Forensic Examination of Road Vehicles. Manual. Tula: University Press, 137 p. (in Russ.)

28. Tolstukhina T.V. (1997) Mathematic Methods in Forensic Science. Manual. Tula: University Press, 215 p. (in Russ.)

29. Tolstukhina T.V. **(**1999**)** The Current Trends of IT-Enabled Forensic Examination. Doctor of Juridical Sciences Thesis. Moscow, 320 p. (in Russ.)

30. Valle V.C., Fuentes-i-Gasó J.R., Ajus A.M. (2023) Decisão judicial assist i daporin teligência artificial e o Sistema Victor do Supremo Tribunal Federal. *Revista de Investigações Constitucionais*, vol. 10, no. 2, pp. 1–38.

31. Zamaraeva N.A. (2001) The Legal, Organizational and Methodological Issues of Forensic Use of Computer Technologies. Candidate of Juridical Sciences Thesis. Moscow, 202 p. (in Russ.)

Information about the author:

N.V. Buzova — Candidate of Sciences (Law), Assistant Professor.

The article was submitted to editorial office 18.10.2024; approved after reviewing 04.04.2025; accepted for publication 04.04.2025.

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

Review
JFL: K1
UDK: 340
DOI:10.17323/2713-2749.2025.1.124.148

Artificial Intelligence and Law: From Theory to Practice

I.Yu. Bogdanovskaya[1], E.V. Vasiakina[2], A.A. Volos[3], N.A. Danilov[4], E.V. Yegorova[5], D.R. Salikhov[6], V.A. Kalyatin[7], O.I. Karpenko[8]

[1, 2, 3, 4, 5, 6, 7, 8] National Research University–Higher School of Economics, 20 Myasnitskaya Str., Moscow 101000, Russian Federation

[1] ibogdanovskaya@hse.ru, SPIN РИНЦ: 9334-5490, ORCID: 0000-0002-6243-4301, Researcher ID: A-9675-2014

[2] evasyakina@hse.ru, SPIN РИНЦ: 3972-4010, ORCID: 0009-0006-9016-988X, Researcher ID: KLZ-2932-2024

[3] avolos@hse.ru, SPIN РИНЦ: 4520-7706, ORCID: 0000-0001-5951-1479, Researcher ID: AAM-7949-2020

[4] danilov@hse.ru, ORCID: 0000-0003-4924-202X, Researcher ID: AAH-7720-2019

[5] evegorova@hse.ru, SPIN РИНЦ: 9101-5201, ORCID: 0000-0002-8424-8980, Researcher ID: M-4716-2015, Scopus Author ID: 57189028712

[6] dsalihov@hse.ru, SPIN РИНЦ: 5813-9980, ORCID: 0000-0001-5247-1312, Researcher ID: AAI-6467-2021

[7] vkalyatin@hse.ru, SPIN РИНЦ: 3312-6790, ORCID: 0000-0002-2927-6591, Researcher ID: M-2393-2015, Scopus Author ID: 55090215100

[8] okarpenko@hse.ru, ORCID: 0000-0003-1456-3261, Researcher ID: M-8288-2016

Abstract

On October 18, 2024 the XIII International Scientific and Practical Conference “Law in the Digital Age” was held at the Faculty of Law of the Higher School of Economics (HSE). This year it was devoted to the topic of artificial intelligence (AI) and law. It was considered from the standpoint of both private and public law. The conference covered the issues of the civil law regime of artificial intelligence technologies and objects created with its use, artificial intelligence and intellectual property law, as well as the topic of generative content and protection of the interests of copyright holders. The topic of regulation and self-regulation of artificial intelligence, including artificial intelligence in Legal Tech, is highlighted. Introduction of Artificial Intelligence Technologies in Labor Relations: Successes, Failures, Prospects Criminal Law Protection of Digital Economy and Finance Entities Using Elements of Artificial Intelligence. Thus, the conference attempted a comprehensive discussion of the role of law in the development of AI technologies. This approach made it possible to show the relationship between the methods of legal regulation in this area, their interaction to create conditions for the development of AI technologies. The conference raised both practical and theoretical issues of the development of law in the new conditions, as well as the problems of the development of legal education.

Keywords

generative artificial intelligence; law; digital technologies; civil law regime; labor law; public law; criminal law.

For citation: Bogdanovskaya I.Yu., Danilov N.A., Egorova E.V., Kalyatin V.O., Karpenko O.I., Salikhov D.R., Vasiakina E.V., Volos A.A. (2024) Artificial Intelligence and Law. *Legal Issues of the Digital Age,* vol. 6, no. 1, pp. 124–148. DOI:10.17323/2713-2749.2025.1.124.148

1. In opening the XIII International Research Workshop “Law in the Digital Age”, **V.A. Vinogradov**, Doctor of Sciences (Law) and Legal Department Dean, HSE, has noted that its main purpose was to exchange the best practices and knowledge in the field of law and digital change, with more than 350 researchers from Russia and other countries (Uzbekistan, Kazakhstan, Belarus, South Africa, Brazil, India, China) having applied to take part in the workshop. **V.A. Vinogradov** has thanked the participants for their desire to be involved in this already traditional research event and wished them fruitful work.

I.Yu. Bogdanovskaya, Doctor of Sciences (Law), Tenured Professor, Editor-in-Chief of the journals *Law*. *Journal of the Higher School* of *Economics* and *Legal Issues in the Digital Age*, has noted that the workshop annually handled legal issues most relevant to the digital age, its main topic this year is *AI and Law*. While the workshop was undoubtedly multidisciplinary, lawyers were proposed to discuss at this stage the legal aspects and development prospects.

Artificial intelligence (AI) permeates different aspects — from fundamental issues of legal understanding to legislative development. On the one hand, artificial intelligence has not resulted in a change of legal paradigm, normativism still predominant in its assessment. But the traditional formal logical approach comes to be supported by technological approach believed to improve the efficiency of the legal system. The issues of legal personality and liability, categorical system, traditional for positive law, are gaining relevance. On the other hand, the question is about further development of traditional legal principles (such as the rule of law) in the AI age. The workshop is called upon to find out whether legal conditions for AI development are being created and how AI affects the legal profession as a whole, legal education and standards of legal studies.

The plenary meeting was moderated by **A.V. Neznamov**, Managing Director, Center for Human-Centric AI Regulation at Sberbank.

