ISSN 2949-2483

Volume 2 Number 3

JOURNAL OF DIGITAL TECHNOLOGIES AND LAW

2024

ELECTRONIC SCIENTIFIC AND PRACTICAL JOURNAL

JOURNAL OF DIGITAL TECHNOLOGIES AND LAW
Volume 2, No. 3
2024
DOI: 10.21202/2949-2483.2024.3
ELECTRONIC SCIENTIFIC AND PRACTICAL JOURNAL
eISSN 2949-2483
Published since 2023, frequency – 4 issues a year. DOI: 10.21202/2949-2483

Editorial Board

Editorial

Address: 42 Moskovskaya Str., 420111 Kazan, Russian Federation
Tel.: +7 (843) 231-92-90
Fax: +7 (843) 292-61-59
E-mail: lawjournal@ieml.ru
Website: https://www.lawjournal.digital
Telegram: https://t.me/JournalDTL_world
VKontakte: https://vk.com/JournalDTL
Yandex.Dzen: https://dzen.ru/JournalDTL
Odnoklassniki: https://ok.ru/JournalDTL

Founder and publisher of the Journal

Kazan Innovative University named after V. G. Timiryasov. Address: 42 Moskovskaya Str., 420111 Kazan, Republic of Tatarstan, Russian Federation. Tel.: +7 (843) 231-92-90. Fax: +7 (843) 292-61-59. E-mail: info@ieml.ru. Website: https://ieml.ru

Certificate on registering a mass medium: EL no. FS 77-84090 of 21.10.2022, issued by Roskomnadzor.
Territory of distribution: Russian Federation, foreign countries.

Date of signing the issue for publication: 2024, September 25. Hosted on the website https://www.lawjournal.digital: 2024, September 30.

JOURNAL OF DIGITAL TECHNOLOGIES AND LAW
Volume 2, No. 3
2024
DOI: 10.21202/2949-2483.2024.3
ELECTRONIC SCIENTIFIC AND PRACTICAL JOURNAL
eISSN 2949-2483

Content

Editorial
UDC 34:004
EDN: https://elibrary.ru/zkbuks
DOI: https://doi.org/10.21202/jdtl.2024.25

Digital and Nature-like Technologies: Features of Legal Regulation

Ildar R. Begishev
Kazan Innovative University named after V. G. Timiryasov, Kazan, Russia

Anna K. Zharova
National Research University «Higher School of Economics», Moscow, Russia

Maksim V. Zaloilo
Institute of Legislation and Comparative Law under the Government of the Russia, Moscow, Russia

Irina A. Filipova
National Research Lobachevsky State University of Nizhny Novgorod, Nizhniy Novgorod, Russia

Albina A. Shutova
Kazan Innovative University named after V. G. Timiryasov, Kazan, Russia

Much has been written in scientific literature about the growing influence of digital technologies on modern society. The most significant digital technologies include, first of all, artificial intelligence, robotics, wireless communications, blockchain, virtual and augmented reality, the Internet of Things, digital twins, and other new industrial technologies. Among them, the group of artificial intelligence technologies is of particular interest, as it outpaces the other groups of technologies in terms of extensive use. Services based on artificial intelligence, especially generative artificial intelligence, are becoming commonplace, transforming work processes, hobbies, and everyday life.

However, it is not only digital technologies (and digital services based on them) in their pure form that are changing the real (physical) world; the influence of nature-like technologies is also growing that allow reproducing living nature systems and processes in the form of technical systems and technological processes. These include, for example, biotechnologies (including genetic engineering), neurotechnologies (neural prosthetics, neural interfaces, etc.). Strictly speaking, the above technologies are at the intersection

of digital and nature-like technologies, as their development became possible due to digitalization of production, business, research, and communications. The currently manifesting trend towards neuromorphization of artificial intelligence also brings it closer to nature-like technologies. As is known, one of the approaches to the creation of artificial intelligence is the ascending (biological) one, associated with the construction of neural networks that artificially model processes similar to those occurring in the human brain.

Whereas a few years ago the question of regulation usually referred only to the use of the above-mentioned technologies, nowadays the opinion about the need to create a system of legal regulation more and more often refers not just to the use of these technologies, but also to the possible ways of their development. The potential of using these technologies is too attractive, and simultaneously with their development and practical dissemination, various risks increase significantly. Parliaments in different countries and international organizations are discussing the inclusion in the legal system of norms regulating the use of these technologies, and often the direction of their evolution.

Some issues are already reflected in existing legislation and judicial practice. For example, the European Union Artificial Intelligence Act of 2024 regulates the use of technologies and products based on artificial intelligence, with a special focus on general-purpose AI models in Chapter 5 of the Act. The Act provides for additional obligations imposed on the providers of such models, and if they are included in the list of models with systemic risk, the number of legal obligations increases. Another example of legal regulation in this area is the “Provisions on the Administration of Deep Synthesis Internet Information Services” published by the Cyberspace Administration of China on November 25, 2022 (it is often referred to as the “Provisions of Deepfake Regulation”). The document contains a number of requirements for the provision of deep synthesis services for the creation of images, videos, audios, and texts. The generated content must comply with information control rules and be labeled as synthetically created, and providers must take measures to prevent misuse of the service and label content created by artificial intelligence.

An example from judicial practice is the decision of the Supreme Court of Chile of August 9, 2023, concerning the right to privacy by protecting the work of the human brain. The issues addressed by the decision can be categorized as personal data, neurodata, and neural rights of the individual. The Supreme Court decision came as a result of handling a constitutional protection lawsuit filed against Emotiv Inc. of San Francisco, USA, which commercialized a wireless headset with sensors that collect neurodata, i.e. information about the electrical activity of the brain. The decision states that privacy is an important aspect of human integrity, human dignity and human rights such as cognitive freedom, freedom of thought and identity. Such a decision was made possible by the deliberate efforts of Chilean parliamentarians to incorporate neurorights into the state legislation.

This issue of the Journal presents research by authors from different countries on the use and regulation of digital and nature-like technologies, the challenges posed by the increasing use of these technologies and products, and proposed solutions to the problems.

The first article of the issue – "Legal issues of ensuring technological sovereignty" (**Maksim Zaloilo (Russia)**) – proposes the theoretical and legal model of ensuring technological sovereignty. It also considers the concepts of technologocentrism and digital (technological) solidarity, as well as the strategic bases of scientific and technological development. The author raises general questions concerning the provision of technological security and the definition of science-based vectors of their solution, and, as a consequence, increasing the importance of maintaining the state independence in the field of science and technology. Without this, effective economic development and the sustainable functioning of state institutions critical for people's lives become impossible. The technological imperative underlying the formation of modern technogenic civilization has become an important factor for the transformation of law. In turn, law as a universal regulator of social relations has to respond, solving the difficult task of protecting the technological security of the country.

The next article – "Human genome editing: managing technological risks through legal means" (**Aleksandra Troitskaya, Konstantin Sharlovskiy (Russia)**) – is devoted to the problems of legal regulation of using genetic engineering as one of the most demanded biotechnologies today. It allows changing DNA and ensuring the transmission of the genetic program to the next generations of living organisms. The article presents the results of the study of various approaches to the regulation of genetic editing for reproductive purposes, defines the conditions and peculiarities of the application of possible regulatory mechanisms and assesses the current legislation in this area.

The issues of legal regulation of digital technologies are of concern to authors from European countries who consider the emerging conflicts and risks between blockchain technology and data protection legislation (**Fabio Severino, Ludovica Sposini, (Italy)**). The most urgent problems in this area are addressed, which are caused by the shortcomings of traditional blockchain models and the "right to be forgotten" enshrined in current European law. Particularly interesting is the analysis of the materials on the emerging issues presented in the study. They describe a hybrid solution to guarantee the right to cancellation and modification of personal data and to address the identified incompatibilities between technology and existing regulation.

It is also interesting to study the emerging approaches to the regulation of technologies in countries whose experience is not so often demonstrated in the scientific literature. This allows taking a broader look at the problem and revealing new facets for further research. For example, one of the articles in this issue identifies the difficulties

on the way to regulating the use of digital technologies in the national cadastral system of Uzbekistan (**Robiya Toshboeva (Uzbekistan)**). The use of artificial intelligence can improve the implementation of cadastral registration, provided that a quality legal framework is established. The latter is difficult to achieve without a clear regulation of the legal regime of artificial intelligence in the national legislation.

The growing use of artificial intelligence technologies in the private sector entails changes in both business processes and relations between employers and employees, thus affecting both business law and labor law. The problems of legal regulation of using artificial intelligence for competitive procurement are analyzed in the next article (**Dmitriy Kazantsev (Russia); Pavel Dohnal (Czech Republic), Pavel Dohnal Jr. (Denmark)**). The authors identify the most promising areas for the creation of legal regulation of the relevant relations. They provide a real-life example of complex procurement of high-tech equipment as an experimental model and predict the use of artificial intelligence in procurement in the future. No less interesting is the topic of forming legal regulation in the sphere of applying artificial intelligence in the recruitment of employees (**Denis Novikov (Russia)**). The problems arising from the introduction of AI-based services in the hiring procedure are manifold. They include the need to protect the applicant's personal data, the risks of discrimination and unjustified refusal to hire due to biased algorithms, and the distribution of responsibility for the decision made with participation of the AI system. In order to avoid additional mistakes, it is worth referring to foreign best practices, which will allow taking into account the available experience and will help to design an optimal national regulation.

Two other articles included in this issue deal with criminal law and criminological problems. The first one (**Fotios Spyropoulos (Cyprus, Greece)**) is devoted to new approaches in criminology. It allows identifying and defining the area of digital criminology, which investigates the potential use of new technologies for criminal purposes. The world is increasingly becoming a "hybrid" world: reality and virtual environment will become more and more intertwined. This will also affect crime, which makes us think about adapting existing criminal legislation to the new phenomena. Another article (**Valentina Babaeva (Russia)**) touches upon the functions of newsmaking criminology, taking into account the "flow" of the bulk of media resources into the Internet and the steadily growing influence of social networks, blogs and video hosting as alternative media on public opinion. The article describes the changing opportunities for interaction between the media and law enforcement agencies and the new risks arising from the coverage of materials about law enforcement and crime in such media.

The next two articles in the issue reflect international legal issues. The first one examines unmanned aerial vehicles, as their development and use leads to violations

of the airspace of other states. The author notes that the topic of unmanned aerial vehicles (drones) as autonomous weapons usually includes a discussion of what rules of international law should govern their use, and the extent to which current international law is in principle capable of responding to changes resulting from digitalization (**Milad Kashi Kamijani (Iran)**). Another article is related to digital technologies used in international justice, namely in the courts of integration associations (**Valentina Talimonchik (Russia)**). Its author aims to analyze the competence and procedures of the courts of integration associations that allow them to resolve disputes related to digital technologies. Ultimately, the prospects for handling this category of disputes are determined. The comprehensive analysis of various sources, including scientific sources, international treaties and acts of judicial practice, results in the proposal to introduce a definition of the content of disputes related to digital technologies in relation to the courts of integration associations.

The scientific review that concludes this issue of the Journal is of particular interest. It deals with the topic of neural rights and the increasing penetration of neurotechnology from research laboratories into ordinary people's lives (**Yan An Cornejo (Ecuador)**). The development of neurotechnologies has opened up tremendous opportunities to understand and improve the functioning of the human brain, but it also led to serious concerns about the protection of human rights, privacy, and mental autonomy. Today, medical devices based on neurotechnologies can significantly improve the lives of people with certain diseases, but, in parallel, they collect data on brain activity and can be used to "hack" the mind. The latter necessitates the discussion of establishing a legal framework to guarantee the responsible development and use of neurotechnologies. Such legislation should include the rights to mental privacy, neurotechnological non-discrimination (the right to equal treatment regardless of a person's neurobiological characteristics), and access to one's neurodata. Equally important is the right to personal identity and free will as the ability to make decisions independently without external interference.

The presented achievements of legal doctrine in the studies of digital and nature-like technologies show that the practice of their use gives rise to many complex ethical, social, legal issues at the "intersection of law, science and technology". Law is changing in response to changes in science and technology and is becoming more dynamic. The topics touched upon in this issue encourage discussion of new global challenges and risks that require the development of a strategic consensus in understanding the latest legal phenomena and processes. They also demand searching for adequate and scientifically grounded answers that open new horizons and perspectives, transforming the existing ideas about law.

We hope that this issue of the Journal will be of interest to a wide range of readers, and the articles that have been published will serve as a good motivator for those potential authors who would like and are ready to demonstrate their promising scientific results and developments in the sphere of innovations and law on the pages of our periodical (Fig. 1).

Fig. 1. Geography of the visitors of the Journal of Digital Technologies and Law website (160 countries as of September 30, 2024)

The Journal has a large audience of Russian readers and publishes a significant number of Russian authors (Fig. 2). An important milestone in its scientific activity this year was indexing in the authoritative source of bibliographic information on national periodicals – the largest Russian bibliographic database of scientific citation – RSCI, which accumulates not only the research works, but also information about their citations. Inclusion of the Journal into RSCI is an important step towards recognizing the high scientific level of the Journal. It opens new opportunities for authors and editorial staff, provides the system users, readers and researchers all over Russia with a wide access to the papers of the authors who have published the results of their scientific work with us. The system is interesting for its analytical capabilities. It allows not only tracking the publications of Russian researchers in scientific editions and their citations in other journals, but also forming various scientometric indicators of the Journal based on the obtained information.

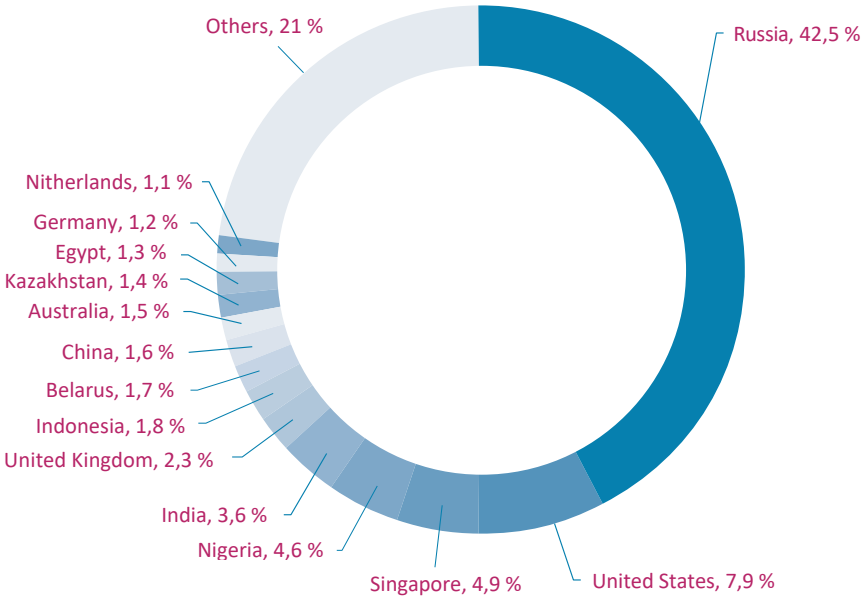


Fig. 2. Statistics of visiting the Journal of Digital Technologies and Law website (as of September 30, 2024)

In 2024, Journal of Digital Technologies and Law was the general information partner of the 3rd International Scientific and Practical Conference "Digital Technologies and Law", the largest in Russia and the Commonwealth of Independent States. This is a large-scale event, organized annually as part of the International Forum Kazan Digital Week 2024 jointly by Kazan Innovation University named after V. G. Timiryasov and the Ministry of Digital Development of State Administration, Information Technologies and Communications of the Republic of Tatarstan with the assistance of Rifkat Minnikhanov, President of the Academy of Sciences of the Republic of Tatarstan, Chairman of the Council of the Association for Assistance to Digital Development of the Republic of Tatarstan. Every year the conference gathers thousands of participants from dozens of countries around the world.

In order to further develop international dialog, we are ready to interact with leading and young specialists, researchers, experts, and practicing lawyers to publish their scientific developments on improving current approaches and creating new methods in the field of ethics, legal regulation and protection of public relations associated with digital technologies.

We would like to express our gratitude to the authors, reviewers, members of the editorial board, and ambassadors of the Journal for their cooperation and to the readers for their growing interest in our publication.

Research article
UDC 34:004:342.3:004.8
EDN: https://elibrary.ru/ypfqzd
DOI: https://doi.org/10.21202/jdtl.2024.26

Legal Issues of Ensuring Technological Sovereignty

Maksim V. Zaloilo

Institute of Legislation and Comparative Law under the Government of the Russian Federation, Moscow, Russia

Keywords

digital solidarity,
digital technologies,
law,
sovereignization of legal regulation,
strategic autonomy,
strategic planning,
technological leadership,
technological mode,
technological security,
technological sovereignty

Abstract

Objective: to identify the legal issues of ensuring technological sovereignty and to determine scientifically grounded vectors of their solution.

Methods: the study is based on formal-legal, historical-legal, comparative-legal methods, as well as the methodology of soft systematicity, legal forecasting, and legal modeling.

Results: the article presents a theoretical and legal approach to understanding sovereignty and differentiating its types. Under modern conditions, a significant role is given to the independence and autonomy of the state in the technological sphere. The correlation of digital and technological sovereignty is considered; the latter notion is outlined taking into account the gaining popularity of the Western concept of digital (technological) solidarity. The regulatory foundation of the state strategic autonomy is legal regulation, in which the concept of technology-centrism has been firmly established in recent years. The technological paradigm of modern legal regulations was identified. It consists in strategizing the scientific and technological innovations in strategic planning documents, as well as in sovereignization and cyclization of the legal sphere, digital transformation of the culture of lawmaking and law enforcement, technologization of the legal language, expansion of the scope of legislative regulation and the volume of subordinate legislation. The analysis of the correlation between the legislative and subordinate law levels of technological positioning of the Russian Federation in strategic areas has allowed to emphasize the important systemic interrelation of the involved traditional and innovative law-making tools as they ensure technological development. The author also identifies the risks of expanding legal experimentation in the digital area of public relations, which should exclude the possibility of circumventing the established critical limitations.

Scientific novelty: the work forms a theoretical and legal model of ensuring technological sovereignty, which is of strategic importance for the preservation of the Russian Federation sovereignty in its classical understanding as the main and most important feature of the state.

Practical significance: the results can be used in law-making activities of public authorities to create legal mechanisms for research, development and implementation of critical and end-to-end technologies and the production of high-tech products based on them in order to ensure national security of the Russian Federation.

For citation

Zaloilo, M. V. (2024). Legal Issues of Ensuring Technological Sovereignty. *Journal of Digital Technologies and Law, 2*(3), 500–520. https://doi.org/10.21202/jdtl.2024.26

Contents

Introduction

Epochal comprehensive transformation of the global social and political processes, civilizational challenges of the modern world order, aggravated by the strengthening technological competition between states under the growing sanctions confrontation and acute geopolitical context – all this puts on the agenda of legal science the search for new approaches to the protection of the national security foundations, reliable guarantees of its preservation and stable existence of society and the state in general. One of the urgent tasks in this regard is to ensure technological security of the state as the most important component of national security, interdependent with its other components: economic, social, informational, etc.

Technological security implies, first of all, the sustainable functioning of technologies critical for ensuring people's lives, competitive economic development and effective public management of technologies (information infrastructure, energy, communications, transport, defense, health care, food supply, etc.) that can be created, modernized, implemented and successfully maintained in an autonomous mode, regardless of the

presence or absence of the political, commercial, or other economic interaction with foreign states, and notwithstanding periodical internal and external disturbances.

The dominant function in the conceptualization of technological security is performed by the technological mode. Its theory was developed within the Russian doctrine for the periodization of current and future changes in science (Glazyev & Kharitonov, 2009; Pashentsev et al., 2021). Currently, it is customary to talk about the transition to the sixth technological mode, the core of which consists of nano-, bio-, and information technologies, spliced with anthropo- and techno-environment (Glazyev & Kosakyan, 2024). This transition is relevant primarily for developed countries, since changes in technological modes occur in differently in different countries, and often several technological modes may coexist in the same country (Tikhomirov, 2023). The seventh and eighth technological modes are also predicted, the innovations of which should be reflected in the model of socio-normative anticipatory impact on them.

With the establishment of technogenic civilization, the need for society and the state to ensure their sustainable organization and further development becomes paramount. At that, technology plays the most important role in solving global problems of humanity. This, in particular, was demonstrated by the coronavirus pandemic of 2020–2021. Academician V. S. Stepin outlined the axiological potential of sustainable development for technogenic civilization several years ago. Now the need for sustainable development has been elevated to the constitutional level in the Russian Federation, as reflected in Article 751 of the Constitution transformed in 2020. Under the world order turbulence, sanctions and geopolitical confrontations, the model of sustainable development of the Russian Federation is directly related to the level of the country's actual independence in the field of science, engineering and technology. The concept of technological security is closely related to the concept of technological sovereignty[1]. The task of long-term provision of the latter is strategically important for the preservation of the sovereignty of the Russian Federation in its classical understanding as the main and most important feature of the state[2].

Placed in the strategic basis for ensuring the technological sovereignty of the Russian Federation, the Strategy for Scientific and Technological Development[3] highlights the great challenges of scientific and technological development of the country. Responding to these challenges requires both the acquisition of new knowledge in fundamental science, the creation of scientific and technological platforms, the implementation of a set

---

1 The presence in the country (under national control) of critical and cross-cutting technologies, its own development lines and conditions for the production of goods based on them, which provides a sustainable ability of the state and society to achieve national development goals.

2 Kucherov, I. I., Nudel, S. L., & Semykina, O. I. (Eds.) (2023). Criminal-legal guarantees of a state sovereignty (comparative legal study): scientific and practical manual. Moscow: Prospect. https://clck.ru/3EFbfw

3 Decree of the President of the Russian Federation No. 145 of February 28, 2024 (2024). Collection of Legislation of the Russian Federation, 10, Art. 1373.

of organizational and coordination measures, and the development and implementation of a wide range of legal solutions.

Vectors of humanity development are changing, while "traditional" threats are simultaneously preserved; the latter have been emerging for a number of years and pose risks to the strategic security of the country and its citizens. Under these complex conditions, one of the main guarantors of the viability and normal functioning of social and political institutions is the timely response of state-legal mechanisms, including lawmaking, to the tasks of society and state management that require daily solutions. The task of ensuring technological sovereignty was set at a high state level. It requires not only a breakthrough in technological terms (Bergek et al., 2015; Luan et al., 2024; Ulmanen & Bergek, 2021), qualitative changes in approaches to scientific development (Lapaeva, 2023; Acosta et al., 2020), but also large-scale innovations in the legal sphere to be transformed under the influence of the technological imperative. The present study is devoted to the search for ways to resolve the legal problems arising in this process.

1. Theoretical and legal approach to the understanding of sovereignty

Sovereignty is one of the main features of the state. According to the Constitution of the Russian Federation, the sovereignty of the Russian Federation extends to its entire territory (part 1 of Article 4), and the Russian Federation ensures the protection of its sovereignty and territorial integrity (part 21 of Article 67). Sovereignty, according to the legal position of the Constitutional Court of the Russian Federation[4], as well as its generally accepted understanding in the Russian doctrine, implies supremacy, independence and autonomy of the state power, the completeness of legislative, executive and judicial power of the state on its territory and independence in international communication. Sovereignty is a necessary qualitative feature of the Russian Federation as a state, characterizing its constitutional and legal status. In Russia, sovereignty belongs to the Russian Federation as a whole, and the sovereignty of its subjects is not allowed.

Since the time of its justification in the works of a thinker J. Bodin in the 16th century, the concept of sovereignty has undergone some changes. These changes are most noticeable under the modern large-scale technological innovations and civilizational challenges to humanity. They reflect the differentiation of sovereignty into several types – economic, industrial, energy, legal, political, network and so on.

The spatial limit of state sovereignty of the Russian Federation is its state border. At the same time, due to the development of information and telecommunication

[4] Resolution of the Constitutional Court of the Russian Federation of June 7, 2000, No. 10-P "On the case of verifying the constitutionality of certain provisions of the Constitution of the Republic of Altai and the Federal Law 'On general principles of organization of legislative (representative) and executive bodies of state power of the subjects of the Russian Federation'. (2000). Bulletin of the Constitutional Court of the Russian Federation, 5.

and digital technologies, spatial boundaries are not the only limit of spreading the independent power of one state in relation to other countries and their citizens (subjects). In the informational (virtual, cyber) space, which is increasingly an alternative environment for human existence, there are no territorial boundaries. Hence, it becomes more complicated both to establish full control over information flows and for the state to maintain its sovereign power. During information and cognitive wars, a struggle for people's consciousness takes place using the latest achievements of information, digital, neuro- and other high technologies through destructive information and psychological influence, disinformation and fakes. The issue of information (digital) sovereignty of the state becomes relevant and is widely discussed in legal scientific and scientific-practical literature (Stepanov, 2024; Adams & Albakajai, 2016; Adonis, 2019; Floridi, 2020; Johnson & Post, 1996; Pizzul & Veneziano, 2023; Timmers, 2019).

In light of the urgent need to overcome the country's critical lagging behind technological leaders, the concept of technological sovereignty has been formalized at a high state level (Maurer et al., 2015; Beltrán, 2016). Its provision is the theme of several strategic planning documents, adopted recently. Fragmentation of sovereignty into types is criticized as reducing the state authority, including in the external environment. However, the adopted strategic planning documents focus on the concept of technological sovereignty as state sovereignty in the relevant sphere, assuming that additional guarantees will be created to strengthen the latter.

In some foreign countries (the European Union, the UK, Canada, the USA), technological sovereignty is equaled to digital sovereignty (Potaptseva & Akberdina, 2023; Couture & Toupin, 2019; da Ponte et al., 2023). Another viewpoint is that digital sovereignty is absorbed by technological sovereignty (Hellmeie & Scherenberg, 2023). The present study proceeds from the compatibility of these concepts, which relate as part and whole.

The concept of sovereignty used in the context of technologization assumes independently generating technological and scientific knowledge in the state or, alternatively, the lowest possible level of structural dependence on other countries (Dosi et al., 2006; Edler et al., 2023). Achieving a sufficient level of technological sovereignty is a preliminary condition for strategic state autonomy (Broeders et al., 2023; Crespi et al., 2021).

The concept of digital (technological) solidarity, as opposed to technological sovereignty, was outlined by the U.S. Department of State in the Strategy for the United States International Policy on Cyberspace and Digital Technologies (May 2024)[5] and presented as a tool for weakening the technological potential of Russia, China, Iran, DPRK, etc. It deserves close attention both on the part of the state and from the standpoint of scientific knowledge, including jurisprudence.

[5] United States International Cyberspace & Digital Policy Strategy. https://clck.ru/3EFd8R

According to this document, digital solidarity is understood as "working together to provide mutual assistance to victims of malicious cyberactivity and other digital harms; helping partners, especially emerging economies, to adopt safe, resilient, and sustainable technologies to achieve their development goals; and building a strong and inclusive innovation economy that can shape our [the U.S. and its allies' – Note by M. Z.] economic and technological future"[6]. However, the obvious risk of implementing the concept of digital solidarity for states that are or may potentially become part of the U.S. sphere of influence could be the loss of their own digital sovereignty. This may have consequences like increased dependence on "digital" leaders, deepening digital inequality among peoples and states, violation of cyber security and cyber resilience, etc., which jeopardizes both technological sovereignty and the sovereignty of state power of such states.

2. Legal regulation as a regulatory foundation of the strategic autonomy of the state

Ensuring technological sovereignty requires both the intensification of scientific and industrial areas and the creation of an appropriate regulatory framework. The challenges of technogenic civilization determine the close interrelation and mutual influence of the legal and technological spheres. On the one hand, technologies (first of all, informational and digital ones) have firmly penetrated into the legal environment, where it is appropriate to discuss their application at different stages of legal regulation. This refers to the development of generative artificial intelligence able to perform lawmaking, monitoring and expert functions, as well as to the sphere of law enforcement (Bex et al., 2017; Ermakova & Frolova, 2022; Pashentsev & Babaeva, 2024; Reiling, 2020), with such relevant functions as automation of routine procedures, self-execution of contractual obligations (smart contracts), machine-readability and machine-execution of law, mediatization of judicial power, e-justice, etc.[7] A future prospect is the introduction of neurotechnologies into the legal sphere (Filipova, 2021; Istace, 2024; Ligthart et al., 2023).

On the other hand, due to its nature as a measure of anticipatory reflection of reality, law expectedly responds to the dynamics of social development, an essential layer of which are technological innovations. The stages of construction of legal reality are transformed, which is reflected in legislation, law enforcement practice, and legal culture of individuals. The individual and collective legal consciousness that changes under the influence of the technological imperative is subsequently reflected in law. Thus, the technological imperative becomes determinant in the evolution of the legal sphere, where it shifts the achievements of anthropocentrism towards technologocentrism.

---

6 Ibid.

7 Pietropaoli, I., Anastasiadou, I., Gauci, J.-P., & MacAlpine, H. Use of Artificial Intelligence in Legal Practice. British Institute of International and Comparative Law. https://clck.ru/3EFdGC

The development of legal regulation of relations in the sphere of ensuring technological sovereignty occurs in the following directions:

– strategizing future changes of science, engineering and technology in program documents;

– growing sovereignization of legal regulation, which is a natural response to the change of the globalization vector in the new geopolitical realities and to the task of legal provision of the state strategic autonomy. Within the 2020 constitutional reform, the constitutional and legal basis of Russian science was strengthened, while constitutional norms in strategic planning documents and normative legal acts regulating state support of the scientific sphere were subsequently concretized. With the aggravation of the geopolitical situation and growing sanctions restrictions, the regulatory potential of international and supranational regulators continues to weaken in the Russian legal system;

– cyclization of the normative legal array, in which atypical legal arrays such as digital law are gaining systemic importance, while the formation of technological law, begins, providing a normative foundation for the country's technological independence;

– technologization of the language of law and the language of legislation, which acquire interdisciplinary character, accompanied by unification of concepts and terms of the digital (more widely – technological) legal array;

– expansion of the sphere of legislative regulation and a natural increase in the volume of subordinate regulation;

– spreading of experimental legal regimes, which test the legal models of new social relations or those significantly changed under the influence of technological imperative;

– digital transformation of the culture of lawmaking and legislative procedure.

3. Technological paradigm of modern legal regulators

From the viewpoint of legal regulation, the technological space is characterized by a significant substantive complexity and, therefore, a variety of sources of regulation of relevant legal relations, i. e., normative legal acts of both legislative and subordinate levels of regulation of social relations.

The needs of society and the state, changed in the course of technological development, inevitably change the system, composition, scope and limits of action, as well as the quantitative expression of the sources of law (Marchant & Allenby, 2017). The transformation of law into a more flexible social regulator is predicted (Pashentsev, 2019), replacing legislative regulation with soft law.

At the same time, at present and in the near future, in the modern Russian legal system, legislation is the main and primary regulator of the most important and stable social relations, giving value-legal orientation to subordinate regulation. Subordinate normative legal acts are consistent with the provisions of laws, which establish the limits of subordinate lawmaking (Abramova, 2019). Concretization of laws is carried out both

horizontally – in other legislative acts (primary sources), and vertically – in subordinate normative legal acts adopted on their basis (documents of secondary property). At that, the problem of determining the limits of such concretization should be solved:

– hierarchical limits, implying the account of subordination of acts in terms of legal force, which is reflected in the peculiarities of their issuance and the conditions that must be observed[8];

– competency limits (observance of law-making powers);

– spatial limits (delimitation of federal and regional subjects of jurisdiction); and

– substantive limits, determined by the scope and object of legal regulation.

Subordinate legal acts, different in form and content, have different functional relationship with the law. For example, presidential decrees and resolutions of the Government can act as a primary source of regulation of certain social relations on issues that constitute their exclusive competence, when these relations are not the subject of legislative regulation, but objectively need legal regulation[9].

The technological paradigm of modern legal regulations is designed to solve the problem of the delayed response of the law to social and technological dynamics. The basic legislative act in this area[10] has long been outdated, and repeated attempts to modernize it (Gabov et al., 2017) have not been successful so far. The new draft law "On scientific and scientific-technical activity", put forward for public discussion in 2019, received critical responses from the scientific and expert community (Semenov et al., 2019). At the same time, the doctrine suggests the overdue need to codify the legislation on science and technology, consolidate all legal norms in this area in a single act, and form a relevant branch of scientific law (Vasiliev, 2020; Lapaeva, 2023). The issue of codification of legislation regulating relations in the sphere of digitalization remains unresolved. Although the adoption of the Digital Code carries a number of risks (first of all, the emergence of conflicts and contradictions, as well as the preservation of fragmentation of legal regulation of the relevant relations), there is no doubt about the need to streamline the digital (and then technological in general) legal array, for example, in the form of consolidation.

The volume of legislative norms regulating social relations associated with the application of technological solutions is constantly increasing. A set of legislative acts of various industry and subject matter (more than 100 federal laws) has been adopted in this area. Along with this, an expanding number of subordinate normative

---

8 Constitution of the Russian Federation (part 3 of Article 90, part 1 of article 115); Resolution of the Government of the Russian Federation No. 1009 of August 13, 1997 (1997). Collection of legislation of the Russian Federation, 33, Art. 3895.

9 For example, as a result of the constitutional reform of 2020, the Russian Government was granted the authority to provide state support for scientific and technological development of the Russian Federation, preservation and development of its scientific potential (para. "c1" of part 1 of Article 114 of the Constitution of the Russian Federation).

10 On science and state scientific-technical policy. No. 127-FZ of August 23, 1996 (1996). Collection of legislation of the Russian Federation, 35, Art. 4137.

legal acts establish mechanisms for implementing legal norms in the sphere of ensuring technological sovereignty.

Today, the basic direction of subordinate regulation of relations in the sphere of technological security is the conceptualization of the model of technological sovereignty and leadership in strategic planning documents. One of the main acts here is the Concept of technological development for the period until 2030[11]. This document highlights the goals of technological development[12] and reveals their implementation mechanisms. An integrated approach to the implementation of technological development goals implies the support of technological sovereignty projects, the taxonomy of which is established at the subordinate legislation level[13].

The President of the Russian Federation has named technological leadership and digital transformation among the national development goals of the country, the achievement of which is characterized by fulfilling a number of target indicators. Among them: ensuring technological independence and the formation of markets in the areas of bioeconomy, means of production and automation, digital transformation, artificial intelligence, advanced space and energy technologies, and increasing the share of domestic high-tech goods and services created on the basis of own development lines, growth of investments in domestic IT solutions, ensuring network sovereignty and information security in the Internet, etc.[14]. An important role is assigned to the scientific sphere, which should create a foundation for the development of relevant technologies, to increase the volume of research and development, including by increasing the state's internal expenditures and private investment for these purposes.

The main characteristics of subordinate normative legal acts are their prompt adoption and expansion of action range. These characteristics are actualized in crises (coronavirus pandemic, sanctions pressure, threats of technological degradation). Under such conditions, the powers to take economic and social measures are concentrated at the subordinate legislation level, the ratio of legislative and subordinate regulation changes, the unit weight of prompt subordinate lawmaking in the total array of adopted acts (both at the federal and regional levels) increases (Tikhomirov, 2022). However, even in such situations, the positive consequences of prompt legal response may collide with the negative results of legality violation. In order to avoid anticipatory subordinate

11 Order of the Government of the Russian Federation No. 1315-r of May 20, 2023 (2023). Collection of legislation of the Russian Federation, 22, Art. 3964.

