Legal Issues in the Digital Age. 2023. Vol. 4. No. 3.
Вопросы права в цифровую эпоху. 2023. Том 4. № 3.

Research article
УДК: 347.962.1
DOI:10.17323/2713-2749.2023.3.59.80

Artificial Intelligence vs. Judicial Discretion: Prospects and Risks of Judicial Practice Automation

Valentina Aleksandrovna Rodikova

Institute of Management, Russian Presidential Academy of National Economy and Public Administration, 66 Eighth March Street, Yekaterinburg 620144, Russia, rodikovajus@gmail.com, SCIENCE INDEX: 4890-5030

Abstract

The paper fits into a wide public discussion of the introduction of artificial intelligence into the national judicial system, with the underlying risks and legal vulnerabilities analyzed on specific examples of enforcement practices. The effective national legislation on the use of artificial intelligence and the latest international laws on the subject including the EC's AI Act Compromise Text were studied. The paper looks into the risk factors characteristic of judicial discretion and judicial AI both on a comparative and standalone basis. Controversial opinions by law enforcement agencies, national and international researchers, AI developers on the prospects of using AI in the justice system were explored. The paper provides conclusive arguments that the introduction of AI is not feasible in the short and medium term in view of the current risks and geopolitical environment, state of the legal framework and judicial principles effective in the Russian Federation.

Keywords

artificial intelligence; neuronet; judicial discretion; strong and weak artificial intelligence; risk-based approach; justice system; forecasting; biometric identification.

For citation: Rodikova V.A. (2023) Artificial Intelligence vs. Judicial Discretion: Prospects and Risks of Judicial Practice Automation. *Legal Issues in the Digital Age,* vol. 4, no. 3, pp. 59–80. DOI:10.17323/2713-2749.2023.3.59.80

“If you can run faster than that you’ll be fine”[1].
E. Musk

Background

In launching the digital transformation of Russia in December 2020, President Vladimir Putin pointed out to a need “to ensure broad introduction of AI technologies and big data analysis” including “experimental legal regimes to use AI in specific economic sectors and social services”[2].

However, self-learning neural networks, technologically in vogue worldwide as the core of generative AI technology, have failed to be enshrined in the national legislation, only to become the apple of discord among law enforcement agencies. The disputes concerning the risks of neural networks used in judicial practice have been especially violent, in particular, because of a lack of the doctrinal definition of artificial intelligence and provisions to regulate and address the likely negative scenarios. Likewise, no final risks of convergence of AI and data science (big data processing) in the process of deep learning of neural networks were defined.

When a majority of researchers date the introduction of the term “artificial intelligence” back to 1956 (G. McCarthy’s presentation) [Smith C., 2006], they forget about three robotic technology laws proposed by Isaac Asimov in 1942 that essentially constrain in relative terms the emerging neural network-based products. Despite more than well-established history of the phenomenon under discussion, its conventional definition is not there yet, largely due to the fact that the term is too common [Kok J. et al., 2009: 2] and that there are legitimate doubts whether AI is a hoax launched in the interest of international corporations such as Intel (along the lines of “greenhouse effect” embedded into the public mind in the interest of Dupont Corporation), still more so since the so-called neural network itself, unlike the proposals to introduce it into social and economic sectors at large, did not evolve much from ABBYY Finereader, a text recognition software marketed in 1993.

[1] You can run away from it: Elon Musk jokes about his «friendly» robot // URL.: https://www.thesouthafrican.com/lifestyle/elon-musk-tesla-bot-humanoid-form-ai-robot-watch/ (last accessed on 22.05.2023).

[2] Putin has announced a need in digital transformation of Russia // Available at: URL: https://tass.ru/ekonomika/10172635 (accessed: 22.05.2023)

While defining AI as a field of science, P. Morkhat believes that "the main problem why an exact and common definition is not yet developed" is "a lack of clarity what is exactly intelligence as such" [Morkhat P.M., 2017: 26]. The author proposes to describe AI via its "key features: learning/self-learning ability, ability to understand and reflect, self-control" [Morkhat P.M., 2017: 31].

S. Russel and P. Norvig identify four main approaches to define "artificial intelligence": those based on human thinking and behavior and on rational thinking and behavior [Russell S., Norvig P., 2010: 1–2]. Some international researchers believe AI (what appears to be an optimal point of view) to be a platform for a number of promising technologies used in automated logic and big data processing [Haskins A., Arora S., Nilawar U., 2017: 4] or a branch of science [Rissland E.L., 1990: 1958–1959].

1. Enshrining AI Regulation in the National Law

Some authors [Laptev V.A., 2021] wrongly assume that the term "artificial intelligence" first appeared in the Action Plan (Roadmap) of the National Technological Initiative Autonet[3] in 2018.

Thus, the term was mentioned in paragraph 20, Presidential Decree No. 642 of 01 December 2016 "On the R&D Strategy of the Russian Federation" and in paragraph 12, Presidential Decree of 09 May 2017 "On the Information Society Development Strategy in Russia for 2017–2030". Further on, AI was repeatedly in the legislative focus: under paragraph 9, Presidential Decree No. 490 of 10 October 2019 "On the Development of Artificial Intelligence in Russia"[4], the use of neural networks was actually restricted to the so-called "weak AI" capable of solving only narrow tasks. AI was described in the document as "a set of technological solutions allowing to mimic human cognitive functions (such as self-learning and search for solutions outside a preset algorithm) and address specific tasks with results at least comparable with those of human intellect". This definition was later reproduced in Article 2 of Federal Law No. 123-FZ "On the Experiment to Introduce Special

[3] Action Plan (Roadmap) of the National Technological Initiative Autonet. Annex No.2 to Minutes No. 1 of 24 April 2018. Moscow, Presidium of the Council for Economic Upgrading and Innovative Development of Russia under the President of Russia, p. 21.