In his report *Weighted approach: maintaining an enabling environment for AI development*, **S.S. Kalashnikov***,* Head, IP/IT legal issues, Yandex, has identified two approaches to AI worldwide: comprehensive normative regulation (China) and regulation/self-regulation mix (in most other countries). The emerging technology ensures the competitive edge of domestic solutions, with the normative regulation to be introduced where it is clear how it will affect the technology. Meanwhile, it is important to encourage the development of sectoral rules.

B.A.Yedidin, Deputy General Director for Legal Issues, Internet Development Institute (IDI), has discussed the *AI's practical and legal aspects for web content creation*. Based on the study of other countries' copyright law, he has identified the trends to deny AI registration as an author/inventor, as well as those to dismiss claims for lack of proof in the event of similarity between the original and AI-generated image or in the event of damage. With regard to deep fakes, there is a trend for the need to seek consent, as well as prohibition to use deep fakes for political, fraudulent and pornographic purposes. AI content labeling regulation in China and EU was specifically discussed.

M.I. Takhaviev, Project officer, Big Data Association, has dwelled on *AI learning data availability and safety*. While noting legislative innovation, he discussed the risk assessment methodology of the Big Data Association. The data leakage model assesses the risk of confidential information leakage from anonym data, as well as probability of identifying or recovering primary data from anonym data sets. The customer data processing risks can (and should) be measured for each specific business case. Available techniques and technologies allow to reduce re-identification risks down to almost zero even where primary data is used. The use of confidentiality enhancing technologies occupies the grey zone where regulation lags behind their progress. With a risk assessment model established and trusted intermediaries regulated, AI learning data will become more readily available and an adequate level of confidentiality will be maintained.

S.A. Makhortov, Head of legal practice at the Radio Frequency Regulation Center, has discussed *Generative AI's risks, challenges, development and regulatory prospects*.

In his report *Concept of a system of coherent subjective rights of man and AI*, **Yu.M. Baturin**, Russian Academy of Sciences corresponding member, Doctor of Sciences (Law) has proposed to abandon the track of apparently unpromising discussion on whether AI could have a number of subjective rights, and to consider instead the *man-AI* pair from the perspective of very large (complex) systems with collective behavior of constituent parts, that is, coordinated (coherent) action within the said pair exercised via the roles assumed by each one. By doing this, we can drop the customary pattern "subject A's right is matched by subject B's duty and vice versa" and discuss "AI rights" as coherent to those of human operator and exercised via the latter. AI's role duties encourage team work with human operator like in sports or ballet where coherent interaction is so harmonious that player's right to pass a ball or dancer's right to take a step cannot be challenged. In a way, regulation of specific interactions resembles the Confucian tradition in the Eastern law where the ritual *li* (role duty in AI case) functions along with the law *fa,* with *li* controlling and *fa* assisting with control; *li* and *fa* complement each other by allowing to accentuate now *li*, now *fa*; *li* ensures harmony while *fa* restores broken harmony.

This approach is doubtless largely different from the Western (and Russian) legal principle whereby "I respect your right and do not trespass unless your right is contrary to mine". As a matter of conclusion, instead of attempting to regulate the use of and interaction with such complex thing as AI along the lines of legal tradition, it would be reasonable, as an option, to adopt the principle of respecting AI's role duties in its interaction with man. It is feasible to regulate coherent rights and role duties via the development of collaboration standards between AI and man.

At the plenary meeting, the national approaches to the issue "AI and Law" were discussed.

In discussing the *Legal principles of using AI technology: the experience of Uzbekistan*, **A.Kh. Saidov**, Academician of the Academy of Sciences of the Republic of Uzbekistan, Doctor of Sciences (Law), Professor, Deputy of the Legislative Chamber of the Oliy Majlis of the Republic Uzbekistan, has noted that discussion of cross-cutting and multidisciplinary issues had gained theoretical and practical/regulatory value both in Uzbekistan and Russia: optimal AI regulatory models; proposals of AI model codes; AI's place within the national legal system; legal response to AI-related threats and risks; introducing AI to legal education, regulatory drafting and enforcement; legal framework dynamics for AI creation and use: practices approved by countries and international institutions — UN, EU, CIS, SCO etc.; prospects of developing global legal standards for AI development and usage; impact of AI public law implementation on legal awareness, legal culture of individuals and communities, cognitive basis of law and order; development of AI conceptual basis in accounting for specific regulation of AI technology and its impact on legal understanding, regulatory drafting and enforcement.

To create a legal framework for introducing AI in public law, social sector and national economy, and making Uzbekistan one of the world's advanced countries in terms of AI use, it is proposed to establish the notion of "artificial intelligence" in national legislation; define a tentative list of "digital human rights"; legislatively enshrine the principle of human rights for Internet users and non-discrimination in the digital space; enshrine the concept of digital gap (including gender-related); enshrine the principle of cultural diversity in the digital space; and enshrine the concepts of "cyber-violence" and "cyber-bullying".

S.G. Cornelius, Professor, University of Pretoria, South Africa, described the *Comparative prospects of future law at the time of AI*. He has noted that jurisdictions worldwide were attempting to cope with AI regulation in focusing on liability, protection of consumer rights, data security and intellectual property, as well as market regulation. The regulatory authorities will have to take into account AI's purpose for human progress; its safe and ethical development for the avoidance of technological colonialism, lower human risk and impact; as well as regulation of intellectual property, industrial relations, health, law enforcement practices and military applications.

C. Lucena, Professor, Center for Legal Studies, Paraiba State University of Brazil, has explained the specifics of legal approach to AI in Brazil. Currently, AI is governed in Brazil by legislative provisions concerning elections and data security, with further regulation across various spheres being proposed. There is a need to reduce AI-related risks and possible negative impact on the basis of safer, more ethical and reliable development of these technologies.

R. Soni, Associate Professor, Center for the Study of Law and Governance, Jawaharlal Nehru University, Deli, India, has noted a need to build user confidence, enhance data security, maintain transparency, accountability and compliance in order to guarantee ethical use of technologies, support innovation and reduce risks. India is taking vigorous steps to regulate AI by passing the new Digital Personal Data Protection Act (DPDP) and pursuing the AI-related governance project. Thus, India is putting in place a framework for AI development, protection of data and human rights, and promoting innovation.

In conclusion, **A.A. Skovpen**, Senior lawyer on intellectual property at Nestlé, has discussed the *Comparative analysis of approaches to generative outcomes and TDM rights protection*.

2. At the panel **Civil law regime applicable to AI technologies and AI-enabled objects** moderated by **A.A.Volos**, Candidate of Sciences (Law), Associate Professor, HSE, researchers and legal practitioners presented their reports, with panel participants discussing a variety of issues: compensation for AI-related damage, legal concepts of authorship regarding AI-assisted works, personal data protection, confidential data processing, AI use for the purpose of inheritance and corporate law.