12 Ensuring national control over the reproduction of critical and cross-cutting technologies; transition to innovation-oriented economic growth, strengthening the role of technology as a factor of economic and social development; technological support of sustainable operation and development of industrial systems.

13 Order of the Government of the Russian Federation No. 603 of April 15, 2023 (2023). Collection of legislation of the Russian Federation, 17, Art. 3141.

14 Decree of the President of the Russian Federation No. 309 of May 7, 2024 (2024). Collection of legislation of the Russian Federation, 20, Art. 2584.

regulation of those social relations that are the subject of legislative regulation, which diminishes the role of the law in the system of law and the mechanism of legal regulation, it is necessary that a subordinate act does not contradict the law but corresponds to it (Abramova, 2019).

The doctrine rightly emphasizes that the poor effectiveness of many laws is due to the lag in the development and application of subordinate legislation (Baranov, 2022). In this context, it is important to ensure the direct effect of laws and avoid the unjustified inclusion of an excessive number of reference norms, which imply further sub-law specification, into the projected legislative acts. The benchmark of optimal sub-legal specification of the norms of the law is "achievement of the necessary effect of legal regulation in the relevant sphere of social relations, its completeness in terms of the needs of social development" (Abramova, 2019).

The problem of ensuring compliance and prompt development of subordinate norms persists, which is conditioned by the adoption of relevant legislative acts. Its solution is both in simultaneously developing legislative and concretizing subordinate legal norms, and in postponing the law entry into force, correlating it to the development of subordinate normative legal acts concretizing its provisions.

At the same time, for the Russian Federation, the adoption of the concept of digital solidarity in unfriendly states makes it necessary to strengthen legal, institutional and organizational steps to ensure national security and technological sovereignty. These issues not only relate to the external manifestations of the state power sovereignty, but directly affect the internal sovereignty of the state. The latter implies the independence of the state from any other political force within the country and building a national legal system based on the established legal values, legal traditions and needs of the country. Developing the digital solidarity concept requires either amendments to existing program-strategic acts or the development of new ones to take into account new threats in cyberspace. This refers, in particular, to the Doctrine of Information Security, which was approved back in 2016[15], while the development of informational-telecommunicational, digital and other high technologies requires advanced regulation. Strategic documents, which in legal form determine the directions and prospects of the state development, play a crucial role under the continuous and accelerating technological transformations. They create the legal foundation of innovative development, defining the bases of state policy. The idea of developing an Information Security Strategy has certain prospects. As a system of formally-defined provisions, setting forth the strategic goal, tasks and directions of activities of public authorities to achieve it, means and resources that can be spent on it, the Strategy

[15] Decree of the President of the Russian Federation No. 646 of December 5, 2016 (2016). Collection of legislation of the Russian Federation, 50, Art. 7074.

differs significantly from such a strategic planning document as a doctrine. The Strategy should describe a comprehensive systematic approach to the implementation of the specified goal and objectives, coordinated and interrelated actions and measures, which would be based on target indicators at each stage of implementation.

There is a significant number of still unremoved legal barriers to technology development and to ensuring technological leadership of the country. This is evidenced by the albeit positive but spreading practice of applying experimental legal regimes, based on the Law on experimental legal regimes in the sphere of digital innovations in the Russian Federation[16]. On the other hand, there are still risks of using experimental legal regimes for illegal purposes to circumvent critical restrictions. In this regard, it is advisable to ensure the systemic interconnection of the law-making tools for the technology development (regulatory impact assessment, "regulatory guillotine", regulatory roadmaps for eliminating the barriers of the National Technological Initiative[17]).

4. Sub-legal level of technological positioning in strategic areas

Subordinate regulation of relations in the sphere of ensuring technological sovereignty is the most significant legal array among the variety of adopted acts, the main features of which are as follows:

– strategic importance of qualitative and optimal subordinate regulation, taking into account the emerging external and internal conditions; it arises from the strategic importance of the technological security sphere, the stable and uninterrupted functioning of which is a necessary prerequisite for ensuring normal life and a guarantor of protection of the society and state basic interests;

– content diversity and a complex system of subordinate normative legal acts;

– uniqueness of subordinate regulation in the sphere of ensuring technological sovereignty (the content of subordinate normative legal acts is largely specific and complicated due to the use of special terminology, special legal constructions of mechanisms applicable to activities to ensure technological sovereignty);

– special practical (economic) value of subordinate regulatory legal acts for the effective development of the economy spheres affected by them (by creating conditions of maximum favorability for the development of modern technologies in the relevant spheres);

– rapidity of development and adoption of subordinate normative legal acts if a need for the relevant regulation is identified, in view of the fact that such a need is of strategic importance for the security of the state as a whole.

---

16 On experimental legal regimes in the field of digital innovation in the Russian Federation. No. 258-FZ of July 31, 2020 (2020). Collection of legislation of the Russian Federation, 31 (part I), Art. 5017.

17 Order of the Government of the Russian Federation No 317 of April 18, 2016 (2016). Collection of legislation of the Russian Federation, 17, Art. 2413.

In addition, the peculiarities of subordinate regulation of relations arising and developing under the influence of the technological imperative are expressed in the need for simultaneous implementation of both the legally established bases for the regulation of relevant legal relations[18], and systemic strategic directions of development and priority protection of this sphere determined at the highest level of public administration. Often the tasks of developing the sphere of technological security (which should be solved, including at the level of subordinate normative legal regulation) are defined in strategic documents[19].

Taking into account the above-mentioned and other legally established and determined by strategic planning documents priority directions of technological security development, we can distinguish several blocks of tasks to be solved at the level of subordinate normative regulation. These blocks include ensuring information, industrial, energy, transport security and technological independence of the defense-industrial complex.

The above are just a few aspects of technological security and subordinate normative legal acts aimed at their regulation. The sphere of technological security is extensive and covers all possible cases of application of various kinds of technologies for a variety of human needs.

Subordinate normative legal regulation in this area is a vast array of existing normative prescriptions, providing the solution of a wide range of practical tasks to ensure technological sovereignty in the relevant legislative and politically determined priorities. It is a necessary element in the system of legal regulation of the relations under consideration, without which it is impossible to ensure the effective mechanisms of protection and improvement of the state technological security.

Conclusions

In relation to the sphere of ensuring technological sovereignty, law fulfills a number of functions:

– regulatory (creating a normative framework for the functioning and development of science and technology),

– stimulating (introduction of technologies into various spheres of life),

– restrictive (aimed at preventing technological and legislative singularity).

[18] On the security of critical information infrastructure of the Russian Federation. No. 187-FZ of July 26, 2017 (2017). Collection of legislation of the Russian Federation, 31 (Part I), Art. 4736; On the safety of fuel and energy complex facilities. No. 256-FZ of July 21, 2011 (2011). Collection of legislation of the Russian Federation, 30 (part 1), Art. 4604; On transport security. No. 16-FZ of February 9, 2007 (2007). Collection of legislation of the Russian Federation, 7, Art. 837; et al.

[19] Decree of the President of the Russian Federation No. 400 of July 2, 2021 (2021). Collection of legislation of the Russian Federation, 27 (part II), Art. 5351.

Ensuring technological sovereignty implies doctrinal substantiation and solution of overdue and potential legal tasks, among which are:

– legal identification of strategic technologies;

– creating an updated legal standard of scientific and scientific-technological activity;

– streamlining the normative array in the sphere of technological security;

– unification of concepts and terms of the technological legal array;

– correlating the adopted normative legal acts with the model of technological sovereignty conceptualized in the existing strategic planning documents;

– ensuring the direct effect of the law;

– observing the limits of horizontal and vertical concretization of the legal norms;

– ensuring compliance and prompt development of subordinate norms conditioned by the adoption of relevant legislative acts.

References

Abramova, A. I. (2019). By-law-making in the Modern Understanding: Realities and Prospects. *Journal of Russian Law*, *8*, 25–35. (In Russ.). https://doi.org/10.12737/jrl.2019.8.3

Acosta, M., Coronado, D., León, M., & Moreno, P. (2020). The Production of Academic Technological Knowledge: an Exploration at the Research Group Level. *Journal of the Knowledge Economy*, *11*, 1003–1025. https://doi.org/10.1007/s13132-019-0586-9

Adams, J., & Albakajai, M. (2016). Cyberspace: A New Threat to the Sovereignty of the State. *Management Studies*, *4*(6), 256–265. https://doi.org/10.17265/2328-2185/2016.06.003

Adonis, A. A. (2019). Critical Engagement on Digital Sovereignty in International Relations: Actor Transformation and Global Hierarchy. *Global: Jurnal Politik Internasional*, *21*(2), 262–282. https://doi.org/10.7454/global.v21i2.412

Baranov, V. M. (2022). References in Law-Making Acts: Technical and Legal Defects and Ways to Overcome Their Harmful Consequences. *Journal of Russian Law*, *26*(3), 5–21. (In Russ.). https://doi.org/10.12737/jrl.2022.025

Beltrán, N. C. (2016). Technological Sovereignty: What Chances for Alternative Practices to Emerge in Daily IT Use? *Hybrid [Online]*, *3*. https://doi.org/10.4000/hybrid.987

Bergek, A., Hekkert, M., Jacobsson, S., Markard, J., Sandén, B., & Truffer, B. (2015). Technological innovation systems in contexts: Conceptualizing contextual structures and interaction dynamics. *Environmental Innovation and Societal Transitions*, *16*, 51–64. https://doi.org/10.1016/j.eist.2015.07.003

Bex, F., Prakken, H., van Engers, T., & Verheij, B. (2017). Introduction to the special issue on Artificial Intelligence for Justice (AI4J). *Artificial Intelligence and Law*, *25*, 1–3. https://doi.org/10.1007/s10506-017-9198-5

Broeders, D., Cristiano, F., & Kaminska, M. (2023). In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions. *JCMS: Journal of Common Market Studies*, *61*, 1261–1280. https://doi.org/10.1111/jcms.13462

Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? *New Media & Society*, *21*(10), 2305–2322. https://doi.org/10.1177/1461444819865984

Crespi, F., Caravella, S., Menghini, M., & Salvatori, C. (2021). European Technological Sovereignty: An Emerging Framework for Policy Strategy. *Intereconomics*, *56*(6), 348–354. https://doi.org/10.1007/s10272-021-1013-6

da Ponte, A., Leon, G., & Alvarez, I. (2023). Technological Sovereignty of the EU in Advanced 5G Mobile Communications: An Empirical Approach. *Telecommunications Policy*, *47*(1). https://doi.org/10.1016/j.telpol.2022.102459

Dosi, G., Llerena, P., & Labini, M. S. (2006). The relationships between science, technologies and their industrial exploitation: An illustration through the myths and realities of the so-called 'European Paradox'. *Research Policy*, *35*, 1450–1464. https://doi.org/10.1016/J.RESPOL.2006.09.012

Edler, J., Blind, K., Kroll, H., & Schubert, T. (2023). Technology sovereignty as an emerging frame for innovation policy. Defining rationales, ends and means. *Research Policy*, *52*(6). https://doi.org/10.1016/j.respol.2023.104765

Ermakova, E. P., & Frolova, E. E. (2022). Using Artificial Intelligence in Dispute Resolution. In A. O. Inshakova, E. E. Frolova. (Eds.), *Smart Technologies for the Digitisation of Industry: Entrepreneurial Environment. Smart Innovation, Systems and Technologies* (Vol. 254). Springer. https://doi.org/10.1007/978-981-16-4621-8_11

Filipova, I. A. (2021). Neurotechnologies: Development, practical application and regulation. *Vestnik of Saint Petersburg University. Law*, *3*, 502–521. (In Russ.). https://doi.org/10.21638/spbu14.2021.302

Floridi, L. (2020). The Fight for Digital Sovereignty: What It IS, and Why It Matters, Especially for the EU. *Philosophy & Technology*, *33*(3), 369–378. https://doi.org/10.1007/s13347-020-00423-6

Gabov, A. V., Putilo, N. V., & Gutnikov, O. V. (2017). The Draft Federal Law on Science – a New Format of Legal Regulation of Scientific and Innovation Activities. *Perm University Herald. Juridical Sciences*, *38*, 385–399. (In Russ.). https://doi.org/10.17072/1995-4190-2017-38-385-399

Glazyev, S. Yu., & Kharitonov, V. V. (Eds.) (2009). *Nanotechnology as a key factor of the new technological mode in the economy*: monograph. Moscow: Trovant. (In Russ.).

Glazyev, S. Yu., & Kosakyan, D. L. (2024). State and Prospects of 6th Technological Mode in Russian Economy. *Economics of Science*, *10*(2), 11–29. (In Russ.). https://doi.org/10.22394/2410-132X-2024-10-2-11-29

Hellmeier, M., & Scherenberg, F. V. (2023). A Delimitation of Data Sovereignty from Digital and Technological Sovereignty. In *European Conference on Information Systems 2023 Research Papers*, Kristiansand. https://aisel.aisnet.org/ecis2023_rp/306

Istace, T. (2024). Human rights law: an incomplete but flexible framework to protect the human mind against neurotechnological intrusions. *Law, Innovation and Technology*, *16*, 309–340. https://doi.org/10.1080/17579961.2024.2313796

Johnson, D. R. & Post, D. G. (1996). Law and Borders – the Rise of Law in Cyberspace. *Stanford Law Review*, *48*, 1367–1402. https://dx.doi.org/10.2139/ssrn.535

Lapaeva, V. V. (2023). Technological sovereignty of Russia: legal issues. *Science Studies*, *2*, 60–72. (In Russ.).

Ligthart, S., Ienca, M., Meynen, G., Molnár-Gábor, F., Andorno, R., Bublitz, C., Catley, P., Claydon, L., Douglas, T., Fins, J. J., Goering, S., Haselager, W. F., Jotterand, F., Lavazza, A., McCay, A., Paz, A. W., Rainey, S., Ryberg, J., & Kellmeyer, P. (2023). Minding rights: Mapping ethical and legal foundations of 'neurorights'. *Cambridge quarterly of healthcare ethics*, *32*(4), 461–481. https://doi.org/10.1017/S0963180123000245

Luan, C., Deng, S., Porter, A. L., & Song, B. (2024). An Approach to Construct Technological Convergence Networks Across Different IPC Hierarchies and Identify Key Technology Fields. In I*EEE Transactions on Engineering Management*, *71*, 346–358. https://doi.org/10.1109/TEM.2021.3120709

Marchant, G. E., & Allenby, B. R. (2017). Soft law: New tools for governing emerging technologies. *Bulletin of the Atomic Scientists*, *73*, 108–114. https://doi.org/10.1080/00963402.2017.1288447

Maurer, T., Skierka, I., Morgus, R., & Hohmann, M. (2015). Technological sovereignty: Missing the point? In *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*, 53–68. https://doi.org/10.1109/CYCON.2015.7158468

Pashentsev, D. A. (Ed.) (2019). *Digitalization of Law-Making: the Research for New Solutions*: monograph. Moscow: ILCL: INFRA-M. (In Russ.).

Pashentsev, D. A., & Babaeva, Y. G. (2024). Artificial intelligence in law-making and law enforcement: Risks and new opportunities. *Vestnik of Saint Petersburg University. Law*, *15*(2), 516–526. https://doi.org/10.21638/spbu14.2024.214

Pashentsev, D. A., Zaloilo, M. V., & Dorskaya, A. A. (2021). *Changing of Technological Orders and Legal Development of Russia*: monograph. Moscow: ILCL: Norma: INFRA-M. (In Russ.).

Pizzul, D., & Veneziano, M. (2023). Digital sovereignty or sovereignism? Investigating the political discourse on digital contact tracing apps in France. *Information, Communication & Society*, *27*(5), 1008–1024. https://doi.org/10.1080/1369118X.2023.2232840

Potaptseva, E. V., Akberdina, V. V. (2023). Technological Sovereignty: Concept, Content, and Forms of Implementation. *Journal of Volgograd State University. Economics*, *25*(3), 5–16. (In Russ.). https://doi.org/10.15688/ek.jvolsu.2023.3.1

Reiling, A. D. (2020). Courts and Artificial Intelligence. *International Journal for Court Administration*, *11*(2), 8. https://doi.org/10.36745/ijca.343

Semenov, E. V., Gutnikov, O. V., Putilo, N. V., Postnikov, A. E., Andrichenko, L. V., Egerev, S. V., Tambovtsev, V. L., Dementiev, A. N., Lapaeva, V. V., Borinskaya, S. A., Salitskaya, E. A., & Vaganov, A. G. (2019). Draft Federal Law "On scientific and scientific-technical activity". *Upravlenie naukoj: teoriya i praktika*, *1*, 13–50. (In Russ.).

Stepanov, P. V. (2024). Approaches to Understanding Russia's Digital Sovereignty. *Journal of Russian Law*, *28*(4), 37–51. (In Russ.). https://doi.org/10.61205/jrp.2024.4.1

Tikhomirov, Yu. A. (Ed.) (2022). *Legal Management in Crisis Situations*: monograph. Moscow: Prospect. (In Russ).
Tikhomirov, Yu. A. (Ed.) (2023). *Interests in the mechanism of public power: issues of theory and practice*: monograph. Moscow: Prospect. (In Russ.).
Timmers, P. (2019). Ethics of AI and Cybersecurity When Sovereignty is at Stake. *Minds and Machines*, *29*(4), 635–645. https://doi.org/10.1007/s11023-019-09508-4
Ulmanen, J., & Bergek, A. (2021). Influences of technological and sectoral contexts on technological innovation systems. *Environmental innovation and societal transitions*, *40*, 20–39. https://doi.org/10.1016/j.eist.2021.04.007
Vasiliev, A. A. (2020). Scientific law as a branch of Russian law. *Science Management: Theory and Practice*, *2*(4), 52–70. (In Russ.). https://doi.org/10.19181/smtp.2020.2.4.3

Author information

Maksim V. Zaloilo – Cand. Sci. (Law), Leading Researcher of the Department of Theory of Law and Interdisciplinary Research of Legislation, Institute of Legislation and Comparative Law under the Government of the Russian Federation
Address: 34 Bolshaya Cheremushkinskaya Str., 117218 Moscow, Russia
E-mail: z-lo@mail.ru
ORCID ID: https://orcid.org/0000-0003-4247-5242
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57215428686
WoS Researcher ID: https://www.webofscience.com/wos/author/record/S-4168-2018
Google Scholar ID: https://scholar.google.ru/citations?hl=ru&user=_5-4AjwAAAAJ
РИНЦ Author ID: https://www.elibrary.ru/author_profile.asp?id=595876

Conflict of interests

The author is the Deputy Editor-in-Chief of the Journal; the article was reviewed on general terms.

Financial disclosure

The research was performed within the framework of the 2024 state assignment of the Institute of Legislation and Comparative Law under the Government of the Russian Federation.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – June 8, 2024
Date of approval – June 16, 2024
Date of acceptance – September 25, 2024
Date of online placement – September 30, 2024

Научная статья
УДК 34:004:342.3:004.8
EDN: https://elibrary.ru/ypfqzd
DOI: https://doi.org/10.21202/jdtl.2024.26

Правовые проблемы обеспечения технологического суверенитета

Максим Викторович Залоило

Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации, Москва, Россия

Ключевые слова

право,
стратегическая автономия,
стратегическое планирование,
суверенизация правового регулирования,
технологическая безопасность,
технологический суверенитет,
технологический уклад,
технологическое лидерство,
цифровая солидарность,
цифровые технологии

Аннотация

Цель: выявить правовые проблемы обеспечения технологического суверенитета и определить научно обоснованные векторы их решения.

Методы: в основе исследования лежат формально-юридический, историко-правовой, сравнительно-правовой методы, а также методология мягкой системности, юридического прогнозирования, правового моделирования.

Результаты: в статье представлен теоретико-правовой подход к пониманию и разграничению суверенитета на виды, где в современных условиях значительная роль отводится независимости и самостоятельности государства в технологической сфере. Рассмотрено соотношение цифрового и технологического суверенитета, а понятие последнего изложено с учетом набирающей популярность западной концепции цифровой (технологической) солидарности. Регулятивным фундаментом стратегической автономии государства служит правовое регулирование, в сфере которого в последние годы прочно закрепляется концепция технологоцентризма. Выявленная технологическая парадигма современных правовых регуляторов заключается в стратегировании научно-технологических новаций в документах стратегического планирования, суверенизации и циклизации правовой сферы, цифровой трансформации культуры правотворчества и правоприменения, технологизации юридического языка, расширении сферы законодательного регулирования и объема подзаконного правового массива. Проведенный анализ соотношения законодательного и подзаконного уровней технологического позиционирования Российской Федерации в стратегических областях позволил подчеркнуть важность системной взаимосвязи задействованных традиционных и инновационных инструментов правотворческого процесса в обеспечении технологического развития и выявить риски расширения правового экспериментирования в цифровой области общественных отношений, которое должно исключать возможность обхода таким образом установленных критически важных ограничений.

Научная новизна: в работе сформирована теоретико-правовая модель обеспечения технологического суверенитета, имеющего стратегическое значение для сохранения суверенитета Российской Федерации в его классическом понимании как основного и важнейшего признака государства.

Практическая значимость: полученные результаты могут найти применение в правотворческой деятельности органов государственной власти по созданию правовых механизмов исследования, разработки и внедрения критических и сквозных технологий и основанному на них производству высокотехнологичной продукции в целях обеспечения национальной безопасности Российской Федерации.

Для цитирования

Залоило, М. В. (2024). Правовые проблемы обеспечения технологического суверенитета. *Journal of Digital Technologies and Law*, *2*(3), 500–520. https://doi.org/10.21202/jdtl.2024.26

Список литературы

Абрамова, А. И. (2019). Подзаконное правотворчество в современном понимании: реалии и перспективы. *Журнал российского права*, *8*, 25–35. https://doi.org/10.12737/jrl.2019.8.3

Баранов, В. М. (2022). Ссылки (отсылки) в актах правотворчества: технико-юридические дефекты и пути преодоления их вредных последствий. *Журнал российского права*, *3*, 5–21. https://doi.org/10.12737/jrl.2022.025

Васильев, А. А. (2020). Научное право как отрасль российского права. *Управление наукой: теория и практика*, *2*(4), 52–70. EDN: https://elibrary.ru/xjobbj. DOI: https://doi.org/10.19181/smtp.2020.2.4.3

Габов, А. В., Путило, Н. В., Гутников, О. В. (2017). Проект федерального закона о науке – новый формат правового регулирования научной и инновационной деятельности. *Вестник Пермского университета. Юридические науки*, *38*, 385–399. https://doi.org/10.17072/1995-4190-2017-38-385-399

Глазьев, С. Ю., Косакян, Д. Л. (2024). Состояние и перспективы формирования 6-го технологического уклада в Российской экономике. *Экономика науки*, *10*(2), 11–29. https://doi.org/10.22394/2410-132X-2024-10-2-11-29

Глазьев, С. Ю., Харитонов, В. В. (ред.) (2009). *Нанотехнологии как ключевой фактор нового технологического уклада в экономике*: монография. Москва: Тровант. https://elibrary.ru/quaadz

Лапаева, В. В. (2023). Технологический суверенитет России: правовые проблемы. *Науковедческие исследования*, *2*, 60–72. EDN: https://elibrary.ru/mntsbs. DOI: https://doi.org/10.31249/scis/2023.02.04

Пашенцев, Д. А. (ред.) (2019). *Цифровизация правотворчества: поиск новый решений*: монография. Москва: ИЗиСП: ИНФРА-М. https://elibrary.ru/qrnijy

Пашенцев, Д. А., Залоило, М. В., Дорская, А. А. (2021). *Смена технологических укладов и правовое развитие России*: монография. Москва: ИЗиСП: Норма: ИНФРА-М. https://elibrary.ru/tqiyan

Потапцева, Е. В., Акбердина, В. В. (2023). Технологический суверенитет: понятие, содержание и формы реализации. Вестник Волгоградского государственного университета. *Экономика*, *25*(3), 5–16. EDN: https://elibrary.ru/vdglxr. DOI: https://doi.org/10.15688/ek.jvolsu.2023.3.1

Семенов Е. В., Гутников О. В., Путило Н. В., Постников А. Е., Андриченко Л. В., Егерев С. В., Тамбовцев В. Л., Дементьев А. Н., Лапаева В. В., Боринская С. А., Салицкая Е. А., Ваганов А. Г. (2019). Проект федерального закона «О научной и научно-технической деятельности». *Управление наукой: теория и практика*, *1*, 13–50. https://elibrary.ru/tzhvio

Степанов, П. В. (2024). Подходы к пониманию цифрового суверенитета России. *Журнал российского права*, *28*(4), 37–51. https://doi.org/10.61205/jrp.2024.4.1

Тихомиров, Ю. А. (ред.) (2022). *Правовое управление в кризисных ситуациях*: монография. Москва: Проспект. https://elibrary.ru/medwfm

Тихомиров, Ю. А. (ред.) (2023). *Интересы в механизме публичной власти: проблемы теории и практики*: монография. Москва: Проспект. https://elibrary.ru/gryaci

Филипова, И. А. (2021). Нейротехнологии: развитие, применение на практике и правовое регулирование. *Вестник Санкт-Петербургского университета. Право*, *3*, 502–521. https://doi.org/10.21638/spbu14.2021.302

Acosta, M., Coronado, D., León, M., & Moreno, P. (2020). The Production of Academic Technological Knowledge: an Exploration at the Research Group Level. *Journal of the Knowledge Economy*, *11*, 1003–1025. https://doi.org/10.1007/s13132-019-0586-9

Adams, J., & Albakajai, M. (2016). Cyberspace: A New Threat to the Sovereignty of the State. *Management Studies*, *4*(6), 256–265. https://doi.org/10.17265/2328-2185/2016.06.003

Adonis, A. A. (2019). Critical Engagement on Digital Sovereignty in International Relations: Actor Transformation and Global Hierarchy. *Global: Jurnal Politik Internasional*, *21*(2), 262–282. https://doi.org/10.7454/global.v21i2.412

Beltrán, N. C. (2016). Technological Sovereignty: What Chances for Alternative Practices to Emerge in Daily IT Use? *Hybrid [Online]*, *3*. https://doi.org/10.4000/hybrid.987

Bergek, A., Hekkert, M., Jacobsson, S., Markard, J., Sandén, B., & Truffer, B. (2015). Technological innovation systems in contexts: Conceptualizing contextual structures and interaction dynamics. *Environmental Innovation and Societal Transitions*, *16*, 51–64. https://doi.org/10.1016/j.eist.2015.07.003

Bex, F., Prakken, H., van Engers, T., & Verheij, B. (2017). Introduction to the special issue on Artificial Intelligence for Justice (AI4J). *Artificial Intelligence and Law*, *25*, 1–3. https://doi.org/10.1007/s10506-017-9198-5

Broeders, D., Cristiano, F., & Kaminska, M. (2023). In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions. *JCMS: Journal of Common Market Studies*, *61*, 1261–1280. https://doi.org/10.1111/jcms.13462

Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? *New Media & Society*, *21*(10), 2305–2322. https://doi.org/10.1177/1461444819865984

Crespi, F., Caravella, S., Menghini, M., & Salvatori, C. (2021). European Technological Sovereignty: An Emerging Framework for Policy Strategy. *Intereconomics*, *56*(6), 348–354. https://doi.org/10.1007/s10272-021-1013-6

da Ponte, A., Leon, G., & Alvarez, I. (2023). Technological Sovereignty of the EU in Advanced 5G Mobile Communications: An Empirical Approach. *Telecommunications Policy*, *47*(1), 102459. https://doi.org/10.1016/j.telpol.2022.102459

Dosi, G., Llerena, P., & Labini, M. S. (2006). The relationships between science, technologies and their industrial exploitation: An illustration through the myths and realities of the so-called 'European Paradox'. *Research Policy*, *35*, 1450–1464. https://doi.org/10.1016/J.RESPOL.2006.09.012

Edler, J., Blind, K., Kroll, H., & Schubert, T. (2023). Technology sovereignty as an emerging frame for innovation policy. Defining rationales, ends and means. *Research Policy*, *52*(6). https://doi.org/10.1016/j.respol.2023.104765

Ermakova, E. P., & Frolova, E. E. (2022). Using Artificial Intelligence in Dispute Resolution. In A. O. Inshakova, E. E. Frolova. (Eds.), *Smart Technologies for the Digitisation of Industry: Entrepreneurial Environment. Smart Innovation, Systems and Technologies* (Vol. 254). Springer. https://doi.org/10.1007/978-981-16-4621-8_11

Floridi, L. (2020). The Fight for Digital Sovereignty: What It IS, and Why It Matters, Especially for the EU. *Philosophy & Technology, 33*(3), 369–378. https://doi.org/10.1007/s13347-020-00423-6

Hellmeier, M., & Scherenberg, F. V. (2023). A Delimitation of Data Sovereignty from Digital and Technological Sovereignty. In *European Conference on Information Systems 2023 Research Papers*, Kristiansand. https://aisel.aisnet.org/ecis2023_rp/306

Istace, T. (2024). Human rights law: an incomplete but flexible framework to protect the human mind against neurotechnological intrusions. *Law, Innovation and Technology*, *16*, 309–340. https://doi.org/10.1080/17579961.2024.2313796

Johnson, D. R. & Post, D. G. (1996). Law and Borders – the Rise of Law in Cyberspace. *Stanford Law Review*, *48*, 1367–1402. https://dx.doi.org/10.2139/ssrn.535

Ligthart, S., Ienca, M., Meynen, G., Molnár-Gábor, F., Andorno, R., Bublitz, C., Catley, P., Claydon, L., Douglas, T., Fins, J. J., Goering, S., Haselager, W. F., Jotterand, F., Lavazza, A., McCay, A., Paz, A. W., Rainey, S., Ryberg, J., & Kellmeyer, P. (2023). Minding rights: Mapping ethical and legal foundations of 'neurorights'. *Cambridge quarterly of healthcare ethics*, *32*(4), 461–481. https://doi.org/10.1017/S0963180123000245

Luan, C., Deng, S., Porter, A. L., & Song, B. (2024). An Approach to Construct Technological Convergence Networks Across Different IPC Hierarchies and Identify Key Technology Fields. In *IEEE Transactions on Engineering Management*, *71*, 346–358. https://doi.org/10.1109/TEM.2021.3120709

Marchant, G. E., & Allenby, B. R. (2017). Soft law: New tools for governing emerging technologies. *Bulletin of the Atomic Scientists*, *73*, 108–114. https://doi.org/10.1080/00963402.2017.1288447

Maurer, T., Skierka, I., Morgus, R., & Hohmann, M. (2015). Technological sovereignty: Missing the point? In *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*, 53–68. https://doi.org/10.1109/CYCON.2015.7158468

Pashentsev, D. A., & Babaeva, Y. G. (2024). Artificial intelligence in law-making and law enforcement: Risks and new opportunities. *Вестник Санкт-Петербургского университета. Право*, *15*(2), 516–526. https://doi.org/10.21638/spbu14.2024.214

Pizzul, D., & Veneziano, M. (2023). Digital sovereignty or sovereignism? Investigating the political discourse on digital contact tracing apps in France. *Information, Communication & Society*, *27*(5), 1008–1024. https://doi.org/10.1080/1369118X.2023.2232840

Reiling, A. D. (2020). Courts and Artificial Intelligence. *International Journal for Court Administration*, *11*(2), 8. https://doi.org/10.36745/ijca.343

Timmers, P. (2019). Ethics of AI and Cybersecurity When Sovereignty is at Stake. *Minds and Machines*, *29*(4), 635–645. https://doi.org/10.1007/s11023-019-09508-4

Ulmanen, J., & Bergek, A. (2021). Influences of technological and sectoral contexts on technological innovation systems. *Environmental innovation and societal transitions*, *40*, 20–39. https://doi.org/10.1016/j.eist.2021.04.007

Сведения об авторе

Залоило Максим Викторович – кандидат юридических наук, ведущий научный сотрудник отдела теории права и междисциплинарных исследований законодательства, Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации
Адрес: 117218, Россия, г. Москва, ул. Большая Черемушкинская, 34
E-mail: z-lo@mail.ru
ORCID ID: https://orcid.org/0000-0003-4247-5242
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57215428686
WoS Researcher ID: https://www.webofscience.com/wos/author/record/S-4168-2018
Google Scholar ID: https://scholar.google.ru/citations?hl=ru&user=_5-4AjwAAAAJ
РИНЦ Author ID: https://www.elibrary.ru/author_profile.asp?id=595876

Конфликт интересов

Автор является заместителем главного редактора журнала, статья прошла рецензирование на общих основаниях.

Финансирование

Исследование проведено в рамках государственного задания Института законодательства и сравнительного правоведения при Правительстве Российской Федерации на 2024 год

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.07.45 / Право и научно-технический прогресс
Специальность ВАК: 5.1.1 / Теоретико-исторические правовые науки

История статьи

Дата поступления – 8 июня 2024 г.
Дата одобрения после рецензирования – 16 июня 2024 г.
Дата принятия к опубликованию – 25 сентября 2024 г.
Дата онлайн-размещения – 30 сентября 2024 г.

Research article
UDC 34:004:342.721:612.6
EDN: https://elibrary.ru/tklbsa
DOI: https://doi.org/10.21202/jdtl.2024.27

Human Genome Editing: Managing Technological Risks through Legal Means

Aleksandra A. Troitskaya
Lomonosov Moscow State University, Moscow, Russia

Konstantin A. Sharlovskiy
Pepelyaev Group LLC, Moscow, Russia

Keywords

digital technologies,
genetic editing,
genetic technologies,
human genome,
law,
legal liability,
legislation,
reproductive technologies,
risk-based approach,
technological risk

Abstract

Objective: to determine theoretical approaches to the legal regulation of reprogenetic editing, taking into account the risk-oriented approach and the practice of regulation of such breakthrough technologies in different jurisdictions; to outline further regulatory and managerial steps to be taken for the technology development.

Methods: general scientific methods of analysis and synthesis, classification, system and functional approaches; specific scientific methods: formal-legal, comparative-legal, and historical-legal.

Results: the research shows the possible approaches to the regulation of genetic editing for reproductive purposes. The considered variants are evaluated from the viewpoint of risk-oriented approach; conditions and peculiarities of various regulatory mechanisms' application are determined; the current Russian regulation in this sphere is assessed. The analysis allows concluding that the prohibition or significant restriction of the developing technology of reprogenetic editing has no irrefutable grounds. Moreover, it may lead to the results opposite to those declared by its proponents. In this regard, it is necessary to develop the discussion in a constructive and iterative way and involve all stakeholders in it, including the scientific community.

✉ Corresponding author

Scientific novelty: the international practice of legal regulation of reprogenetic technologies within different jurisdictions was generalized and conceptually interpreted; the natural scientific arguments in assessing the implemented regulation effectiveness were analyzed. This not only allows systematically considering the current and hypothetical risks of genetic technologies' development and use, but also provides an opportunity to use a risk-oriented approach to the analysis of legal regulation of genome editing technologies. The next step in comprehending the phenomenon of genetic editing becomes possible.

Practical significance: the study results can be used for building further constructive dialog on applying legal mechanisms to human genome editing. The study can also be a basis for iterative approach in the future discussion.