[4] Presidential Decree No. 490 of 10 October 2019 "On the Development of Artificial Intelligence in Russia" // Available at: URL.: http://www.kremlin.ru/acts/bank/44731 (accessed: 20.05.2023)

Regulation for Creating Necessary Conditions for the Development and Introduction of AI Technologies in a Constituent Territory of the Russian Federation — Federal City of Moscow — and on Amending Articles 6 and 10 of the Federal Law "On Personal Data" dated 24 April 2020.

The experimental regime introduced by this law has not been extended to other constituent territories, in particular, because of numerous problems regarding the implementation of the embedded substantive imperatives (copyright to neural network's outcomes, personal data processing, security, confidentiality etc.).

The legislation has not defined to what extent AI could be used to process specific categories of anonymized personal data (such as medical data) for more efficient public and municipal governance — data which, according to A. Saveliev, have "a special legal status due to potentiality of highly negative implications for the person if the processing terms were violated"[5]. There is no legal basis for AI to assume liability for the harm to human life and health as well as no understanding whether neural networks have a legal personality.

At the same time, experts in the military use of AI note that the three reasons for choosing the incoming data as the principal target are, by the order of priority, "complete dependence of insights on the amount and quality of inputs; difficulty to establish the fact of data diddling or editing; opportunity to gain a major advantage over a party in a dispute/conflict if decisions were made on the basis of analysis of misleading information" [Galkin D.V., Stepanov A.V., 2021: 73]. This is also true where AI is embedded into the system of justice.

Domestic technical regulations present artificial intelligence as a simulatable (artificially mimicable) intellectual activity of human mind (paragraph 3.17, GOST R 43.0.5-2009 "Information support of technologies and operator activities. Data exchange processes in technologies. General provisions)[6].

Starting from Presidential Decree No. 490 of 10 October 2019 "On the Development of Artificial Intelligence in Russia", AI has been qualified as

[5] Artificial intelligence and law: a link between the two? // Available at: URL.: https://www.garant.ru/news/1401154/ (accessed: 20.05.2023)

[6] National standard of the Russian Federation. Information support of technologies and operator activities. Data exchange processes in technologies. General provisions // Available at: URL.: https://docs.cntd.ru/document/1200079262 (accessed: 17.05.2023).

either "strong" or "weak" in the wake of the Western approach contained in the latest IBM research[7] of 2023. Thus, the Russian legislator and international developers believe "weak" ("narrow") AI to be the one focused on specific practical problems (Apple's Siri, Amazon's Alexa, IBM's Watson, autonomous vehicles, systems for voice recognition, virtual agents, computer vision, advisory mechanisms etc.). In contrast, "strong" AI is a combination of artificial general intelligence (AGI) and artificial super intelligence (ASI), the latter being a theoretical form that provides a device with an intellect superior to that of man (self-consciousness capable of solving problems, learning and planning for the future). For the national legislator it is associated with high risks since end results are not predictable and decision-making algorithms unclear.

There is currently no single document in Russia to regulate the development, implementation and use of AI, and to define the acceptable level of risks, legal personality of the parties involved, etc.

2. Latest European Law on Artificial Intelligence

Since AI systems, along with huge potential to boost economic growth, innovative development and global competitiveness, obviously carry major risks for security and protection of the core human rights and liberties, the European Commission published back in February 2020 the so-called "White Book" on artificial intelligence with a proposal to set up the European framework on AI and the limits of its use.

In October 2020 the European Parliament adopted 3 AI-related legislative resolutions on ethics, civil liability and intellectual property; in April 2021, the European Commission made proposals on the so-called AI Act which contained a technologically neutral definition of AI systems and also four risk categories for AI applications: unacceptable (contrary to EU values), high-risk (negatively affecting the security and core values of individuals), limited risk (those that meet specific transparency obligations) and minimal risk (those without obligations except those of the effective law).

On 6 December 2022 the European Council approved the general approach to the AI Act[8] explaining the requirements to high-risk AI systems

[7] What is Artificial Intelligence // Available at: URL.: https://www.ibm.com/topics/artificial-intelligence (last accessed on 23.05.2023).

[8] Council, Artificial Intelligence Act: Council calls for promoting safe AI that respects fundamental rights // Available at: URL.: https://www.consilium.europa.eu/en/press/press-

which identifies the general purpose AI systems, defines the regulatory scope (for example, national security, defense and related areas including law enforcement are ruled out) and proposes to create "regulatory sandboxes" to support AI-enabled innovations and open-code AI components[9]. As a result of discussions in the European Parliament, the world's first Transparency and Risk Management Rules for AI[10] were approved on 11 May 2023.

The drafters follow a risk-oriented approach to establish obligations for both AI suppliers and users depending on the aforementioned risk levels generated by artificial intelligence. However, before engaging in negotiations with the European Council to finalize the AI Act, the European Parliament will have to approve the draft "negotiating mandate" at its session scheduled for 12–15 June 2023.

The Rules completely prohibit the following AI practices:

real-time remote biometric identification systems in publicly accessible spaces;

remote biometric categorization using sensitive characteristics (such as sex, race, ethnicity, citizenship, religion, political orientation);

enforcement forecasting systems (based on profiling, location or past criminal behavior);

emotion detection systems at enforcement and judicial bodies, workplaces and education institutions;

indiscriminate deletion of biometric data from social networks, using video footage generated by surveillance cameras to create face recognition databases (in violation of human rights such as the right to privacy).