D.A. Kazantsev, Senior Expert, Greenatom, ROSATOM State Corporation, has made a presentation *AI delictual capacity: fiction or requirement?* He has noted rightly that with the use of AI-controlled robots in everyday life the problem of liability including regulation of obligations in the event of AI-related damage had moved from theory to practice. From the perspective of current regulatory development, on the one hand, and technologies, on the other hand, we cannot conceive AI as a legal entity, let alone the one with delictual capacity. Today delictual responsibility can be assumed only by legal entities that control AI action in any way, that is, developers, owners, users, etc. With an optimal model for allocation of subsidiary responsibility between them yet to be developed, this is unlikely to require new legal institutions: adjustments in this area could be almost for sure restricted to efforts to complement and specify the existing civil law provisions. However, the fact that AI is now deprived of delictual capacity does not mean it will be so in the near or distant future. The legal profession should be ready now to conceptualize, substantiate and integrate legal provisions regulating operations and responsibility of new legal entities — those endowed with non-human consciousness.

In their collective presentation *Legal concept of authorship with regard to AI-assisted works*, **E.V. Zainutdinova**, Candidate of Sciences (Law), Associate Professor, Institute of Philosophy and Law, Novosibirsk State University, and **K.V. Sergeeva**, Manager of legal projects at Catrix LLC, discussed both the theme of copyright to the works created by generative AI models and current copyright concepts. They have presented summary conclusions on relevant enforcement practices and regulations effective in EU and elsewhere, as well as on the latest regulations in force in Russia in the area under study. They have formulated conclusions on legal aspects of "input" and "output" content as applied to AI. In the context of creative work, the software owner's and user's exclusive rights and copyright to AI-assisted output were discussed. In their presentation, the authors used images created through the use of AI.

A.A. Ambros, Head of legal support of corporate procedures and investment projects at Vkusvill, and **K. Kuzhanova**, his Deputy, discussed confidential data processing issues in the presentation *Confidential information (including personal data) processing problems at the data collection and instruction stage of neural network learning in automated contracting systems*. It was noted that confidential data disclosure issues occurred at the AI output stage when a neural network trained on confidential data would accidentally/unintentionally disclose such data in response to a request. Thus, when neural networks are trained on confidential data, they can "memorize" and reproduce data fragments. For instance, a neural network trained on a customer database can accidentally read out personal data in response to a similar request. As a possible solution, the speakers proposed to use regularization for lower probability of memorizing specific data, and to introduce stricter procedures for request management and output checkup.

As for the panel's main conclusions, it should be underlined that speakers and listeners shared in the opinion that the use of AI-produced decisions and outcomes would result in a number of problems, only to require changes to the regulatory framework and improvements to legal and business practices. It is these situations that highlight a need for changes to the regulatory framework, and for case-by-case establishment of rights and duties of AI users. Thus, regulation of relationships should not be focused, from the perspective of private law, on AI itself — for instance, it is unreasonable to struggle with definitions, attributes and regulation of relationships involving AI. It is more important to focus the new law and practice on the stage of using AI-produced decisions and outputs.

3. The first presentation of the panel **Artificial intelligence and intellectual property right** was devoted to a general question of a link between the two. **E.R. Valdes-Martinez**, Senior Teacher, HSE, UPRAVIS Association Director, has noted that AI permeated today all spheres of human activity undoubtedly including intellectual property. However, experts are divided as to the means, mechanism and structure of AI regulation in this domain, primarily because the established system of provisions governing intellectual property is aimed largely at protecting man's (not machine's) creative products. The World Intellectual Property Organization's position in this regard is straightforward: AI has nothing to do with intellectual property as regards regulation. Such approach, however, does not bring us any nearer to solution. What could be currently observed is the practice of the existing legal constructs of intellectual property ranging from text and data mining (EU) to fair use doctrine (United States) being applied to AI.

Developing this subject, **M.Yu. Proksh**, Chairman, IP Chain Association, has told in his presentation to what extent the protected intellectual assets could be used for machine learning. Creating and improving AI requires to use lots of intellectual property assets owned by other persons, only to conflict with intellectual property law. The question is how the regulation applicable to creation and use of intellectual property assets should evolve in the current social context. The speaker specifically has discussed the theme of AI-created intellectual property assets being exempt from legal protection, with the current doctrine protecting only those created by man. However, this practice is threatening human creativity since, where a machine-made product meeting minimal requirements is available for free, hardly anybody will be willing to pay for a man-made one, except in the event of niche applications.

In her presentation **M.A. Kolzdorf**, Senior Teacher, HSE, consultant, has noted that datasets for AI learning could be counted as copyrightable assets. Making a dataset normally involves creating copies of works, only to affect the right to reproduce. Under the general rule, one has to seek authors' consent to use such works. In the speaker's opinion, cases of free use are currently not enough to support legal AI learning. Once a new restriction of exclusive right is added to Part 4 of the Civil Code of

Russian Federation (hereinafter — the Civil Code), one will have to observe a three-stage test established by Article 9 (2) of the Berne Convention. Such restriction should probably depend on AI model (generative, predictive etc.) and impact on author's royalties (whether the outcome will compete with the original work). The speaker also has noted that establishing the fact of unauthorized use of copyrighted assets for AI learning was now problematic ones, unless AI operators themselves decided to report the use of certain data (for instance, music of a band), with AI-produced outcome reflecting parts of such works.

I.L. Litvak and **S.Yu. Lagutin**, testers of CSD HSE developer team (MIFT and RANE), shared valuable experience of using learning datasets to create AI that efficiently analyzed legal cases and helped to prepare for trial. This project is a major step forward to openness and availability of legal information. The content being prepared is distributed under GPLv3 free license, something that allows all parties concerned to study, modify and disseminate datasets for free, as well as to learn the underlying methodology.

O.A. Polezhaev, Associate Professor, RSPL, Kutafin State University, has discussed the problem of AI widely used for creative purposes. In this regard, a discussion of the procedure for protecting human intellectual outcomes was analyzed. It was noted that lower protection criteria coupled with the admissibility of copyright protection of AI-assisted creative outcomes significantly undermined both the stability of civil law transactions and efficient regulation of the relations in question. In the speaker's view, while AI outcomes could be monopolized by creators or users, relations of appropriation of such outcomes should not rely on copyright law in general and exclusive rights in particular.