For citation

Troitskaya, A. A., & Sharlovskiy, K. A. (2024). Human Genome Editing: Managing Technological Risks through Legal Means. *Journal of Digital Technologies and Law, 2*(3), 521–543. https://doi.org/10.21202/jdtl.2024.27

Contents

Introduction

Genome editing is one of the technologies that has progressed markedly due to advances not only in molecular biology but also in digital tools (Atimango et al., 2024; Pombo, 2011; Wilson, 2023; Tan et al., 2023; Sharif et al., 2023). It is because of these tools that big data on nucleotide sequences, genetic expression, gene interactions with aligned amino acids, etc. could be processed in genetics (Balashenko, 2016). The same applies to the results of CRISPR technologies application for genome editing.

There are different types of human genome editing. Not only from the biomedical, but also from the legal viewpoint, there is a significant difference between editing for medical

and non-medical purposes, as well as somatic cell editing, affecting only a particular patient, and editing of a germline, the alteration of which can manifest itself in future generations (Yu et al., 2012).

In Russia, the legal regulation of inheritable editing of the human genome for any purpose remains uncertain, while a number of ethical issues in this area remain unresolved. In fact, inheritable editing is carried out at the level of fundamental research (albeit with a lack of control over it), and is not carried out for reproductive purposes. Meanwhile, the development of this biomedical sphere should be as safe as possible both for the individual participants (donors of genetic material, potential parents and children, and researchers themselves) and for the population as a whole. Such development requires a clear legal framework to ensure not only predictability but also programmable improvement of the technology, procedures, and results of its application.

The article is organized as follows. First, it will present the current state of human genome editing in Russia, focusing on the risks usually associated with the technology and the existing (actually, rather non-existing) legal norms related to it. Then, we will consider possible specific regulatory mechanisms that could ensure an adequate combination of genetic and reproductive technologies for strictly medical purposes, with appropriate oversight by public authorities and the scientific community. On this basis, conclusions will be drawn regarding the prospects for legal regulation of the technology in Russia.

1. Human genome editing: current situation in Russia

1.1. Biomedical component

At its core, genome editing is a purposeful alteration of an organism's DNA by adding, eliminating, or translocating genetic material. As such, it can be applied to a wide variety of organisms and is therefore in actual or potential demand in fields ranging from agriculture and industry to health care and biosecurity (Asquer & Morrison, 2022). The most serious expectations were related to the CRISPR-Cas9 editing technology. According to some descriptions, it claimed to be relatively (compared to other methods such as viral vectors, zinc finger nucleases (ZFNs), or TALENs) accuracy, efficiency, and cheapness to use (Barnett, 2017). However, one could notice that the cheerful assessment was somewhat refuted by data on actually performed experiments with a very low success rate at the output (Liang et al, 2015; Ma H. et al., 2017; Ledford, 2017). This method was claimed in the sensational story of the Chinese researcher He Jiankui, who changed the gene encoding the protein that allows HIV to enter the body and transplanted (against

the existing legal prohibition in China) the altered embryos into the uterus. The result was the birth of two girls (and criminal punishment for the researcher)[1].

The Russian Federation also undertakes fundamental research involving embryonic genome modification. The work by D. V. Rebrikov's group became famous, especially after numerous publications in the media about the researcher's willingness to use the technology for reproductive purposes, following the Chinese scientist[2]. It should be clarified that over time the group's focus was shifted from created immunity to some HIV variants (which, although it had obvious medical purposes, but still meant not curing the existing disease as such, but rather acquiring a "superpower" to avoid infection[3]) to hereditary hearing loss. At first glance, the disease's autosomal recessive type of inheritance does not require such drastic measures as genetic editing. The disease manifests itself only in the homozygous state, i.e. when both copies of the gene located on homologous autosomes are defective. According to Mendel's law, even if both parents are the disease carriers, the probability of giving birth to a sick child is 25 % and can be offset, e.g., by vitro fertilization and preimplantation genetic testing to select embryos without the disease[4]. In fact, the situation changes significantly when the sociocultural aspect is also taken into account. If families are created within a community of people with a hereditary hearing loss (which is often the case), a couple may not have a single embryo without the disease. In such a case, editing looks like a counteraction to the disease of the future offspring and, in addition, in a situation with no clear alternatives.

Nevertheless, to date there has been no explicit approval from the public authorities in Russia to conduct editing for reproductive purposes[5]. In the absence of such approval,

---

1 See, e.g.: Cyranoski, D. (2018, November 28). CRISPR-Baby Scientist Fails to Satisfy Critics. Nature. https://clck.ru/3DrtT2

2 See, e.g.: In Russia they create children with the altered DNA. How this threatens the country. (2019, June 14). RIA Novosti. https://clck.ru/3DrtV2

3 Thus, in addition to all other criticisms of He Jiankui, it produced additional reproaches for moving towards non-medical goals of creating offspring with given characteristics (the problem of so-called designer babies). See, e.g.: Chinese scientist who produced genetically altered babies sentenced to 3 years in jail. (2019, December 30). Science. https://clck.ru/3DrtWp

4 The construct is certainly not free from criticism, primarily of an ethical nature (Henaghan, 2006), but it is quite legally applicable, including in Russia. See: Order of the Russian Ministry of Healthcare No. 803n of 31.07.2020; para. 10 of the Order explicitly provides for such indications for ART as "hereditary diseases for the prevention of which pre-implantation genetic testing (hereinafter – PGT) is necessary, regardless of fertility status".

5 In 2019, the Ministry refused to issue such an authorization, referring to unexplored potential complications in the short and long term, as well as the WHO position. See: the Ministry of Healthcare said that it is premature to issue an authorization to alter the human genome. (2019, October 6). TASS. https://clck.ru/3Drtgc

as far as can be seen, editing does not go beyond the stage of fundamental research. This is facilitated, among other things, by the uncertain legal consequences for Russian scientists if they decide to follow their Chinese colleague.

1.2. Legal component

The legal component of the development and application of the discussed technology in Russia remains uncertain. Not that there is no regulatory framework in the field of genetic engineering at all, but there are no clear enough regulations on making inheritable changes to the human genome.

In particular, the Federal Law of July 5, 1996 No. 86-FZ "On state regulation in the field of genetic engineering"[6] (with subsequent amendments) specifies in Article 1 that "the order of genetic engineering and application of its methods to human beings, tissues and cells in human organism, except for gene diagnosis and gene therapy (genotherapy), is not the object"[7] of its regulation. At the same time, according to Article 2, gene therapy (genotherapy) is understood as "a set of genetic engineering (biotechnological) and medical methods aimed at introducing changes in the genetic apparatus of human somatic cells for the treatment of diseases"[8]. Since it explicitly refers to somatic cells only, the introduction of changes in the germ line (inheritable changes proper) is not explicitly regulated by this law.

The question of where embryos for fundamental research may or may not come from deserves special attention. In this context, the 1997 Council of Europe Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine is often cited. According to its Article 18, "the creation of human embryos for research purposes is prohibited"[9]. This norm seems quite unambiguous, and in two aspects: it prohibits the creation of embryos specifically for research and does not prohibit the use of those left over from the use of assisted reproductive technologies. In this article we deliberately do not focus on discussing the risks, including ethical ones, arising in this regard, because this is the subject of another detailed publication (Troitskaya, 2022). However, it is easy to see that if it is allowed to create embryos in vitro and test them, and if it is not prohibited to dispose of embryos deemed unsuitable or unclaimed for transplantation (and this is the case in Russia),

6 Federal Law of July 5, 1996, No. 86-FZ "On state regulation in the sphere of genetic engineering". Collection of legislation of the Russian Federation. 1996. No. 28. Art. 3348.

7 Ibid

8 Ibid

9 The Council of Europe Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine of 1997. https://clck.ru/3EBHyX

then the ethical challenge of conducting research on such embryos (again with subsequent disposal[10]) does not seem any more daunting in comparison.

However, the Russian state is not a party to this Convention, and the situation should be clarified accordingly. In the Russian legal space, it is not prohibited to use embryos unclaimed within ART; moreover, there is no explicit prohibition to create them specifically for research. Federal Law No. 180-FZ of June 23, 2016 "On biomedical cell products" prohibits to create human embryos for the production of such products, as well as to use for these purposes the biological material obtained by interrupting or disrupting a human embryo or fetus development. That said, the definition in the same law begs the question of whether an edited embryo is a biomedical cell product. According to the definition, a biomedical cell product is a complex consisting of cell line(s) and auxiliary substances or cell line(s) and auxiliary substances in combination with state-registered medicinal products for medical use, and/or pharmaceutical substances included in the state register of medicinal products, and/or medical devices. Although an embryo may be a source of a cell line, it is not a cell line itself, according to the available definitions[11]. We also believe that in the case of edited embryos the second criterion for classifying the product as a biomedical cell product is not met – namely, the embryo does not include auxiliary substances and/or medicines, pharmaceutical substances, medical devices. In addition, the law specifically states that it does not apply to the use of human sex cells for the purposes of assisted reproductive technologies, as well as to the relations arising from the circulation of human cells and tissues for scientific and educational purposes. Accordingly, the above prohibition

10 As will be shown further, the legal order, allowing embryo experimentation but not the transfer of modified embryos into the uterine, also prohibits the embryos development in vitro beyond a certain period of time, namely, 14 days. This time limit was the result of a consensus reached back in 1979 at the suggestion of the USA. The logic was as follows: up to this point, an embryo can divide into two (resulting in identical twins) or be absorbed by another embryo (in the case of multiple pregnancies); therefore, the emergence of a specific individual before 14 days is out of the question. Recently, however, one can notice a revitalization of the debate allowing a change in this consensus and extending the existence of embryos to 21 or even 28 days. As far as one can understand the arguments of the proponents of extending the time limit, their concern is not centered on some fundamentally new understanding of embryogenesis; it is mainly about having the time (and a developing research object) to better study the consequences of the adjustments made to the genome, to see the slightly more distant effects of editing on the embryo cells and tissues, and in the long run to more reliably control the progression to healthy offspring in humans. See: (McCully, 2021).

11 The Federal Law defines a cell line as a standardized population of cells of the same type with reproducible cellular composition, obtained by withdrawal of biological material from the human body and subsequent cultivation of cells outside the human body. Other definitions are also found in scientific literature, e.g.: a cell line is "a population of cells obtained from primary culture by increasing the number of cells after several generations with a predominance of cells or differentiation lines with a high growth rate and high homogeneity of the cell population". See: (Cherkasova & Brilkina, 2015).

to create embryos for the production of biomedical cell products does not affect the research we are interested in in this case.

The already mentioned Order of the Ministry of Healthcare No. 803n indicates the possibility of diagnosing and storing gametes and embryos, but does not regulate their editing and even less creating embryos for the development of relevant technologies. This is not surprising, since its object is assisted reproductive technologies, not fundamental research.

It seems that in such a situation, the determination of the sources of embryos for research is left to the discretion of a particular research team, and the research per se follows a logic determined by its supervisor.

As for the responsibility in case the edited embryos are transferred into the uterine of a woman (assumingly consenting), it remains not quite clear. Article 235 of the Russian Criminal Code stipulates punishment for medical activities performed by a person who does not have a license for this type of activity, provided that such a license is mandatory, if this has caused harm to human health or (a separate corpus delicti) death by negligence. Article 235 is applicable in the case when editing and transplantation of the edited embryo was carried out outside a medical organization that has the necessary license. In the context of genome editing, it must be a license for medical activity, which provides for the performance of works (services) in genetics and laboratory genetics.

The objective side of the described crime, in addition to carrying out activities without a license, also includes the mandatory infliction of harm to health. Apparently, Article 235 would not be applicable in a situation where the editing went according to the intended plan, spared the future child from the disease and caused no harm. The editing may not be precise and/or effective enough, but how exactly can one prove that specific mutations are a side effect of the editing? Also, in some cases, they may show up at a later stage, after embryo transfer, during prenatal diagnosis. Who will be responsible if a woman decides to prolong her pregnancy and gives birth to a child who is not quite healthy? The list of such questions can be continued. This is not to mention the fact that even a clearly stated prohibition on transferring edited embryos into the uterine can be relatively easily circumvented. By agreement between the doctor and the parents, the fact of editing may be concealed and the genetic variant, which was not expected theoretically but appeared in the end, may be explained by a random miraculous mutation. In fact, who and how would be able to refute this?

The Criminal Code also establishes liability for the provision of services, including medical services, that do not meet safety requirements (Article 238 of the Russian Criminal Code). The objective part of the crime is the provision of services that do not meet the requirements for the safety of life or health of consumers. At the same time, the corpus delicti is formal, i.e. the presence of damage to the health of a particular consumer (patient) is not included in the circumstance in proof (except the specific corpus delicti established by parts 2 and 3 of Article 238 of the Russian Criminal Code). It can be assumed that the provision of any

medical service will be recognized as not meeting safety requirements if it is not provided for by the standards and procedures for the provision of medical care and is not conducted as part of a clinical trial or clinical approbation (Art. 36.1 of the Federal Law of November 21, 2011, No. 323-FZ "On the fundamentals of health protection of citizens in the Russian Federation"). For example, the described case of embryo genome editing for the purposes of subsequent transplantation into the uterine involves applying the developed and previously unused methods of prevention, diagnosis, treatment and rehabilitation in the provision of medical care to confirm evidence of their effectiveness. This must be carried out exclusively in the course of clinical approbation. Among other things, it is necessary to obtain the approval of the ethics committee for using the method and the permission of the Ministry of Healthcare for the clinical approbation, which should specify in which medical organizations, on how many patients and in what order such approbation will be carried out. It is obvious that this authorization procedure was introduced to ensure the safety of patients when applying innovative treatment schemes/methods. The failure to comply with the authorization procedure and the genome editing without such authorization may in itself indicate that the service does not meet safety requirements (or at least allows presuming that safety requirements are not met).

The case is not much different at the principle level if we evaluate the norms of the Russian Code of Administrative Offences (the CAO RF). There are general norms relating to the implementation of activities without a license (Art. 14.1 of the CAO RF) and provision of services of improper quality (Art. 14.4 of the CAO RF). They interpret the quality of medical services as compliance with the relevant procedures for the provision of medical care and clinical recommendations (see part 2 of Article 64 of the Federal Law "On the Fundamentals of Health Protection of Citizens in the Russian Federation"), etc. There is also a special norm stipulating liability for offenses committed in the field of genetic engineering: Article 6.3.1 discloses the corpus delicti as "the use of genetically engineered organisms and (or) products obtained using such organisms or containing such organisms, which have not passed state registration if the state registration is provided for by the above legislation [this assumingly refers to the Federal Law "On state regulation in the field of genetic engineering", which, as noted above, does not apply to embryo editing – Authors], or the validity of the state registration certificate has expired, or the use of genetically engineered organisms not in accordance with the purposes for which they are registered, or violation of special conditions of using genetically engineered organisms, including when producing specific type of products"[12]. It is unlikely that the creators of this norm had in mind the situation of embryo editing for reproductive purposes that we are discussing, and there is no other special norm for this situation in the Code.

[12] Code on Administrative Offenses of the Russian Federation. https://clck.ru/3EBJCC

Separate questions arise in the area of civilistics. What can be the commercial potential of development (with prospects of practical application) of genetic editing technology, if Article 1349 of the Russian Civil Code establishes that "methods of modification of genetic integrity of human germ line cells"[13] cannot be the objects of patent rights (although it is clear that the development of these methods per se is not prohibited by any act)?[14]

As a result, Russia faces a situation in which inheritable editing of embryos is not prohibited at the level of fundamental research, although the procedures for controlling the emergence of embryos for these purposes are not at all clear-cut, and the commercial component of potential investments in this area remains "curtained"; as for inheritable editing for reproductive purposes, it remains completely uncertain in terms of legal consequences for its "authors".

However, it seems that the current technological advances, as well as ethical, social and biological concerns of varying degrees of intensity, require from the legislators not to maintain the twilight zone, but to facilitate controlled development in the area in question. Without pretending to absolutize any ideas, let us present possible moves in this direction.

2. Potential regulation mechanisms

In presenting the management tools, we will be guided by the Framework for Governance of Human Genome Editing published in 2021 by the World Health Organization[15], which, along with other scenarios (prenatal and postnatal somatic cell editing), contains scenarios related to inheritable changes. We will also consider the available experience of the countries for which the issue of inheritable editing is relevant in principle, due to their level of technological development, and which have some experience in regulating this sphere. In this regard, we should specially emphasize that the progress of other legal orders in human DNA editing the technology is far from being as modest as is sometimes believed[16].

---

13 Civil Code of the Russian Federation. https://clck.ru/3EBJ6X

14 A competent analysis of the objections raised against patenting genes can be found in the literature (negative consequences of patent protection of such objects for public health and scientific research; the special nature of the gene as a part of the human body and the common heritage of mankind; lack of patentability). See: (Vorozhevich, 2020). Note, however, that some authors discuss the patenting of not the modified gene as such, but the ways to modify it (see, e.g.: Decision of the Intellectual Rights Court of 15.06.2020 in case No. SIP-960/2019). In this case, especially if the state is involved in these relations (as discussed below), all or at least some of the above objections will be removed.

15 WHO. (2021, July 12). Human Genome Editing: a Framework for Governance. https://clck.ru/3DrtyJ

16 See in detail: (Baylis et al., 2020). The study covered 106 countries. As the authors demonstrate, 96 of them have documents (legislation, executive acts, guidelines, codes or international treaties) related to genome editing of early embryos or gametes. Some countries prohibit laboratory research on germline editing (Austria, Croatia, Germany, etc.), some allow it (Ireland, Norway, Japan, United Kingdom, United States, etc.). According to the authors, the use of inheritable editing for reproductive purposes is not authorized in any of the countries studied, although some of them allow the formula "prohibition with exceptions" (Belgium, Italy, etc.), which, of course, is particularly impressive.

In doing so, we take for granted that the priority goal-setting in this sphere includes the development of ideas about the role of genes (as well as their complementary action, the effects of epigenetic factors, etc.). Another priority is the prospect of improving the health of specific patients and future generations of human beings with full respect for their dignity. Moving towards these goals requires an understanding and consideration of the risks (occurring also under uncertainty) that may lie behind particular technologies. In a sense, these ideas can be considered "left aside"; that is, we recognize them and can apply them to all of the above, but no longer specifically repeat them.

2.1. Basic concepts

In a situation where the creation of legal norms adequate to the current challenges is already stalled, it is tempting to skip the stage of discussing key values that would guide future regulation and governance in the field of human genome editing. Nevertheless, it is this stage that should be given attention in the first place. The following starting points could be emphasized here:

– the need to develop fundamental genetics and related fields, in order to understand how the human genome functions, even in the absence of immediate pre-understood applied implications of this knowledge;

– awareness of the link between the development of science and the provision of individual dignity. It results in the desire to improve life quality and the respect for individual autonomy. In practice, it requires an understanding of what exactly is meant by autonomy in the field of genetic inheritance (understandably common to the population) and what kind of improvement in life quality we can talk about. However, it is already clear that medical goals (even those related to obtaining the ability to resist a disease and not only to cure it) are less of a challenge than the "design" of people with predetermined characteristics not linked to medical issues;

– the need for biosecurity. This, however, must be coupled with the idea that genetic editing technology does not emerge in a vacuum, but in the face of a wide variety of factors that affect the genome even without editing (among them, the long-standing use of medical advances that make it possible to maintain a wide variety of gene combinations in the population, including those that lead to disease manifestation; man-made disasters; changes in the system of environmental relations; new types of weapons, etc.).

This list can be continued to include ideas arising from those already voiced. First of all, it concerns the ideology of transparent, accountable and responsible (both on the part of researchers and public authorities) actions, which is promoted by WHO[17]. Admittedly, in WHO wordings it does correlate with expectations of adequate resources and opportunities for scientists and the public to benefit from technological progress[18].

---

17 See: Human Genome Editing: a Framework for Governance. § 14.

18 See: Ibid. § 19.

2.2. Legal frameworks

As foreign experience shows, the overdue need for regulation results in the legislative power creating a comprehensive act which covers, among other things, genome editing. There are two noticeably different examples. The British Human Fertilisation and Embryology Act 1990 with subsequent amendments[19] and clarifications added at secondary rule-making[20] has an independent and clearly delineated subject of regulation. It contains norms on human embryos and any subsequent development of such embryos; prohibition of certain actions in relation to embryos and gametes and on the creation of a special body – Human Fertilisation and Embryology Authority. This Act is linked to other acts, including those on surrogacy, but is itself fully and consistently organized around its subject matter. The French Bioethics Act of 2021[21], a much more challenging reading, is essentially a massive list of amendments to other acts, most notably the Public Health Code, although it carries an explicit desire to address a range of bioethical issues, including those relating to the exercise of reproductive rights.

It is obvious that when moving from scratch in the issue of inheritable human genome editing, both ways (creation of a new independent act or making additions to the existing Federal Law 2011 "On the fundamentals of health protection of citizens in the Russian Federation") are possible. Also possible is the path that has been followed so far in the regulation of assisted reproductive technologies – an order of the Ministry of Healthcare with the most basic guidelines in this Federal Law. Moreover, it seems that this way may prove to be in a certain respect[22] more productive for achieving, first of all, professional consensus on a number of issues. After all, both British and French laws, while allowing manipulation on embryos, equally prohibit the transplantation of an embryo with altered nuclear genes[23] for reproductive purposes. Assumingly, in Russia, too, this issue can be clarified in the norms of different levels, especially if these norms are clear-cut and correlate with the provisions of the Criminal Code and the Code of Administrative Offenses.

---

19 Human Fertilisation and Embryology Act 1990. https://clck.ru/3DruCm; especially notable are the changes of 2022, stipulated by the Health and Care Act 2022. https://clck.ru/3DruDn

20 Human Fertilisation and Embryology (Research Purposes) Regulations, 2001.

21 Loi n° 2021-1017 du 2 août 2021 relative à la bioéthique. https://clck.ru/3DruFq

22 However, one should also keep in mind the flip side of the coin when using such an approach: the introduction of general rules by executive acts implies the possibility of a one-time cancellation or change of such rules. This makes the situation poorly predictable, including for both potential investors and research teams and medical organizations.

23 With regard to British legislation, it allows the use of donor mitochondria (and the relatively small number of genes it contains) in reproductive technologies. Nevertheless, the use of donor organelle, although related to the creation of "genetically modified" children, is not in biomedical terms the same as genome editing.

Hence, the more difficult questions actually lie less in the form than in the content; namely, in determining within what limits, with what procedures and resources one may carry out fundamental research in embryonic or gamete genome editing. Let us name the substantive aspects:

– the constitutionally and statutorily significant purposes of such research;

– the (probably closed) list of indications for editing;

– the expected fundamental or practical benefits to society (versus the substantively identified risks);

– the procedures for raising private or public funds for the research;

– the sources of the actual material involved in the research, especially when embryos are involved;

– the feasible, necessary for the research, and yet ethically acceptable time limits for the edited embryo development;

– the controls over the research conduct and the result quality (publications, possibility of verifying the results, as well as other ex ante (e.g. authorization, licensing, etc.) and ex post (controls, etc.) measures;

– the degree of the true results openness to others and the possibility of their competent discussion, including scientific verification and criticism;

– the degree of openness of genuine results to others and the possibility of their competent discussion, including scientific verification and criticism;

– the features of protection of researchers' intellectual rights for the subsequent commercial application of their results;

– the extent to which available international standards and foreign practices are taken into account.

These are the issues that could be a "starting grid" for the development of the most concise, and even more so a detailed system of regulation in the sphere of inheritable genome editing.

2.3. Management and control

Judging by the available reports, D. V. Rebrikov's team interacted with the Russian Ministry of Healthcare when trying to calculate the "limits of the possible"[24]. The Ministry of Healthcare includes the Department of Science and Healthcare Innovative Development, which, in turn, can interact with the Ministry of Science and Education. By the Order of the Russian Ministry of Healthcare of December 30, 2020, No. 1416, this Department is responsible for the implementation of measures aimed at the innovative development of healthcare and certain priority areas of medical science, including biomedical and genetic technologies. Thus, in principle, there is no vacuum in this sphere in executive system as

[24] What does Rebrikov want? (2019, October 22). PCR.news. https://clck.ru/3EBKYs

there is in legislation. Nevertheless, departmental acts do not stipulate the exact procedures of organization of fundamental research on inheritable human genome editing (except allocation of grants from some foundations), control and evaluation of its results.

Again, from foreign experience we can see various possibilities of organizing management and control. For example, in Great Britain, the Human Fertilisation and Embryology Authority is entitled to issue a license for fundamental research. A prerequisite for applying for such a license is the opinion of a recognized and independent ethical commission which the scientific team must obtain. The Authority sends the application for peer review and in the meantime organizes the inspection of the applicant's premises and equipment. The application, the opinion of the ethics committee, the expert evaluations of the application, and the report on the inspection of the conditions for performing research are submitted to the Licensing Committee, which decides whether to grant the license and, if necessary, accomplishes it with additional conditions (Lawford, 2020). Performing germline manipulations without a license or without complying with its conditions is a criminal deed, with penalties ranging from fines to imprisonment of up to two years. Emphasizing the objectives of purely fundamental research, the Authority has been issuing licenses for editing human embryos with CRISPR technology since 2016. Research licensed in this way also require written informed consent from the donors of gametes or embryos for using the donor material in such activities. Public funding of such research is possible in the UK and is in practice. As far as one may see, this order of interaction ensures the controlled research, but without excesses like the Chinese case.

In turn, it is China's experience that makes it possible to understand which option of organizing control faltered and how the public authorities reacted to it. Before China announced the birth of two girls whose DNA had been artificially altered, genetic editing in this country was regulated by the 2003 Ethical Guidelines for Human Embryonic Cell Research. Article 6 of this document prohibited both research on human embryos 14 days after fertilization and any genetic manipulations of human gametes, zygotes, and embryos for reproductive purposes. Manipulations for research purposes required ethical committee approval from any of the authorized medical institutions. In practice, He Jiankui obtained such approval from a private medical company that is known for controlling about 80 % of all private hospitals in the PRC and also for being involved in a lot of rows revealing its commitment to a purely "commercial ethos". This made it abundantly clear that relying on ethical principles alone in an area as sensitive as genetic editing is hardly a brilliant idea.

To be fair, this conclusion was supported by the PRC's central representative body. In 2020, the National People's Congress included in the Civil Code provisions detailing the constitutional right to dignity and regulating biomedical (including genetic) research. According to Article 1008, any clinical trial in this field requires ethical approval and informed consent of affected subjects in disclosing the purpose, objectives and potential risks of such a trial. Article 1009 states that "any medical research activity involving human genes and human embryos shall be conducted in accordance with relevant laws, administrative

regulations and national regulation, shall not harm individuals, and shall not violate ethical morality and public interests"[25].

Naturally, these changes alone could not block options such as those implemented by He Jiankui. However, the matter did not end with them.

At the same time, a draft amendment to the Criminal Code was developed, according to which the specialized elements of crimes related to the illegal practice of human gene editing, cloning of human embryos and a serious threat to the safety of human genetic resources were sanctioned with fines and imprisonment for up to 7 years[26].

However, the key line of defense is in the PRC executive branch. In terms of establishing administrative regulations, there is a delineation of the powers between the Ministry of Science and Technology (regulation of fundamental research) and the National Healthcare Committee (regulation of clinical trials), while the PRC State Council subsequently adopts relevant acts. In 2019, the regulation on fundamental research was adopted. It stipulates that the collection, storage and use of genetic information is subject to either licensing or administrative registration. The sanctions for violating this requirement are fines of up to 5 million yuan or 10 times the amount of illegal profits (after the amendments to the Criminal Code come into force, there should be sanctions for the crime of seriously jeopardizing the safety of human genetic resources). In the same year, a draft regulation on clinical trials was developed to fundamentally change the approval scheme for clinical trials. The National Healthcare Committee stated that all clinical trials involving innovative biomedical technologies would require administrative approval. The regulations proposed by the Committee would categorize gene editing clinical trials into two levels: (1) high risk and (2) low and medium risk. This said, gene editing technology and related assisted reproductive technologies are categorized as high risk and in the future must be approved by the Committee after considering the scientific and ethical aspects of the project[27]. That is, all clinical trials of innovative biomedical technologies must now undergo a double review: internal, conducted by the medical institution, and external, which is the responsibility of the state administrative bodies. The regulations also stipulate requirements for medical institutions applying to conduct clinical trials and (which seems psychologically significant) sanctions in case of the regulations violation for their heads, not just

25 Civil Code of the People's Republic of China. https://clck.ru/3EBLAd

26 In comparison, the French Penal Code, which considers eugenic practices and reproductive cloning as crimes against humanity, allows for imprisonment of up to 30 years and fines of up to 7,500,000 euros (Articles 214-1 and 214-2).

27 Low and medium risk clinical trials will require administrative approval from a provincial Healthcare Department.

the head of the scientific group, as was the case with He Jiankui. In addition, the PRC is discussing plans to establish a National Ethical Review Committee for Science and Technology, specifically to oversee research that raises significant ethical controversy, such as projects involving gene editing technology (Song & Joly, 2021).

The cited examples crystallize an approach that combines administrative control with professional ethical review of planned research and its results. Despite the seemingly cumbersome nature of this combination, it is likely (with appropriate rules for the formation of ethics committees) to ensure, on the one hand, the development of science in the strategically important area with competent professionals involved in decision-making, and, on the other hand, a manageable and relatively bias-free development.

This said, it is possible to develop the procedures for harmonizing the conducting and reporting on research not only for the purposes of distributing public funding, but also for private initiatives[28].

It is necessary to add one more delicate point related to the verification of the obtained results (required, among other things, if we keep in mind the possible transition from fundamental research to clinical trials and introduction of inheritable changes in the human genome within reproductive technologies). Namely, this is the fact that at the moment in Russia only one team claims to have sufficiently serious advances. At first glance, legal science may not be concerned with the current situation. However, some costs begin to be felt at this point, although it is not easy to verbalize them. This is related to the difficulty, in the current situation, to get a full picture of the existing achievements and to assess the prospect of further development. How accurate and effective, in fact, is the editing technology? Can specific results be confidently replicated? What exactly are the complexities of editing, what exactly separates us from the point where we no longer fear the emergence of real children with edited DNA? What exactly is the effect of existing investments in this area, and what are the benefits and costs of further funding specific areas of science? The list of these questions could be continued, but we strongly suspect that in the absence of scientific competition or collaboration between several teams (or a thorough reconciliation of results with foreign colleagues), the answers to these questions will remain vague. This does not help to bring this research out of the somewhat marginalized shadow in which it now seems to have fallen.

[28] As WHO notes, regulations governing the funding of private and public research may impose a number of conditions that function as a governance tool. E.g., these may include: conditions on the source of gametes or embryos (especially on payment and consent of their donors); limits on the time embryos can be maintained in vitro; rules on the creation of hybrid embryos; rights of ownership and disposition of gametes and embryos; and rules on intellectual property rights and the sharing of data and materials. See: Human Genome Editing: a Framework for Governance. § 70.

At the same time, the problem of information exchange raises two other important issues when we try to understand how governance should be structured. One of them is the functioning of the information base on genetic corrections and research in terms of human genome editing[29]. Judging by the website of the Center for High-Precision Editing and Genetic Technologies for Biomedicine[30], there is an impressive record, but still the information is far from complete. The problem of inaccessibility of detailed information on trials is characteristic not only of the genetic research in question, but also of "classical" pharmaceuticals – and the solutions offered by the current regulation seem to be far from ideal[31].

The second related issue is the patentability of the fundamental research results. The literature has already criticized too rigid approaches to (non-)granting patent legal protection to the results of intellectual activity in the field of human embryo genome editing[32]. We believe it is really necessary to find out if this is a possible growth point not just for the existing teams, but for a larger-scale stimulation of scientific research, but in a slightly different aspect. In particular, researchers discuss such well-known ways of managing scientific results as eligibility for publicly funded inventions, government licenses, thematic restrictions, and others. All of them are provided for cases where the government either has an interest of using the technology on its own behalf within certain boundaries, or compels the patent owner to allow another person to use it as the government sees fit (Scheinerman & Sherkow, 2021).

From the above, it is clear that managing the field of genetic editing requires complex solutions, where expectations on some questions clearly influence answers on others.

---

29 See: Order of the Russian Government No. 479 of 22.04.2019. (2019). Garant.ru. https://clck.ru/3DruV4

30 Center for High-Precision Editing and Genetic Technologies for Biomedicine. https://clck.ru/3DruWd

31 E.g., there is an open register of clinical trials of medicinal products in the Russian Federation (https://clck.ru/3DruYb), but its content does not allow determining how the trial was conducted, how it ended, etc. Moreover, the Federal Law of April 12, 2010 No. 61-FZ "On circulation of medicines" (part 18, 21 of Article 18) implements the so-called institution of "data exclusivity". Given the established judicial practice (see, e.g.: Definition of the Supreme Court of the Russian Federation of 26. 05.05.2016 No. 305-ES16-2399 in case No. A40-188378/14), the said Law encourages pharmaceutical companies to keep secret the results and details of even successfully conducted clinical trials for at least the period of data exclusivity (up to six years from the date of the drug registration based on the conducted trials). At the same time, given the dynamic development of science and the significance of the trial results both for scientific teams and, ultimately, for society, it can be stated for specific patients that withholding such information and protecting it under the trade secret regime (i) is contrary to the public interest, (ii) may hinder the development of science, (iii) does not allow bona fide companies who publish trial data to enjoy protection under the exclusivity period, and (iv) it is not clear what benefits the state, and in particular, the public healthcare system, can derive from this incentive.

32 See: (Borodin & Kryukova, 2021). More moderate positions in science are also presented. See: (Panagopoulos & Sideri, 2021).

Conclusion

Inheritable human genome editing is a technology that already exists in one way or another. The material part, if we may say so, has already been created for this purpose. Research in this direction is being conducted in Russia, and, importantly, not only in Russia. It is known that managing the development and application of technology is always a process. In this case, the regulation of genetic editing and related practices can be compared to a living organism that has already been brought into the world, at least to be developed in the future.

The situation acquires additional interest due to the fact that in this case almost any advancement in the legal field demands competent discussion with the main stakeholders, which should obviously be built on an iterative principle. Even principle bases and starting points should be checked with the participants of what is going on. This is especially true for the further, more detailed mechanism of interaction between public authorities, representatives of legal and ethical sciences, medical organizations that perform key research functions in the field of editing, patients (patient organizations), etc. The creation and preservation of the discussion horizon allow, on the one hand, to moderate the excitement of discoverers, and on the other hand, not to cold-stack the situation up to the point of complete inaction.

We believe that this situation requires special platforms for interdisciplinary discussion of what regulatory and managerial steps should be taken in Russia to develop the technology; here we tried to present several proposals on this issue.

References

Asquer, A., & Morrison, M. (2022). Editorial: Regulation and governance of gene editing technologies (CRISPR, etc.). *Frontiers in Political Sciences*, *4*, 1027410. https://doi.org/10.3389/fpos.2022.1027410

Atimango, A. O., Wesana, J., Kalule, S. W., Verbeke, W., & De Steur, H. (2024). Genome editing in food and agriculture: from regulations to consumer perspectives. *Current Opinion in Biotechnology*, *87*, 103127. https://doi.org/10.1016/j.copbio.2024.103127

Balashenko, N. A. (2016). Information Technologies in Genetics. *Informatization of Education*, *1*, 84–94. (In Russ.).