The Rules provide for obligations (individual legal regimes) shouldered by suppliers of basic models such as GPT, and extra "transparency" requirements, in particular, disclosure of the fact that the content was generated by AI. It is noted that the amendments are designed to establish human control over AI, with neural networks to be "safe, transparent, traceable, non-discriminatory, environmentally friendly"[11]. High-risk categories were expanded to include harm to people's health, safety, core rights and envi-

releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/ (accessed: 23.05.2023)

[9] Ibid.

[10] Al Act: a step closer to the first rules on Artifical Intelligence // Available at: URL.: https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence (accessed: 23.05.2023)

[11] Ibid.

ronment, as well as impact on electors during a political campaign and on trading platforms of social networks with more than 45 million users. It is assumed that both natural and legal persons have the right to make complaints about AI systems and receive explanations of decisions they generate[12].

Of special interest for the issue being discussed is paragraph 38, Chapter 1, Title III of the AI Act Compromise Text of 16 May 2023 which provides key risk scenarios — equally applicable to the Russian regulatory system — of AI use in law enforcement and judiciary activities: "Actions by law enforcement authorities involving certain uses of AI systems are characterized by a significant degree of power imbalance and may lead to surveillance, arrest or deprivation of a natural person's liberty as well as other adverse impacts on fundamental rights guaranteed in the Charter of 07 December 2000. In particular, if the AI system is not trained with high quality data, does not meet adequate requirements in terms of its performance, its accuracy or robustness, or is not properly designed and tested before being put on the market or otherwise put into service, it may single out people in a discriminatory or otherwise incorrect or unjust manner.

Furthermore, the exercise of important procedural fundamental rights, such as the right to an effective remedy and to a fair trial as well as the right of defence and the presumption of innocence, could be hampered, in particular, where such AI systems are not sufficiently transparent, explainable and documented. It is therefore appropriate to classify as high-risk a number of AI systems intended to be used in the law enforcement context where accuracy, reliability and transparency is particularly important to avoid adverse impacts, retain public trust and ensure accountability and effective redress.

In view of the nature of the activities in question and the risks relating thereto, those high-risk AI systems should include in particular AI systems intended to be used by or on behalf of law enforcement authorities or by Union agencies, offices or bodies in support of law enforcement authorities, as polygraphs and similar tools insofar as their use is permitted under relevant Union and national law, for the evaluation of the reliability of evidence in criminal proceedings, for profiling in the course of detection, investigation or prosecution of criminal offences, as well as for crime analytics regarding natural persons. AI systems specifically intended to be used for administrative proceedings by tax and customs authorities should not

[12] Al Act: a step closer to the first rules on Artifical Intelligence // Available at: URL.: https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence (accessed: 23.05.2023)

be classified as high-risk AI systems used by law enforcement authorities for the purposes of prevention, detection, investigation and prosecution of criminal offences.

The use of AI tools by law enforcement and judicial authorities should not become a factor of inequality, social fracture or exclusion. The impact of the use of AI tools on the defence rights of suspects should not be ignored, notably the difficulty in obtaining meaningful information on their functioning and the consequent difficulty in challenging their results in court, in particular by individuals under investigation". [13]

In light of the above reasonably restrictive approach to the use of AI systems in the judicial system, it appears expedient to discuss the risks resulting from AI integration into the national system of justice compared to the established factive presupposition (axiomatic modality which supports the sense and presumption of a statement and, while not being part of the presumption, makes sure that it is true) [Strawson P. , 1952: 113] of judicial discretion.

3. Judicial Discretion: Risks, Limits, Algorithmization

According to some researchers, the existence of judicial discretion as an institution is explained by the existence of objective regulatory peculiarities of some relationships and legislative gaps, where the weight of subjective criteria is minimal or absent [Tretyakova T.N., Karamanukian D.T., 2020: 6].

A number of authors believe judicial discretion to be "a specific type of law enforcement activities based on reasoning as a way to find the best solution in a given situation" [Makarikhina O.A., 2014: 15], something that actually identifies this institution with AI which could be hypothetically used in legal proceedings to algorithmize the process of searching for an optimal solution in a certain context.

I.A. Pokrovsky understood judicial discretion as "the right to interpret the law more freely, complement and even rectify it as may be required by the sense of justice and fairness" [Pokrovsky I.A., 1998: 90]. On the contrary, other researchers perceive the judge's personal conviction as "an outright opportunity for arbitrary judgment" [Morkhat P.M., 2018: 9].

[13] DRAFT Compromise Amendments on the Draft Report Proposal for a regulation of the European Parliament and of the Council on harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts // Available at: URL.: https://www.europarl.europa.eu/resources/library/media/20230516RES90302/20230516RES90302.pdf (accessed: 23.05.2023)

Judicial discretion is apparently an exercise of court powers to solve the case on the legitimate, fair and well-founded basis while using an opportunity to impose sanctions/render a judgment under a number of legitimate options and limits in the context of conflicts of law and legislative gaps.

Judicial discretion actually differs from AI as much as the judge's personal conviction from the standard algorithm of rendering a judgment (since classical AI operates outside a preset algorithm, its decisions are not predictable).

At the same time, the national law does not enshrine a number of key factive presuppositions (presumed judgments) such as definitions of the key concepts that make up constituent elements of a crime, only to multiply a possible risk of unjust, unfounded and illegal decisions in the context of judicial discretion understood as certain freedom of opinion.

Thus, a vast majority of "reputational" disputes involving legal persons as a claimant will be resolved by court on the basis of subjective principles of judicial discretion.

There is no factive presupposition in the national civil law to allow for an objective and impartial assessment of circumstances in cases concerning business reputation of legal persons. Meanwhile, the decision-making powers of a judge are based on a syllogism where one of the components, apart from a legal provision (if any), is the actual circumstances of the case [Barak, A. 1999] whose unambiguous, implicit parameters and matching criteria enable a fair judgment.