I.N. Sarapkin, Information Relations Department of Moscow City, has described in his presentation AI's impact on legal relationships involved in formalization and transfer of rights to computer software including in the context of procurement. He has raised the issue of correlation of the legal regime governing software and literary works highlighted by the importance of new technologies, as well as the issue of divergence between legal regulation and real social relationships in this area. As a possible solution, it was proposed to assess the regulatory practices from the perspective of a search for new approaches beyond the authorship-copyright paradigm.

The presentation triggered active discussion and requests for clarification, as well as proposals to formalize the transfer of rights to intellectual assets along the lines of the regime applicable to digital financial assets. The participants were also invited to complete an online questionnaire on the subject, with its outcomes to be used for shaping new approaches to legal regulation in this area.

In her presentation **R.Sh. Rakhmatulina**, Associate Professor, Financial University under the Government of Russia, has dwelled on the aspects of using AI for design. AI can perform a large part of work involved in designing new products and, while providing new opportunities, creates the risk of contending the rights to design works to be accounted for when using AI in the field.

V.O. Kalyatin, Candidate of Sciences (Law), Associate Professor at the HSE, Professor, Alexeyev Center for the Study of Private Law under the President of Russia, has discussed the theme of intersection between private and public law in regulating AI involved in creation and use of intellectual property. Creating and improving AI requires large-scale use of someone's intellectual assets, thus prompting a need in special exemptions. Since AI is often used in this area for a public good, one can assume that provisions will be interpreted to encourage the use of the underlying intellectual assets. Finally, enormous problems follow from practical difficulties of identifying faked objects created with AI help by which society is so easily misled. It was concluded that in the context of conflict between private use of intellectual assets and their public implications, the intrusion of public law provisions into AI-related private relationships was inevitable.

The panel concluded with a presentation by **Van Bod**, Postgraduate Student, Moscow State University, describing the peculiarities of cross-border/international exchange of AI-related intellectual assets — like challenges, risks and mechanisms for protection of entrepreneurs' rights exemplified by China and Russia. The speaker has pointed out not only the differences of approach between the two countries, but also the basis for harmonizing regulation in this area including international agreements.

4. The panel **Generative content: copyright holder protection problems** discussed the protection of AI-assisted objects and digital images and synthesized voices; use of intellectual property in machine learning systems. The panel was moderated by **N.A. Danilov**, General Director, National Federation of Music Industry, Candidate of Sciences (Law), Associate Professor, HSE, who has noted in his presentation that technological companies would use intellectual assets for machine learning

systems and new digital objects without seeking the copyright holder's consent. This situation has to be addressed by legislation, with a balance of interests to be found between holders of exclusive rights and developers of AI systems. Moreover, a three-stage test should be used as a commonly recognized standard of introducing and applying limitation of exclusive rights in authorizing the use of intellectual assets for machine learning.

T.D. Bogdanova, Candidate of Sciences (Law), Associate Professor, Russian Academy of National Economy and State Service under President of Russian Federation, Senior Lawyer, Announcers' Union, has spoken about the issue of using intangible goods including people's voices to create digital images and synthesized voices of celebrities. She also has reported about Russia's current legislative initiatives to regulate the creation and use of "deep fakes". In particular, a draft of law submitted to the State Duma proposes to add a new article to the Civil Code, Part 1 for protecting people's voices as personal non-property right along the lines of a person's image, including in the event of real-time voice cloning or speech synthesis. The draft of federal law underlines that no recording containing the voice reproduced through the use of specific technologies (meaning those for speech synthesis) could be published and used unless with the voice owner's consent. She also has shared the knowledge of international practices for synthesized voice protection. In judging whether intangible goods including voices are protectable, the following factors should be taken into account: purpose of the performance; where and who will use the synthesized voice; limits of using the synthesized voice; whether generative technologies will be made available to third parties; steps being taken to protect voice recordings and to limit access to cloning technologies.

A.Yu. Byrdin, General Director, Internet Video Association, told about legal problems of generative audiovisual content creation.

O.N. Kim, Advisor to S&P Digital General Director, told about the using AI in music industry where copyright issues abounded, with authoring made more complicated. The simplicity of creating AI-generated tracks coupled with low quality devalues music. Ten million of Suni AI users have created at least one track 8 months after the service launch; at Udio, 10 tracks per second are produced; and Music FX has posted 10 millions tracks 2 months after its launch. If digital music services publish a large part of this music, one can imagine how much will add up to already huge amount of what is weekly produced by artists and music labels. Studies demonstrate that even high quality music uploaded on music services will not always find its way to listeners (an estimated 86% of uploaded tracks were accessed less than 1000 times). The emergence and monetization of AI tracks will deliver a hard blow to musicians' and copyright holders' incomes, making for them even harder to get to listeners' playlists. Moreover, there are fraudsters who use AI generators to earn money by preying on celebrities' music output. Thus, copyright holders are reporting unauthorized covers and remixes of popular songs from their catalogues created through the use of AI and published on digital music servers. It is very difficult to counter this practice by legally available methods as blocking even one such track will require considerable time and resources. Meanwhile, such violations are many because of the ease and low cost afforded by AI generators.

M.E. Riabyko, Board Member, Association for copyright protection in the Internet, Deputy Chairman, Committee on legislation of the Russian Book Union, has discussed the legal aspects of using AI in book publishing sphere. He has noted that intellectual assets were used at all stages of AI system development: constructing a database for AI learning; learning from this database (algorithms using authored content); developing tools for creative transformation (content creating interfaces); producing final outcome (a new or transformed object). It is increasingly hard to track possible violation of exclusive rights. The available legal tools cannot always handle such complicated cases. According to the speaker, technological progress could not be stopped; but *bona fide* standards could be adopted for intermediaries (parties developing and supplying tools for working with AI).

R.L. Lukianov, Managing Partner, Semenov & Pevzner firm, has described business risks of using the content created with the help of generative neural networks. He has noted that creative outcomes produced exclusively by generative neural networks cannot and should not enjoy protection of legal regimes (at least those of copyright or associated rights). Moreover, such creative outcomes should be labeled so that any consumer could unambiguously and without much effort identify them in civil law transactions as different from "classical" creative outcomes. Any commercial exploitation of a generative neural network "trained" on the basis of creative works owned by third parties should assume mandatory consent to be obtained from such third parties. Any violation by the generative system user of third parties' exclusive rights to creative outcomes (including derivative outcomes and other objects to be created with the help of such system) should give rise to regular liability envisaged by law.