Barnett, S. A. (2017). Regulating Human Germline Modification in Light of CRISP. *University of Richmond Law Review*, *51*, 553–591.

Baylis, F., Darnovsky, M., Hasson, K., & Krahn, T. M. (2020). Human Germline and Heritable Genome Editing: the Global Policy Landscape. *The CRISPR Journal*, *3*(5), 365–377. https://doi.org/10.1089/crispr.2020.0082

Borodin, S. S., Kryukova, E. S. (2021). Legal regulation of stimulating the introduction of genetic technologies into economic circulation. In A. A. Mokhov, O. V. Sushkova (Eds.), *Genetic research and medicine* (pp. 23–24). Moscow: Prospect. (In Russ.).

Cherkasova, E. I., Brilkina, A. A. (2015). *Working with cell cultures*. Nizhny Novgorod. (In Russ.).

Henaghan, M. (2006). *Choosing Genes for Future Children: Regulating Preimplantation Genetic Diagnosis*. Dunedin, N.Z.: Human Genome Research Project.

Lawford, D. J. (2020). The Regulation of Human Germline Genome Modification in the United Kingdom. In A. Boggio, C. P. R. Romano, J. Almqvist (Eds.), *Human Germline Genome Modification and the Right to Science. A Comparative Study of National Laws and Policies* (pp. 217–240). Cambridge University Press.

Ledford, H. (2017). CRISPR fixes disease gene in viable human embryos. *Nature*, *548*, 13–14. https://doi.org/10.1038/nature.2017.22382

Liang, P., Xu, Y., Zhang, X., Ding C., Huang R., Zhang Z., Lv J., Xie X., Chen Y., Li Y., Sun Y., Bai Y., Songyang Zh., Ma W., Zhou C., Huang J. (2015). CRISPR/Cas9-Mediated Gene Editing in Human Tripronuclear Zygotes. *Protein Cell*, *5*(6), 363–372. https://doi.org/10.1007/s13238-015-0153-5

Ma, H., Marti-Gutierrez, N., Park, S. W., ... Mitalipov, Sh. (2017). Correction of a pathogenic gene mutation in human embryos. *Nature*, *548*, 413–419. https://doi.org/10.1038/nature23305

McCully, S. (2021). The Time has Come to Extend the 14-Day Limit. *Journal of Medical Ethics*, *7*. https://doi.org/10.1136/medethics-2020-106406

Panagopoulos, A., & Sideri, K. (2021). Prospect patents and CRISPR; rivalry and ethical licensing in a semi-commons environment. *Journal of Law and the Biosciences*, *8*(2), lsab031. https://doi.org/10.1093/jlb/lsab031

Pombo, M. L. (2011). Biotechnological products in Pan American Health Organization (PAHO): Regional efforts towards harmonization of regulation. *Biologicals*, *39*(5), 348. https://doi.org/10.1016/j.biologicals.2011.06.010

Scheinerman, N., & Sherkow, J. (2021). Governance Choices of Genome Editing Patents. *Frontiers in Political Sciences*, *3*, 745898. https://doi.org/10.3389/fpos.2021.745898

Sharif, J., Koseki, H., & Parrish, N. F. (2023). Bridging multiple dimensions: roles of transposable elements in higher-order genome regulation. *Current Opinion in Genetics & Development*, *80*, 102035. https://doi.org/10.1016/j.gde.2023.102035

Song, L., & Joly, Y. (2021). After He Jianku: China's Biotechnology Regulation Reforms. *Medical Law International, 21*(2). https://doi.org/10.1177/0968533221993504

Tan, J., Shen, M., Chai, N., Liu, Q., Liu, Y., & Zhu, Q. (2023). Genome editing for plant synthetic metabolic engineering and developmental regulation. *Journal of Plant Physiology*, *291*, 154141. https://doi.org/10.1016/j.jplph.2023.154141

Troitskaya, A. (2022). Legal answers to questions about editing the human genome (considering CRISPR-Cas9 technology). *Comparative Constitutional Review*, *31*(5), 11–41. (In Russ.).

Vorozhevich, A. S. (2020). Patent rights to the results of genetic research: terms and conditions of acceptance. *Civil Law Review*, *2*, 176–216.

Wilson, L. (2023). Regulation of biological agents and biotechnology. In *Encyclopedia of Forensic Sciences* (Vol. 4, 3rd Ed., pp. 376–386). Elsevier eBooks. https://doi.org/10.1016/b978-0-12-823677-2.00232-4

Yu, H., Taduri, S., Kesan, J., Lau, G., & Law, K. H. (2012). Mining information across multiple domains: A case study of application to patent laws and regulations in biotechnology. *Government Information Quarterly*, *29*, S11–S21. https://doi.org/10.1016/j.giq.2011.08.013

Authors information

Aleksandra A. Troitskaya – Dr. Sci. (Law), Associate Professor, Professor of the Department of Constitutional and Municipal Law, Lomonosov Moscow State University
Address: 1 Leninskiye Gory, building 13, 119991 Moscow, Russia
E-mail: stephany@mail.ru
ORCID ID: https://orcid.org/0000-0002-5025-9905
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=15045938900
WoS Researcher ID: https://www.webofscience.com/wos/author/record/O-5879-2017
RSCI Author ID: https://elibrary.ru/author_items.asp?authorid=629760

Konstantin A. Sharlovskiy – Partner, Head of Life Sciences Practice, Pepelyaev Group LLC
Address: 39 3rd Tverskaya-Yamskaya Str., building 1, 125047 Moscow, Russia
E-mail: K.Sharlovskiy@pgplaw.ru
ORCID ID: https://orcid.org/0000-0003-1091-5338
WoS Researcher ID: https://www.webofscience.com/wos/author/record/AAH-5173-2019

Authors' contributions

The authors have contributed equally into the concept and methodology elaboration, validation, formal analysis, research, selection of sources, text writing and editing, project guidance and management.

Conflict of interests

The authors declare no conflict of interests.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – June 2, 2024
Date of approval – June 18, 2024
Date of acceptance – September 25, 2024
Date of online placement – September 30, 2024

Научная статья
УДК 34:004:342.721:612.6
EDN: https://elibrary.ru/tklbsa
DOI: https://doi.org/10.21202/jdtl.2024.27

Редактирование генома человека: управление технологическими рисками правовыми средствами

Александра Алексеевна Троицкая ✉

Московский государственный университет имени М. В. Ломоносова, Москва, Россия

Константин Александрович Шарловский

Пепеляев Групп, Москва, Россия

Ключевые слова

генетические технологии,
генетическое редактирование,
геном человека,
законодательство,
право,
репродуктивные технологии,
рискориентированный подход,
технологический риск,
цифровые технологии,
юридическая ответственность

Аннотация

Цель: определить теоретические подходы к правовому регулированию репрогенетического редактирования с учетом рискориентированного подхода и практики регулирования такого рода прорывных технологий в различных юрисдикциях, а также наметить дальнейшие нормативные и управленческие шаги, которые должны быть предприняты для развития технологии.

Методы: общенаучные методы анализа и синтеза, классификация, системный и функциональный подходы; частнонаучные методы – формально-юридический, сравнительно-правовой, историко-правовой.

Результаты: проведенное исследование показывает возможные варианты подходов к регулированию генетического редактирования в репродуктивных целях. Рассмотренные варианты оценены с точки зрения рискориентированного подхода, определены условия и особенности применения различных регуляторных механизмов, а также дана оценка текущему отечественному регулированию в этой сфере. По итогам анализа возможно заключить, что запрет или существенное ограничение развивающейся технологии репрогенетического редактирования не имеет под собой неопровержимых оснований, более того, может привести скорее к обратным результатам, нежели те, которые декларируются сторонниками такого подхода. В этой связи необходимо развивать дискуссию в конструктивном итеративном ключе, вовлекая в нее всех стейкхолдеров, в том числе научное сообщество.

✉ Контактное лицо

Научная новизна: обобщение и концептуальное осмысление опыта правового регулирования репрогенетических технологий на международном уровне, в рамках различных юрисдикций, а также анализ естественно-научных доводов в контексте оценки эффективности внедряемого регулирования позволяют не только системно рассмотреть существующие и гипотетически возможные риски развития и использования генетических технологий, но дают возможность использовать рискориентированный подход к анализу проблем правового регулирования технологий редактирования генома человека. Это позволяет сделать следующий шаг в осмыслении феномена генетического редактирования.

Практическая значимость: результаты настоящего исследования могут быть использованы для целей выстраивания дальнейшего конструктивного диалога по поводу применения правовых механизмов к вопросам редактирования генома человека. Исследование также возможно рассматривать в качестве основы для использования итеративного подхода в рамках дальнейшей дискуссии.

Для цитирования

Троицкая, А. А., Шарловский, К. А. (2024). Редактирование генома человека: управление технологическими рисками правовыми средствами. *Journal of Digital Technologies and Law*, *2*(3), 521–543. https://doi.org/10.21202/jdtl.2024.27

Список литературы

Балашенко, Н. А. (2016). Информационные технологии в генетике. *Информатизация образования*, *1*, 84–94. https://elibrary.ru/ywwhqo

Бородин, С. С., Крюкова, Е. С. (2021). Правовая регламентация стимулирования внедрения генетических технологий в экономический оборот. В кн. А. А. Мохов, О. В. Сушкова (ред.), *Генетические технологии и медицина* (с. 23–24). Москва: Проспект. https://elibrary.ru/nmxhrw

Ворожевич, А. С. (2020). Патентные права на результаты генетических исследований: условия предоставления, допустимые изъятия и ограничения. *Вестник гражданского права*, *2*, 176–216. https://elibrary.ru/gcgapa.

Троицкая, А. (2022). Правовые ответы на вопросы о редактировании генома человека (с учетом технологии CRISPR-CAS9). *Сравнительное конституционное обозрение*, *5*, 11–41. https://doi.org/10.21128/1812-7126-2022-5-11-41

Черкасова, Е. И., Брилкина, А. А. (2015). *Работа с культурами клеток*. Нижний Новгород: ННГУ им. Н. И. Лобачевского.

Asquer, A., & Morrison, M. (2022). Editorial: Regulation and governance of gene editing technologies (CRISPR, etc.). *Frontiers in Political Sciences*, *4*, 1027410. https://doi.org/10.3389/fpos.2022.1027410

Atimango, A. O., Wesana, J., Kalule, S. W., Verbeke, W., & De Steur, H. (2024). Genome editing in food and agriculture: from regulations to consumer perspectives. *Current Opinion in Biotechnology*, *87*, 103127. https://doi.org/10.1016/j.copbio.2024.103127

Barnett, S. A. (2017). Regulating Human Germline Modification in Light of CRISP. *University of Richmond Law Review*, *51*, 553–591.

Baylis, F., Darnovsky, M., Hasson, K., & Krahn, T. M. (2020). Human Germline and Heritable Genome Editing: the Global Policy Landscape. *The CRISPR Journal*, *3*(5), 365–377. https://doi.org/10.1089/crispr.2020.0082

Henaghan, M. (2006). *Choosing Genes for Future Children: Regulating Preimplantation Genetic Diagnosis*. Dunedin, N.Z.: Human Genome Research Project.

Lawford, D. J. (2020). The Regulation of Human Germline Genome Modification in the United Kingdom. In A. Boggio, C. P. R. Romano, J. Almqvist (Eds.), *Human Germline Genome Modification and the Right to Science. A Comparative Study of National Laws and Policies* (pp. 217–240). Cambridge University Press.

Liang, P., Xu, Y., Zhang, X., Ding C., Huang R., Zhang Z., Lv J., Xie X., Chen Y., Li Y., Sun Y., Bai Y., Songyang Zh., Ma W., Zhou C., Huang J. (2015). CRISPR/Cas9-Mediated Gene Editing in Human Tripronuclear Zygotes. *Protein Cell*, *5*(6), 363–372. https://doi.org/10.1007/s13238-015-0153-5

Ledford, H. (2017). CRISPR fixes disease gene in viable human embryos. *Nature*, *548*, 13–14. https://doi.org/10.1038/nature.2017.22382

Ma, H., Marti-Gutierrez, N., Park, S. W., ... Mitalipov, Sh. (2017). Correction of a pathogenic gene mutation in human embryos. *Nature*, *548*, 413–419. https://doi.org/10.1038/nature23305

McCully, S. (2021). The Time has Come to Extend the 14-Day Limit. *Journal of Medical Ethics*, *7*. https://doi.org/10.1136/medethics-2020-106406

Panagopoulos, A., & Sideri, K. (2021). Prospect patents and CRISPR; rivalry and ethical licensing in a semi-commons environment. *Journal of Law and the Biosciences*, *8*(2), lsab031. https://doi.org/10.1093/jlb/lsab031

Pombo, M. L. (2011). Biotechnological products in Pan American Health Organization (PAHO): Regional efforts towards harmonization of regulation. *Biologicals*, *39*(5), 348. https://doi.org/10.1016/j.biologicals.2011.06.010

Scheinerman, N., & Sherkow, J. (2021). Governance Choices of Genome Editing Patents. *Frontiers in Political Sciences*, *3*, 745898. https://doi.org/10.3389/fpos.2021.745898

Sharif, J., Koseki, H., & Parrish, N. F. (2023). Bridging multiple dimensions: roles of transposable elements in higher-order genome regulation. *Current Opinion in Genetics & Development*, *80*, 102035. https://doi.org/10.1016/j.gde.2023.102035

Song, L., & Joly, Y. (2021). After He Jianku: China's Biotechnology Regulation Reforms. *Medical Law International, 21*(2). https://doi.org/10.1177/0968533221993504

Tan, J., Shen, M., Chai, N., Liu, Q., Liu, Y., & Zhu, Q. (2023). Genome editing for plant synthetic metabolic engineering and developmental regulation. *Journal of Plant Physiology*, *291*, 154141. https://doi.org/10.1016/j.jplph.2023.154141

Wilson, L. (2023). Regulation of biological agents and biotechnology. In *Encyclopedia of Forensic Sciences* (Vol. 4, 3rd Ed., pp. 376–386). Elsevier eBooks. https://doi.org/10.1016/b978-0-12-823677-2.00232-4

Yu, H., Taduri, S., Kesan, J., Lau, G., & Law, K. H. (2012). Mining information across multiple domains: A case study of application to patent laws and regulations in biotechnology. *Government Information Quarterly*, *29*, S11–S21. https://doi.org/10.1016/j.giq.2011.08.013

Сведения об авторах

Троицкая Александра Алексеевна – доктор юридических наук, доцент, профессор кафедры конституционного и муниципального права, Московский государственный университет имени М. В. Ломоносова
Адрес: 119991, Россия, г. Москва, Ленинские горы, 1, стр. 13
E-mail: stephany@mail.ru
ORCID ID: https://orcid.org/0000-0002-5025-9905
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=15045938900
WoS Researcher ID: https://www.webofscience.com/wos/author/record/O-5879-2017
РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=629760

Шарловский Константин Александрович – партнер, руководитель практики «Фармацевтика и здравоохранение», ООО «Пепеляев Групп»
Адрес: 125047, Россия, г. Москва, ул. 3-я Тверская-Ямская, 39, стр. 1
E-mail: K.Sharlovskiy@pgplaw.ru
ORCID ID: https://orcid.org/0000-0003-1091-5338
WoS Researcher ID: https://www.webofscience.com/wos/author/record/AAH-5173-2019

Вклад авторов

Авторы внесли равный вклад в разработку концепции, методологии, валидацию, формальный анализ, проведение исследования, подбор источников, написание и редактирование текста, руководство и управление проектом.

Конфликт интересов

Авторы сообщают об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.07.45 / Право и научно-технический прогресс
Специальность ВАК: 5.1.1 / Теоретико-исторические правовые науки

История статьи

Дата поступления – 2 июня 2024 г.
Дата одобрения после рецензирования – 18 июня 2024 г.
Дата принятия к опубликованию – 25 сентября 2024 г.
Дата онлайн-размещения – 30 сентября 2024 г.

Research article
UDC 34:004:349.4:004.8:528
EDN: https://elibrary.ru/blqkuz
DOI: https://doi.org/10.21202/jdtl.2024.28

Digital Technologies in the National Cadastre System of Uzbekistan: Issues of Legal Regulation

Robiya S. Toshboyeva

Tashkent State University of Law, Tashkent, Uzbekistan

Keywords

artificial intelligence,
cadastre infomation,
digital technologies,
ethics,
law,
legal regulation,
national legislation,
special legal regime,
state cadastre,
Uzbekistan

Abstract

Objective: to critically analyze the state of national legislation of Uzbekistan in terms of legal regulation of digitalization and the use of artificial intelligence in the cadastral sphere.

Methods: the research is based on such methods of scientific cognition as formal-legal and comparative-legal analysis, induction and deduction.

Results: the provisions that regulate digitalization and the use of artificial intelligence in the cadastral sphere were analyzed, legal gaps were identified. It was determined that the practical application of artificial intelligence technologies outpaces its legal regulation. The shortcomings of legal regulation in this sphere were noted (lacking legal definition of the legal status of artificial intelligence in the national legislation; regulation of business entities' participation in the management of artificial intelligence, etc.). The said shortcomings hinder its full application and harmonization with traditional sources of cadastral information. The author substantiated the need for universal digitization of the national cadastre and predicts the possibility of wider application of artificial intelligence in the natural-resource cadastral system. It is argued that the existing system in its current state may lead to wrong decisions and cadastral errors, hence, it is necessary to improve the legal regulation of cadastre.

Scientific novelty: for the first time the results of the national cadastre digitization were assessed. Forecasts were given about the possibility of using artificial intelligence in this area, subject to further improvement of legal regulation. The latter is fundamentally important for reforming the cadastral system, since the technological basis of this system does not fully meet the needs of the digital economy.

Practical significance: it is due to the lack of legal regulation of the artificial intelligence concept and legal status in the national legislation, as well as a unified approach to the cadastral system digitalization. Modern technologies are actively used in practice, but lack a sufficient legal basis. The main conclusions, proposals and recommendations of the study can be a basis for further improvement of the legal framework of Uzbekistan in terms of the application of artificial intelligence technologies.

For citation

Toshboyeva, R. S. (2024). Digital technologies in the national cadastre system of Uzbekistan: issues of legal regulation. *Journal of Digital Technologies and Law, 2*(3), 544–564. https://doi.org/10.21202/jdtl.2024.28

Contents

Introduction

The cadastral system of Uzbekistan includes more than 20 types of state cadastres, the objects of which are both natural resources and non-natural objects. This system contains a huge database, which reliability influences the course of economic reforms. Therefore, the application of artificial intelligence (hereinafter – AI) in working with cadastral information is one of the relevant topics of the environmental and cadastral practice in Uzbekistan.

Analysis of the international Government Artificial Intelligence Readiness Index, conducted by Oxford Insights, shows that Uzbekistan is making great efforts in the field of implementation of artificial intelligence technologies. For example, ranking 158th among 160 countries in 2019, Uzbekistan ranked 95th in 2020, 93rd in 2021 and 79th in 2022[1]. Thus, the country's position in the application of artificial intelligence has improved almost twofold in five years. To a great extent, this is due to the application of artificial intelligence in the sphere of cadastre.

[1] Digitalization: Uzbekistan raises its international ranking. (2022, December 29). UZA. https://clck.ru/3CsERN

The publication of the UNESCO Recommendations on Ethical Aspects of Artificial Intelligence in 2021, as well as the adoption by the European Union of the world's first AI Act at the end of 2023, became an impetus for Uzbekistan to further improve the regulatory framework for the application of artificial intelligence technologies (Podshivalov, 2022; Sladić et al., 2020).

The application of artificial intelligence in the national cadastre is still fragmentary, which indicates its latent level. Practical application of artificial intelligence technologies is ahead of its legal regulation and is expressed in the form of 3D, 4D and 5D computer modeling.

In terms of practical results of 3D-models implementation, it is worth mentioning the creation of 3D-models for certain types of mineral resources, envisaged as early as in 2020 within the cadastre of deposits, mineral occurrences and technogenic mineral formations. Creation of 3D models of buildings and structures is widely practiced (Przewięźlikowska, 2020).

Based on the Administrative Regulations on state services on providing information on the history of a real estate (building), it is possible to obtain a certificate on the history of a real estate (building) directly at the State Services Center, or through the Unified Portal of Interactive State Services, or on the website davreestr.uz, which is the first experience of 4D-cadastre.

5D modeling is also successfully applied to such objects as industrial enterprises, boiler houses, logistics centers, shopping centers and other complex property units. In particular, the official website of the Cadastre Agency https://kadastr.uz/ru/kadastr-qiymatini-hisoblash provides a service for calculating the value of buildings based on a BIM model of the building.

However, artificial intelligence does not cover all types of state cadastres and its practical application is not supported by legal regulation.

1. State of legal regulation

1.1. State of the national legislation

The legal regulation of AI application in cadastre is related to the regulation of the legal status of artificial intelligence in general.

As for the general issues of legal regulation of artificial intelligence, Tables 1–3 analyze the fundamental directions of legislation. The national projects using artificial intelligence are funded through international financial institutions, grants, contractors' funds, international grants, Foreign Governmental Financial Organization and alliances.

Table 1. Law-making activity in the sphere of AI application

No.	Legal act	Presence
1	Law "On artificial intelligence"	no
2	Strategy for artificial intelligence development	no
3	National standards in the sphere of artificial intelligence application	no
4	Ethical code of using artificial intelligence	no
5	Special regime of using artificial intelligence technologies	yes

Table 2. Education in the sphere of artificial intelligence

Higher professional education		Post-university education	
special	juridical	special	juridical
231 quotas for Bachelor students, 14 quotas for Master students majoring in “Artificial intelligence” in six national universities	no	5 quotas for doctoral students and independent research in “Digital technologies and artificial intelligence”	no

Table 3. Information on mineral resources available in open access to implement projects in the sphere of artificial intelligence

Information on	Yes (+) / No (-)
climate and weather conditions	+
vegetation	-
water resources	+
animal world	-
land resources	+
forest resources	-
protected natural zones	-
mineral resources	-

In particular, fundamental and conceptual acts of legal regulation in this sphere are still not adopted, while the special regime of support for AI technologies is limited in time and applies only to residents of IT parks, which, in our opinion, limits the opportunities of other entities engaged in this sphere.

The organizational aspect of governance is limited only to the functioning of a state administrative body and a consulting structure, while there is no private sector participation in the field of AI governance. If we take into account that all over the world the main developers of AI are large private companies[2], then the future of AI application in Uzbekistan will also be concentrated in the hands of business entities. Consequently, their participation in the management of AI should also be regulated.

There is no regulation of teaching legal knowledge as part of the formation of specialized knowledge in the field of AI. Although Tashkent State University of Law (TSUL) is included in the list of universities that introduce training courses and subjects on the applied aspects of artificial intelligence technologies in the system of public administration, the target indicators for personnel training (bachelor’s, master’s and doctoral studies) in the field of AI application have not been developed. Insufficient attention to the development of general scientific activity is obvious against the background of the almost absent legal scientific activity.

[2] According to 2023 statistics, the world’s largest IT companies are Google, OpenAI, Microsoft, Huawei, Yandex, etc.

Financing of projects with AI is mainly carried out by extra-budgetary funds, with public funding present only in one new institution, the Alliance, which is a combination of finances of state bodies and business entities.

The composition of natural resource data that can be used in algorithms is also limited. Open cadastral information on land and water resources are now used in AI projects, while data on other natural resources are not available.

Analysis of the general legal norms shows that there is no regulation of such concepts as "3D plot", "3D property". All available cadastral information is related to 2D cadastre. The Land Code of the Republic of Uzbekistan states that "a land plot is a part of the land fund having a fixed boundary, area, location, legal regime and other characteristics reflected in the state land cadastre". At the same time, the concept of "land fund" is not defined, but only its constituent parts are listed[3]. The Law "On State Land Cadastre" does not define a land plot[4]. The Law "On Mineral Resources" defines mineral resources as a part of the earth's crust located below the soil, and in its absence – below the earth's surface or the bottom of water bodies, and extending to depths accessible for geological study and development, while a mining allotment is defined as a subsoil plot limited in area and depth[5]. Such objects as bridges, underground facilities, stadiums, engineering communication, tunnels are partially regulated and are the objects of separate cadastres. The Civil Code of the Republic of Uzbekistan understands immovable property as plots of land, subsoil areas, buildings, structures, perennial plantings and other property firmly connected with the land, i.e. objects which cannot be move without disproportionate damage to their purpose[6]. However, the concept of "vertical real estate" is not regulated in the Civil or Urban Planning Codes of the Republic of Uzbekistan[7].

1.2. International norms and their implementation into legislation

The main international norm, the implementation of which in the national legislation we consider appropriate, is the Recommendations on the Ethical Aspects of Artificial Intelligence (hereinafter – the Recommendations), which provide the main criteria for the use of AI today. The document began to be developed back in 2019 and was adopted in November 2021 by the UN General Conference on Education, Science and Culture (UNESCO). The purpose of adopting this document is to regulate the use of AI for peaceful purposes, directing it to serve for the benefit of man, society and the environment (Table 4).

3 The Land Code of the Republic of Uzbekistan. https://clck.ru/3CsFj2

4 The Law of the Republic of Uzbekistan "On State Land Cadastre". https://clck.ru/3CsFjX

5 The Law of the Republic of Uzbekistan "On Mineral Resources". https://clck.ru/3CsFkX

6 The Civil Code of the Republic of Uzbekistan. https://clck.ru/3CsFm9

7 The Urban Planning Codes of the Republic of Uzbekistan. https://clck.ru/3CsFms

Table 4. Ethical values and principles of artificial intelligence activities enshrined in the Recommendations on Ethical Aspects of AI

Values	Principles of activity
– Respect, protection and promotion of human rights and fundamental freedoms and human dignity; – well-being of the environment and ecosystems; – ensuring diversity and inclusion; – living in peaceful, just and interconnected communities	– Proportionality and non-harm; – safety and security; – fairness and non-discrimination; – sustainability; – right to privacy and data protection; – accountability and subordination to the individual; – transparency and explainability; – responsibility and accountability; – awareness and literacy; – multi-stakeholder and adaptive governance and engagement

The above attitudes and principles generally correspond to the fundamental principles of the national cadastral legislation.

Although this act is called Recommendations on Ethical Aspects of Artificial Intelligence, it also contains legal recommendations, which before the adoption of a separate law may serve as legal norms regulating AI use in the countries that have implemented it.

In particular, this document contains recommendations regarding legal liability, delineation of areas in which artificial intelligence can and cannot be used, mandatory control over artificial intelligence by humans, etc.

The use of AI in the sphere of environment and ecosystems, of which natural resource cadastres are an integral part, is an area that requires the adoption of strategic measures for the artificial intelligence application as recommended by the UNO.

Norms directly regulating the application of AI in the field of cadastre are absent in the national legislation.

Comparing the above norms with the Recommendations, we found that they lack some fundamental requirements (Table 5).

Table 5. Consequences related to the drawbacks of legal regulation

Lacking norms	Imbricated with
The concepts of “artificial intelligence” and “artificial intelligence life cycle” are not regulated	Artificial intelligence is identified with traditional objects of legal relations
Minimization of possible negative consequences of AI application	The obtained positive result is devalued, creating a threat to other people
Control of AI activity throughout its life cycle, including public control	Total domination of machines over humans
Limits of human responsibility in AI application	Violation of human rights and interests, when using AI, will remain unpunishable
Guaranteeing the interests of marginalized groups based on the digital divide at the national level	Creates a limited circle of subjects using AI
Mechanism of compensation for harm caused by the application of AI technologies	The right to compensation for material and moral damage will not be implemented
Soft governance system for AI applications	Lack of unified requirements in regulating the activities of AI developers
AI cannot have legal personality	Claims to AI as an independent subject of law, a subject of private and public law

Thus, the above analysis shows that the fundamental principles and guidelines in the sphere of application of AI technologies in Uzbekistan cadastral legislation are partially regulated at present. It should be noted that some provisions of the Recommendations are already in force in the studied area of legislation.

In particular, this concerns the establishment of a transparent system of coordination with private legal entities having publicly significant information. Such a system is in place in the Law "On Environmental Audit"[8], according to which the conclusions of environmental audit are not disclosed without the client's consent.

1.3. Advanced foreign practices

Based on the foreign practice of legal regulation of the use of artificial intelligence in cadastre, the following trends in the use of 3D cadastre can be identified:

– the existence of a separate law regulating the use of 3D cadastre. For example, in China there is a separate law on 3D cadastre, which registers buildings and structures along with land plots that are in exclusive state ownership;

– absence of a separate law, with amendments and additions to the existing legislation regulating the legal status of 3D cadastres. Such countries include Australia (Queensland), Hungary, Sweden, the Netherlands, Poland, Turkey, etc. This system is very flexible, as it is based on the use of land plot boundaries within a two-dimensional cadastre to form information on the 3D cadastre object. At the same time, this system has some disadvantages. For example, when information on an object within the 3D cadastre is formed, information on several land plots within the 2D cadastre is used. This practice may fail in the future, when the issue of legal recognition of 3D cadastres arises;

– the inadmissibility of using 3D cadastre under current legislation, despite its widespread use in practice. In Greece and Cyprus, the use of 3D cadastre is contrary to the Civil Code.

The birthplace of using artificial intelligence in cadastre is Australia. In 1997, it was one of the first countries in the world to introduce 3D modeling in the sphere of real estate cadastre. Therefore, 3D cadastre information is valid equally with 2D and 4D cadastre information. Paper-based cadastral information operates in parallel with electronic information, with the former being characterized by too much detail, whereas 3D is a simple graphical representation. Thus, paper-based and digital cadastral information complement each other. All types of property rights can be registered in both 3D and 2D cadastres. In addition, objects of 3D modeling are distinguished separately: bridges, underground facilities, parking easements, lease agreements, utility networks, pipelines, stadiums and others. A 3D plot may be subject to a lien just like a regular plot, despite the fact that 3D cadastral information is not the final truth in the cadastre.

[8] The Law of the Republic of Uzbekistan "On Environmental Audit". https://clck.ru/3CsGZk

The legislation of Argentina does not regulate the legal status of 3D cadastre, despite its widespread use in practice. In Austria, for all the desire to fully switch to 3D cadastre, digitalization of cadastre is not fully implemented. In Bulgaria there is a partial application of 3D modeling, so, while in Sofia 3D cadastre is considered necessary, in other cities of the country it is not the main source of information. At the same time, the legislation does not regulate its legal status. The Canadian cadastre is characterized by daily updating of cadastral maps, books, and reports, although in fact it is a multi-purpose cadastre; there is no separate law on 3D cadastre, but objects of 3D cadastre are separately regulated.

2. Uzbekistan's experience of applying artificial intelligence

2.1. Normative-legal framework

The absence of a law on the use of artificial intelligence in Uzbekistan is compensated by a limited legal regulation – the Special Regime for the Support of Artificial Intelligence Technologies and the Order of its Functioning, which refers to the order of legal regulation of testing based on artificial intelligence technology, the creation of organizational and legal conditions for legal entities and scientific organizations, the creation of favorable conditions in legal relations during the activities related to developing software and rendering services, testing software and introducing them as part of "smart" regulation[9]. The Regime is a part of the Technological Park of software products and information technologies.

The working body of the Special Regime is the Ministry of Information Technologies and Communications Development of the Republic of Uzbekistan. The tasks of the working body include the following:

– to approve the application form and the list of necessary information to be submitted by applicants for the status of the Special Regime participant, and to organize the reception of applications;

– to approve the charter of the Special Regime Expert Council, as well as the form of the agreement on the terms of functioning to be signed by its participants;

– to form and approve the composition of the Special Regime Expert Council together with interested ministries and agencies;

– to submit proposals on inclusion and exclusion of criminals from the Special Regime to be considered by the Coordination Commission;

– to engage personnel of the Research Institute for the Digital Technologies and Artificial Intelligence Development to monitor the scientific activities of the Special Regime participants;

– to provide organizational, legal and advisory support during the implementation of pilot projects of the Special Regime participants;

[9] Housing Code of the Republic of Uzbekistan. https://clck.ru/3CsGch

– based on the conclusion of the Coordination Commission, to make a decision on granting, rejecting or depriving the project initiators of the status of a Special Regime participant;

– to submit an annual official report to the relevant ministries and departments on the projects successfully implemented by Special Regime participants.

Uzbekistan maintains a special Unified Register of Special Regime Participants, which contains publicly available and open information on legal entities and scientific organizations that are the Special Regime participants – residents of IT parks. To become a Special Regime participant, an application should be submitted to the Coordination Commission.

The legal status of the Special Regime participants is very specific, as the Regulation stipulates only their duties. The rights of the participants are set forth in a bilateral agreement between the Coordination Commission and the participant. The Regulation provides great preferences and benefits to the Special Regime participants. In particular, the funds spent on professional development and retraining of personnel are compensated; the right is granted to receive information and documents necessary for the pilot projects implementation (except for information containing state secrets and other confidential information protected by law), as well as personal information from ministries, departments and organizations; the list of documents necessary for obtaining the relevant permissive documents is reduced by the relevant state body; the fee for obtaining the relevant permissive documents is reduced twofold; a minimum of requirements and conditions for operation is set by the relevant state body.

At the same time, the Regulation enshrines seven reasons for deprivation of the status of a Special Regime participant (e.g., failure to fulfill contractual relations with the working body, recognition of a legal entity bankrupt, provision of unreliable information, non-compliance of the activities of a Special Regime participant with the types of activities specified in the project). This list is not exhaustive, as the legislator leaves also other reasons stipulated by law.

However, this document cannot be called ideal, as it contains a number of provisions that contradict the legislation:

– first, the refusal to register a Special Regime participant in case of taxes and other mandatory payments contradicts the legislation on entrepreneurial activity;

– second, the absence of a final list of reasons for deprivation of the status of a Special Regime participant creates grounds for corruption;

– third, the regime of issuing conclusions on obtaining the status of a Special Regime participant is non-transparent.

2.2. Literature review

In the scientific literature there is no unified approach to the definition of AI. For example, scientists from Uzbekistan S. Gulyamov and I. Rustambekov defined AI as a large area of scientific and applied research[10].

Andreas Kaplan and Michael Haenlein (2019) wrote that artificial intelligence is "a system's ability to correctly interpret external data, to learn from such data, and to use those learnings to achieve specific goals and tasks through flexible adaptation".

Elaine Rich and Kevin Knight (1991) define AI as a kind of science that teaches computers to perform functions of humans that give them superiority over them. Ronal Chandra and Yoga Prihastomo (2012) distinguish AI as a type of intelligent software.

An important part of using artificial intelligence is the problem of liability. In this regard, it is interesting to consider the position of an Uzbekistan researcher S. S. Bozarov. He considered approaches to the legal liability of artificial intelligence, like equating the artificial intelligence objects to legal entities or objects of increased public danger, and proposed as a solution the need to establish proprietary (limited) rights to AI[11].

EU researchers comprehensively studied the issues of artificial intelligence application in 3D and 4D cadastres. For example, I. Williamson (1997) substantiated the necessity of transition to 3D cadastre. S. Hendriatiningsihs et al. (2007) proposed a hybrid version of 3D cadastre combining the main provisions of 2D cadastre with 3D modeling. Mohamed El-Mekawy et al. (2014) highlighted the main advantages of 3D cadastre.