One example is where a court has (or does not have) reasonable grounds supported by law to qualify the defendant's statement as an asserted fact/ personal opinion, and reasonable grounds to qualify as irrelevant the defendant's statements addressed to the claimant. Different legal regimes applied by courts in considering business defamation cases where they ratify the defendant's subjective opinion or statement of fact, as well as the criteria to refer them to a given presupposition, are not enshrined in law. In the Defamation Review of Practice of 16 March 2016, the delineation of these regimes given a lack of clear reference criteria was claimed to be "the hardest decisions for courts"[14], only to "cause judicial errors"[15].

[14] Defamation Review of Practice (approved by the Presidium of the Supreme Court of Russia on 16 March 2016) // Available at: URL.: https://www.vsrf.ru/documents/thematics/15165/ (laccessed: 04.11.2021)

[15] Ibid.

Meanwhile, the initiatives to build neural networks into the national judicial system such as proposed by V.A. Laptev [Laptev V.A., 2021] appear to be fraught with even greater risks than judicial activism and multiplicity of imperfect opinions and personal convictions, and regulatory gaps.

4. Prospects and Risks of Judicial Practice Automation in Russia

Under the most likely scenario of the phased introduction of AI systems into judicial practice envisaged, in particular, by V. Laptev, AI will be implemented consecutively as an assistant judge as part of legal proceedings and in considering cases on their merits (short-term prospects); for evaluation of evidence and expert assessments (medium-term prospects); and as a possible replacement of judges to perform specific functions (long-term prospects) [Laptev V.A., 2021].

Meanwhile, recognizing and translating audio minutes of court sessions and documents provided by the parties into a machine-readable format will predictably involve putting sensitive information (including personal data) within reach of an unlimited range of people, both developers of an interface and other individuals, at the risk of unauthorized access and theft of "big data".

A "restricted" approach to storing and processing personal data — including those generated and processed in the judicial system — seems to be more effective, including in the context of current geopolitical threats, since it rules out sporadic and other mechanic "failures" related to the use of controversial technologies such as AI.

One example is China where relevant resolutions were adopted for National Data Administration[16] for control of the privacy and security of data of this newly created agency established, among other things, to secure full state control over all sensitive data of both individuals and economic institutions which are not designed to be processed, transmitted or used outside the government system. The Judicial AI (AI for legal assistance) actually handle in China more than 200 thousand cases a month [Stepanov, O.A., 2022: 229-237], with the neural network integrated into cloud-based national Big Data systems controlled by a number of public agencies. Mean-

[16] Available at: URL.: https://www.technologyreview.com/2023/03/15/1069814/china-new-bureau-data-economiy/ (accessed: 23.05.2023)

while, on 11 April 2023 the Cyberspace Administration of China published for public discussion the draft of Administrative Policies for Managing Generative AI-Enabled Services[17] which was innovative in imposing the responsibility for the content created by generative AI (chat bots etc.) on "suppliers" — developers and/or distributors of software solutions, with operators assuming an additional obligation to protect personal data where their processing is envisaged by the product.

However, the concept of AI learning on open judicial data (AI-Ready Open Juridical Data) does not stand up to criticism as there is neither a national strategy to publish such data for machine and deep learning nor quality (maturity) criteria of such data.

The government's involvement as a customer, regulator and contributor to AI implementation including in the judicial system makes it principally impossible to use an open code in this process (decentralized model of software development and management), something also contrary to the requirements of FSS Order No. 97 of 16 March 2022[18]and FSS Order No. 171 of 01 May 2021[19]. Not surprisingly, Russia is not in the index of responsible AI users created by Canada's IDRC CRDI including in the judicial system because participation requires a large amount of strategically important data to be provided.

Using AI for legal assessment of evidence including to analyze handwriting and forgery is unlikely because AI has so far failed to pass even CAPTCHA test (Completely Automated Public Turing Test to Tell Computers and Humans Apart), to say nothing about its ability to reliably determine the ownership of texts, their context, language nuances or abstract concepts.

Making judicial Big Data available to judicial AI, just like a need to digitize the judicial system across the board advocated by some of those who

[17] Notice of the State Internet Agency to seek public opinion on the Administrative Policies for Managing Generative AI-Enabled Services (draft for comments) // Available at: URL.: http://www.cac.gov.cn/2023-04/11/c_1682854275475410.htm (accessed: 26.05.2023).

[18] On providing FSS officers with powers to send requests to credit institutions, tax authorities, agencies for state registration of real estate transactions and data system operators for digital financial assets: Order No. 97 of 16.03.2022 // Available at: URL: https://www.garant.ru/products/ipo/prime/doc/404342484/ (accessed: 11.05.2022)

[19] On approving organizational and technical data security requirements to authorized officers of certification centers of the federal executive agency authorized to register legal persons: FSS Order No. 171 of 01.05.2021 // Available at: URL: https://ppt.ru/docs/prikaz/fsb/n-171-250719 (accessed: 11.05.2022)

represent the community of judges [Laptev V.A., 2021] with all incoming documents to be put into digital form, will not only fail to remove the technological inequality (because of variable IT literacy of the population, disparity of documents filed with courts, lack of adequate technical support etc.) but will also require to assign an operator responsible for the integrity of all sensitive data of the parties to legal proceedings. No system of those currently available seems to be able to ensure either security of this process or a definitively objective outcome of automated rendering of justice through the use of AI.

In this regard, the proposed development of cloud-based AI administered via Internet is so much more risky that the access to the potential software's interface will be left actually unprotected from third-party hacking since the golden rule "an offline computer cannot be hacked" will not be observed.