G.I. Uvarkin, Candidate of Sciences (Law), General Director, Omega Law Bureau, has discussed using generative AI to create professional and amateur content. He has stressed that this field has produced numerous regulatory and enforcement problems — such as inability to establish the sources of content's borrowings, despite a need to assess the outcome as likely derivative work; erosion of user creativity criteria due to unpredictability of specific outcome; lack of principles to judge who and when could be considered the author/copyright holder of the resulting text, image or other outcome. The specifics of using AI for professional content creation require that lawyers assume additional tasks to ensure its legitimate use and contractual compliance in respect of customers and licentiates. In particular, there is a need to develop contractual mechanisms to control AI's operational use, agree on the use of specific versions, check for likely restrictions, and also provide customers with intermediate results (output data) for judging the author's creative input.

E.I. Tkach, lawyer, Managing Partner, Tkach & Partners law firm, has spoken about the aspects of authorship and legal regime with regard to AI-assisted outcomes. She shared the knowledge of international experience of protecting the interests of copyright holders and relevant national practices.

V.V. Arabina, founder of the Laboratory for Mathematical Modeling, advisor to the President of Association for Export of Technological Sovereignty, and **M.A. Shakhmuradian**, founder of the Laboratory for Mathematical Modeling and of Ai Mono, author of "How AI Changes Business Practices" Telegram channel, has discussed regulatory aspects of machine learning from the perspective of those who developed technologies.

5. At the panel **Role of public law in shaping an optimal regulatory model for digital technologies and artificial intelligence**, participants exchanged their views on current challenges and prospects of public law regulation of AI and other digital technologies in Russia and elsewhere, and highlighted the issues of shaping a public law regulatory model for artificial intelligence.

According to the panel's moderator **E.V. Vasiakina**, Candidate of Sciences (Law), Associate Professor, HSE, all of the presentations mentioned below could be subsumed under specific subtopics that dealt with the key aspects of public law regulation of digital technologies, with the first group of speakers focusing on the issues of use of such technologies by public authorities.

In opening the panel with a report Shaping an advanced model of justice in Russia with digital technology components, **O.A. Stepanov**, Doctor of Sciences (Law), Chief Researcher, Institute of Legislation and Comparative Law under the Government of the Russian Federation, discussed the examples of using innovative technologies around the world and concluded on the need to attach a technical assistant status to AI technologies likely to be used in Russia including at court. AI cannot be an independent party in trial while the contrary practice available internationally is not convincing enough to be adopted by the national legal system. Therefore, despite all the benefits and progressiveness of the idea to enhance the efficiency and accessibility of the legal system through technologies, there is a need to take into account legal and ethical aspects of implementation.

The issues of explainability and transparency of automatic decision-making in governance were discussed by **P.P. Kabytov**, Candidate of Sciences (Law), Senior Researcher, Institute of Legislation and Comparative Law under the Government of the Russian Federation, who has underlined the importance of regulatory framework for transparency of the algorithms used by public authorities. Governance as a whole needs to be modified including by way of developing legal mechanisms for transparency and confidence in automatic decision-making systems. Implementation of such mechanisms needs to rely on such criteria as "explainability" and "transparency" of algorithms whose characteristics were proposed by the author.

Specific aspects of digital technologies were discussed in light of their active use by individuals to exercise their rights and legitimate interests. In her report *The use of digital technologies for public service provision: problems and risk*s, **G.A. Grischenko**, Candidate of Sciences (Law), Associate Professor, Kutafin State University, has highlighted the aspects of digitization of public services including data security and accessibility. She has argued that the available examples of digital technologies for public service delivery in Russia allowed not only to build people's trust in digital change, but also to upgrade public governance as a whole.

In her report *Neural network as a means of protecting voting rights*, **N.N. Kuleshova**, Candidate of Sciences (Law), Associate Professor, Institute of Law under S.A. Esenin State University of Ryazan, has proposed to use AI for better protection of individual voting rights and discussed possible legal and technological obstacles. The speaker has stressed the need for public services and voting rights to adapt to digital realities. While introducing AI in these areas can improve the quality of election procedures, this will require to maintain the security of data and individuals as an issue of higher priority.

In his report *Observing the balance of interests as a key factor of shaping an optimal regulatory model for digital technologies*, **D.V. Bolshakov**, founder of Botman.one low-code platform, has raised the issue of searching for an optimal model of using digital technologies by pointing out a need to account for the interests of businesses, government and individuals to harmonize the underlying regulation. He has noted that the development of digital technologies involved considerable financial complications currently faced by businesses. Apart from the theme of resources, there is a need to address those of data used by companies to train AI systems, to be handled in such a way as to avoid violation of personal rights. In the speaker's view, it is comprehensive regulation that should ensure the balance of all interests that intersect in digital technologies.

E.V. Zadorozhnaya, Candidate of Sciences (Law), Associate Professor, Moscow International University, has focused her presentation on the priority of securing individual rights based on the concept of personal digital sovereignty. To implement it, she has proposed to introduce legal mechanisms for protection of personal digital rights on the basis of the priority of personal data and security of digital identity.

The speakers legitimately argued for the importance of a balance between the interests of various stakeholders to achieve optimal regulation of the digital space. Protecting individual rights including digital sovereignty and personal data in the area of digital technologies is becoming a regulatory drafting priority.

A number of speakers have discussed the issue of regulating high technologies such as AI, quantum and block chain technologies, from the perspective of public law.

D.L. Kuteinikov, Candidate of Sciences (Law), Tyumen State University, presented a report *Advanced fundamental AI models: limits of regulation* focusing on the peculiarities of terminological understanding of artificial intelligence in various jurisdictions. In addition, he has formulated the most acceptable criteria of the need in adequate legal regulation of advanced AI technologies.

O.A. Izhaev, Candidate of Sciences (Law), Associate Professor, Tyumen State University, has made a presentation *Regulatory concepts for artificial intelligence: Brazil's experience* describing the evolution of Brazil's national law governing digital technologies. In discussing current models, the speaker has identified the specifics of AI regulation in Brazil and concluded that the government approved the basic regulatory principles effective in the EU: individual rights protection, non-discrimination and clarity. Another focus of the report was on categorization of risks involved in AI use under Brazil's law. Under the approach approved by Brazil's government, basic services, biometric control and admission to employment were associated with "high risk" while exploitation of vulnerable groups and social scoring with "excessive risk".