A separate issue is the study of legal regulation of the use of 3D cadastre data as an object of artificial intelligence. Given the presence of different practices, there is still no unified approach to this issue.

In particular, one group of scientists proposed to regulate the AI use in the form of a 3D cadastre object concept, a separate regulatory act, or in the form of systematization of norms related to the AI use (Stoter & Zevenbergen, 2001; Karki et al., 2011).

Another group puts forward the idea of restrictive regulation (Sandberg, 2001; Stoter & Ploeger, 2003; Tan & Hussin, 2012). Other scholars considers the legal status of 3D cadastre as a result of interaction between public and private law (Navratil, 2012). Still others adhere to the position of common property law (Paulsson, 2012).

The most prominent proponents of legal regulation of 3D cadastre use – P. Van Oosterom, J. Stoter, H. Ploeger, R. Thompson, and S. Karki – propose to recognize 3D

[10] Gulyamov, S., Rustambekov, I. (2021, March 2). Artificial intelligence – the modern requirement in the development of society and state. Pravda Vostoka, 43(29547).

[11] Bozarov, S. S. (2023). Legal liability in the framework of artificial intelligence: Abstract of Dr. Sci. (Philosophy) thesis. Tashkent: TSUL.

cadastre as an independent right on a par with such rights as to own, use and dispose (Van Oosterom et al., 2011).

Fatih Do¨nera et al. (2011) consider the problems of registration of utilities in the cadastre in four dimensions on the example of legislation of three countries in terms of legal, organizational and technical cadastral requirements, based on a prototype from the Netherlands, and substantiate its prospects.

Peter Van Oosterom and co-authors (2006), justifying the advantages of 4D-cadastre in the Australian and Dutch practice, analyze legal aspects of registration of temporary land titles within the framework of Eigentum, droit de propriété and their security guarantees, as well as the consequences of selling real estate to several persons at the same time, validity of the time scale of a timeshare cadastre object based on the Queensland Code requirements.

The advantages of artificial intelligence over traditional technologies in the field of cadastre do not require proving; they are obvious.

The current stage of economic reforms necessitates the transition to the use of more sophisticated AI systems (e.g. neural networks) in the national cadastre. The reason is that the functioning 2D cadastral model in Uzbekistan does not meet the needs of the digital green economy, which is being formed in the country.

Factors contributing to the use of artificial intelligence in cadastres include:

– modern national cadastres of natural resources are systems of geographic information due to full-fledged application of GIS technologies. An electronic map of land plots has been created on their basis;

– in 2017, Uzbekistan switched to international standards in the field of geodesy – the World Geodetic System (WGS-84), which is an Earth-bound global reference system, including the Earth model, defined by a set of basic and auxiliary parameters. Previously, Uzbekistan used the 1942 Coordinate System (SK-42), inherited from the socialist system of economic management, which allows obtaining data on objects with an error of 2 cm;

– there is an intensive growth of urbanization in the country, including the expansion of urban areas with complex infrastructure, construction of high-rise buildings and underground facilities (tunnels, underground networks and infrastructure facilities), dense developments with complex structures and infill developments. All this happens against the background of limited area of settlements and the growth of demographic processes that strengthen the demand for real estate. In particular, Article 42 of the Housing Code of the Republic of Uzbekistan established the social norm of housing per person not less than 16 square meters, and for wheelchair users – not less than 23 square meters[12]. According to forecasts, the country's population is expected to grow to 40 million by 2030[13], compared

[12] In the nearest years the population of Uzbekistan will reach 40 mln people. (2023, 9 November). Daryo. https://clck.ru/3CsGsn

[13] Tasks for the efficient use of land resources have been identified. (2023, 21 November). Official website of the President of the Republic of Uzbekistan. https://clck.ru/3CsGxD

to the current figure of about 37 million. This means that the need for housing will grow. Therefore, land plots of other categories will be utilized by changing their category, which, in turn, will affect the credibility of the entire land fund.

At the same time, we can identify a number of factors that significantly hinder the implementation of artificial intelligence technologies. Let us dwell upon some of them.

First, the formation of natural resource cadastres is incomplete. For example, in 2023, 460 thousand hectares of land, more than 900 thousand hectares of agricultural land, as well as land along canals and collectors, near natural lakes and rivers, were not included in the cadastre and their legal status was not determined[14]. Taking into account that artificial intelligence can only process the data algorithms that were set by a human, the prepared content will also be incomplete in case of incomplete algorithms. Hence, the result presented by the artificial intelligence will be unreliable. The question arises as to the feasibility of using artificial intelligence under such conditions. That is why the cadastre completeness should be the main condition for the artificial intelligence application.

Second, the old technological base does not meet the needs of the digital economy. While there is a global trend to abandon cadastral mapping, we still use such technologies of cadastral information collection as topographic-geodetic, cartographic, soil science, agrochemical and geobotanical surveys. Uzbekistan still does not have its own space observation satellite, but has to rent foreign ones. Major shifts in this direction started in 2023. In particular, 600 Matrice drones and various software were purchased; funds were allocated to upgrade existing drones; airplanes for aerial surveys were purchased, and the purchase of 80 stations for satellite surveillance is planned for this year. However, this is not enough to form a complete and reliable cadastre.

Third, Uzbekistan did not participate in the Cadastr-2014 project and does not participate in the Cadastr-2034 project, which directly provide for the artificial intelligence application in the form of 3D and 4D cadastre.

Fourth, the mechanism of formation of legal knowledge in the field of artificial intelligence technologies is still unsettled. At present, five higher educational institutions of the country (Tashkent University of Information Technologies named after Muhammad al-Khorazmiy, National University of Uzbekistan named after Mirzo Ulugbek, Tashkent State Technical University named after Islam Karimov, Samarkand State University named after Sharaf Rashidov, and Research Institute for the Development of Digital Technologies and Artificial Intelligence) train specialists in the field of “Artificial Intelligence”. However, training specialists in the field of AI legal regulation has not been considered yet. Tashkent State Law University, the basic educational institution in the field of jurisprudence, is included in the list of universities where disciplines on AI application in public administration are

[14] Decree of the President of the Republic of Uzbekistan No. PP-4996 dated February 17, 2021. https://clck.ru/3CsGzX

taught[15]. However, the training of specialists in the field of legal regulation of AI application is still not been established.

Fifth, the state of scientific activity is unsatisfactory. To date, the country has no scientific research in the field of legal regulation of activities using AI in the cadastral sphere. Today, Uzbekistan does not belong to the countries with a high level of development of artificial intelligence technologies; however, the application of artificial intelligence is quite in demand in the field of cadastre. This, in turn, requires active and in-depth research of legal problems of regulating the AI application in cadastre in parallel with specialist training.

Sixth, the state is rather passive in financing projects in AI application. To date, AI projects financing is carried out mainly by non-state (developer) funds, or by pooling the capital of large state-owned entities with businesses (Alliance).

Seventh, there is a lack of international standards implementation in this sphere. The fundamental UNESCO Recommendations on the Ethical Aspects of Artificial Intelligence, adopted in 2021, has not been implemented yet.

In our opinion, the use of artificial intelligence in the sphere of cadastre will help to solve a number of existing problems.

First, it will help to raise the national cadastre to the international level. In all developed countries, as well as in many developing countries, the cadastre is the main source of information in ensuring the inviolability of private property.

Second, it will increase the prestige of the cadastre as the main reliable legal source to guarantee the right of real estate ownership. In foreign countries the prestige of the cadastre is high due to its reliability and accuracy. This cannot be said about the cadastre in Uzbekistan, which is not fully formed even on the threshold of the second quarter of the 21st century.

Third, it will significantly reduce the level of corruption and the possibility of making "cadastral" errors, because the human factor will be excluded from the formation and provision of cadastral information.

Fourth, it will significantly reduce the time of decision-making. Introduction of AI technologies will allow processing and updating big cadastral data quickly and will high quality. This will make it possible to receive and change information online. In addition, it will help to avoid unjustified costs for inefficient technical means of collecting and processing of cadastral information and will significantly reduce the time for forming the required content.

Thus, the introduction of artificial intelligence in cadastre will contribute to obtaining reliable data and results with complete and reliable information available. This will also contribute to increasing the prestige of cadastre.

---

[15] Constitution of the Republic of Uzbekistan. https://clck.ru/3CsH5i

Conclusions

The use of artificial intelligence as the next stage of information automation can be viewed as the future of the entire national cadastral system.

On the agenda in Uzbekistan is the development of the Strategy of Artificial Intelligence Development, which should have been adopted as early as 2022. This act should contain a state program to support scientific research and innovative projects in the field of artificial intelligence, formation of a large amount of digital data in the state language, creation of modern high-tech infrastructure and hardware complexes to solve the problems of artificial intelligence, training of personnel, as well as improving the system of control and risk prevention in the sphere of artificial intelligence.

At the same time, we consider it advisable to include the following issues in this document:

1. Basic theoretical concepts (including the concepts of "artificial intelligence", "artificial intelligence life cycle" and "artificial intelligence developer").

2. Legal status of artificial intelligence. To date, in our opinion, it is too early to speak about artificial intelligence as an independent object or subject of national law. It is reasonable to consider the joint responsibility of the artificial intelligence developer and the algorithms owner.

3. Compulsory licensing of activities with the use of artificial intelligence. Currently, the Coordination Commission[16] gives its opinion on the results of studying the submitted documents of applicants to be IT-park participants.

4. Development of a system of ethical principles of AI application in accordance with international and constitutional norms.

5. Legislative stipulation of a certain limit of obligatory financial state support of AI application in cadastre. Direct financing from the state budget of this sphere, in our opinion, would clearly express the state's interest in the wide application of AI. At present, the state supports this sphere by granting privileges and preferences, free use of buildings, compensation of personnel training costs, etc. The state supports this sphere by granting privileges and preferences, free use of buildings, compensation of personnel training costs, etc.

6. We propose to include Melbourne University (Australia) in the list of foreign research and higher educational institutions in the field of cadastre. This is a world's leading university in studying the legal regulation of 3D, 4D and 5D cadastres.

7. We propose to consider the issue of Uzbekistan joining the global Cadastr-2034 project. This will help to form a systematic approach in the use of AI through the formation of 3D, 4D and 5D cadastres.

[16] Coordination Commission for the implementation of the "Digital Uzbekistan - 2030" strategy, approved by the Decree of the President of the Republic of Uzbekistan No. PF-6079 of October 5, 2020.

Artificial intelligence for the national cadastre is as necessary as air. Currently, we see attempts to adapt the old cadastre to the needs of the new economy – digital green economy, which needs reliable information about the state of natural resources. Reforming the management of the national cadastre, namely, the creation of a special body – the Cadastre Agency, was a turning point for the national cadastre in terms of updating the technological base of this activity. In Uzbekistan, a certain base for application of artificial intelligence has already been formed, which shows in the functioning of geographic information systems, digital electronic maps and systems for cadastre objects assessment. A promising area for the national cadastre is the use of artificial intelligence for registering real estate rights, as well as for document recognition. Nevertheless, the practical application of artificial intelligence in the cadastre is ahead of its legal regulation, which creates ambiguities in recognizing it as an official source of cadastral information.

References

Ameyaw, P. D., & De Vries, W. T. (2023). Blockchain technology adaptation for land administration services: The importance of socio-cultural elements. *Land Use Policy*, *125*, 106485. https://doi.org/10.1016/j.landusepol.2022.106485

Chandra, R., & Prihastomo, Y. (2012). *Artificial Intelligence Definition: A Review*. https://doi.org/10.22541/au.164670471.11415616/v1

Do¨nera, F., Thompson, R., Stoterd, J., Lemmenc, Ch., Ploegerd, H., van Oosterom, P., & Zlatanova, S. (2011). Solutions for 4D cadastre – with a case study on utility networks. *International Journal of Geographical Information Science*, *25*(7), 1173–1189. https://doi.org/10.1080/13658816.2010.520272

El Mekawy, M., Paasch, J., & Paulsson, J. (2014). Integration of 3D Cadastre, 3D Property Formation and BIM in Sweden. In *4th International Workshop on 3D Cadastres*, Dubai, United Arab Emirates (pp. 17–34).

Hendriatiningsihs, S., Soemarto, I., Laksono, B. E., Kurniawan, I., Dewi, N. K., & Soegito, N. (2007). Identification of 3-Dimensional Cadastre Model for Indonesian Purpose. In *Strategic Integration of Surveying Services FIG Working Week 2007*, Hong Kong SAR, China.

Kaplan, A., & Haenlein, M. (2019). Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. *Business Horizons*, *62*(1), 15–25. https://doi.org/10.1016/j.bushor.2018.08.004

Karki, S., Thompson, R., McDougall, K., Cumerford, N., & van Oosterom, P. (2011). ISO land administration domain model and LandXML in the development of digital survey plan lodgement for 3D cadastre in Australia. In *Proceedings of the 2nd International Workshop on 3D Cadastres*, Delft, the Netherlands (pp. 65–84).

Navratil, G. (2012). Combining 3D cadastre and public law – an Austrian perspective. In *3rd International Workshop on 3D Cadastres: Developments and Practices*, 25–26 October 2012, Shenzhen, China (pp. 61–72).

Paulsson, J. (2012). Swedish 3D property in an international comparison. In *3rd International Workshop on 3D Cadastres: Developments and Practices*, 25–26 October 2012, Shenzhen, China (pp. 23–40).

Podshivalov, T. P. (2022). Improving implementation of the Blockchain technology in real estate registration. *Journal of High Technology Management Research*, *33*(2), 100440. https://doi.org/10.1016/j.hitech.2022.100440

Przewięźlikowska, A. (2020). Legal aspects of synchronising data on real property location in polish cadastre and land and mortgage register. *Land Use Policy*, *95*, 104606. https://doi.org/10.1016/j.landusepol.2020.104606

Rich, E., & Knight, K. (1991). *Artificial Intelligence*. New York: McGraw-Hill.

Sandberg, H. (2001). Three-dimensional division and registration of title to land: Legal aspects. In *Proceedings of the International Workshop on 3D Cadastres*, 2001, Delft (pp. 201–209).

Sladić, D., Radulović, A., & Govedarica, M. (2020). Development of process model for Serbian cadastre. *Land Use Policy*, *98*, 104273. https://doi.org/10.1016/j.landusepol.2019.104273

Stoter, J., & Ploeger, H. (2003). Registration of 3D objects crossing parcel boundaries. In *Proceedings of 2003 FIG Working Week, Paris, France*, April 13–17, 2003.

Stoter, J., & Zevenbergen, J. (2001). Changes in the definition of property: A consideration for a 3D cadastral registration system. In *Proceedings of the FIG Working Week*, Seoul.

Tan, L. C., & Hussin, K. B. (2012). Establishing 3D Property Rights in Malaysia. In *Proceedings of the 2012 FIG Working Week, Knowing To Manage The Territory, Protect The Environment, Evaluate The Cultural Heritage*, Rome, Italy, 6–10 May 2012 (pp. 1–24).

Van Oosterom, P., Ploeger, H., Stoter, J., Thompson, R., & Lemmen, Ch. (2006). Aspects of a 4D Cadaster: a first exploration. In *XXIII FIG Congress*, Munich, Germany.

Van Oosterom, P., Stoter, J., Ploeger, H., Thompson, R., & Karki, S. (2011). World-wide inventory of the status of 3D Cadastres in 2010 and expectations for 2014. In *Proceedings of the 2011 FIG Working Week, Bridging the Gap between Cultures*, Marrakech, Morocco.

Williamson, I. P., (1997). Strategic Management of Cadastral Reform – Institutional Issues. In *FIG Commission 7 Symposium on Cadastral Systems in Developing Countries*, Penang, Malaysia.

Author information

Robiya S. Toshboyeva – Dr. Sci. (Law), Associate Professor, Department of Business Law, Tashkent State University of Law
Address: 35 Sayilgokh Str., 100047 Tashkent, Uzbekistan
E-mail: robiyatoshboeva@gmail.com
ORCID ID: https://orcid.org/0000-0003-2898-2109
Google Scholar ID: https://scholar.google.com/citations?user=OXu7SxQAAAAJ

Conflict of interests

The author declare no conflict of interests.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – April 14, 2024
Date of approval – April 25, 2024
Date of acceptance – September 25, 2024
Date of online placement – September 30, 2024

Научная статья
УДК 34:004:349.4:004.8:528
EDN: https://elibrary.ru/blqkuz
DOI: https://doi.org/10.21202/jdtl.2024.28

Цифровые технологии в национальной кадастровой системе Узбекистана: проблемы правового регулирования

Робия Собировна Тошбоева

Ташкентский государственный юридический университет, Ташкент, Узбекистан

Ключевые слова

государственный кадастр,
искусственный интеллект,
кадастровая информация,
национальное законодательство,
право,
правовое регулирование,
специальный правовой режим,
Узбекистан,
цифровые технологии,
этика

Аннотация

Цель: проведение критического анализа состояния национального законодательства Узбекистана на предмет правового регулирования цифровизации и использования искусственного интеллекта в кадастровой сфере.

Методы: основу проведенного исследования составляют такие методы научного познания, как формально-юридический и сравнительно-правовой анализ, индукция и дедукция.

Результаты: проанализированы положения, которые регламентируют цифровизацию и применение искусственного интеллекта в кадастровой сфере, выявлены правовые пробелы. Определено, что практическое применение технологий искусственного интеллекта опережает его правовое регулирование. Отмечаются недостатки правового регулирование в указанной сфере (отсутствие легальной дефиниции и определения правового статуса искусственного интеллекта в национальном законодательстве, регламентация участия субъектов предпринимательской деятельности в управлении искусственным интеллектом и др.), что затягивает процесс его полноценного применения и уравнения наряду с традиционными источниками кадастровой информации. Обоснована необходимость всеобщей оцифровки национального кадастра. Спрогнозирована возможность более широкого применения искусственного интеллекта в природно-ресурсной кадастровой системе. Утверждается, что существующая система в ее текущем состоянии в последующем будет приводить к принятию неправильных решений и появлению кадастровых ошибок, в связи с чем необходимо совершенствование правового регулирования в сфере кадастра.

Научная новизна: впервые представлена оценка итогов оцифровки национального кадастра и даны прогнозы о возможности применения искусственного интеллекта в данной сфере при условии дальнейшего совершенствования правового регулирования, которое имеет принципиальное значение для реформирования кадастровой системы, поскольку технологическая основа указанной системы не в полной мере отвечает потребностям цифровой экономики.

Практическая значимость: обусловлена отсутствием правовой регламентации понятия и правового статуса искусственного интеллекта в национальном законодательстве, а также единого подхода к цифровизации кадастровой системы. Современные технологии активно применяются на практике, однако не имеют под собой достаточной правовой основы. Основные выводы, предложения и рекомендации по теме исследования могут служить основой для дальнейшего совершенствования нормативно-правовой базы Узбекистана в части применения технологий искусственного интеллекта.

Для цитирования

Тошбоева, Р. С. (2024). Цифровые технологии в национальной кадастровой системе Узбекистана: проблемы правового регулирования. *Journal of Digital Technologies and Law*, *2*(3), 544–564. https://doi.org/10.21202/jdtl.2024.28

Список литературы

Ameyaw, P. D., & De Vries, W. T. (2023). Blockchain technology adaptation for land administration services: The importance of socio-cultural elements. *Land Use Policy*, *125*, 106485. https://doi.org/10.1016/j.landusepol.2022.106485

Chandra, R., & Prihastomo, Y. (2012). *Artificial Intelligence Definition: A Review*. https://doi.org/10.22541/au.164670471.11415616/v1

Do¨nera, F., Thompson, R., Stoterd, J., Lemmenc, Ch., Ploegerd, H., van Oosterom, P., & Zlatanova, S. (2011). Solutions for 4D cadastre – with a case study on utility networks. *International Journal of Geographical Information Science*, *25*(7), 1173–1189. https://doi.org/10.1080/13658816.2010.520272

El Mekawy, M., Paasch, J., & Paulsson, J. (2014). Integration of 3D Cadastre, 3D Property Formation and BIM in Sweden. In *4th International Workshop on 3D Cadastres*, Dubai, United Arab Emirates (pp. 17–34).

Hendriatiningsihs, S., Soemarto, I., Laksono, B. E., Kurniawan, I., Dewi, N. K., & Soegito, N. (2007). Identification of 3-Dimensional Cadastre Model for Indonesian Purpose. In *Strategic Integration of Surveying Services FIG Working Week 2007*, Hong Kong SAR, China.

Kaplan, A., & Haenlein, M. (2019). Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. *Business Horizons*, *62*(1), 15–25. https://doi.org/10.1016/j.bushor.2018.08.004

Karki, S., Thompson, R., McDougall, K., Cumerford, N., & van Oosterom, P. (2011). ISO land administration domain model and LandXML in the development of digital survey plan lodgement for 3D cadastre in Australia. In *Proceedings of the 2nd International Workshop on 3D Cadastres*, Delft, the Netherlands (pp. 65–84).

Navratil, G. (2012). Combining 3D cadastre and public law – an Austrian perspective. In *3rd International Workshop on 3D Cadastres: Developments and Practices*, 25–26 October 2012, Shenzhen, China (pp. 61–72).

Paulsson, J. (2012). Swedish 3D property in an international comparison. In *3rd International Workshop on 3D Cadastres: Developments and Practices*, 25–26 October 2012, Shenzhen, China (pp. 23–40).

Podshivalov, T. P. (2022). Improving implementation of the Blockchain technology in real estate registration. *Journal of High Technology Management Research*, *33*(2), 100440. https://doi.org/10.1016/j.hitech.2022.100440

Przewięźlikowska, A. (2020). Legal aspects of synchronising data on real property location in polish cadastre and land and mortgage register. *Land Use Policy*, *95*, 104606. https://doi.org/10.1016/j.landusepol.2020.104606

Rich, E., & Knight, K. (1991). *Artificial Intelligence*. New York: McGraw-Hill.

Sandberg, H. (2001). Three-dimensional division and registration of title to land: Legal aspects. In *Proceedings of the International Workshop on 3D Cadastres*, 2001, Delft (pp. 201–209).

Sladić, D., Radulović, A., & Govedarica, M. (2020). Development of process model for Serbian cadastre. *Land Use Policy*, *98*, 104273. https://doi.org/10.1016/j.landusepol.2019.104273

Stoter, J., & Ploeger, H. (2003). Registration of 3D objects crossing parcel boundaries. In *Proceedings of 2003 FIG Working Week, Paris, France*, April 13–17, 2003.

Stoter, J., & Zevenbergen, J. (2001). Changes in the definition of property: A consideration for a 3D cadastral registration system. In *Proceedings of the FIG Working Week*, Seoul.

Tan, L. C., & Hussin, K. B. (2012). Establishing 3D Property Rights in Malaysia. In *Proceedings of the 2012 FIG Working Week, Knowing To Manage The Territory, Protect The Environment, Evaluate The Cultural Heritage*, Rome, Italy, 6–10 May 2012 (pp. 1–24).

Van Oosterom, P., Ploeger, H., Stoter, J., Thompson, R., & Lemmen, Ch. (2006). Aspects of a 4D Cadaster: a first exploration. In *XXIII FIG Congress*, Munich, Germany.

Van Oosterom, P., Stoter, J., Ploeger, H., Thompson, R., & Karki, S. (2011). World-wide inventory of the status of 3D Cadastres in 2010 and expectations for 2014. In *Proceedings of the 2011 FIG Working Week, Bridging the Gap between Cultures*, Marrakech, Morocco.

Williamson, I. P., (1997). Strategic Management of Cadastral Reform – Institutional Issues. In *FIG Commission 7 Symposium on Cadastral Systems in Developing Countries*, Penang, Malaysia.

Сведения об авторе

Тошбоева Робия Собировна – доктор юридических наук, доцент, доцент кафедры бизнес-права, Ташкентский государственный юридический университет
Адрес: 100047, Узбекистан, г. Ташкент, ул. Сайилгох, 35
E-mail: robiyatoshboeva@gmail.com
ORCID ID: https://orcid.org/0000-0003-2898-2109
Google Scholar ID: https://scholar.google.com/citations?user=OXu7SxQAAAAJ

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.91 / Государство и право отдельных стран
Специальность ВАК: 5.1.2 / Публично-правовые (государственно-правовые) науки

История статьи

Дата поступления – 14 апреля 2024 г.
Дата одобрения после рецензирования – 25 апреля 2024 г.
Дата принятия к опубликованию – 25 сентября 2024 г.
Дата онлайн-размещения – 30 сентября 2024 г.

Research article
UDC 34:004:347.211:004.8
EDN: https://elibrary.ru/mloxmi
DOI: https://doi.org/10.21202/jdtl.2024.29

Overcoming the Friction between the "Right to be Forgotten" and Blockchain Technology through a New Approach

Fabio Severino

Traent SRL, Pisa, Italy

Ludovica Sposini ✉

Sant'Anna School of Advanced Studies, Pisa, Italy

Keywords

digital technologies,
European Union,
General Data Protection Regulation,
Hybrid blockchain,
law,
Legislation,
Personal data protection,
private blockchain,
public blockchain,
right to be forgotten

Abstract

Objective: this paper explores the challenges arising from the conflict between blockchain technology and the "right to be forgotten" as provided by the European data protection framework.

Methods: in the First Section, the author provides a brief description of the evolution of blockchain technology and the most pressing issues between traditional blockchain models and UE's legislations. Among the latter, the author analyzes the specific issue concerning the clash between the traditional blockchains (both private and public models), typically immutable, and the individual's right to cancellation or modification of own personal data. This section emphasizes the importance of personal data protection, which has always been one of the main tasks for supranational legislators. The legal regulation of data protection and the relevant judicial practice of the European Court of Human Rights is analyzed. The author raises the problem of expressing the free self-determination of an individual in the form of controlling their personal data on the Internet. The Second Section of this contribution is dedicated to the study of probable ways to solve the existing incompatibility and to make the distributed ledger system compatible with the European data protection legislation. An emphasis is made on the model provided by "Traent" company, which ensures the right to data cancellation or modification. The capability of this model to solve the said contradiction is analyzed.

✉ Corresponding author

Results: the study delves into the peculiar features of the new model to understand how it strategically utilizes the advantages of public and private blockchains guaranteeing not only the validity and authenticity of the chain where the transaction was performed, but, most importantly, the modification and granular cancellation of client's personal data. This innovative solution offers a potential path forward for navigating the complex intersection of data privacy and blockchain innovation in the European context.

Scientific novelty: Traent has implemented a "hybrid" model blockchain that, incorporating both public and private components, to achieve an effective compliance with the European Union regulations, especially those concerning data protection and privacy.

Practical significance: the obtained conclusions and proposals can be taken into consideration in improving the compliance of blockchain technologies with the European Union General Data Protection Regulation.

For citation

Severino, F., & Sposini, L. (2024). Overcoming the Friction between the "Right to be Forgotten" and Blockchain Technology through a New Approach. *Journal of Digital Technologies and Law, 2*(3), 565–584. https://doi.org/10.21202/jdtl.2024.29

Contents

Introduction

2008 represents a turning point in the era of the so-called "Digital Revolution" as it saw the publication of Satoshi Nakamoto's article entitled "Bitcoin: A Peer-to-Peer Electronic Cash System"[1]. The latter was part of the "cypherpunk" movement, which, in order to oppose the

[1] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. https://clck.ru/3EGDkg

restrictions on individual freedoms and, in particular, on the right to privacy resulting from the new technologies, had identified bitcoin as a useful tool for this purpose: an electronic currency that would make use of cryptographic technologies on a large scale and that would make it possible to create exchange systems (goods, services and, above all, information) that were secure and respectful of irrefutable.

Nakamoto proposed the creation of a communication protocol, i.e. an immutable ledger organised into separate "blocks", each of which contains one or more transactions. These were linked together to form a chain, hence the name "blockchain". Each block had a "header" within which was contained the hash, an alphanumeric string, of all transactions recorded in that block; the time stamp and the hash of the previous block.

This technology utilised various technologies including: i) asymmetric key encryption which allows verification of the paternity of messages as well as its integrity; ii) the peer-to-peer system which has the advantage of eliminating the need for a central authority to validate transactions; iii) the "proof of work", a consensus-building mechanism based on the use of computational resources to solve a mathematical problem. In short, the node that first manages to propagate the correct solution to the rest of the network receives reward for the service rendered. At the same time, the system is sure of the correctness of this result precisely because a large number of resources had to be used to arrive at it[2].

It was based, then, on a network of computers sharing between them a distributed register containing a copy of all transactions made on the chain. In this way, it was possible to guarantee, on the one hand, a secure registration system since it would be very hard to rewrite all the blocks; on the other hand, it was transparent because each time a new transaction was made, it was recorded on each "copy" of the distributed register. This meant that each participant could verify the transactions and have access to the data without the necessary presence of a centralised higher entity. On the contrary, it redistributed validation power among users in substantially equal parts, contributing to the creation of an effectively transparent and, above all, more democratic system[3]. This technology, which was originally created for the exchange of cryptocurrencies, has, thanks to

[2] It should be noted that this is only one of many consensus mechanisms that have been developed, including: i) the so-called "Proof of Stake" (PoS) according to which the possibility of validating transactions is directly proportional to the amount of assets that node possesses; ii) the "Delegated Proof of Stake" which is based on a sort of vote whereby each user who possesses assets in the system can delegate the validation of the transaction to another; iii) the "Deposit-based consensus" whereby in order to add a blockchain block it is necessary to first make a binding deposit; iv) the "Proof of Existence" whereby only those with specific authorisations or documents can validate; v) "Proof of Authority" (PoA) whereby authorisation to validate transactions is granted solely on the basis of the identity of the node itself. For a comprehensive explanation of each mechanism, see (Sarzana & Nicotra, 2018).

[3] European Parliament. (2017). How blockchain technology could change our lives – In-depth analysis, where it is said that: "Blockchains shift some control over daily interactions with technology away from central elites, redistributing it among users. In doing so, they make systems more transparent and, perhaps, more democratic" (4). See also (Lacity & Treiblmaier, 2022).

its potential, immediately spread far beyond the mere exchange of cryptocurrencies (Sarzana & Nicotra, 2018; Rajasekaran et al., 2022; Belotti et al., 2019; Michael et al., 2018; Ammous, 2016)[4]: from the financial services sector, healthcare, supply chain management, the so-called "e-voting"[5] and, recently, to digital goods (such as NFT) and product passports.

2015 marked the transition to its so-called "second generation" when Ethereum, the first programmable blockchain, was developed, contributing to the emergence of smart contracts and the development of decentralised applications on blockchain. Moreover, the merits of this technology were also soon recognised by the European legislator, who stated that its use could speed up the way transactions are negotiated and executed, with major advantages for the development of the internal market[6]. However, he also noted that EU legislation, which came into being before blockchain, was inadequate to deal with the possible risks and dangers that blockchain poses for fundamental rights and, above all, for the protection of personal data[7].

1. Definition, functioning, and basic features of Blockchain

Since 2008, several blockchains have been implemented, each with peculiar characteristics that differentiate them from one another. Due to this heterogeneity, it is very difficult (if not impossible) to provide a unified and shared definition of the phenomenon[8]. Nevertheless, some general considerations can be made.

First of all, blockchain technology is a sub-category of "Distributed Ledgers Technology" (henceforth DLT), i.e. special types of databases in which data are recorded, shared and synchronised on a distributed network of computers. The data can represent any exchangeable value susceptible to economic valuation such as money, contracts, medical records, buying and selling of goods and services as well as birth or marriage certificates. However, it should be noted that DLTs differ from blockchain in the way they record and verify information.

---

4 Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. https://clck.ru/3EGEp4

5 For an in-depth analysis of the areas mentioned, see (European Parliament. (2017). How blockchain technology could change our lives – In-depth analysis; Gupta et al., 2023; Mccorry et al., 2021).

6 European Parliament. (2022). Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology, and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65/EU (Text with EEA relevance).

7 Ibid.

8 (Walch, 2016). It is worth noting that the extreme diversity of blockchain does not allow for the construction of a universally accepted (and acceptable) inclusive definition of all platform types currently on the market (and those to come). However, if a definition of the phenomenon would make it possible to circumscribe it and thus treat it in a unified manner, it would, however, suffer from a rigidity that is ill-suited to technological change. It therefore seems preferable, as already observed by authoritative doctrine regarding the definition of a digital platform, to adopt a functional case-based approach. In this regard, see (Bertolini et al., 2021).

As just mentioned, they are distributed databases because they operate on a network of multiple nodes, typically installed on a single computer (technically a server). When a party wants to execute a transaction, it is transmitted to the network that validates it according to the consensus algorithm (Sarzana & Nicotra, 2018). In this way, each block in the chain that forms the ledger is immutably linked to the previous one as well as the next. In other words, once a block is added, it can no longer be modified without altering the subsequent part of the chain. More specifically, the integrity of the ledger is guaranteed because rewriting the following blocks would require solving the puzzle multiple times in a timely manner, an operation infeasible due to the cost and computational power required. Everything is then shared by every node in the network and is always updated and synchronised.

1.1. One technology, different classifications

In common parlance, the term "blockchain" is used to refer generically to technology based on distributed ledgers. In reality, this category contains different types of blockchain, each with its own characteristics and peculiarities.

There are the so-called "public" blockchains whose fundamental element is their "decentralization". First of all, they are typically "permissionless", meaning that users can do any operations, including reading and proposing new blocks as well as validating transactions. That is, these blockchains (e.g. the Bitcoin platform) do not require any central authority to act as an intermediary or to validate the transactions that take place in the network. On the contrary, it uses a peer-to-peer mechanism by directly connecting users, who become, at the same time, active subjects for the validation of transactions and passive ones because they hold all the information. As we mentioned above (Sarzana & Nicotra, 2018), it is a system based on the so-called "consensus mechanism" because all participants are obliged to verify and create transactions following specific rules that have already been encoded in blockchain software. For example, one of the most widely used consensus algorithms is Proof of Work (PoW) which relies on the computing or processing power of computers (called "miners") to solve mathematical problems (puzzle), which becomes increasingly complex after each validated transaction, as quickly as possible. Not only that, but each participant keeps a copy of the ledger, so that everyone can participate in the network and all their data is accessible anytime, anywhere.

This peer-to-peer system makes the system much more resistant to possible attacks because it would be necessary to hit the majority of the nodes distributed on the network (Aponte-Novoa et al., 2021). In fact, every change is quickly visible to all participants and cryptographic signatures guarantee the integrity and authentication of transactions (this is referred to as "tamper-resistant" (Austin & Di Troia, 2022)).

Therefore, various remuneration systems have been implemented for each correctly validated transaction as well as protocols to make it extremely difficult to engage in abusive conduct.

From these brief considerations, it is already possible to understand the advantages and criticalities of this type of open blockchain. Being based on a decentralized (and, therefore, distributed) system ensures both the integrity of transactions and greater security as it is more challenging to attack. Moreover, transactions are stored indefinitely to guarantee the verifiability of the entire chain. Finally, they are public and, thus, freely accessible, as there is no centralised control by an authority.

On the other hand, however, public blockchains tend to be very slow in handling transactions and, therefore, not entirely adequate to handle large volumes. This is because they have the major problem of scalability, i.e. as the number of nodes in the network increases, the speed of executing and handling transactions are reduced[9]. Not to mention the environmental impact that public models have[10].