Pursuant to Article 1, Federal Law No. 3132-1 FZ "On the Status of Judges" dated 26 June 1992, the judicial power is autonomous, independent and exercised by judges as natural persons, not by a neural network. A number of institutions of law are not objectively liable to be assessed by artificial intelligence:

evaluating a need in compensation for moral harm and relevant amount;

measuring the extent of influence of the controlling parties on the situation of a corporate debtor in a bankruptcy case;

identifying the nature of complicity pursuant to Article 33 of the Criminal Code;

choosing a sanction among several alternatives;

assessing whether a compensation for damage and reparation for wrong are adequate in imposing a fine to waive criminal liability or whether imprisonment (a term of sentence) should be chosen etc.

Thus, it is not quite clear how AI will assess Supreme Court Determination of 16 February 2023 on case No. 67-UD22-30-K8 that "a crime against the public order, interests of public and local government service does not prevent the case to be closed and a criminal sanction imposed"[20] — as a provision or its interpretation by a judicial authority.

Major conflicts of law in legal instruments of any branch of law, subjective glossaries and comments interpreting a particular disputable situation

[20] Cassation Court Determination on case No. 7-UD22-30-K8 of 16.02.2023 // Available atr: http://vsrf.ru/stor_pdf.php?id=2215490 (accessed:24.05.2023)

challenge the validity of a neural network's decision to identify the prevailing provision and to make the only right choice.

The criminal justice experience of algorithmic forecasting (profiling) in the United States (PSA (Public Safety Assessment), COMPAS (Courcional Offender Management Profiling for Alternative Sanctions)) has shown the highly random nature of the resulting assessment, only to undermine the constitutional rights of individuals to "fair trial and individualized sanction, once algorithmic assessment becomes the only basis for a court ruling" [Talapina E.V., 2022: 4–27], the more so since the responsibility for wrong predictive decisions made by AI is not assigned to anyone.

Neither the national nor international legal doctrine can answer the question who will select judicial practices for machine and subsequent deep learning and on what criteria and basis, given that AI is trainable only on Big Data. There could be hundreds of thousands or even millions of such "impeccable solutions" for each branch of law, each type of cases and issues handled by courts of all instances and panels of all competences.

It is unclear whether this should cover the cases reviewed by higher instance courts, largely insufficient for neural network learning, who will finally determine the "proper" decision-making algorithm, and whether AI will rely exclusively on statistical information generated by the analysis of absolutely all court decisions.

Thus, in late 2021 the Supreme Court of Russia adopted Determination No. 305-EC21-14231 to formulate a critically important stance whereby an enterprise or organization did not have to prove the fact of established reputation and adverse effect of defamation if no claim was made to make up for reputational loss[21]. A year later, on 8 November 2022, the same authority indicated in Determination No. 78-KG22-44-K3 that pursuant to Article 56 of the Code of Civil Procedure the claimant had to prove the circumstances underlying his claims, that is, to prove the fact of established reputation in the given field of business relationships (industry, services, education etc.) which was not at all presumed. One can only guess which of the two opposed decisions by the same authority will be assessed by AI as the only right choice.

Likewise, the proponents of judicial AI never explain whether deep learning will involve exclusively the cases which stood up on appeal or

[21] Determination No. 305-EC21-14231 on case No. A41-54681/2020 //Available at: URL: https://kad.arbitr.ru/Kad/Card?number=A41-54681%2F2020 (accessed: 09.12.2021)

whether the list will include those never appealed against irrespective of the impulsive cause. An appeal to a higher court against the trial court's decision involving AI will algorithmically mean the decision will be upheld if considered by the appeal and cassation courts using same interface. Thus, a "traditional" way of considering such cases has to be envisaged starting with the court of appeal.

The variable approach of courts at different levels to consider even standard cases; legal paradoxes and lack of consensus between the doctrine and enforcement practices; courts addressing certain cases on an exceptional basis for lack of clear definitions of major concepts in the national law and given a considerable number of value judgments (good faith, materiality of harm, insignificance, permanent disfigurement, mitigating circumstances, generality, custom etc.) — these things are contrary to the algorithmic nature of machine learning, only to result in probable errors both in AI-enabled analysis of certain facts and "unbiased" decision making.

One example of likely fallacies can be a hypothetically broad interpretation by AI of the provisions of the Supreme Court Plenum Resolution of 18 April 2023 on "the relatives of a police officer, military serviceman or public official"[22]. Thus, according to D. Veretennikov, "such wording… can result in neighbors, doormen (watchmen), utility workers, postmen etc. wrongly considered as relatives on the sole basis that the victim gave such evidence"[23]. Since deep learning makes AI operate on the basis of formal mathematical logic outside any preset algorithm, there is no telling what a neural network will be guided by in associating a person with "other relatives" in light of the Supreme Court's explanations.

Even basic ("narrow") AI interfaces for technical judicial functions such as recognizing and digitizing handwritten and audio documents; referring cases to the courts of relevant jurisdiction; collecting legal statistics, searching for party contact details for service of process; or performing expert functions are not feasible in the short and medium term for the said reasons such as vulnerabilities in sensitive data processing and a lack of functional operator; possible threats to national security; extensive value

[22] Supreme Court Plenum Resolution No. 11 "On handling criminal cases of martial offenses" dated 18 April 2023 // Available at: URL.: https://www.vsrf.ru/documents/own/32440/ (accessed: 25.05.2023)

[23] SC to protect relatives of police officers. Advokatskaya Gazeta.18.04.2023 // Available at: URL.: https://www.advgazeta.ru/novosti/vs-predlagaet-zashchitit-blizkikh-pravo-okhranitelyam-lits/ (accessed: 25.05.2023)

judgments and conflicts of law; lack of universal criteria to select “impeccable” verdicts for deep learning of neural networks; lack of multi-layered neural networks capable of evaluating actual circumstances of the case; low digital literacy of legal profession etc.