In his report *Prospects of public law regulation of quantum technologies*, **A.A. Efremov**, Doctor of Sciences (Law), Professor, Kutafin State University, has shared the findings of how the technologies in the field were regulated. He described the regulatory approaches to new technologies such as quantum computing opening up considerable opportunities and warranting special attention both at the national and international level. A need for international law to address this sphere follows, in particular, from the threat of possible abuse of quantum technologies that, once widely disseminated, can be used to destabilize the international financial system, violate data confidentiality and security, undermine trust in new technologies, etc.

In his report *Public interests and financial privacy: regulatory specifics of blockchain technologies*, **S.D. Afanasiev**, Candidate of Sciences (Law), Researcher, State Academic University for the Humanities, has dwelled on the data privacy problem in block chain technologies.

In the course of discussion, the speakers agreed that the study of international experience and adaptation of the best global practices could promote a successful regulatory model in Russia allowing to account for global trends and guarantee the protection of individuals. Meanwhile, quantum computing, block chain and AI technologies need to be regulated with a view to both their innovation potential and the risks for individual rights. Introducing advanced technologies requires to draft special legal provisions in support of their safe and ethical use.

Apart from the main panel, findings of young researchers were presented at the meeting. **K.A. Zyubanov**, Postgraduate Student, HSE, has presented a report *Contextual integrity as a criteria of legitimacy of personal data processing* where he proposed to take the context into account in assessing the legitimacy of processing. **Z.O. Mityanov**, Postgraduate Student, Department of Law, HSE, Nizhny Novgorod branch, has proposed for discussion his paper *Defining biometric personal data in the context of progress of AI-enabled biometric technology*, in which he argued for a need to clearly define biometric data for effective protection. With the digital change giving rise to numerous data security issues, the theme of personal data regulation is currently high on the agenda.

Young researchers also discussed specific aspects of regulating both AI and virtual/augmented reality. In her report *Risk-oriented approach to regulating AI in Russia's financial market*, **V.S. Kalinina**, winner of the All-Russia digital contest in specialist training organized by the Council for Digital Economic Development under the Federation Council and the Presidential Academy, has proposed to take into account international trends of AI regulation for efficient enforcement practices. **V.S. Dolunts**, Postgraduate Student, Kutafin State University, has argued in his report *Legal aspects of using virtual reality in operations of public authorities* in favor of regulation of this area, with implications of actions to be extended to real relationships.

The presentations discussed at the panel **Role of public law in shaping an optimal regulatory model for digital technologies and artificial intelligence** confirmed the relevance and need in public law regulation of this are P. in Russia. A special focus was on protecting individual rights, transparency and explicacy of automated systems, international experience, specific use of high technologies in governance. The participants have agreed on the need to develop a relevant regulatory model to encourage a safe and ethical approach to introducing digital technologies across the board and to protection of human rights.

6. The panel **Regulation and self-regulation of artificial intelligence: AI in Legal Tech** was split into two thematic blocks: AI regulation and self-regulation and AI-based Legal Tech applications.

In his opening speech, the panel moderator **D.R. Salikhov**, Head, legal support group for regulatory initiatives at Yandex, Candidate of Sciences (Law), Associate Professor, HSE, has raised conceptual issues for discussion including the balance of interests regarding the method and extent of regulation, prospects of "soft law" in this area taking into account the international experience and domestic practices (such as the AI Good Practice Code and the Declaration of Responsible Generative AI). The moderator also mentioned possible transformation vectors of the legal profession, given the progress of AI technologies and technological, legal and ethical constraints of introducing AI solutions in the legal sector.

Under the first thematic block, a total of eight reports were presented. **E.I. Svischeva**, Director for legal issues at the VEB.RF group, has shared her vision of the relative proportion of regulation and self-regulation in view of the need, on the one hand, to support the development of technologies and advanced domestic solutions and, on the other hand, to achieve a balance of interests between the government, developers and individuals.

N.A. Falshina, Southern Federal University, has shared a comprehensive theoretic vision of shaping and promoting the general legal approaches to the category of "digital rights" and their role in the Russian legal system.

A.V. Fedotov, Senior Teacher, HSE, has discussed the questions of making the Russian law more specific in the context of current technological change.

In her presentation, **A.K. Lebedeva**, Associate Professor, Kutafin State University, has discussed the technological and regulatory issues of deep fakes including from the perspective of expert activities. In the presentation she has described current challenges and complications related to technological change and emerging approaches to expert work.

A.N. Izotova, Candidate of Sciences (Law), Associate Professor, HSE, has raised in her report the issue of allocating liability for the damage caused by AI technologies, with analysis based on the existing approaches related to liability for the damage caused by automated vehicles under different legal regimes.

A.S. Romanova, MIFT, has devoted her report the application of algorithms for standalone corporate governance systems. She also has presented in technical terms her vision of the prospects of using algorithms in traditionally "non-algorithm" spheres.

V.A. Trubina, Candidate of Sciences (Law), Associate Professor, HSE, has focused her report on the aspects of regulating AI's medical applications by describing the e-regulatory approaches and issues, in particular, related to systems for support of medical decision-making and AI-enabled medical appliances.

Yu.S. Varusha, Russian Academy of National Economy and State Service under President of the Russian Federation, has discussed in her presentation theoretical and practical issues related to AI-enabled transformation of enforcement.

The second thematic block comprised presentations on AI-enabled Legal Tech applications and digitization of the legal function.

D.D. Toropova, Expert, Doczilla LLC, has shared her vision of AI applicability scenarios for the legal function in light of the current demands of businesses as well as the present-time technological and legal constraints. The report has concluded that despite a large potential to handle routine labor-intensive tasks, AI had numerous limitations to be accounted for.

A.A. Nakhushev, SSLA, has covered in his presentation methodological and theoretical issues of introducing AI in the legal function.

M.E. Plugin, SSLA, has focused his report on practical issues of introducing AI at arbitration tribunals while proposing a number of scenarios of AI applications to streamline secretarial staff operations.

7. A round table **AI technologies for industrial relations: advancements, failures, prospects** held as part of the workshop moderated by **O.I. Karpenko**, Candidate of Sciences (Law), Associate Professor, HSE, has evoked an active discussion of urgent digitization and AI-related questions, such as the role of AI in industrial relations; opportunities and challenges of legal protection of labor rights "violated" by AI. A general problem being discussed was raised in the following terms: AI and human factor in industrial relations — alliance or conflict?

Since the round table was attended not only by students of labor law, but also representatives of employers and trade unions. It has provided a unique opportunity for discussing the positions of stakeholders in industrial relationship, with the general direction set by **D.L. Kuznetsov**, Tenured Professor, HSE, who has highlighted the current digitization and AI trends affecting both the labor market and regulation of industrial relations.