Then there are "private" blockchains that are accessible only by specifically authorised users. Consequently, the personal (and other) data of network participants is shared within the network. In particular, it involves users whose identity is well known, since in order to become a node, it is necessary to fulfill a series of requirements and to have obtained the approval of a central administrator. Not only that, but those wishing to join the network are often required to subscribe to terms of service describing their respective rights and obligations. It is evident then why particularly stringent consensus mechanisms are not required in this case: here the system does not have to "earn" the trust of operators through costly consensus mechanisms because each node, being easily identified and recognisable, can be held responsible (Raymond Choo et al., 2020). In these types of systems, transaction validation is usually delegated to a trusted subset of nodes. In other words, if the public blockchain can in some ways be said to be the emblem of democracy and decentralisation, in the private ones the paradigm is that of oligarchy: not all nodes have equal importance.

This system undoubtedly has several technical advantages. First, it is much faster (as only a very small group of nodes are responsible to verify and propagate new blocks) and, secondly, thanks to the possibility of restricting access to the content of the blockchain, it appears to be more secure from a confidentiality and privacy point of view. However, one of the main weaknesses of private models lies precisely here. If it is true that the security of this technology derives from the distribution and decentralisation of the register, in private ones, the latter is not distributed but concentrated in the hands of a single (or few) entity.

---

9 Proof of Work (PoW) scalability issues stem from its design, which requires significant computational effort to validate transactions and add blocks. As more nodes join, they still must process and validate all transactions independently, not increasing overall throughput. Additionally, PoW's high energy consumption and latency in block propagation further constrain scalability, leading to longer transaction times and higher fees during peak demand. On the matter, see (Gramoli, 2022).

10 For more on the environmental impact of blockchain see Bitcoin Energy Consumption Index. Digiconomist. https://clck.ru/3EGHgF

Both categories just described can in turn be "permissioned" or "permissionless"[11]. Thus, one can have "public permissionless blockchains" in which anyone can participate in the consensus mechanism and propose transactions (this is the case, for example, of platforms such as Bitcoin or Ethereum) as well as "public permissioned blockchains" that allow all users to see the transaction log and conclude any type of operation, even though only a small number of nodes are allowed to participate in the consensus mechanism. A clear example of this is Ripple[12].

The same applies to private ones[13], where a distinction is made between "private permissioned blockchains" that limit the transaction and display capacity of the ledger to only those nodes that participate in the network, and it is the platform operator who chooses who to let participate in the consensus mechanism. This happens, for instance, in the case of Rubix[14]. Exactly the opposite happens in "private permissionless blockchains"[15], which limit the parties allowed to perform transactions and access the ledger, but unlike the former, here the consensus mechanism is open to anyone.

1.2. Public and private blockchains… and the third way

Both public and private blockchains have advantages and disadvantages. The former, as we have seen, is "universally" transparent (as transactions are visible to all participants in the network), reliable (due to their decentralised nature, they are less prone to single points of system failure), decentralised and accessible (they are managed by a globally distributed network of nodes which makes them highly resilient) and immutable; however, they are very slow because they suffer from scalability problems due to the volume of transactions and the need for decentralised confirmation, they have very high transaction costs and they do not guarantee privacy as they are public. Similarly, the latter are certainly more efficient because they are scalable and faster (this is explained by the fact that there is no need for decentralised confirmation and, therefore, transactions are processed faster), they guarantee the privacy of the information contained in the network and the network organisers have complete control over the governance and rules of the network; on the other hand, however, private blockchains are less transparent, centralised and less secure.

To solve some of the inherent problems of these two models, a third type of 'hybrid' blockchain has been developed that lies, we might say, somewhere in between the two.

11 Ismail, A. (2020). Permissioned Blockchains for Real World Applications. Lakehead University.

12 Ripple. https://clck.ru/3EGDyK

13 Nascimento, S. et al. (2019). Blockchain Now and Tomorrow: Assessing Multidimensional Impacts of Distributed Ledger Technologies. European Commission. https://clck.ru/3EGDUk

14 Rubix. https://clck.ru/3EGE3L

15 However, it should be noted that this is a very rare case as A private permissionless blockchain is a bit of a contradiction in terms, as «private» typically implies restricted access, while «permissionless» implies open access. However, a blockchain could be designed with certain hybrid characteristics.

In other words, these models have characteristics of public and private blockchains, but offer greater flexibility and adaptability to a wide range of use cases. Firstly, they are flexible because they allow the degree of decentralisation and privacy to be customised to the specific needs of the application for which they are used. On the other hand, these systems are also more reliable because, by combining public and private elements, the overall robustness and resilience of the network can be increased (Smith, 2020). Moreover, they are interoperable and can address scalability issues by balancing control and decentralisation. However, the combination of public and private factors may lead to a higher degree of complexity in the system, from which, in turn, comes the risk of introducing new security vulnerabilities into the system. Finally, the design and implementation of a hybrid blockchain may require significant resources and very high costs.

1.3. Case study: Traent and advantages of hybrid blockchain

The move to hybrid blockchain represents an important point of evolution in the discipline, which is particularly flexible and adaptable. These objectives prompted Traent[16], an Italian company, to implement a hybrid blockchain model capable of cumulating the advantages (and solving the criticalities) of both public and private systems[17].

As mentioned earlier, in public blockchains each node participating in the network has a copy of the ledger, so that each replica contains all transactions and cryptographic evidence associated with each block in the chain. For this reason, the public blockchain is more secure, since to modify a transaction would require all nodes, which are in a potentially infinite number, to modify the chain ("fork-resistance"[18]). However, precisely because it is particularly difficult to modify the chain and rewrite it, once data has been published on it, it can no longer be modified or deleted.

On the other hand, private blockchains try to precisely solve this problem: since they are shared among a limited number of participants, it is possible to limit the sharing of data. The criticality of this mechanism stems precisely from the fact that users, by definition not impartial, are also those who validate the transactions that take place on the platform. This implies, therefore, that they could easily decide to change what is written on the chain, since there is no third party with a super partes controller function. The third-party user then has no way of verifying whether or not the chain has been altered.

---

16 Traent. https://clck.ru/3EGJHN

17 It should be noted that the description of the technical functioning of the platform is beyond the scope of this discussion, and therefore we refer to (Pelosi, 2023). However, it seems useful to attempt to describe only briefly how Traent's system operates so as to allow the reader to better appreciate the reflections on the right to be forgotten and blockchain.

18 Fork resistance is the ability of a blockchain network to withstand and recover from a hard fork, which is a permanent divergence in the blockchain caused by conflicting rules. Hard forks can be the result of contentious network upgrades and can lead to the creation of a new cryptocurrency. See (Golden et al., 2020).

The blockchain proposed by Traent, on the other hand, succeeds in achieving "external" (or even "public") auditability precisely by adopting a hybrid model. Specifically, the company provides interested users with a private blockchain to perform any transaction, which is materialised on the private ledger in a block together with a cryptographic proof. Subsequently, the latter is published – via a system component called Notary (Pelosi et al., 2023) – on an external public blockchain. This way, the cryptographic proofs associated with the individual blocks written on the (private) ledger are published on the (public) blockchain. Thus, when an outsider wants to participate in the chain, he can be sure that transactions have not been altered by others verifying on the external blockchain thanks to the externalised cryptographic evidence – that there has been no fork in the private chain.

2. The clash between blockchain technology and the "right to be forgotten" in the context of the European data protection legislation. The solution adopted by Traent

Recognition of the right to be forgotten as a fundamental element in the protection of personal identity and human freedoms is a recent achievement for modern society, which is based on the platform economy model (Xue et al., 2020; Cohen, 2017; Kenney & Zysman, 2016; Stark & Pais, 2020; Acs et al., 2021). The protection of personal data has always been a primary objective for supranational legislators, so much so that it has already been recognised in the EU Charter of Fundamental Rights as an autonomous and independent right[19] to private and family life[20]. To apply this principle effectively and, at the same time, ensure the free movement and protection of data within the Union, the Commission presented in 2012 a package aimed precisely at ensuring harmonisation between the Member States.

In this respect, an essential contribution came from the case law of the Court of Justice of the European Union (henceforth CJEU) and, in particular, the well-known Google Spain case[21]. The case concerned a Spanish citizen who had addressed both the internet site operator and Google – as search engine – to obtain the removal of his data published several years ago in a national newspaper. In particular, the plaintiff complained that the data were no longer up-to-date and claimed the right so that the search engine would not redirect users to the page that reported the inaccurate news. In this judgment, the Court laid down some basic principles for the effective implementation of the right of users to have their personal data deleted online. Among the various issues addressed in this decision, it recognised

19 Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012 (pp. 391–407), Art. 8.

20 Ibid., Art. 7.

21 CJEU, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12, 13 May 2014, ECLI:EU:C:2014:317.

the user's right to demand that certain harmful content was no longer available online and that, consequently, it was no longer indexed among the platform's results. This is because, according to the CJEU, the fundamental rights under Articles 7 and 8 of the Nice Charter must prevail over the economic interest of the provider as well as the public in information.

Although the supranational court is crystal clear in affirming the prevalence of the reasons of the user claiming the right to erasure, the same cannot be said in the jurisprudence of the European Court of Human Rights. An example is the case of Węgrzynowski and Smolczewski v. Poland where the conclusions were quite different[22]. In this decision, the ECtHR does not recognise the user's right to remove online information but rather tries to strike a balance between freedom of expression under Article 10 of the ECHR and the right to be forgotten. In other words, while the complete removal of the content was deemed disproportionate, the most appropriate remedy was found in requiring the online publisher to publish additional clarifications to the article in question, to provide an update of the subject matter.

Subsequently, in 2016 the EU adopted the General Data Protection Regulation 2016/679 (henceforth GDPR)[23], with which it was finally expressly recognised in Article 17 – headed "Right to erasure ('right to be forgotten')" – that "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay"[24].

This provision thus recognises two precise rights: on the one hand, the right to "erasure of data", which allows the data subject to request the deletion of data concerning him on the assumption that after a certain period of time they are no longer of collective interest and no longer correctly represent his personal identity. On the other hand, this provision also recognises the "right to be forgotten" in the strict sense, which is broader than the former,

22 CEDU, Węgrzynowski and Smolczewski v. Poland, Application No. 33846/07, 16 July 2013. https://clck.ru/3EGJgf

23 European Parliament and Council. (2016). 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, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).

24 The rule goes on to identify the prerequisites necessary for this right to be activated by the user: "(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); (d) the personal data have been unlawfully processed; (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1)". In addition, Article 16 provides for the right to rectification of data. For an in-depth discussion of the right to be forgotten after the adoption of the GDPR, see (Alessi, 2017; Kocharyan et al., 2021; Mantelero, 2013; Politou et al., 2018; Finocchiaro, 2010; Peguera, 2019).

and which requires the data controller not only to delete all information concerning the data subject but also any link, copy or reproduction that may refer to that specific data. In other words, the intention is that the user should enjoy broader control over the management of his or her data on the web, as an expression of free individual self-determination.

2.1. The incompatibility between the right to be forgotten and blockchain

A fundamental characteristic of the blockchain is its immodifiability, which appears, however, to be completely at odds with Article 17 GDPR, which instead allows users to request and obtain at any time the modification of their data as well as their complete deletion. This is true for both public and private blockchain models. The former, in fact, are extremely secure because they make use of a distributed system where every participant in the network has a copy of the ledger. This advantage, however, has the downside that modifying or deleting data once it has been entered into the chain is not possible, because the information would have to be deleted from each node (the so-called principle of unchangeability of the public blockchain applies). The latter, on the other hand, tries to solve this problem by allowing users to choose which data to publish and which not to publish (and with whom to share it) at the expense, however, of a system that is not totally secure. The same can be said of the simple modification or correction of data because in the blockchain each block knows whether the previous one contains the data entered. This means that if an attempt were made to change the information in one block of the chain, subsequent blocks would fail verification.

Several alternative solutions were developed to make the system compatible with European data protection law, since Article 17 does not specify how the "erasure" of data is to be concretely achieved. Some considered that mere anonymisation of the data was sufficient, while others proposed "putting the data out of use", i.e. ensuring that the data controller is no longer able to use the information for decision-making purposes, does not pass it on to any other third party, takes technical measures to secure the data and, finally, is obliged to delete the data when possible. Others, on the other hand, suggest making the data completely inaccessible by destroying the private key corresponding to the public key that every user of the network possesses. In this regard, even the CJEU does not perfectly clarify the interpretation of the rule of the regulation, but seems to recognise, however, that erasure means the complete destruction of data. In particular, the case of Peter Nowak v Data Protection Commissioner recognised a candidate in a written examination "the right to ask the data controller to ensure that his examination answers and the examiner's comments with respect to them are, after a certain period of time, erased, that is to say, destroyed"[25]. On this point, also the European Parliamentary Research Service (EPRS)[26] stated that "whether

[25] CJEU, Peter Nowak v Data Protection Commissioner, Case C-434/16, 20 December 2017, ECLI:EU:C:2017:994.

[26] Service EPR. (2019). Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?

this can be seen as a blanket statement that erasure always amounts to destruction in unclear, especially since the case at issue did not directly deal with the right to erasure. The statement could thus also be explained by the specific context at hand and the fact that outright destruction of the examination copy may be the most straightforward means of destruction (although the blackening out of the relevant information is another obvious option)"[27].

2.2. The model developed by Traent to guarantee the right to data removal and modification

An interesting solution to guarantee respect for the right to be forgotten is the one provided by Traent in its hybrid blockchain. This model does not provide for the entire data to be written in the block of the (private) ledger, but only a "reference"[28] to it, which refers to the outside of the chain where the entire data is actually saved. In addition, a cryptographic proof ("digest") is also inserted in the same block. In this way, thanks to the reference written in the (private) chain, the user concerned can access the complete externalised data and verify, thanks to the digest, that it has not been altered.

This dual mechanism not only makes the system more secure – because it allows the authenticity of the information contained in the blockchain to be ascertained – but also allows users to delete the data entered: since these are outside the private blockchain, it becomes possible to delete them without altering the chain. Thus, the verification of the blockchain remains valid because, in fact, the blocks of the ledger are never actually altered. However, since the digest is associated with those externalised data (which no longer exist because they have been deleted) it stops working. At this point, the hybrid model developed by Traent creates a new block – inserted in the private ledger – in which the data (to which the reference and the cryptographic proof refer) in the previous one is accounted for as having been deleted. Thanks to this system, the user can verify that the chain has not been fraudulently changed and, at the same time, that the data is genuine because it is clear from the next block that a data deletion operation has been performed.

Already from these brief considerations, it is clear that the solution proposed by Traent is the one that is certainly the most compliant with Article 17 GDPR because it allows the complete deletion of data but also their simple modification. It thus succeeds in fully implementing the European regulation as well as the interpretation that the CJEU seems to have given of it.

---

27 Ibid.

28 This could be, for instance, a URL.

Conclusions

The European Parliament recently passed the Artificial Intelligence Act (henceforth AIA)[29] intending to increase trust in AI systems and mitigate their risks. For this, it bans or severely restricts the use of those systems that present unacceptable risks to the safety, health, dignity, and autonomy of people. However, efforts are made to support innovation and the development of increasingly sophisticated technologies to exploit their full potential for the internal market[30].

Despite the adoption of this law, the accountability of AI systems remains an issue that continues to preoccupy experts in the field. This is mainly due to the lack of effective technical solutions to fully explain the reasoning that led an algorithm to provide a certain output rather than another, so much so that it is not uncommon to hear talk of "black box solutions" (Springer et al., 2017; Veale & Zuiderveen Borgesius). Blockchain can, then, be a valuable tool to achieve the goal of a "trustworthy AI"[31]. First, it can lead to greater transparency and visibility of algorithms since ledger status and transaction logs are stored securely, decentralized, and accessible to all node participants. Moreover, it can help guarantee the immutability of the results: the ledger is composed of numerous blocks, each of which contains a series of transactions and data and is protected by a cryptographic hash that refers to the same hash contained in the previous block. Therefore, even the smallest change to one of the blocks invalidates the entire chain.

In conclusion, it can be said that blockchain seems to be, to date, the most appropriate – and perhaps the only – solution to meet the requirements of the most recent European legislation on both data protection and AI systems. However, this technology still presents several challenges that need to be addressed, among which guaranteeing the user's right to delete and modify his or her information is particularly pressing. In this sense, then, the hybrid model implemented by Traent can provide, as briefly demonstrated, a particularly effective alternative to[32]. By doing so, it becomes possible to fully exploit the potential of blockchain for the development of truly explainable algorithms and AI systems, as well as to eliminate – or at least alleviate – any doubts about blockchain's compatibility with the GDPR.

---

29 European Commission. (2021). Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).

30 Ibid

31 Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), where it is said that: "This proposal aims to implement the second objective for the development of an ecosystem of trust by proposing a legal framework for trustworthy AI. The proposal is based on EU values and fundamental rights and aims to give people and other users the confidence to embrace AI-based solutions, while encouraging businesses to develop them" (1). See also (Nassar et al., 2019).

32 For a more in-depth look at Traent's technology and the benefits it can bring regarding specific case studies, see the following link: Traent. https://clck.ru/3EGKux

References

Acs, Z. J., Song, A. K., Szerb, L., Andretsch, D. B., & Komlósi, E. (2021). The evolution of the global digital platform economy: 1971–2021. *Small Business Economics*, *57*, 1629–1659. https://doi.org/10.1007/s11187-021-00561-x

Alessi, S. (2017). Eternal sunshine: The right to be forgotten in the European Union after the 2016 General Data Protection Regulation. *Emory International Law Review*, *32*(1), 145.

Ammous, S. (2016). *Blockchain technology: What is it good for?* http://dx.doi.org/10.2139/ssrn.2832751

Aponte-Novoa, F. A., Orozco, A. L. S., Villanueva-Polanco, R., & Wightman, P. (2021). The 51% Attack on Blockchains: A Mining Behavior Study. *IEEE Access*, *9*, 140549–40564. https://doi.org/10.1109/ACCESS.2021.3119291

Austin, T. H., & Di Troia, F. (2022). A Blockchain-Based Tamper-Resistant Logging Framework. In L. Bathen, G. Saldamli, X. Sun, T. H. Austin, & A. J. Nelson (Eds.), *Silicon Valley Cybersecurity Conference. SVCC 2022. Communications in Computer and Information Science* (vol. 1683, pp. 90–104). Springer, Cham. https://doi.org/10.1007/978-3-031-24049-2_6

Belotti, M., Božić, N., Pujolle, G., & Secci, S. (2019). A Vademecum on Blockchain Technologies: When, Which, and How. *IEEE Communications Surveys & Tutorials*, *21*(4), 3796–3838. https://doi.org/10.1109/comst.2019.2928178

Bertolini, A., Episcopo, F., & Cherciu, N.-A. (2021). *Liability of online platforms*. European Parliamentary Research Service (EPRS).

Cohen, J. E. (2017). Law for the platform economy. *UC Davis Law Review*, *51*, 133–204.

Finocchiaro, G. (2010). La memoria della rete e il diritto all'oblio. *Il Diritto Dell'informazione e Dell'informatica*, *3*, 391–404. (In Italian).

Golden, E. J., Najahi, J. J. V., & Jhanjhi, N. Z. (2020). *Blockchain Technology: Fundamentals, Applications, and Case Studies*. Taylor & Francis Ltd. https://doi.org/10.1201/9781003004998

Gramoli, V. (2022). *Blockchain Scalability and its Foundations in Distributed Systems*. Springer Cham. https://doi.org/10.1007/978-3-031-12578-2

Gupta, S., Gupta, A., Pandya, I. Y., Bhatt, A., & Mehta, K. (2023). End to end secure e-voting using blockchain & quantum key distribution. *Materials Today: Proceedings*, *80*, 3363–3370. https://doi.org/10.1016/j.matpr.2021.07.254

Kenney, M., & Zysman, J. (2016). The rise of the platform economy. *Issues in Science and Technology*, *32*(3), 61–69.

Kocharyan, H., Vardanyan, L., Hamuľák, O., & Kerikmäe, T. (2021). Critical views on the right to be forgotten after the entry into force of the GDPR: Is it able to effectively ensure our privacy? *International and Comparative Law Review*, *21*(2), 96–115. https://doi.org/10.2478/iclr-2021-0015

Lacity, M. C., & Treiblmaier, H. (Eds.) (2022). *Blockchains and the Token Economy: Theory and Practice (Technology, Work and Globalization)* (1st ed.). Palgrave Macmillan.

Mantelero, A. (2013). The EU Proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten'. *Computer Law & Security Review*, *29*(3), 229–235.

Mccorry, P., Mehrnezhad, M., Toreini, E., Shahandashti, S. F., & Hao, F. (2021). On Secure E-Voting over Blockchain. *Digital Threats: Research and Practice*, *2*(4), 33. https://doi.org/10.1145/3461461

Michael, J., Cohn, A., & Butcher, J. R. (2018). Blockchain technology and regulatory investigations. *The Journal Litigation*, *1*, 35–44.

Nassar, M., Salah, K., & Svetinovic, D. (2019). Blockchain for explainable and trustworthy artificial intelligence. *WIREs Data Mining and Knowledge Discovery*, *10*(1), e1340. https://doi.org/10.1002/widm.1340

Peguera, M. (2019). The Right to Be Forgotten in the European Union. In G. Frosio (Ed.), *Oxford Handbook of Online Intermediary Liability*. Oxford University Press.

Pelosi, A., Felicioli, C., Canciani, A., & Severino, F. (2023). A Hybrid-DLT Based Trustworthy AI Framework. In *2023 IEEE International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)* (pp. 1–6). https://doi.org/10.1109/wetice57085.2023.10477792

Politou, E., Michota, A., Alepis, E., Pocs, M., & Patsakis, C. (2018). Backups and the right to be forgotten in the GDPR: An uneasy relationship. *Computer Law & Security Review*, *34*, 1247–1257. https://doi.org/10.1016/j.clsr.2018.08.006

Rajasekaran, A. S., Azees, M., & Al-Turjman, F. (2022). A comprehensive survey on blockchain technology. *Sustainable Energy Technologies and Assessments*, *52*, 102039. https://doi.org/10.1016/j.seta.2022.102039

Raymond Choo, K.-K., Dehghantanha, A., & Parizi, R. M. (Eds.) (2020). *Blockchain Cybersecurity, Trust and Privacy (Advances in Information Security* (1st ed.). Springer Cham. https://doi.org/10.1007/978-3-030-38181-3

Sarzana, F., & Nicotra, M. (2018). *Diritto della blockchain, intelligenza artificiale e IoT*. Ipsoa. (In Italian).

Smith, S. S. (2020). *Blockchain, Artificial Intelligence and Financial Services (Future of Business and Finance)*. Springer Cham.

Springer, A., Hollis, V., & Whittaker, S. (2017). Dice in the Black Box: User Experiences with an Inscrutable Algorithm. In *The AAAI 2017 Spring Symposium onDesigning the User Experience of Machine Learning Systems Technical Report SS-17-04* (pp. 427–430).

Stark, D., & Pais, I. (2020). Algorithmic management in the platform economy. *Sociologica*, *14*(3), 47–72. https://doi.org/10.6092/issn.1971-8853/12221

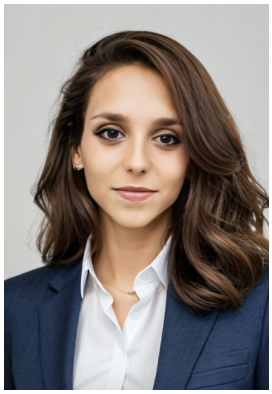
Veale, M., & Zuiderveen Borgesius, F. (2021). Demystifying the Draft EU Artificial Intelligence Act. *Computer Law Review International*, *22*(4), 97–112. https://doi.org/10.9785/cri-2021-220402

Walch, A. (2016). The Path of the Blockchain Lexicon (and the Law). *Review of Banking and Financial Law*, *36*, 713–765.

Xue, C., Tian, W., & Zhao, X. (2020). The literature review of platform economy. *Scientific Programming*, *2020*(1), 8877128. https://doi.org/10.1155/2020/8877128

Authors information

Fabio Severino – CTO, Traent SRL
Address: Borgo Stretto 3, 56127, Pisa, Italy
E-mail: fabio.severino@traent.com
ORCID ID: https://orcid.org/0000-0002-9538-1218



Ludovica Sposini – PhD Candidate (Law), DIRPOLIS Institute (Institute of Law, Politics and Development), Sant'Anna School of Advanced Studies
Address: Via Domenico Vernagalli 22R, 56127 Pisa, Italy
E-mail: ludovica.sposini@santannapisa.it
ORCID ID: https://orcid.org/0000-0003-2188-8996
Google Scholar ID: https://scholar.google.com/citations?user=AVR7_bMAAAAJ

Authors' contributions

The authors have contributed equally into the concept and methodology elaboration, validation, formal analysis, research, selection of sources, text writing and editing, project guidance and management.

Conflict of interest

The authors declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Acknowledgements

The authors would like to thank Traent SRL for providing all the technical documentation concerning its technology for the purpose of this article. In addition, we would also like to thank the Jean Monnet Centre of Excellence on the Regulation of Robotics and AI (EURA) for the support.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – June 16, 2024
Date of approval – July 2, 2024
Date of acceptance – September 25, 2024
Date of online placement – September 30, 2024

Научная статья
УДК 34:004:347.211:004.8
EDN: https://elibrary.ru/mloxmi
DOI: https://doi.org/10.21202/jdtl.2024.29

Новый подход к преодолению конфликта между «правом на забвение» и технологией блокчейн

Фабио Северино

Traent SRL, Пиза, Италия

Людовика Спозини ✉

Школа перспективных исследований Сант'Анна, Пиза, Италия

Ключевые слова

блокчейн гибридный,
блокчейн публичный,
блокчейн частный,
Европейский союз,
законодательство
защита персональных данных,
Общий регламент по защите данных,
право,
право на забвение,
цифровые технологии

Аннотация

Цель: в статье рассматриваются проблемы, связанные с конфликтом между технологией блокчейн и «правом на забвение», предусмотренным европейской системой защиты данных.

Методы: в первом разделе кратко описаны эволюция технологии блокчейн, а также наиболее актуальные проблемы, возникающие между традиционными моделями блокчейна и законодательством Европейского союза. Среди последних проанализирован конкретный вопрос конфликта между природой традиционных блокчейнов (как частных, так и публичных моделей), как правило, неизменяемых, и правом индивида требовать удаления или изменения своих персональных данных. В этом разделе отмечается важность задачи по защите персональных данных, которая всегда была одной из главных для наднациональных законодателей. Приводится анализ правового регулирования защиты данных и соответствующей практики Европейского суда по правам человека. Поднимается проблема выражения свободного самоопределения личности в виде контроля над управлением персональными данными в Интернете. Второй раздел посвящен изучению возможных путей решения сложившегося противоречия, позволяющих сделать систему распределенных реестров совместимой с европейским законодательством о защите данных. Сделан акцент на модели, предложенной компанией Traent, гарантирующей право на удаление и изменение данных. Анализируются возможности данной модели по разрешению указанного противоречия.

✉ Контактное лицо

Результаты: рассмотрены особенности новой модели и ее возможности по стратегическому использованию преимуществ публичных и частных блокчейнов. Показано, что данная модель гарантирует не только достоверность и подлинность цепочки, по которой была проведена транзакция, но и, что особенно важно, изменение и полное удаление персональных данных пользователя. Это инновационное решение потенциально дает возможность справиться с противоречием между требованиями конфиденциальности данных и развитием блокчейна в европейском контексте.

Научная новизна: компании Traent удалось реализовать «гибридную» модель, которая включает в себя как публичные, так и частные компоненты блокчейна, что позволяет достичь эффективного соответствия нормам Европейского союза в отношении защиты и конфиденциальности данных.

Практическая значимость: полученные выводы и предложения могут учитываться при совершенствовании соответствия блокчейн-технологий принципам Общего регламента Европейского союза по защите персональных данных.

Для цитирования

Северино, Ф., Спозини, Л. (2024). Новый подход к преодолению конфликта между «правом на забвение» и технологией блокчейн. *Journal of Digital Technologies and Law*, *2*(3), 565–584. https://doi.org/10.21202/jdtl.2024.29

Список литературы

Acs, Z. J., Song, A. K., Szerb, L., Andretsch, D. B., & Komlósi, E. (2021). The evolution of the global digital platform economy: 1971–2021. *Small Business Economics*, *57*, 1629–1659. https://doi.org/10.1007/s11187-021-00561-x

Alessi, S. (2017). Eternal sunshine: The right to be forgotten in the European Union after the 2016 General Data Protection Regulation. *Emory International Law Review*, *32*(1), 145.

Ammous, S. (2016). *Blockchain technology: What is it good for?* http://dx.doi.org/10.2139/ssrn.2832751

Aponte-Novoa, F. A., Orozco, A. L. S., Villanueva-Polanco, R., & Wightman, P. (2021). The 51% Attack on Blockchains: A Mining Behavior Study. *IEEE Access*, *9*, 140549–140564. https://doi.org/10.1109/ACCESS.2021.3119291

Austin, T. H., & Di Troia, F. (2022). A Blockchain-Based Tamper-Resistant Logging Framework. In L. Bathen, G. Saldamli, X. Sun, T. H. Austin, & A. J. Nelson (Eds.), *Silicon Valley Cybersecurity Conference. SVCC 2022. Communications in Computer and Information Science* (vol. 1683, pp. 90–104). Springer, Cham. https://doi.org/10.1007/978-3-031-24049-2_6

Belotti, M., Božić, N., Pujolle, G., & Secci, S. (2019). A Vademecum on Blockchain Technologies: When, Which, and How. *IEEE Communications Surveys & Tutorials*, *21*(4), 3796–3838. https://doi.org/10.1109/comst.2019.2928178

Bertolini, A., Episcopo, F., & Cherciu, N.-A. (2021). *Liability of online platforms*. European Parliamentary Research Service (EPRS).

Cohen, J. E. (2017). Law for the platform economy. *UC Davis Law Review*, *51*, 133–204.

Finocchiaro, G. (2010). La memoria della rete e il diritto all'oblio. *Il Diritto Dell'informazione e Dell'informatica*, *3*, 391–404. (In Italian).

Golden, E. J., Najahi, J. J. V., & Jhanjhi, N. Z. (2020). *Blockchain Technology: Fundamentals, Applications, and Case Studies*. Taylor & Francis Ltd. https://doi.org/10.1201/9781003004998

Gramoli, V. (2022). *Blockchain Scalability and its Foundations in Distributed Systems*. Springer Cham. https://doi.org/10.1007/978-3-031-12578-2

Gupta, S., Gupta, A., Pandya, I. Y., Bhatt, A., & Mehta, K. (2023). End to end secure e-voting using blockchain & quantum key distribution. *Materials Today: Proceedings*, *80*, 3363–3370. https://doi.org/10.1016/j.matpr.2021.07.254

Kenney, M., & Zysman, J. (2016). The rise of the platform economy. *Issues in Science and Technology*, *32*(3), 61–69.

Kocharyan, H., Vardanyan, L., Hamuľák, O., & Kerikmäe, T. (2021). Critical views on the right to be forgotten after the entry into force of the GDPR: Is it able to effectively ensure our privacy? *International and Comparative Law Review*, *21*(2), 96–115. https://doi.org/10.2478/iclr-2021-0015

Lacity, M. C., & Treiblmaier, H. (Eds.) (2022). *Blockchains and the Token Economy: Theory and Practice (Technology, Work and Globalization)* (1st ed.). Palgrave Macmillan.

Mantelero, A. (2013). The EU Proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten'. *Computer Law & Security Review*, *29*(3), 229–235.

Mccorry, P., Mehrnezhad, M., Toreini, E., Shahandashti, S. F., & Hao, F. (2021). On Secure E-Voting over Blockchain. *Digital Threats: Research and Practice*, *2*(4), 33. https://doi.org/10.1145/3461461

Michael, J., Cohn, A., & Butcher, J. R. (2018). Blockchain technology and regulatory investigations. *The Journal Litigation*, *1*, 35–44.

Nassar, M., Salah, K., & Svetinovic, D. (2019). Blockchain for explainable and trustworthy artificial intelligence. *WIREs Data Mining and Knowledge Discovery*, *10*(1), e1340. https://doi.org/10.1002/widm.1340

Peguera, M. (2019). The Right to Be Forgotten in the European Union. In G. Frosio (Ed.), *Oxford Handbook of Online Intermediary Liability*. Oxford University Press.

Pelosi, A., Felicioli, C., Canciani, A., & Severino, F. (2023). A Hybrid-DLT Based Trustworthy AI Framework. In *2023 IEEE International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)* (pp. 1–6). https://doi.org/10.1109/wetice57085.2023.10477792

Politou, E., Michota, A., Alepis, E., Pocs, M., & Patsakis, C. (2018). Backups and the right to be forgotten in the GDPR: An uneasy relationship. *Computer Law & Security Review*, *34*, 1247–1257. https://doi.org/10.1016/j.clsr.2018.08.006

Rajasekaran, A. S., Azees, M., & Al-Turjman, F. (2022). A comprehensive survey on blockchain technology. *Sustainable Energy Technologies and Assessments*, *52*, 102039. https://doi.org/10.1016/j.seta.2022.102039

Raymond Choo, K.-K., Dehghantanha, A., & Parizi, R. M. (Eds.) (2020). *Blockchain Cybersecurity, Trust and Privacy (Advances in Information Security* (1st ed.). Springer Cham. https://doi.org/10.1007/978-3-030-38181-3

Sarzana, F., & Nicotra, M. (2018). *Diritto della blockchain, intelligenza artificiale e IoT*. Ipsoa. (In Italian).

Smith, S. S. (2020). *Blockchain, Artificial Intelligence and Financial Services (Future of Business and Finance)*. Springer Cham.

Springer, A., Hollis, V., & Whittaker, S. (2017). Dice in the Black Box: User Experiences with an Inscrutable Algorithm. In *The AAAI 2017 Spring Symposium onDesigning the User Experience of Machine Learning Systems Technical Report SS-17-04* (pp. 427–430).

Stark, D., & Pais, I. (2020). Algorithmic management in the platform economy. *Sociologica*, *14*(3), 47–72. https://doi.org/10.6092/issn.1971-8853/12221

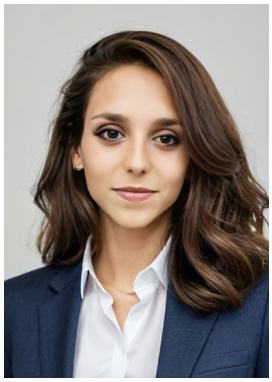
Veale, M., & Zuiderveen Borgesius, F. (2021). Demystifying the Draft EU Artificial Intelligence Act. *Computer Law Review International*, *22*(4), 97–112. https://doi.org/10.9785/cri-2021-220402

Walch, A. (2016). The Path of the Blockchain Lexicon (and the Law). *Review of Banking and Financial Law*, *36*, 713–765.