Contrary to the opinion of judicial AI proponents such as P. Morkhat and V. Momotov, Supreme Court Presidium member, there are grounds to believe that AI will not only fail to ensure “barrier-free access to justice for population” [Morkhat P.M., 2018: 6–11] and “an space for legal proceedings” [Momotov V.V., 2020] but can result in new obstacles to proper implementation of Article 46 of the Russian Constitution. The Machine-Readable Law Concept Note drafted by the Skolkovo Center in 2021 and submitted for approval to the Ministry of Economic Development has likewise failed to be implemented due to the emerging risks and despite the belief that its planned introduction would allow to reduce legal costs of individuals and to ensure transformative change of the regulatory and supervisory domains and those of administrative and legal proceedings[24].

Unlike judges, the developers of AI interfaces and of relevant roadmaps for AI implementation in the system of justice are not subject to higher reputation and qualification requirements, only to increase the likelihood of legal and reputational risk scenarios in the course of third-party development of judicial AI despite all declarations of openness and independence.

Meanwhile, neither the Supreme Court of Russia or the Constitutional Court of Russia proposed to “administer” judicial AI (GosTech (Federal Government) could not a priori administer the digitization process at courts since the judicial branch is separated from the legislative and executive branches under Article 10 of the Constitution) have adequate skills and knowledge to analyze machine learning algorithms and assess AI decision-making methodologies in a given case.

As we mentioned above, non-legislated ways to protect the personal data of litigants are a separate category of risk factors realized in using AI technologies in court practice. Utilization of AI systems in legal proceedings leads to an exponential growth in the probability of data array hacking through API-technology (Application Programming Interface, a set of tools and functions describing the interaction between the interface user (e.g., the Pravosudiye (Justice) State Automated System portal etc.) and

[24] Machine-readable law: a likely future? // Available at: URL.: https://www.garant.ru/news/1464143/ (accessed: 19.05.2023)

the personal data operator). Russian laws do not list information, including personal data, which AI is entitled to access through API technology; there is no actual state supervision over the transfer of information containing personal data of individuals within the subsystems of government agencies, including courts, etc. on the basis of the person's consent to each such operation, which is expressly stipulated by the requirements of Law No. 152-FZ. At the same time, utilization of cloud-based distributed registry technologies with one-way encryption to collect, process and store personal data without the involvement of a single operator (Proton.mail, a webmail service with encryption, Mega file-sharing service, use a similar approach) fails to meet the provisions of Federal Security Service Order No. 97 of 16 March 2022[25] , FSS Order No. 171 of 01 May 2021[26].

If we look at blockchain technologies as a method of secure storage and decomposition of personal data in order to anonymize them and further endow them with negotiability, which a range of researchers propose as a secure alternative to steganographic and cryptographic methods of personal data protection, including data potentially processed by Judicial AI in judicial practice[27] , we see that they are not supported by the necessary legal basis required for their implementation as a protection method. Their mechanical introduction in the civil law regulation of relevant metadata circulation poses fundamental risks, both reputational and legal, for personal data operators (here, the judiciary system) and the state.

Courts lawfully process personal data (People Data), namely Volunteered Data, except for Observed & Inserved Data relating to an indirectly identifiable person, in accordance with the provisions of Russian law (Articles 6, 10, 11 of Federal Law of 27.07.2006 "On Protection of Personal Data" No. 152-FZ ;hereinafter: Law No. 152-FZ.) Other essential require-

[25] On Authorizing Federal Security Service Officials to Send Requests to Credit Institutions, RF Tax Bodies, Bodies Responsible for the State Registration of Rights to Immovable Property and Transactions Therewith and to Operators of Information Systems in Which Digital Financial Assets are Issued: FSS Order No. 97 of 16 March 2022 // URL: https://www.garant.ru/products/ipo/prime/doc/404342484/ (Last accessed: 11 May 2022).

[26] On Approval of Organizational and Technical Requirements in the Field of Information Security for Authorized Persons of the Certification Centre of the Federal Executive Body Authorized to Perform State Registration of Legal Entities: FSS Order No. 171 of 01.05.2021 // Available at: URL: https://ppt.ru/docs/prikaz/fsb/n-171-250719 (Last accessed: 11 May 2022).

[27] Kozin I.S. A Method of Ensuring Secure Personal Data Processing on the Basis of Blockchain Technology. Scientific and Technical Bulletin of Information Technologies, Mechanics and Optics. 2019. No. 5. Pp. 892–899.

ments include compliance with general principles of processing (Article 5, Federal Law No. 152-FZ)[28] ; the operator should perform data localization, notify Roskomnadzor (Federal Service for Supervision of Communications, Information Technology, and Mass Media), and undertake organizational and technical measures for personal data protection (Articles 22, 18, 18.1–19 of Federal Law No. 152-FZ)[29] , and the person in question should give a specific, conscious and informed consent.

In its decision on Case No. A40-5250/17-144-51, Roskomnadzor expressed a more stringent position stating: "It is not possible to assert without the written consent of the user that the data was provided by the person in question and that the applicant's actions violate Paragraph 1, Part 1, Article 6 of Federal Law No. 152-FZ (processing of data without the person's consent)."[30]

Hence, blockchain technology as a method for AI to ensure secure storage and use of People Data arrays in course of judicial activities contradicts the very idea of both the law on personal data and the regulator's position because it implies decentralization and public availability of information, where personal data can be provided to all participants of the distributed registry. While preventing direct data leaks at any given moment, the distributed registry (e.g., containing data of litigants in concrete proceedings) violates the basic principle of law: one purpose—one consent—one recipient.