As representatives of large employers, **S.S. Dombaev**, Vice-Principal, Senior Director for Staff, HSE, **A.V. Bezukladnikova**, Deputy Director for Legal Issues, HSE**, A.V. Zamoskovniy**, President of the Energy Sector Employers Association of Russia, have shared their experience of corporate use of digital technologies as well as plans to introduce AI-enabled components into production processes. **A.V. Zamoskovniy** has mentioned the experience when electric companies had to abandon AI applications until the technology was refined.

Trade union representatives **A.F. Valkova**, Head, Legal Labor Inspection, Moscow Trade Union Federation, and **M.R. Rozhko**, Senior Legal Counsel, Legal Labor Inspection, Moscow Trade Union Federation, have noted weak activity of workers in legal protection of labor rights as well their low literacy in legal matters.

The keynote report was presented by **I.A. Filipova**, Candidate of Sciences (Law), Associate Professor, Lobachevsky State University of Nizhny Novgorod. She has proposed a concept of AI, highlighted regulatory issues and impact on labor and outlined the objectives of labor law in an AI-driven world. Also she has presented and suggested to panelists to discuss her proposed amendments to the Labor Code of Russia. Her position and initiative has encountered an active opposition from **S.Yu. Chucha**, Doctor of Sciences (Law), Professor, Institute of State and Law, Russian Academy of Sciences.

O.Yu. Pavlovskaya, Candidate of Sciences (Law), Associate Professor, State Academic University for the Humanities, and **A.S. Kashlakova**, Candidate of Sciences (Law), Associate Professor, Sochi State University, have shifted the subject towards employment relations that preceded industrial relations by raising the issue of discrimination (so-called "hidden discrimination"), with employers actively using the latest computer tools to substantially change the process of administering employment relations at hire. It was noted, in particular, that posting job offers on a platform and receiving CVs did not create any obligation for the employer. However, job seekers often fail to see the difference between a standard electronic reply at the employer's website denying an invitation for interview and a refusal to hire in response to a written request. It was underlined that the risk of implicit discrimination by a potential employer on the grounds of the candidate's digital profile rather than his business qualities could not be excluded.

M.O. Buyanova, Doctor of Sciences (Law), Professor-Researcher, HSE, has shared the practices of digital technologies in a number of CIS countries.

As a matter of conclusion, the participants have agreed that there was no clear and unambiguous understanding of "artificial intelligence" either in society or among labor law practitioners. Where the concept is manipulated, AI is often mistaken for digital technologies that are essentially only a tool based on high technology that contributes to abandon outdated personnel management methods.

The round table participants also have discussed the situation of employers and workers, main parties to industrial relationship, in the age of artificial intelligence. It was concluded that in this duos the employer would be better positioned that the worker: firstly, because of his administrative power and key role in the production process, with the worker in subordinated and passive roles, and, secondly, because it was the employer (and only him) who was introducing digitization at his offices and would implement AI technologies in the future. This is likely to result in an absurd situation, with man having to compete with AI for vacancies. A concern was expressed about possible redundancies, especially in technology-driven sectors, with unemployment on the rise. However, Professor **S.Yu. Chucha** was confident that with expansion of the service sector and emerging new occupations, man would not be left behind.

Meanwhile, moral issues associated with the social aspect of AI technologies were a matter of much more concern. With a majority of workers psychologically ill-prepared for digital change at their organizations, more vigorous efforts were required to make people better prepared for forthcoming changes in the economy and daily life, as well as to promote education.

Unless AI technologies have become a sustainable practice and a duly part of legal transactions, it is premature to amend labor law. However, realities cannot be ignored. Advancing in quantum leaps, digital technologies undoubtedly impact the evolution of law, and we should be ready to promptly and effectively respond to inevitable future transformations of industrial relationship. Prohibitive tactics is not an option. The progress of AI technologies cannot be stopped despite prohibitions already imposed on them in some countries.

The HSE has launched a large-scale project to train teachers, research fellows and postgraduate students as well as administrative and managerial staff in using AI as part of the Priority 2030 Academic Leadership Strategic Program, with more than 1000 participants already completing the course. Upon completion, participants will be able to use the available AI services to considerably simplify and streamline their work processes while enrolment in the program will introduce them to opportunities and constraints of neural networks and AI.

If AI is a technology capable of independent creative work challenging that of human intellect, it appears premature to discuss whether it is technically applicable to industrial relations since there is no such technology yet. Industrial relations are now evolving towards flexible options of digital change while building up digital capital as a tool for a phased transition to AI.

8. The panel *AI-enabled criminal law protection of agents of digital economy and finance* was moderated by **S.V. Rastoropov**, Doctor of Sciences (Law), Professor, HSE, who in his presentation *Specifics of staff training for criminal law protection of subjects of digital rights* has underlined digital technologies were fraught with new threats and challenges for mankind, only to require from legal practitioners to develop new approaches to the emerging issues including new algorithms to apply criminal and criminal procedural law. According to him, a profound study of digital technologies and their underlying risks should become part of education in criminal law. In this regard, the Department of Criminal Law is developing a new master's program *Criminal justice in regulatory drafting and enforcement*.

V.A. Prorvich, Doctor of Sciences (Law), Professor-Researcher, HSE, has presented a report *Mathematical aspects of criminal regulatory drafting and enforcement in modern economy and finance* where he argued that due to its practically unlimited potential AI had to be limited in criminal law and procedure. Lawyers have to do a good deal of drafting to remove gaps in provisions of both criminal and criminal procedural law that regard modern technologies (in particular, part 6 *Electronic documents and process document forms*, Law of Criminal Procedure of Russia). In these efforts one can use matrix systems to assess legal provisions that help to identify gaps and conflicts, something that will require to describe legal provisions in algorithmic language.

In his report *Social dangers of the Metaverse: issues of qualification and criminalization* **A.A. Bakradze**, Doctor of Sciences (Law), Professor, HSE, has evoked the need for criminal law regulation of metaverse. The metaverse, that is, online virtual space where avatar owners act via digital proxies, will be completed over the next 3—5 years. The avatar's behavior can later become self-referential, with the course of action determined without reference to the owner and developers. In this regard he has proposed that lawyers and developers joined their efforts to ensure algorithmic control of avatar behavior for compliance with law.