Xue, C., Tian, W., & Zhao, X. (2020). The literature review of platform economy. *Scientific Programming*, *2020*(1), 8877128. https://doi.org/10.1155/2020/8877128

Сведения об авторах

Фабио Северино – технический директор, компания Traent S.r.l.
Адрес: 56127, Италия, г. Пиза, ул. Борго Стретто, 3
E-mail: fabio.severino@traent.com
ORCID ID: https://orcid.org/0000-0002-9538-1218



Людовика Спозини – соискатель степени PhD в области права, Институт права, политики и развития (DIRPOLIS), Школа перспективных исследований Сант'Анна
Адрес: 56127, Италия, г. Пиза, ул. Виа Доменико Вернагалли, 22R
E-mail: ludovica.sposini@santannapisa.it
ORCID ID: https://orcid.org/0000-0003-2188-8996
Google Scholar ID: https://scholar.google.com/citations?user=AVR7_bMAAAAJ

Вклад авторов

Авторы внесли равный вклад в разработку концепции, методологии, валидацию, формальный анализ, проведение исследования, подбор источников, написание и редактирование текста, руководство и управление проектом.

Конфликт интересов

Авторы сообщают об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Благодарность

Авторы выражают благодарность компании Traent SRL за предоставление всей технической документации, касающейся данной технологии, для написания статьи. Кроме того, авторы благодарят за оказанную поддержку Центр передового опыта в области регулирования робототехники и искусственного интеллекта имени Жана Монне (Jean Monnet Centre of Excellence on the Regulation of Robotics and AI, EURA).

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.19.31 / Право на информацию
Специальность ВАК: 5.1.2 / Публично-правовые (государственно-правовые) науки

История статьи

Дата поступления – 16 июня 2024 г.
Дата одобрения после рецензирования – 2 июля 2024 г.
Дата принятия к опубликованию – 25 сентября 2024 г.
Дата онлайн-размещения – 30 сентября 2024 г.

Research article
UDC 34:004:347.4:004.8
EDN: https://elibrary.ru/dladns
DOI: https://doi.org/10.21202/jdtl.2024.30

Using Artificial Intelligence for Competitive Procurements: Legal Regulation Issues

Dmitriy A. Kazantsev ✉
Chamber of Commerce and Industry of the Russian Federation, Moscow, Russia

Pavel Dohnal
Technical University of Ostrava, Ostrava, Czech Republic

Pavel Dohnal Jr.
IT University of Copenhagen, Copenhagen, Denmark

Keywords

artificial intelligence,
auction,
competition,
digital technologies,
law,
legislation,
neuron network,
procurement,
regulation,
tender

Abstract

Objective: to substantiate the promising directions of legal regulation of relations in the use of artificial intelligence technologies in competitive (commercial and public) procurement.

Methods: the study was conducted using induction, synthesis, analogy, decomposition of problems and generalization of conclusions. The reasoning was based on the experience of a complex procurement of high-tech equipment. This real-life example was considered as an experimental model for the study and subsequent prediction of the potential use of artificial intelligence technologies in competitive procurement procedures.

Results: advantages and potential risks of using artificial intelligence technologies in procurement work were formulated; recommendations on regulating such use were given. The authors highlighted recommendations of general legal nature concerning the legal personality and delictual capacity of artificial intelligence and proposed the wordings for new norms and options for regulating the use of new procurement tools. It was proved that artificial intelligence technologies, if used thoughtfully, may not only improve the work quality and significantly reduce organizational costs, but also help to develop the basic principles of regulated procurement: transparency of procedures, development of competition for contracts

✉ Corresponding author

between qualified suppliers, reasonableness of decisions, and economic efficiency of the customer's expenditures.

Scientific novelty: despite a large number of works devoted to both the problems of artificial intelligence in general and its use in procurement in particular, the article considers this topic on the basis of mainly inductive reasoning, built on handling a particular case and experience of complex procurement for knowledge-intensive research, refracted through the prism of essential correlation between the basic concepts of "digitalization", "automation", "robotization" and so on.

Practical significance: the directions of using artificial intelligence described in this paper can be implemented by corporate and, in the future, by public customers to improve the quality of their procurement. At the same time, the recommendations on the normative regulation of such innovation seem to be in demand both at the legislative and local levels.

For citation

Kazantsev, D. A., Dohnal, P., & Dohnal Jr., P. (2024). Using Artificial Intelligence for Competitive Procurements: Legal Regulation Issues. *Journal of Digital Technologies and Law, 2*(3), 585–610. https://doi.org/10.21202/jdtl.2024.30

Contents

Introduction

Competitive procurement is traditionally a regulated activity. The methods of such regulation and the tools prescribed by the regulator vary, while public procurement as a concept does not remain unattended by the legislator in any of the European states. Competition for contracts between potential suppliers remains one of the foundations of public procurement.

At the same time, competition for contracting, being not an end in itself, but only one of the tools to ensure the quality of procurement, exists in the form of various instruments. These tools are gradually changing as economic relations evolve. One of the consequences of this situation is that the qualitative transformation of procurement relations inevitably requires the transformation of the relevant legal regulation. It may

be a question of modernization of existing norms, as well as modernization of the legal doctrine of competitive procurement per se. In the latter case, legal professionals may face the formation of a fundamentally new system of norms.

A new system of legal regulation of procurement may emerge even without regard to economic and technological development, but simply due to the traditions and specificity of the development of local legislation. For example, today we may observe various approaches to competitive procurement, like those provided for by the legislation on the U.S. federal contract system, the Russian legislation on the contract system, the EU Public Procurement Directive of 2014, and the Italian Procurement Code. However, below we will talk only about the problems of legal regulation caused by the use of qualitatively new tools in procurement, and first of all, the so-called artificial intelligence (hereinafter – AI).

For the sphere of legal regulation of procurement today, such a perspective is no longer just abstract theorizing. The digital transformation of modern economic and social relations is manifested, among other things, in the widespread introduction of technologies (conventionally referred to as artificial intelligence) into the business processes of commercial and public procurement. It should be mentioned from the very beginning: at the current level of technology development it is somewhat premature to talk about artificial intelligence in the direct sense of the word. International studies question the correctness of the very naming of neural networks as a full-fledged artificial intelligence and recognizing the possibility of their full-fledged thinking and solving creative tasks (Lee et al., 2021). This basic thesis is important as a starting point in arguments about the applicability and necessity of innovative big data technologies in the activities related to the preparation and conduct of procurement.

It should be noted also that in modern procurement there is no universal tool capable of leveling, or at least minimizing, the risks of any procurement. E-auction, for example, failed to become such a tool. Neural networks will not become such a tool in the foreseeable future. Moreover, when purchasing standardized, serial products, the use of neural networks for market analysis and selection of the winner often appears redundant.

However, when purchasing complex, and even more so unique equipment, the number of factors influencing the quality of the purchase, as well as the interrelations of these factors, is so large that machine processing of information is necessary for successful selection of the winner. Sometimes such processing requires not just automated calculation of parameters according to a matrix predetermined by a human, but the participation of artificial intelligence.

Actually, the amount of data to be processed for a quality purchase, if not beyond human capabilities, then sometimes requires an unjustified amount of resources – in other words, a lot of time of highly qualified specialists. Even worse, while processing this massive amount of data, such specialists will spend most of their time not on expert assessment, but on routine work: comparing indicators, making tables, etc.

Artificial intelligence can do this job incomparably faster, and perhaps better. However, the problem is that decision-making by artificial intelligence within the business processes cannot be fully transparent. Big data processing remains a "black box" for an outside observer to a certain extent: input parameters and the result obtained are clear, but transforming one into the other cannot be fully controlled by a human being.

This raises several questions that require, among other things, legal resolution. Is it appropriate to use artificial intelligence in business processes in general and in procurement in particular? Who is responsible for the decisions made by artificial intelligence? What is the role of humans in this relationship?

Using inductive reasoning from particular to general, as well as based on the methods of synthesis, analogy, generalization and using a practical situation as an experimental model, we will try to answer these questions on the example of procurement of complex products for high-tech research. Below, the basic parameters of this procurement will be presented in the description of the case study; then, the key theses will be proposed in the discussion section and summarized in the conclusion.

1. Subjectivity of AI in procurement relations

First of all, it should be noted that there is no universally established definition of artificial intelligence in general and neural networks in particular. It does not exist in normative acts or legal doctrine. As a rule, researchers write about the combination of digital environment, autonomous functioning of an algorithm, and its ability to self-learning and targeted processing of large arrays of information.

For example, it is proposed to view AI as an electronic system capable of physically manifesting itself, including the ability to sense, process information and influence the world around it to some extent (Calo, 2015). In extreme expression, this approach is manifested in the concept of so-called strong artificial intelligence, under which researchers understand the technology which, by its mental properties and the nature of processing the information available to it, is identical to human consciousness, including in terms of complex interpretation of information and ability to creativity and intuition (Searle, 1990).

An alternative approach to understanding artificial intelligence is based not on the external expression and consequences of its activity, but on the subjective factors of its work. The followers of this approach are ready to call artificial intelligence any intelligence that realizes itself as an independent personality, regardless of whether it is comparable to human intelligence or even inferior to it in terms of intellectual capabilities (Bokovnya et al., 2020). Despite the apparent simplicity of this approach, in today's practice it is not easy to find an example of an AI that identifies itself as not just a thinking subject, but as an independent individual. This is not only due to the imperfection of robotics technologies. Despite the active development of science, the thesis remains relevant that attempts to create artificial intelligence in the true sense of the word have not yet reached the expected level due to discrepancies between the humanity's knowledge of the brain

structure and the capabilities of neurobiology, psychology, and cybernetics (Hawkins & Blakeslee, 2004).

Therefore, today one should recognize that the most realistic concept of artificial intelligence is that of a hardware-software complex having nothing in common with the human mind in terms of the essence of thinking, but capable of solving tasks similar in complexity or more complex (Bokovnya et al., 2020).

For example, in the variant proposed by N. N. Chernogor, the definition of artificial intelligence is as follows: "A technology that defines the ability of some information system to correctly interpret external data (external information) without direct human participation, to refine the database(s) taking these data into account, to learn from the mistakes made and to use the knowledge gained to achieve specific goals, solve specific tasks through flexible adaptation in a poorly defined situation" (Chernogor, 2022). These attributes are best suited, if not for the theory of procurement activity, then, at least, for its practice.

Thoughtful regulation of procurement relations, implemented with the use of artificial intelligence technologies, is impossible without resolving basic questions about the correlation of rights and obligations. In the context of using artificial intelligence technologies, these questions are directly determined by the problem of artificial intelligence subjectivity. Simply put, can we consider artificial intelligence as a subject of legal relations or only as a tool used by other subjects to implement their legal relations?

It is necessary to specify from the very beginning that the issue of the legal subjectivity of artificial intelligence cannot be solved once and for all. "What constitutes AI is subjective and best described as moving target. What AI is for one person may not necessarily be AI for another, what was considered AI say fifteen years ago is nowadays considered commonplace and even the question of 'what is intelligence?' is contested and debated" (Greenstein, 2022). This is the case when not only individual legal relations, but also basic aspects of legal capacity and legal personality depend on the level of technology achieved at a particular time (we are talking not only about the parameters of technology itself, but also about the quality of its application, including in economic relations).

However, today, even with the active development of neural networks and the widespread robotization of production, the thesis remains relevant that the existing concepts of legal capacity and legal capability obviuosly do not provide for even the theoretical possibility that artificial intelligence possesses them, and the application of legal subjectivity to artificial intelligence means only a mechanical extrapolation of human rights to the actions of artificial intelligence (Nevejans, 2016).

This is largely due to the fact that law as a product of human intellectual activity and a result of social relations development is anthropocentric by its very nature. Not even subjectivity as such, but the legal subjectivity of entities that are not identical to humans, is a fundamentally new category for the system of existing legal institutions. But no less important is the fact that AI activity in its external expression today does not imply, not to mention identity, but even close similarity to human activity, even taking into account

that the speed and volume of information processing by a neural network quantitatively incomparably exceed human abilities. This means that "the approaches proposing to justify the legal personality of robots and AI taking into account the essence of animated subjects who have real, not only formal-legal will, will be developed only after the development of digital technologies reaches an objectively high level" (Begishev, 2020).

At the same time, the conventionality of the term "artificial intelligence" does not mean that the technology itself is doubtful. Self-learning algorithms for big data processing are already showing their applied significance. Not being a panacea, big data processing technologies, and in particular, those called neural networks, are a factor of economic success in the modern world.

Undoubtedly, economic success requires rational and thoughtful "targeted" application of neural networks in those spheres of economic relations where they can bring maximum benefit. This, in turn, requires modern regulation based both on understanding of the essence of economic relations and on understanding of modern technologies.

The use of such technologies in procurement should be based on the primacy of the fact that "relations with the use of artificial intelligence are always relations between subjects of law or in relation to objects of law. In any case, these are relations that at one stage or another are initiated, or programmed, by a person – a subject of law with a certain degree of liability (including within the activities of legal entities). The human will for certain actions of artificial intelligence can be expressed in different degrees: from AI actions under the full control of human will to autonomous AI actions, also allowed and realized in their possible limits and consequences by a person (group of persons)" (Shakhnazarov, 2022). Only this approach today allows us to solve a number of organizational and legal issues: from the definition of the sphere of effective AI application to the distribution of responsibility for the consequences of its functioning.

Today, we can only partially agree with the thesis that "legal professionals do not have to comprehend the mathematical and technical mysteries of digitalization; digitalization is not a matter of legal science. We have to write about this because many of those who have devoted their research to digitalization ignore the fact that sciences are divided into technical and social ones; legal sciences are social ones and technical norms are not the subject matter of their analysis" (Lazarev, 2023). However, this thought reminds us of the most important thesis: a regulator must not and cannot replace an engineer. The law created by the regulator must be adequate to the regulated relations, which in the case of AI regulation is impossible without participation of experts in modern technologies.

At the same time, experts in digital technologies, AI in particular, must not replace the regulator and try to use legal categories that are not typical for certain relations to regulate them. This is especially important when we talk about the legal consequences of relations implemented with the use of modern digital technologies. "From the ontological viewpoint, all advanced technologies are not subjects but objects, and there is no reason to grant them rights or hold them legally liable. Even in light

of the existing rules of legal liability, based on various legal criteria, it is always theoretically possible to identify a person who would be liable for damages resulting from the production or operation of a device with an AI system" (Ivliev & Egorova, 2022).

A specific consequence of the AI legal personality issue is the question of its tortability. Regulation of AI is required, among other things, to prevent the dilution of responsibility for the consequences of AI operation. The matrix of such liability is a topic for a separate study, but in any case, today it is important to remember the basic principle: a definite physical or legal person is liable for the consequences of the work of artificial intelligence.

Due to the specificity of AI tortability, or rather due to its absence at the current stage of its development, the introduction of this technology can only be heterogeneous. Maximally simplifying, the degree of AI diffusion should be inversely proportional to the risk to human life and health in the relevant sphere.

In practice, the use of AI in economic activities is associated with the risk of harm caused by it, which is also the subject of special research (Bertolini, 2013). At the same time, US experts are already discussing the need to implement the concept of criminal liability for AI actions, taking into account the guilt of the creator, programmer, user and other persons involved in the work of AI (Hallevy, 2013). An alternative solution to the issue is to give artificial intelligence the legal personality of legal entities, such as corporations: this approach allows applying liability to AI with the help of legal fiction and at the same time provide real compensation for the damage caused (Chesterman, 2020).

On the one hand, the use of AI technologies in the preparation of procurement, in the description of requirements to the products to be procured, in the selection of the winner of the procurement and at other stages of procurement process allows minimizing the risk of subjectivism of the customer's official. This risk is traditionally considered to be one of the fundamental risks in procurement. On the other hand, AI technology gives rise to a number of specific risks due to its use, or, more precisely, its imperfections.

"Using AI models may lead to risks based on incorrect or misinterpreted model results. The risk actualization may lead to financial losses, erroneous decisions, and reputational consequences. <...> The model may contain fundamental errors (e.g., program code errors), which may lead to incorrect calculations and inaccurate forecasts. The model may be misused. Because AI models are trained to solve specific problems, applying them to solve other problems may lead to erroneous performance results. The data used in the model operation may differ significantly in statistics from the data on which it was developed. Inaccurate and incomplete data may distort the process of identifying patterns and lead to erroneous results"[1].

[1] Bank of Russia. (2023). Using artificial intelligence in financial markets: report for public consultations (pp. 28–29). Moscow.

The risks associated with information security are also intuitively obvious in the context of using AI. Moreover, these risks can be actualized both as confidential information leakage and as malicious influence on the algorithms of information processing in order to distort the results of such processing.

Finally, it should be mentioned that both researchers and practitioners note that neural networks are subject to the risk of "drift": the functional abilities of the model in solving individual tasks regress over time[2]. The question of the reasons for such regression remains open, but the very existence of such a risk should be taken into account, both when AI is introduced into business processes and when the relevel regulatory norms are formulated.

2. Sphere of using AI in procurement

To determine where AI can be used effectively, at least two factors should be combined. First, the customer must have well-developed and streamlined procurement practices with completed stages of digitalization and automation. It is extremely difficult and often unreasonable to use AI technologies where some procurement documents are paper-based and decisions are made by nontransparent rules. Secondly, it is necessary to identify those procurements where the use of AI would have an obvious positive impact on the result. And, of course, the introduction of modern AI technologies requires organizational, financial and time investments; therefore, one must make sure that these investments will pay off with the effect of AI application.

Speaking of the first factor, we should first of all distinguish between the concepts of digitalization and automation. Digitalization refers to the transfer of business processes into an electronic environment. As a rule, digitalization involves executing business processes on the Internet and certifying transactions with electronic signatures. Digitalization is a necessary but not sufficient condition on the way to automation, as it often does not imply optimization of existing business processes. On the contrary, automation means exactly the optimization of business processes through the introduction of machine processing of information, thus representing the next qualitative step in the introduction of electronic technologies.

The Russian contract system (although it is not unique in terms of the aspects listed below) can be given as an example. Its digitalization began in the early 21st century. At first, the institute of electronic signature was legally regulated to serve as a legal basis for performing legally significant actions in the electronic environment. Soon after that, electronic trading platforms – specialized portals for competitive procurement in electronic form – began to emerge. Then the largest customers gradually digitized the entire cycle of procurement relations from procurement forecasting and planning to contract conclusion and execution.

---

[2] Chen, L., Zaharia, M., & Zou, J. (2023, July). How is ChatGPT's Behavior Changing over Time? https://clck.ly/3CdmQ3

The Law of the People's Republic of China dated August 31, 2018 "On E-Commerce" regulated the concept of an operator of an electronic trading platform as an organization that provides two or more parties with the opportunity to trade services, run online stores, search for sellers and buyers, and publish information necessary for such activities[3]. The Chinese legislator distinguished three types of similar entities involved in the operation of ETPs:

– an ETP operator as an incorporated or unincorporated entity that offers an online space for digital business and the parties' mutual settlements, information exchange and other services that facilitate the conclusion of an e-commerce transaction by its parties;

– an operator functioning on an ETP, i.e. a user of an electronic trading platform;

– an online seller as a participant in the e-commerce market that does not use an ETP, but sells goods, works or services via one's own website or via other information channels on the Internet.

This said, the ETP operator has the obligation to ensure cybersecurity[4], as well as the formation and maintenance of a system evaluating the users conducting business activities via the ETP[5].

Procurement in electronic form allowed significantly increasing the transparency of work (which is especially important for public procurement), as well as to optimize organizational costs of procurement business processes. But in essence, these were the same business processes that had previously taken place outside the digital environment. To qualitatively modernize the business processes, automation tools were gradually introduced into procurement, namely, processing of certain amounts of information according to a set algorithm without human participation. An example of such automation in procurement is end-to-end data inheritance: information of the previous document is pre-filled in the forms of each subsequent document within a single procurement cycle. Another example is the automated selection and ranking of preliminary offers for supply; in Russia the procedure is called small electronic procurement, and in international practice – dynamic procurement ("Dynamic purchasing systems" in the Directive 2014/24/EU on public procurement[6] and "Sistemi dinamici di acquisizione" in the Italian Procurement Code[7]).

Hence, it can be stated that since the beginning of the 21st century, "qualitative changes have taken place in Russian procurement. At the moment, not only the issues of modernization of business processes and economic efficiency come to the forefront. The state is trying to systematically approach the procurement issues by optimizing all

3 Art. 9 Law of the People's Republic of China dated August 31, 2018 "On E-Commerce".

4 Art 30. Law of the People's Republic of China dated August 31, 2018 "On E-Commerce".

5 Art 39. Law of the People's Republic of China dated August 31, 2018 "On E-Commerce".

6 Art. 34 Directive 2014/24/EU on public procurement.

7 Art. 55 Codice dei contratti pubblici.

related processes at each stage of the procedure and introducing end-to-end automation. As noted by customers, electronic procurement procedures provide optimization of budget and labor costs, increasing procurement efficiency by an average of 25–30%" (Shmeleva, 2019a).

If end-to-end digitalization is implemented and automation tools of at least the basic "nodes" of procurement are introduced, we can talk about the presence of prerequisites for using artificial intelligence technologies. However, even with such a basis, one should not strive for total application of AI to the entire spectrum of procurement activities. From the viewpoint of optimizing business processes, neural networks are needed only where their application will help to significantly reduce time costs and at the same time improve the quality of procurement.

As a practical example, consider a procurement that actually took place during the construction of a magnetic path on a project at one of Europe's largest research centers specializing in nuclear physics. The project required a new accelerator facility to study the properties of dense baryonic matter.

The magnetic path necessary for the operation of this particle accelerator facility is a quickly erectable structure weighing more than 700 tons with special material and magnetic properties. The magnetic path housing is a key part of the detector operating as part of the accelerator complex. Both the purpose of this complex and the technical characteristics of the magnetic path can undoubtedly be categorized as science-intensive.

The Research and Development Center as the project's lead organization developed the design documentation of the future magnetic path. According to the design documentation, the production of the main parts of the magnetic path was divided between two manufacturers, which were to perform production in parallel. Parallel production, in turn, was necessary to meet the project implementation deadlines.

Manufacturers were plants in different countries: one of them was located in Kramatorsk and the other in Genoa. The parts manufactured at these plants were sent to the Czech Republic for processing and preliminary assembly. Also, in the Czech Republic, structures were produced to transport the individual parts of the product to the R&D center, the place of their final installation.

After manufacturing at the factories, the basic construction elements underwent a complex process of acceptance testing, in which parameters of each element, such as size, chemical composition, mechanical properties, magnetic properties, etc., were strictly checked. If even one of the parameters was found to be deviated, the entire project could have been jeopardized.

After successful acceptance at the manufacturing plants, the semiproducts were shipped to the Czech Republic. Given that the semiproducts were produced in different countries, it was important to ensure that the correct customs regime for importing them into the Czech Republic was selected for their subsequent simultaneous processing. In order to start processing the supplied semiproducts, the Czech plant developed its

own engineering documentation based on the R&D center's documentation, which included the following sections:

1. Input inspection of semiproducts: measurement of dimensions, measurement of parts geometry, preparation of technical data sheets.

2. Procedure for processing of semiproducts.

3. Requirements for the manufacture of parts necessary for the assembly of the magnetic path.

4. Requirements for the manufacture of tooling for the assembly and disassembly of the magnetic path.

5. Worksheet of the magnetic path control assembly at the factory with the participation of representatives of the research center, including installation and adjustment of the mutual arrangement of the cradle parts.

6. Methodology for measuring the horizontality of the base plates and control measurements of the plate geometry at various stages of assembly.

7. Procedure of preparation for shipment: drilling of holes and location of fixing pins after control assembly, marking of pins, creation of a map of pin location, disassembly, packing, loading, and transportation.

Finally, the R&D center organized a temporary customs zone for customs clearance of components imported from the Czech Republic. This was due to the size and weight of the individual parts, which did not allow the said products to be brought to standard customs terminals.

The example briefly described above shows that the integrated procurement of high-tech products is a full-fledged multi-stage project that may involve enterprises from different countries. This procurement is not limited to a tender, but includes tasks in a wide range of areas. Each of these tasks is closely related to adjacent ones and directly affects the success of the entire project. Successful implementation of such a purchase requires expert research in engineering and technology, logistics, customs clearance, accounting, the tender per se, and the preparation and conclusion of an international contract. The procurement complexity is aggravated by the fact that failure in any of these areas makes it impossible for the end user to run the high-tech product.

What key risks can be seen in the above example?

First of all, it is the risk of choosing a supplier. An inexperienced, unskilled manufacturer (or simply a plant without the necessary equipment) will not be able to produce the relevant high-tech products.

The second risk is the risk of errors in technical documentation. Incorrect calculation or just incorrect description of data at one of the manufacturing or assembly stages can jeopardize the result of the entire delivery.

The third risk is the risk of transportation. It is important to take into account that the dimensions and weight of individual elements of the described equipment required a dozen trucks for transportation. At the same time, the cost of high-tech products dictated increased requirements for safety during transportation.

Since the purchase of high-tech products is often associated with international cooperation, the risk of customs clearance is next to the logistics risk. The fact that the end

user was a scientific organization located outside the EU only increased the significance of this risk.

Finally, one cannot discount the risk of errors in contractual arrangements and payments for manufacturing, set-up and transportation. Correct, timely and accurately executed settlements for such a purchase are a challenge. Unforeseen offsets and the need, for example, to purchase additional tools for the contractor at the customer's expense only add to the difficulties and increase the risk of unintentional error.

Traditionally, such risks are fully assigned to the customer and supplier employees. In this situation, the possibility of minimizing each risk depends entirely on the employee's qualification, level of knowledge, the amount of information available and the time for its processing. However, the modern level of information and management technologies makes it possible to separate human professional knowledge and competence from the tasks of collecting and processing information. After all, AI is capable of processing incomparably large amounts of information in much less time.

It seems that for solving exactly such tasks in the field of business management, the key issue is not the essence of cognitive processes or self-identification, but the ability to process large volumes of information in less time and at lower costs compared to a human or a group of people. Big data processing is an area of effective application of artificial intelligence. In the above example, it can be, first, data on the qualifications of potential producers, including information about their experience, qualification of employees, production culture, availability of necessary equipment, compliance with social and environmental responsibility, financial sustainability, etc. Secondly, it is data on possible logistical combinations and related transportation, administrative, weather and other risks. Thirdly, it is processing an array of engineering and technical information and forming proposals for the optimal parameters.

"When making purchases, managers and specialists have to study a huge amount of information to make the best decision. A lot of processes depend on the human factor, subjective opinion, established stereotypes of thinking. Artificial intelligence in procurement has a number of undeniable advantages. These are, for example:

1. Analyzing information about suppliers. Artificial intelligence is able to quickly and effectively provide work with suppliers. It easily finds counterparties and their contacts, provides information about the company financial condition and analyzes customer feedback on the quality of their work. At the same time, the time to process information is significantly reduced and its quantity is increased.

2. Cost management. Artificial intelligence based on machine learning can analyze costs for a certain period of time and identify situations in which there was a real opportunity to save money. Program complexes are able to quickly compare purchase prices, compare them with indices on the market and recommend a more favorable offer.

3. Risk management. Artificial intelligence collects information about possible risks in the supply chain. In doing so, the business can increase the speed of order processing, optimize costs and improve the quality of purchased products <...>.

4. Planning the purchase volume and price. Artificial intelligence takes into account average costs for the previous period and significant changes that can make differences. To calculate the optimal price, it uses data on the company's budget, general market situation, characteristics of demand and tax obligations"[8].

It is important to emphasize: information processing is not the same as decision making. In the case of robotic procurement, this means that the expertise of authorized employees is not removed from procurement preparing and conducting. The AI merely offers the experts collected, prepared and structured information. At the same time, the expert has the authority to both verify and supplement the data provided by the AI and to formulate conclusions based on that data. In other words, the rational use of AI technologies in procurement does not exclude, but enhances the expert component of human work.

3. AI when preparing procurement

Conventionally, the use of AI in procurement can be divided into robotization of procurement preparation and robotization of procurement implementation. These two areas can be developed and regulated in parallel and separately.

For example, today market research as a crucial stage of regulated procurement is often ignored or largely reduced. However, it is market research that can give an adequate answer to the question not only about the initial (maximum) price, but also about the most effective procurement method. Neural network is able to collect and process information from the maximum number of open sources in minimal time, as well as to structure it according to the parameters set by a human.

Thus, for a reasonable price calculation, it is important to take into account not only abstract indicators like inflation rate or several price lists from randomly selected suppliers, but also factors of seasonality, logistics, availability of production facilities and volumes of these facilities, cost of ownership, costs of potential equipment repairs and associated downtime, etc. Taking into account all these factors, the price becomes not a rather conventional indicator, but the results of actual market research. Also, by using a neural network, the much-speculated human factor, which in one form or another has a significant impact on the results of determining the initial maximum price (hereinafter – IMP), can potentially be minimized to a certain extent, if not completely eliminated.

No less important is the choice of a relevant procurement method based on the market research results: the statistics of failed auctions inevitably suggests that classical price competition may not always give the expected effect to a customer. To choose the best method, it is important to take into account the level of formal and actual competition in the market of products to be purchased, the degree of price elasticity (without which the auction loses much of its meaning), the importance of non-price factors in choosing

8 Big data in procurement management. Platforma. https://clck.ly/3CdmRP

the best offer, and in the case of public procurement – also the reputation of the contract system among local suppliers. Such research requires processing of even larger amount of information than when justifying the IMP. A neural network could well serve as a tool for processing such information.

One cannot but mention such labor-intensive work as compiling requirements to the products to be procured and requirements to the procurement participants. Both categories of requirements must simultaneously satisfy the utmost accuracy of description (to guarantee the delivery of quality products to the customer) and universality of wording (to avoid unreasonable restriction of competition). If we are not talking about ordering serial mass-market products, but, for example, about installing engineering infrastructure, then the urgent need to draw up complex technical documentation is added to the above.

Procurement preparation has traditionally remained an internal matter for the client. This is true even though public procurement laws in most countries regulate some elements of such preparation in one way or another – for example, selection of the procurement method, drafting requirements for potential suppliers, etc. It can be argued that the introduction of AI technologies in preparation for the competitive procurement announcement will not require breaking existing norms or radical changes in legal relations in procurement. It is more appropriate to speak not so much about changing the legislation, but about supplementing it.

For example, the choice of a procurement method from among the tools provided for by the legislation may be legally stipulated based on not only formal attributes of procurement (such as the size of IMP or the category of products to be purchased), but also the results of market research conducted by AI. In both cases, the human factor, potentially involving a risk of abuse, is excluded from decision-making. In both cases, the grounds for selecting a procurement method remain transparent. At the same time, the selection of a procurement method based on the results of AI research may in many cases be more effective in terms of actual procurement practice than making the same decision based on formal criteria.

Simply put, all that is needed to use AI in procurement preparation is its legalization. The procurement preparation may become simpler and more efficient. At the same time, the introduction of AI will neither fundamentally revise nor dilute the procurement preparation process.

4. AI when conducting procurement

The situation is somewhat different when it comes to the introduction of AI into the procedure of competitive supplier identification. This activity traditionally belongs to the tender commission. Although the AI use will not lead to the exclusion of the commission from the procurement work (key decisions on the selection of the tender winner will in any case be taken collegially), but the AI involvement in the commission

work will require an essential adjustment not only of the norms, but partly even of the established institutions of procurement legislation.

New technologies do not and should not encroach on such fundamental principles as transparency and efficiency of public procurement. The use of these technologies should not lead to unreasonable restriction of competition between potential suppliers. However, the very tools for implementing these basic principles in practice may undergo significant change with the introduction of AI.

For example, traditionally, the powers of the tender commission include the decision on the compliance or non-compliance of a bidder with the requirements of the procurement documentation. This is one of the key decisions in the procurement process, as only suppliers recognized as compliant with the requirements of the procurement documentation can claim victory. Often, making this decision involves the examination of a large volume of documents submitted by suppliers. But we should not forget that the use of AI will help to significantly reduce the labor costs of such in-house procedures.

Already today, a participant in a regulated procurement declares its compliance with a number of requirements. If the status of the declaration legally included the right of the customer to verify its contents, then such verification could be entrusted to a neural network. Of course, both positive and negative results of the verification should contain a reference to the information sources that served as a justification for the decision, while the decision itself remains with the procurement commission.

Reducing the cost of checks through the use of AI will allow taking into account a wider range of factors affecting the supply quality during such checks. For example, already today, PRC legislation very rationally requires: "If the matter of a tender is a project involving construction work, the bid shall contain brief biographical information and work experience of the prospective project manager and key technical personnel, as well as the technical specifications of the equipment that will be involved in the project"[9]. Not only work experience, but also the history of interaction with previous customers, the equipment used for production, the culture of production and even the chain of suppliers – all these factors are essential and sometimes decisive for the selection of a contractor, especially when ordering the manufacture of complex and high-tech products.

At the same time, we should not think that AI will autonomously select the procurement winner and reject the proposals of their competitors. Here it is appropriate to recall the theses with which this article began: if we consider AI not as a subject, but as a tool for procurement, then authorized specialists should be responsible for the consequences of processing information with the help of a neural network. This means that first in the corporate and then in the normative regulation it is necessary to establish a matrix distributing responsibility for the consequences of the use of neural network

[9] Art. 27 of the Law of the People's Republic of China of 30.08.1999 "On tenders".

between such specialists and other subjects that influenced the AI in processing particular information.

At the same time, it would be wrong to assume that the distribution of responsibility for the AI work means an increase in the responsibility of authorized subjects. By and large, there is no question of new spheres of responsibility at all: today, tender commission specialists are just as responsible for the validity of decisions to evaluate and compare bids, and tools like neural networks only facilitate the preparatory work for making such a decision.

This thesis is also true for one of the boldest areas of AI potential use in procurement – selecting the procurement winner. Of course, we are talking about multifactor selection. After all, to speed up an auction, a combination of automation tools and suppliers' preliminary offers is largely sufficient. But if one needs to find the balance between price and quality, then it is neural networks that can be authorized for such multi-criterial comparison.

Without being a subject of a legal relationship, AI can become a participant in it simply because it can ensure higher efficiency of economic relations. "Lawyers should already develop norms regulating situations where autonomous algorithms will be able to complement and replace human discretion in determining optimal legal norms and will be able to find relevant differences between people and use them to personalize sanctions, rights and obligations" (Kharitonova & Qi Sun, 2023). With AI, it is possible to use a large number of criteria for comparing offers while maintaining the overall transparency of the comparison logic. This approach, among other things, will help to significantly minimize the risk of subjectivity in evaluation. After all, this risk is one of the most popular arguments when criticizing any alternative to the auction.

One should not forget the dynamic procurements mentioned above. For their success, suppliers need to place and duly update their preliminary offers for supply on a specialized platform. When the customer declares the need for a particular product on that platform, the platform algorithms automatically select preliminary offers relevant to this need. Thus, a full-fledged comparison of competing offers is carried out, but due to the automation of collecting these offers, the whole procedure takes a few days, not weeks, as it is required by the classical tender.

However, the success of such a competitive procedure requires the quality of not only the customer's description of their need, but also the potential supplier's description of their preliminary offer. Today, AI technologies are already quite capable of optimizing both descriptions (of course, the final revision is left to humans in any case). In addition, in dynamic procurement, AI could remind suppliers of factors that may require them to update their preliminary offers.

Finally, it is appropriate to use a neural network for such highly specialized, yet extremely important work as determining the category of products offered by a supplier, because the accuracy of the category definition may determine whether a preliminary offer gets into the automated sample. "When users post information about their products in the catalog, they have to assign them to a certain category: paper, printing products, medical

products, pet products, stationery, textiles, engineering and construction products, furniture, etc. Earlier, they had to manually select the right category from a long list, which was time-consuming. Neural network has spared suppliers from the routine procedure. It is sufficient to upload a picture of the product, and the artificial intelligence will analyze it in a few seconds, then offer suitable categories to choose from. According to statistics, the accuracy of the category definition today is 92 %. This figure will grow as the neural network, like a chatbot, is constantly learning and adding to its knowledge based on different models"[10].