If AI is utilized to administer a distributed registry (appoint a person responsible for inclusion/exclusion from the register; for completeness, reliability and procedure of information use), then such register ceases to be a distributed register. If it is a classical peer-to-peer blockchain with free data flow, it is impossible to prevent misuse of data, including personal data.

The above entails clear legal risks for the corporate data operator (registry holder) (in this case, a specific judicial authority) arising from the use of personal data by AI systems. The risks, in particular, include penalties under criminal liability (Art. 137 of the RF Criminal Code "Violation of Personal Privacy"), administrative liability (Art. 13.11 of the RF Code of

[28] Available at: URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (accessed: 08.05. 2022)

[29] Ibid.

[30] Judgment of Arbitration Court of Moscow on Case No. A40-5250/17-144-51. 05 May 2017 // Available at: URL: https://sudact.ru/arbitral/doc/YLVZ7F3cAwU0/ (accessed: 04.05. 2022)

Administrative Offences “Violation of the Law of the Russian Federation in the Field of Personal Data”), civil liability (Art. 15 “Recovery of Losses due to Violation of Personal Data Processing Rules”, Art. 151 of RF Civil Code “Compensation of Moral Damages”, Art. 24 of Federal Law No. 152-FZ “Infliction of Emotional Distress (Moral Suffering) to a Citizen due to Violation of Personal Data Processing Rules”), and disciplinary liability (Art. 90, 192 “Other Violations in the Field of Personal Data Processing”, subparagraph “C”, Paragraph 6, Subparagraph 1, Art. 81, “Disclosure of Personal Data by an Employee” of the RF Labor Code.)

If the above risk scenarios are realized through the fault of the data operator, this will not only entail quite material losses for the judicial system, but also a heavy blow to the business reputation of the judiciary bodies.

The law does not regulate the issue of civil and criminal liability arising from the use of AI systems in the administration of justice: e.g., the person responsible for making a likely inappropriate, unlawful, erroneous decision in a particular AI technology case has not been identified.

In the case of the “Chinese” scenario of introducing AI into judicial practice, the software developer is likely to become the responsible person. In this case, the courts will additionally have the responsibility to protect data processed by AI.

It is worth noting that, unlike the Peoples’ Republic of China, the Russia does not have a structure, which is similar to the National Data Administration of China (so there is a reason why NDA, the acronym name of this body, coincides with the common designation of a confidentiality agreement) and which should be responsible, among other things, for the circulation of personal data processed by AI.

Several foreign researchers note that as a result of implementation of AI technologies in the judicial practice, e.g., in China, “one should get ready for the undermining of the judiciary by technology companies and the capital .”[31] The intelligent judicial SoS (system of systems) is now connected to the desktop of each judge in the PRC. Based on machine learning technology, it automatically searches for similar cases, “suggests” laws and regulations, drafts legal documents, and modifies alleged human errors in the verdict, if any. According to Xu Jianfeng, director of the Information Centre of the

[31] China’s court AI reaches every corner of justice system, advising judges and streamlining punishment // URL.: https://www.scmp.com/news/china/science/article/3185140/chinas-court-ai-reaches-every-corner-justice-system-advising (accessed: 27.05. 2023)

Supreme People's Court of China[32] , this raises a number of questions about determining who is liable for a judgement that is made using robotic systems. While Artificial Intelligence advises judges and optimizes punishment, including through the Smart Court interface that allows the system to access police, prosecution and government databases and integrate with China's social credit system, it is not an entity responsible for the decisions it actually makes as a result of certain generative actions.

The Supreme People's Court of the People's Republic of China requires that a judge must consult with artificial intelligence on every case; if the judge rejects the AI's recommendation, the system requires a written explanation for subsequent audit. As a result, judges predictably strive to follow recommendations to avoid having to "challenge the system," even if the artificial intelligence chooses a less appropriate reference or law in a particular case. The result is a decision that is not always optimal and lawful.

In this regard, it has a sense to believe that even before the introduction of Judicial AGI elements into the domestic judicial practice, it would be justified and necessary to legally assign the responsibility for errors or other legal consequences arising in the process of judicial proceedings involving AI to the institution (authority) that licensed a particular AI interface to participate in judicial practice. An institution (authority), which actually owns a certain software product and recognizes its "legal integrity" for participation in the judicial process (in Russia it is the Judicial Department at the Russian Supreme Court), thereby assumes the burden of responsibility for judgments made using this product. A similar conclusion can be drawn in cases where an unmanned aerial system involving artificial intelligence makes decisions on the elimination of a person in a combat, and the responsibility rests not with the developer of the UAV interface or the executor of the order (the serviceman), but with the agency that is the balance holder of the unmanned system equipped with a particular software program.

The legislator and law enforcement agencies advocating the use of AI in the system of justice have equally failed to fully appreciate the risk of discrimination against the parties to legal proceedings created or reproduced by AI as a result of algorithmic bias [Kharitonova Yu. S., Savina V.S., Panyini F., 2021: 488–515], as well as risk scenarios related to vulnerabilities, automation errors, network failures. For example, network gateways (traf-

[32] Ibid.

fic control servers between the local network of the national justice system and the Internet) are fully produced by international companies such as Cisco, Huawei, Panasonic etc. Thus, the system cannot be safe from possible attacks either now or in the near future. While a sensitive data theft in a cellular network is a dangerous invasion of privacy, a potential hacking of the judicial system relying on the infrastructure of unfriendly countries is fraught with violation of human rights and liberties envisaged by Chapter 2 of the Constitution, particularly in AI-enabled decision-making on criminal cases.