In her report *On video conferencing in investigation involving undercover persons*, **E.A. Artamonova**, Doctor of Sciences (Law), Professor, HSE, has noted that while the criminal procedure as a whole is conservative with regard to new technologies, the Criminal Process Code allows to use video conferencing in investigation (for face-to-face questioning, interrogation, identification). Despite undeniable benefits, video conferencing creates new problems of theoretic and applied nature if “undercover” persons are involved. **E.A. Artamonova** has proposed a number of amendments to the law of criminal procedure to limit the use of video conferencing in investigation involving “undercover” persons.

In her report *Conceptual erosion of the object of theft in modern criminal law*, **I.I. Nagornaya**, Candidate of Sciences (Law), Associate Professor, HSE, has argued that emerging technologies transformed the object of theft in modern criminal law. Technological change apparently requires to renovate the well-established provisions describing the classical institutions of criminal law (such as the object of theft). Virtual property is currently not subject to crime, something that calls for amendment of the law in line with the progress of digitization and artificial intelligence.

In her report *Modern view on crime prevention*, **O.Yu. Tsurluy**, Associate Professor, Russian State University of Justice, central branch, Voronezh, has noted that the concept of technology should be understood in much broader terms by studying not only theoretical, but also practical aspects. Crime prevention today comprises activities to study and analyze regular patterns of committing a crime with a view to defining adequate responses (legislative, organizational, technical, criminal, social, psychological, pedagogical) to neutralize or considerably hamper specific criminal behavior. The predictive function of criminalistics should be implemented towards anticipating the threats of using technologies for criminal ends: predicting potential threats and developing effective responses. It is inefficient and harmful to prohibit and negate technologies. With a universal conceptual framework required for regulation of technologies, its absence should not halt the process of studying, regulating and responding to the use of technologies for criminal ends.

A.V. Valter, Senior Teacher, Tyumen Skill Development Institute, Ministry of Interior of Russian Federation, has made a presentation *Artificial intelligence against tax crime,* in which he has argued that AI could dramatically change both tax crime and response to it, with AI technologies providing a range of tax monitoring and crime detection opportunities.

In her report *AI applications for crime detection and prosecution*, **A.Yu. Churikova**, Associate Professor, State Law Academy of Saratov, while analyzing the rise of IT-assisted crimes, has underlined the need for an application with preset search algorithms as well as AI software for promoting legal regulation of these issues.

F.M. **Fazilov**, Acting Professor, State Law University of Tashkent, has focused his report *Criminal liability of artificial intelligence* on AI's criminal liability emphasizing that while civil law provided for the relevant regulation, criminal law did not. The main question is who will be liable — developers? operators? legal entities owning AI? The speaker has reported that Uzbekistan had passed an AI development strategy for the period until 2030.

In speaking on the subject *Using artificial intelligence for response to crimes committed by convicts*, **V.M. Yakovleva**, Senior Teacher, HSE, has highlighted the increasing role of AI in detecting crimes by allowing law enforcement bodies to analyze large arrays of data for suspicious patterns. Machine learning systems are capable to predict crimes thus ensuring more effective use of resources by security services. While the use of AI for face recognition and video analytics largely accelerates the process of suspect identification, it is important to observe ethical standards and protect confidentiality of individual, something that requires careful regulation.

In her report *Limits of admissible use of AI in criminal procedure at the stage of trial*, **D.A. Rudenko**, Lenrezerv Bar Association, Saint Petersburg, has expressed opinion that while AI could be used in criminal proceedings at the stage of trial, it should not be allowed to make final decisions (deliver a sentence). AI can be used at the stage of intermediate decision-making.

In his report *Problems of ensuring the reliability of information contained in electronic/digital form*, **V.V. Moiseev**, Postgraduate Student, Institute of Legislation and Comparative Law under the Government of Russian Federation, has noted that, while civil law had a definition of AI, criminal law did not. The legislation does not define what information contained in electronic form can be considered reliable.

In his presentation *Prospects of improving committal for trial in the context of Russia's transition to information society*, **A.D. Poliakov**, Postgraduate Student, Institute of Legislation and Comparative Law under the Government of Russian Federation, has stressed that no investigation could be conducted virtually, unless a criminal case was maintained in electronic format. Meanwhile, already AI can be trusted to make intermediate decisions: for example, imposing a fine or referring someone to medial treatment. The speaker compared the committal for trial in the context of information society in Russia and in the United States.

Information about the authors:

1. Yu. Bogdanovskaya — Doctor of Sciences (Law), Tenured Professor.
2. N.A. Danilov — Candidate of Sciences (Law), Associate Professor.
3. E.V. Egorova — Candidate of Sciences (Law), Associate Professor.
4. V.O.Kalyatin — Candidate of Sciences (Law), Associate Professor.
5. O.I.Karpenko — Candidate of Sciences (Law), Associate Professor.
6. D.P. Salihov — Candidate of Sciences (Law), Associate Professor.
7. E.V. Vasiakina — Candidate of Sciences (Law), Associate Professor.
8. A.A. Volos — Candidate of Sciences (Law), Associate Professor.

The article was submitted to editorial office 25.10.2024; approved after reviewing 01.11.2024; accepted for publication 01.11.2024.

Legal Issues in the **DIGITAL AGE**

AUTHORS GUIDELINES

The submitted articles should be original, not published before in other printed editions. The articles should be topical, contain novelty, have conclusions on research and follow the guidelines given below. If an article has an inappropriate layout, it is returned to the article for fine-tuning. Articles are submitted Word-processed to the address: lawjournal@hse.ru

Article Length

Articles should be between 60,000 and 80,000 characters. The size of reviews and the reviews of foreign legislation should not exceed 20,000 characters.

The text should be in Times New Roman 14 pt, 11 pt for footnotes, 1.5 spaced; numbering of footnotes is consecutive.

Article Title

The title should be concise and informative.

Author Details

The details about the authors include:

- Full name of each author
- Complete name of the organization — affiliation of each author and the complete postal address
- Position, rank, academic degree of each author
- E-mail address of each author

Abstract

The abstract of the size from 150 to 200 words is to be consistent (follow the logic to describe the results of the research), reflect the key features of the article (subject matter, aim, methods and conclusions).

The information contained in the title should not be duplicated in the abstract. Historical references unless they represent the body of the paper as well as the description of the works published before and the facts of common knowledge are not included into the abstract.

Keywords

Please provide keywords from 6 to 10 units. The keywords or phrases are separated with semicolons.

References

The references are arranged as follows: [Smith J., 2015: 65]. See for details http://law-journal.hse.ru.

A reference list should be attached to the article.

Footnotes

The footnotes include legal and jurisprudencial acts and are to be given paginaly.

The articles are peer-reviewed. The authors may study the content of the reviews. If the review is negative, the author is provided with a motivated rejection.