"We first create the core of the model and teach it to operate with words, remember their combinations, make logical chains… Next comes a superstructure to carry certain meanings… It will later manage all processes. If we adjust (the superstructure) to handle regulations, it will produce — just as a lawyer –specific answers to specific questions without any offhand interpretations… The software will develop an understanding of what is expected from it. The question is who sets the selection criteria as an expert and for what purpose"[33] — this is how a domestic developer describes the creation of a next judicial AI interface.

Conclusion

The disparity of learning sources and their selection criteria, uncertainty of input meanings currently appear to be a key problem that cannot be resolved in the current regulatory and enforcement context in introducing AI and its derivatives into the national system of justice. The lack of legislative recognition of subjects of responsibility for decisions made using AGI makes the corresponding initiatives for its implementation in judicial practice not only careless, but dangerous.

In this regard, the reference of AI proponents to Argentine where Prometea, an AI-enabled interface, has been used since 2018 for independent analysis of circumstances on standard lawsuits, with the decisions 100 percent ratified by judges [Atazhanov A., Ismailov B., 2020: 269-284] appears to be misplaced. The Laser Program to generate well-founded decisions "on the basis of in-depth analysis of case circumstances and similar decisions" [Stepanov O.A., 2022: 229–237] has failed to be implemented in

[33] Russia to actively develop substitutes for ChatGPT // Available at: URL.: https://therussiannews.ru/news/technologies/v-rossii-aktivno-razrabatyvayut-analogi-chatgpt/ (accessed: 25.05.2023).

the national justice system largely because of the emerging risk scenarios. V. Shananin noted in addition that "artificial intellect should be implemented exclusively on the principles of human control, selection and priority" [Shananin V.A., 2022: 143–146].

At the same time, an optimal combination of the national justice system with AI as a key digitization technology without drifting towards regulatory arbitration; proactive compliance policy of development companies and enforcement agencies coupled with active adoption of new regulations can provide an adequate basis for supporting a global trend to make AI a major competitive factor in both domestic and international markets and an additional driver of economic growth of the Russian business.

References

1. Atazhanov A., Ismailov B. (2020) International experience of introducing modern technologies into the justice system. *Obschestvo i innovatsii*=Society and Innovations, no. 2, pp. 269–284 (in Russ.)

2. Barak A. (1999) *Judicial discretion*. Moscow: Norma, 376 p. (in Russ.)

3. Galkin D.V., Stepanov A.V. (2021) Security aspects of military AI applications. *Voennaya mysl*=Military Thought, no. 4, pp. 72–79 (in Russ.)

4. Haskins A., Arora S., Nilawar U. (2017) Impact of artificial intelligence on Indian real estate: transformation ahead. Madras: Colliers Radar Property Research, 13 p.

5. Kharitonova Yu.S., Savina V.S., Panyini F. (2021) A bias of AI algorithms: issues of ethics and law. *Vestnik Permskogo* gosudarstvennogo *universiteta*=Perm State University Bulletin, issue 53, pp. 488–515 (in Russ.)

6. Kok J., Boers E., Kosters W. et al. (2009) Artificial intelligence: definition, trends, techniques, and cases. In: Encyclopedia of life support systems. Artificial intelligence. J.N. Kok (ed.). Paris: Eolss Publishers, 401 p.

7. Laptev V.A. (2019) The concept of artificial intelligence and liability. *Pravo. Zhurnal Vysshey shkoly ekonomiki*=Law. Journal of the Higher School of Economics, vol. 12, no. 2, pp. 79–102 (in Russ.)

8. Makarikhina O.A. (2014) On judicial discretion in civil and arbitration proceedings. *Arbitrazhniy i grazhdanskiy protsess*=Arbitration and Civil Process, no. 6, pp. 14–17 (in Russ.)

9. Morkhat P.M. (2018) Judicial AI as a way to overcome judicial discretion. *Teoriya i istoriya prava i gosudarstva*=Theory and History of Law and State, no. 5, pp. 6–11 (in Russ.)

10. Morkhat P.M. (2017) On defining the concept of artificial intelligence. *Teoriya i istoriya prava i gosudarstva*=Theory and History of Law and State, no. 12, pp. 25 –32 (in Russ.)

11. Pokrovskiy I.A. (1998) Main problems of civil law. Moscow: Statut, 349 p. (in Russ.)

12. Rissland E. (1990) Artificial Intelligence and Law: Stepping Stones to a Model of Legal Reasoning. *Yale Law Journal,* vol. 99, no. 8, pp. 1957–1981.

13. Russell S., Norvig P. (2010) Artificial intelligence: a modern approach. Boston: Prentice Hall, 1132 p.

14. Shananin V.A. (2022) Using AI system in judicial practice. *Yuridicheskaya nauka*=Legal Science, no. 11, pp. 143–146 (in Russ.)

15. Stepanov O.A., Basangov D.A. (2022) On the prospects of AI impact on legal proceedings. *Vestnik Tomskogo* gosudarstvennogo *universiteta*=Bulletin of Tomsk State University, no. 5, pp. 229–237 (in Russ.)

16. Strawson P. (1952) *Introduction to logical theory.* London: Macmillan, 266 p.

17. Talapina E.B. (2022) AI-aided data processing and discrimination risks. *Pravo. Zhurnal Vysshey shkoly ekonomiki*=Law. Journal of the Higher School of Economics, vol.15, no. 1, pp. 4–27 (in Russ.)

18. Tretyakova T.N., Karamanukyan D.T. (2020) The concept of judicial discretion. *International journal of professional science,* no. 2, pp. 5–8 (in Russ.)

Information about the author:

V.A. Rodikova — Postgraduate Student.

The article was submitted to editorial office 30.06.2023; approved after reviewing 10.08.2023; accepted for publication 10.08.2023.