The examples described above do not exhaust the potential of using AI in competitive procurement. Some of the directions described above practically do not require adjustment of the legislation – for example, the use of neural networks to improve the efficiency of dynamic procurement. Other directions will require the formulation of norms and rules for the use of new, previously unknown tools – for example, multi-criteria selection of the winner with participation of AI. But in any case, we can say that the use of digital technologies is already becoming a factor in the quality of procurement.

Conclusions

Summarizing the above, we should recognize that it is impossible to introduce artificial intelligence technologies in procurement without adjusting the existing regulations. However, it is in the field of procurement that we are talking only about adjustments, not about breaking the entire regulatory system. At the same time, from the viewpoint of the regulated relations, the introduction of artificial intelligence technologies seems both appropriate and justified. These technologies, if used thoughtfully, can not only improve the quality of work and significantly reduce organizational costs, but also serve to develop the basic principles of regulated procurement: transparency of procedures, development of competition for contracts between qualified suppliers, reasonableness of decisions, and economic efficiency of using the customer's money.

As a minimum, the following areas of AI potential introduction into procurement can be identified:

1. Forecasting the need for purchased products and managing warehouse reserves in general.
2. Managing current contracts, controlling their execution.
3. Assessing the needs and evaluating the necessity of procurement to fulfill them.
4. Assessing risks.
5. Formulating a list of requirements for the subject matter of the procurement, preparing procurement documentation.

[10] Smart procurement: how artificial intelligence and API services help the users of Suppliers' platform. (2023, March 17). Tadviser. https://clck.ly/3CdnFb

6. Preliminary research of the market for the products to be procured, selecting procurement tools.

7. Collecting proposals from potential suppliers.

8. Evaluating and comparing proposals of potential suppliers.

9. Managing supplies.

In each of these areas, AI does not replace humans, but only helps them to make better-informed decisions while spending less time and effort on such decisions. "Artificial intelligence should replace routine processes: collecting, filtering and classifying data on expenditures, after which signs of irrational spending are identified in an automated mode. Analytics is primarily based on information about purchases already made. As a result, the use of artificial intelligence technologies in the procurement automation will significantly expand program capabilities in the areas of automated price monitoring, comparison of procured goods, which will make it possible to select the most optimal contractor" (Sergeeva, 2022).

Therefore, the enquiry for the legal expert community consists only in identifying pilot areas for the use of neural networks in procurement, outlining the framework for the use of this technology in these areas, and regulating the powers and responsibilities of the subject of the use of neural networks. This work will require technological expertise. However, it does not look unfeasible. Then, its results will serve as a basis for the gradual introduction of modern technologies in related industries (Siciliani et al., 2023; Burger & Nietsche, 2023).

Yes, within the current norms, the implementation of neural networks in all the named fields is not an easy task. Even generalizing as much as possible, it is worth remembering that "the digitalization of public procurement is not just a matter of acquiring the most advanced technologies. It also requires changes in procurement tools and methods that would allow the state to interact with new technologies, as well as effectively and quickly integrate them into practical reality" (Shmeleva, 2019b). However, fundamental, revolutionary transformations in such implementation may well be avoided.

The point is that in all the situations described above, the neural network remains a tool by its status, while a human being remains the decision-maker. Moreover, when using a digital tool, both the input parameters, set to the neural network for information processing, and the output parameters are fixed and thus become transparent. The authorized entity may accept or change them. The justification for the changing is also recorded in the electronic environment.

In other words, it is in the field of procurement that the introduction of artificial intelligence as one of the tools is possible while preserving the body of the current legislation in general and the system of information support of procurement in particular. It will only require to supplement certain norms, such as norms on IMP justification, evaluation of procurement participants, etc., through legalization of an alternative decision-making mechanism. It is important that this mechanism is aimed not only at increasing the speed of processing large amounts of information, but also at minimizing the risk of subjectivity

in decision-making. Simply put, the use of neural networks does not violate, but develops the principles of procurement regulation.

It is by no means a question of completely replacing contractual services with neural networks, as is often discussed in relation to other professions. In procurement, the task of a neural network is exactly the opposite: firstly, to facilitate the work of the contract service by "taking over" labor-intensive routine, and secondly, to enable contract service staff to focus on issues requiring high professional expertise.

References

Begishev, I. R. (2020). Artificial intelligence and robot as legal categories. *Bezopasnost Biznesa*, *6*, 32–36. (In Russ.).

Bertolini, A. (2013). Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules. *Law, Innovation and Technology*, *5*(2), 214–247. https://doi.org/10.5235/17579961.5.2.214

Bokovnya, A. Y. Begishev, I. R., Khisamova, Z. I., Narimanova, N. R., Sherbakova, L. M., & Minina, A. A., (2020). Legal Approaches to Artificial Intelligence Concept and Essence Definition. *Revista San Gregorio*, *41*, 115–121. https://doi.org/10.36097/rsan.v1i41.1489

Burger, M., Nitsche, A., & Arlinghaus, J. (2023). Hybrid intelligence in procurement: Disillusionment with AI's superiority? *Computers in Industry*, *150*, 103946. https://doi.org/10.1016/j.compind.2023.103946

Calo, R. (2015). Robotics and the New Cyberlaw. *Californian Law Review*, *103*(3), 513–563.

Chernogor, N. N. (2022). Artificial intelligence and its role in the transformation of the modern law and order. *Journal of Russian Law*, *4*(26), 5–15. (In Russ.). https://doi.org/10.12737/jrl.2022.037

Chesterman, S. (2020). Artificial intelligence and the limits of legal personality. *International and Comparative Law Quarterly*, *69*(4), 819–844. https://doi.org/10.1017/S0020589320000366

Greenstein, S. (2022). Preserving the rule of law in the era of artificial intelligence (AI). *Artificial Intelligence and Law*, *30*, 291–323. https://doi.org/10.1007/s10506-021-09294-4

Hallevy, G. (2013). *When Robots Kill: Artificial Intelligence under Criminal Law*. University Press of New England.

Hawkins, J., & Blakeslee, S. (2004). *On Intelligence*. Times Books, Henry Holt and Co.

Ivliev, G. P., & Egorova, M. A. (2022). Legal issues of the legal status of artificial intelligence and products created by artificial intelligence systems. *Journal of Russian Law*, *6*(26), 32–46. (In Russ.). https://doi.org/10.12737/jrl.2022.060

Kharitonova, Yu. S., & Qi Sun. (2023). Rule of law and algorithmization of decision-making in Russia, China, and Europe: prospects for personalization of legal regulation. *Law and Business*, *2*, 11–17. (In Russ.).

Lazarev, V. V. (2023). Legal science in the light of the prospects of digitalization. *Journal of Russian Law*, *2*(27), 5–19. (In Russ.). https://doi.org/10.12737/jrp.2023.013

Lee, J-.A., Hilty, R., & Liu, K-.C. (Eds.). (2021). *Artificial intelligence and intellectual property*. Oxford University Press. https://doi.org/10.1093/oso/9780198870944.001.0001

Nevejans, N. (2016). *European Civil Law Rules in Robotics: Study*. Brussels: European Parliament's Committee on Legal Affairs.

Searle, J. R. (1990). Is the Brain's Mind a Computer Program? *Scientific American*, *262*(1), 26–31. https://doi.org/10.1038/scientificamerican0190-26

Sergeeva, S. A. (2022). Artificial intelligence in the field of procurement: opportunities and prospects. *Innovations and Investments*, *12*, 216–219. (In Russ.).

Shakhnazarov, B. A. (2022). Legal regulation of relations using artificial intelligence. *Acrual Problems of Russian Law*, *9*(17), 63–72. https://doi.org/10.17803/1994-1471.2022.142.9.063-072

Shmeleva, M. V. (2019a). Digital Technologies in State and Municipal Procurement: The Future or Reality. *Actual Problems of Russian Law*, *1*(12), 36–42. (In Russ.) https://doi.org/10.17803/1994-1471.2019.109.12.036-042

Shmeleva, M. V. (2019b). Digital transformation of the system of state and municipal procurement. *Jurist*, *7*, 15–22. https://doi.org/10.18572/1812-3929-2019-7-15-22

Siciliani, L., Taccardi, V., Basile, P., Di Ciano, M., & Lops, P. (2023). AI-based decision support system for public procurement. *Information Systems*, *119*, 102284. https://doi.org/10.1016/j.is.2023.102284

Authors information

Dmitriy A. Kazantsev – Cand. Sci. (Law), member of the Council on Purchasing Development, Chamber of Commerce and Industry of the Russian Federation
Address: 6/1 Ilyinka Str., building 1, 109012 Moscow, Russia
E-mail: info@dkazantsev.ru
ORCID ID: https://orcid.org/0000-0003-2182-5776
RSCI Author ID: https://elibrary.ru/author_items.asp?authorid=1149755

Pavel Dohnal – PhD Candidate, Technical University of Ostrava
Address: 17.listopadu 15/2172, 708 33 Ostrava, Czech Republic
E-mail: pavel.dohnal@vsb.cz
ORCID ID: https://orcid.org/0009-0001-2733-7418

Pavel Dohnal Jr. – graduate student, IT University of Copenhagen
Address: Rued Langgaards Vej 7, 2300 Copenhagen, Denmark
E-mail: pavd@itu.dk
ORCID ID: https://orcid.org/0009-0005-6457-1982

Authors' contributions

The authors have contributed equally into the concept and methodology elaboration, validation, formal analysis, research, selection of sources, text writing and editing, project guidance and management.

Conflict of interest

The authors declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – March 11, 2024
Date of approval – March 26, 2024
Date of acceptance – September 25, 2024
Date of online placement – September 30, 2024

Научная статья
УДК 34:004:347.4:004.8
EDN: https://elibrary.ru/dladns
DOI: https://doi.org/10.21202/jdtl.2024.30

Использование искусственного интеллекта для проведения конкурентных закупок: проблемы правового регулирования

Дмитрий Александрович Казанцев ✉

Торгово-промышленная палата Российской Федерации, Москва, Россия

Павел Догнал

Остравский технический университет, Острава, Чехия

Павел Догнал – младший

ИТ-университет в Копенгагене, Копенгаген, Дания

Ключевые слова

аукцион,
законодательство,
закупка,
искусственный интеллект,
конкуренция,
нейросеть,
право,
регулирование,
тендер,
цифровые технологии

Аннотация

Цель: обоснование перспективных направлений правового регулирования отношений, связанных с использованием технологий искусственного интеллекта в конкурентных (коммерческих и публичных) закупках.

Методы: исследование проводилось на основе индукции, синтеза, аналогии, декомпозиции проблематики и обобщения выводов. Рассуждения строились на опыте проведения сложной закупки высокотехнологичного оборудования. Этот реальный пример был рассмотрен в качестве экспериментальной модели для исследования с последующим прогнозированием потенциального использования технологий искусственного интеллекта в конкурентных закупочных процедурах.

Результаты: сформулированы преимущества и потенциальные риски использования технологий искусственного интеллекта в закупочной работе, а также даны рекомендации по регулированию такого использования. Выделены рекомендации общеправового характера, касающиеся правосубъектности и деликтоспособности искусственного интеллекта, предложены формулировки новых норм, варианты регулирования использования новых инструментов проведения закупок. Доказано, что технологии искусственного интеллекта при продуманном использовании способны не только повысить качество работы и существенно снизить организационные издержки, но и при этом послужить развитию базовых принципов регулируемых закупок:

✉ Контактное лицо

прозрачности процедур, развития конкуренции за подряд между квалифицированными поставщиками, обоснованности решений, экономической эффективности использования денежных средств заказчика.

Научная новизна: несмотря на большое количество работ, посвященных как проблематике искусственного интеллекта в целом, так и его использованию в закупках в частности, данная проблематика рассматривается в статье на основе преимущественно индуктивного рассуждения, строящегося на рассмотрении частного случая и опыте проведения сложной закупки для цели наукоемких исследований, преломляющегося через призму сущностного соотнесения между собой базовых понятий «цифровизация», «автоматизация», «роботизация» и т. п.

Практическая значимость: описанные в настоящей работе направления использования искусственного интеллекта могут быть реализованы корпоративными, а в перспективе и государственными заказчиками для повышения качества своих закупок. При этом рекомендации по нормативному регулированию такой инновации представляются востребованными как на законодательном, так и на локальном уровне.

Для цитирования

Казанцев, Д. А., Догнал, П., Догнал – младший, П. (2024). Использование искусственного интеллекта для проведения конкурентных закупок: проблемы правового регулирования. *Journal of Digital Technologies and Law*, *2*(3), 585–610. https://doi.org/10.21202/jdtl.2024.30

Список литературы

Бегишев, И. Р. (2020). Искусственный интеллект и робот как правовые категории. *Безопасность бизнеса*, *6*, 32–36. https://elibrary.ru/fnittf

Ивлиев, Г. П., Егорова, М. А. (2022). Юридическая проблематика правового статуса искусственного интеллекта и продуктов, созданных системами искусственного интеллекта. *Журнал российского права*, *6*(26), 32–46. https://doi.org/10.12737/jrl.2022.060

Лазарев, В. В. (2023). Юридическая наука в свете перспектив цифровизации. *Журнал российского права*, *2*(27), 5–19. EDN: https://elibrary.ru/wzftgd. DOI: https://doi.org/10.12737/jrp.2023.013

Сергеева, С. А. (2022). Искусственный интеллект в сфере закупок: возможности и перспективы. *Инновации и инвестиции*, *12*, 216–219. https://elibrary.ru/glsnmk

Харитонова, Ю. С., Ци Сунь. (2023). Верховенство закона и алгоритмизация принятия решений в России, Китае, Европе: перспективы персонализации правового регулирования. *Право и бизнес*, *2*, 11–17.

Черногор, Н. Н. (2022). Искусственный интеллект и его роль в трансформации современного правопорядка. *Журнал российского права*, *4*(26), 5–15. EDN: https://elibrary.ru/daazjp. DOI: https://doi.org/10.12737/jrl.2022.037

Шахназаров, Б. А. (2022). Правовое регулирование отношений с использованием искусственного интеллекта. *Актуальные проблемы российского права*, *9*(17), 63–72. EDN: https://elibrary.ru/yownjo. DOI: https://doi.org/10.17803/1994-1471.2022.142.9.063-072

Шмелева, М. В. (2019a). Цифровые технологии в государственных и муниципальных закупках: будущее или реальность. *Актуальные проблемы российского права*, *1*(12), 36–42. EDN: https://elibrary.ru/frvgyv. DOI: https://doi.org/10.17803/1994-1471.2019.109.12.036-042

Шмелева, М. В. (2019b). Цифровая трансформация системы государственных и муниципальных закупок. *Юрист*, *7*, 15–22. EDN: https://elibrary.ru/cirwbi. DOI: https://doi.org/10.18572/1812-3929-2019-7-15-22

Bertolini, A. (2013). Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules. *Law, Innovation and Technology*, *5*(2), 214–247. https://doi.org/10.5235/17579961.5.2.214

Bokovnya, A. Y. Begishev, I. R., Khisamova, Z. I., Narimanova, N. R., Sherbakova, L. M., & Minina, A. A., (2020). Legal Approaches to Artificial Intelligence Concept and Essence Definition. *Revista San Gregorio*, *41*, 115–121. EDN: https://elibrary.ru/efscya. DOI: https://doi.org/10.36097/rsan.v1i41.1489

Burger, M., Nitsche, A., & Arlinghaus, J. (2023). Hybrid intelligence in procurement: Disillusionment with AI's superiority? *Computers in Industry*, *150*, 103946. https://doi.org/10.1016/j.compind.2023.103946

Calo, R. (2015). Robotics and the New Cyberlaw. *Californian Law Review*, *103*(3), 513–563.

Chesterman, S. (2020). Artificial intelligence and the limits of legal personality. *International and Comparative Law Quarterly*, *69*(4), 819–844. https://doi.org/10.1017/S0020589320000366

Greenstein, S. (2022). Preserving the rule of law in the era of artificial intelligence (AI). *Artificial Intelligence and Law*, *30*, 291–323. https://doi.org/10.1007/s10506-021-09294-4

Hallevy, G. (2013). *When Robots Kill: Artificial Intelligence under Criminal Law*. University Press of New England.

Hawkins, J., & Blakeslee, S. (2004). *On Intelligence*. Times Books, Henry Holt and Co.

Lee, J-.A., Hilty, R., & Liu, K-.C. (Eds.). (2021). *Artificial intelligence and intellectual property*. Oxford University Press. https://doi.org/10.1093/oso/9780198870944.001.0001

Nevejans, N. (2016). *European Civil Law Rules in Robotics: Study*. Brussels: European Parliament's Committee on Legal Affairs.

Searle, J. R. (1990). Is the Brain's Mind a Computer Program? *Scientific American*, *262*(1), 26–31. https://doi.org/10.1038/scientificamerican0190-26

Siciliani, L., Taccardi, V., Basile, P., Di Ciano, M., & Lops, P. (2023). AI-based decision support system for public procurement. *Information Systems*, *119*, 102284. https://doi.org/10.1016/j.is.2023.102284

Сведения об авторах

Казанцев Дмитрий Александрович – кандидат юридических наук, член Совета по развитию системы закупок, Торгово-промышленная палата Российской Федерации
Адрес: 109012, Россия, г. Москва, ул. Ильинка, 6/1с1
E-mail: info@dkazantsev.ru
ORCID ID: https://orcid.org/0000-0003-2182-5776
РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=1149755

Павел Догнал – соискатель степени PhD в области права, Остравский технический университет
Адрес: 708 33, Чехия, г. Острава, ул. 17.листопаду, 15/2172
E-mail: pavel.dohnal@vsb.cz
ORCID ID: https://orcid.org/0009-0001-2733-7418

Павел Догнал – младший – магистрант, ИТ-университет в Копенгагене
Адрес: 2300, Дания, г. Копенгаген, ул. Руэд Ланггаардс Вей, 7
E-mail: pavd@itu.dk
ORCID ID: https://orcid.org/0009-0005-6457-1982

Вклад авторов

Авторы внесли равный вклад в разработку концепции, методологии, валидацию, формальный анализ, проведение исследования, подбор источников, написание и редактирование текста, руководство и управление проектом.

Конфликт интересов

Авторы сообщают об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.27.41 / Сделки
Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 11 марта 2024 г.
Дата одобрения после рецензирования – 26 марта 2024 г.
Дата принятия к опубликованию – 25 сентября 2024 г.
Дата онлайн-размещения – 30 сентября 2024 г.

Research article
UDC 34:004:349.2:004.8
EDN: https://elibrary.ru/chpesp
DOI: https://doi.org/10.21202/jdtl.2024.31

Using Artificial Intelligence in Employment: Problems and Prospects of Legal Regulation

Novikov Denis A.

Saint Petersburg State University, Saint Petersburg, Russia

Keywords

algorithm,
artificial intelligence,
digital technologies,
employee,
employer,
hiring of an employee,
labor law,
law,
legislation,
personal data

Abstract

Objective: to identify the legal problems of using artificial intelligence in hiring employees and the main directions of solving them.

Methods: formal-legal analysis, comparative-legal analysis, legal forecasting, legal modeling, synthesis, induction, deduction.

Results: a number of legal problems arising from the use of artificial intelligence in hiring were identified, among which are: protection of the applicant's personal data, obtained with the use of artificial intelligence; discrimination and unjustified refusal to hire due to the bias of artificial intelligence algorithms; legal responsibility for the decision made by a generative algorithm during hiring. The author believes that for the optimal solution of these problems, it is necessary to look at the best practices of foreign countries, first of all, those which have adopted special laws on the regulation of artificial intelligence for hiring and developed guidelines for employers using generative algorithms for similar purposes. Also, the European Union's and USA's legislative work in the area of managing risks arising from the use of artificial intelligence should be taken into account.

Scientific novelty: the article contains a comprehensive study of legal problems arising from the use of artificial intelligence in hiring and foreign experience in solving these problems, which allowed the author to develop recommendations to improve Russian legislation in this area. As for the problem of applicants' personal data protection when using artificial intelligence for hiring, the author proposes to solve it by supplementing the labor legislation with norms that enshrine the requirements for transparency and consistency in the collection, processing and storage of information

when using generative algorithms. The list and scope of personal data allowed for collection should be reflected in a special state standard. The solution to the problem of discrimination due to biased algorithms is seen in the mandatory certification and annual monitoring of artificial intelligence software for hiring, as well as the prohibition of scoring tools for evaluating applicants. The author adheres to the position that artificial intelligence cannot "decide the fate" of a job seeker: the responsibility for the decisions made by the algorithm is solely on the employer, including in cases of involving third parties for the selection of employees.

Practical significance: the obtained results can be used to accelerate the development and adoption of legal norms, rules, tools and standards in the field of using artificial intelligence for hiring. The lack of adequate legal regulation in this area creates significant risks both for human rights and for the development of industries that use generative algorithms to hire employees.

For citation

Novikov, D. A. (2024). Using Artificial Intelligence in Employment: Problems and Prospects of Legal Regulation. *Journal of Digital Technologies and Law, 2*(3), 611–635. https://doi.org/10.21202/jdtl.2024.31

Contents

Introduction

In recent years, in the field of labor relations, artificial intelligence (further – AI) has become the most important tool for implementing management processes and procedures. Large companies and corporations are increasingly inclined to outsource hiring functions to AI technology. For example, the multinational corporation Unilever already processes 1.8 million job applications with AI and hires 30,000 new employees per year (Ginu & Anson, 2021); 99% of Fortune 500 companies (the 500 largest US companies by annual revenue) rely on AI to hire workers (Fuller et al., 2021). Foreign countries use platforms such as AllyO, Arya, BambooHR, Entelo, Ideal, Jibe, Talenture, Taleo, TextRecruit, Textio, Toptal, TurboHire, Turing, Paradox, Recruitee, Upwork, Zoom.ai, and ZohoRecruit.

Russian companies (Alfa-Bank, VTB, Dodo Pizza, Megafon, MTS, Russian Railways, Rostelecom, Sberbank, Yandex, etc.) are gradually integrating AI for hiring into their HR solutions[1]. According to HRlink research, 24% of Russian companies are already using AI in their hiring processes, 6% are planning to implement such solutions within a year, and 71% of HRs positively perceive the introduction of AI in their work[2]. Among AI tools used for hiring in Russia, there are such platforms as AmazingHiring, FriendWork Recruiter, GoRecruit Hireman, HireVue, Hurma, My new job, PeopleForce, Playhunt, Recright, Talantix, uForce, Yva.ai, Robot Vera, SberPodbor, and others[3]. It should be taken into account that these AI services for hiring employees are constantly being improved and supplemented with new functions, including those based on machine learning technology.

The rapid development of software for hiring and its practical application by employers in the Russian Federation raises the question of developing a state policy in this area. The passport of the national program "Digital Economy of the Russian Federation" (approved by the protocol of the Presidium of the Presidential Council for Strategic Development and National Projects of 04.06.2019 No. 7) notes the strengthening of digitalization processes in the sphere of employment and indicates the need to approve the concept of comprehensive legal regulation of relations arising in connection with the digital economy development. In 2020, the authors of this

1 Artificial intelligence started to select personnel in Russia. (2023, 11 August). Ura.ru. https://clck.ru/3CVvmv

2 HRlink research: 71 % of HRs treat AI positively. (2023, 26 December). Artificial intelligence in the Russian Federation. https://clck.ru/3CVvqB

3 In August 2023, the Ministry of Digital Development, Communications and Mass Media of the Russian Federation announced the launch of the State Personnel experiment on the Gostech platform, which involves the use of AI for hiring in the civil service. By 2030, it is planned to create a new information HR system for the development of civil servants based on AI. See: Artificial intelligence will hire civil servants: will the technology replace a tender commission? (2023, August 23). RG.ru. https://clck.ru/3CVvvC

Concept pointed out that in order to transform legislation in the digital economy, it is necessary to focus on changes in labor legislation that relate to the legal protection of citizens under the "information technological innovations in the field of labor and remote employment"[4].

In addition, given that AI has already changed and in the future will change even more the ways in which data on potential employees are collected, processed and analyzed, there are additional risks of human rights violations in labor. Therefore, employees, employers, developers and the state face a logical question about the legal implications of AI in hiring. It is necessary to take into account that along with the allegedly positive consequences of the global transformation of labor relations in the spheres using new information means of production, there are real adverse consequences associated with the redistribution of capital in society and the reduction of social protection of employees (Novikov, 2023). Consequently, the legal problematic of the AI use in hiring is how the relations arising from the AI use for hiring should be regulated and how to evaluate the decisions made by the algorithm from the legal viewpoint.

The problem of using AI for hiring has been discussed in the Russian (Shcherbakova, 2021; Serova & Shcherbakova, 2022) and foreign legal science (De Stefano, 2019; Köchling & Wehner, 2020; Reddy, 2022; Hunkenschroer & Kriebitz, 2023, Basu & Dave, 2024). However, to date, most studies have been fragmentary, covering some parts of this scientific problem. As a consequence, we should pay more attention to the legal problems of using AI in recruitment and try to develop recommendations to solve them within the regulatory framework.

1. Legal problems of using artificial intelligence for hiring employees

The hiring procedure is a series of activities that can be categorized into four main stages: searching, screening, interviewing and selecting[5]. Accordingly, AI in hiring should be understood as an algorithm trained to make automatic hiring decisions at each of the stages (Haenlein & Kaplan, 2019). In hiring algorithms, AI is trained on data from previous candidates before and after hiring in order to make predictions about the employability of potential candidates (Kuncel et al., 2014). Technologies containing such algorithms include asynchronous video interviews, chatbots, and other automated platforms that interpret and evaluate a candidate's response in real time and provide an interview score (Langer et al., 2019). AI algorithms define a set of rules used to transform input data into output decisions and can be trained to mimic human hiring decisions.

---

4 Fund for the Center for new technologies development and commercialization. (2020). Concept of comprehensive regulation (legal regulation) of relations arising in connection with the digital economy development. Moscow.

5 Bogen M., & Rieke A. (2018). Help wanted: an examination of hiring algorithms, equity, and bias. https://goo.su/wc44

Employers using such technologies assume that AI tools are objective and therefore can manage the decision-making free from biases that affect human judgment[6], so that companies can improve employee selection, professional development, retention and performance management (Estrada et al., 2024). Accordingly, it seems logical to conclude that the risk of discrimination and unreasonable rejection of a job application is reduced when using AI, as is the risk of hiring an underqualified worker.

In turn, as was shown in a research by M. K. Lee (2018), workers believe it is fair that humans make the final decision when it comes to employee potential or career development. If people agree that an algorithmic system performs analytical tasks (e.g., job scheduling), then human tasks (e.g., hiring, job evaluation) should be performed by humans. M. Langer et al. (2023) note that the use of AI technology in hiring, coupled with a lack of knowledge and transparency of how algorithms work, increases emotional tensions and decreases interpersonal relations and social interaction. Thus, sociological researches demonstrate that employees recognize the supportive role of AI in hiring, emphasizing the importance of the final decision made by the employer.

On the other hand, a study conducted by Y. Bigman et al. (2023) demonstrated that people are less morally outraged when the hiring decision is made by an AI algorithm rather than a human. However, this result does not prove the impartiality of an algorithm compared to a human decision, but rather confirms people's loyalty to information technology, from which they are less likely to expect bias than from humans. Furthermore, this assumption implies that the developers of such algorithms, the data on which these technologies are built, and the organizations in which they are used, are unbiased. As A. Köchling and M. C. Werner (2020) point out, research of AI-based hiring technologies found that the algorithm can be discriminatory, but the question remains open whether algorithms are fairer than humans.

It can be stated that the use of AI algorithms to hire employees creates a foundation for social contradictions between the parties of labor relations, not to mention the legal issues discussed below.

1.1. Protection of applicant's personal data obtained using artificial intelligence for hiring purposes

On the one hand, personal data can be part of training data used to create new algorithm models by identifying patterns. On the other hand, these mathematical models can be applied to personal data to make inferences or predictions about job applicants. AI allows automatic decision making based on factors and criteria that are not predetermined but vary depending on the database "feeding" the algorithm (Lukács & Váradi, 2023). That is, the entire functioning of an AI-assisted hiring system is based on the processing

[6] UNESCO. Artificial Intelligence: Examples of ethical dilemmas. (2023, 21 April). https://clck.ru/3CVwHU

of employees' personal data. Therefore, it is obvious that automated AI-based hiring decisions come into significant conflict with the requirements of personal data protection.

Current legislation establishes an exhaustive list of documents to be submitted by an employee during hiring. However, the scope and types of information voluntarily submitted to the employer when selecting and interviewing are not defined by law. To date, there is no unified list of personal data that can be used by AI in hiring, as well as no legal mechanism to control their collection, processing and analysis. In addition, the legislation does not limit the employer in the methods and ways of checking business qualities (the wording "in particular" when describing the content of the "business qualities" concept in the Resolution of the Plenum of the Supreme Court of the Russian Federation No. 2 of 17.03.2004 indicates that the attributes of business qualities are not exhaustive). A similar position is presented in judicial practice on cases of various, including psychological, testing during hiring to check business qualities (definition of the Moscow City Court of 24.02.2016 No. 33-3692/16, decision of the Mytishchi City Court of the Moscow region of 21.01.2016 No. 2-396/2016, definition of the Moscow City Court of 21.12.2017 No. 33-52746/2017).

Thus, the procedure for assessing the future employee's business qualities during hiring is not normatively regulated; therefore, the employer is entitled to independently choose the form (including with the use of AI) in which such an assessment is conducted and to fix it in the local acts of the organization. The aspect of transparency and consistency of applicant's data collection using AI is also important and should be formalized in a separate agreement.

Another vector of this problem is that personal data about the job seeker, obtained by the employer as a result of its collection by AI, are confidential and should not be used in any way other than making hiring decisions, nor stored by third parties (e.g., developers) or transferred to them. In this aspect, the greatest risk is the use of "open" AI systems such as ChatGPT, Bard and other chatbots[7]. Information entered into an "open" AI system may be inadvertently transferred to another user and stored in the AI neural network for further training of the system. When using "closed" AI systems (i.e. special developer programs), there is a risk of poor quality data protection and storage protocols, which may provoke leakage and dissemination of personal data of job seekers. It is necessary to take into account the problem of legal consequences of unauthorized use of personal data, which the employer received about the job seeker by means of AI and which were intentionally or negligently (due to unreliable information protection protocols) misused or transferred to third parties.

[7] Markel, K. A., Mildner, A. R., & Lipson, J. L. (2023, September 29). AI and employee privacy: important considerations for employers. Reuters. https://clck.ru/3CVwcu

1.2. Discrimination and unjustified refusal to hire due to the bias of artificial intelligence algorithms for hiring employees

B. Sivathanu and R. Pillai (2018) point out that AI performs the necessary filtering of candidates based on various human characteristics such as experience, age, gender, and qualifications. Accordingly, using machine learning algorithms encoded in AI, patterns or preferences may be found for any of the characteristics that were not perceived by other people, including the data subject. This, in turn, sets the stage for discrimination in hiring and may increase the risks of unwarranted rejections. As a result, problems may arise when employers program an AI system not to hire a particular person or group of people for a particular position, and the system is subsequently trained not to hire that person or that group of people for other positions. It should be noted that an AI system designed to hire workers can only do this if it had been programmed and trained in a certain way using previous hiring data. For example, Sberbank has been using scoring AI to assess the likelihood of quitting when hiring an applicant since 2019. Using the system, the bank assigns a score to a candidate and calculates how soon he or she may decide to quit. The system analyzes job applicants' resumes, previous work experience and other parameters from public sources, the consent to use of which is provided by the applicant[8].

The consequences of using scoring models for hiring is well illustrated by the case of Amazon. This multinational company has not only been actively using AI to recruit employees since 2015, but has already faced legal problems as a result. Amazon's algorithm made discriminatory decisions on hiring exclusively men, and the HR department did not check these decisions (the system was trained on resumes submitted by applicants who had been employed over a ten-year period, most of whom were men). The case came to lawsuits and eventually Amazon had to stop using AI to hire employees[9]. The bias of AI scoring models for hiring is also confirmed by academic research. For example, L. Chen and colleagues (2018) confirmed that women are ranked slightly lower than men by AI in search engines.

Thus, depending on how AI systems are configured, they can discriminate and weed out those people who are not suitable for them, or rank resumes based on unfair criteria developed by machine learning.

Similarly, the use of Emotion AI technology creates the risk of discrimination and unjustified refusal of employment, when emotions and intonations at the interview

---

8 Sberbank taught artificial intelligence to predict quits. (2019, October 18). Forbes. https://clck.ru/3CVwoY

9 Oppenheim, M. (2018, 11 October). Amazon scraps "sexist AI" recruitment tool. Independent. https://clck.ru/3CVwqY

are read using video, audio and other biometric sensors. As O. V. Fedoseeva (2021) points out, AI performs emotion recognition using optical sensors that capture facial expressions in real time or in webcam recordings. The obtained data are processed by machine learning algorithms, determining the type of micro-expressions, tone and emotionality of the vocal response. In a broad sense, "reading" facial micro-expressions and voice tones allows AI to detect emotions of potential employees and perform occupational prediction.

Applying the Emotion AI, an employer wants not just to verify the professional competence of a potential employee, but to diagnose his or her emotional reactions to certain questions related to labor activity at a given employer (for example, these may be mimic or intonation reactions to questions about willingness to work overtime, about the reasons for leaving a previous job, etc.). For example, VCV software by Moscow developers allows viewing video interviews and, prior to face-to-face meeting, excluding obviously unsuitable candidates, as well as pre-assessing soft skills and compliance with the company's values in order to score the applicants' mood and behavior. The software products of another Moscow-based company, Sever.AI, make it possible to view video with answers, analyze image (candidate's external behavior), sound (candidate's speech, pitch), and text (content of answers).

Investigating the risks of using such software when hiring employees, employees of the Moscow Institute of Technology conducted an experiment with MyInterview and Curious Thing software products in 2021. It was found that they differently read the emotions of applicants with different cameras and microphones, at different head turns and in different areas of the screen. They also poorly understand intonations in voices spoken with a strong accent[10]. As T. Pradeep points out, network connectivity problems, attention deficit disorder, or lack of candidate concentration may negatively affect the applicant's assessment when conducting interviews using AI, so human involvement is necessary to make the final decision on employment (Pradeep, 2024).

As we can see, since AI tools are driven by data derived from objective reality, it is difficult, if not impossible, to avoid the risk that AI tools encode and exacerbate certain biases. Therefore, one of the biggest challenges in AI hiring is the presence of biased algorithms – those that lead to discriminatory, not objective and illegal decisions. M. Jackson (2021) called algorithms biased if AI can replicate biases when making decisions.

[10] MTI: AI interview software doesn't even understand what language a candidate speaks. (2021, 8 July). Habr. https://clck.ru/3CVxKF

The main characteristics of biased algorithms in AI-assisted hiring are:

1) sampling bias – the data on which AI learns do not accurately reflect the real world picture. As J. Chen (2023) points out, almost every machine learning algorithm relies on biased databases;

2) algorithmic bias, which arises because of the algorithm rather than the data. In algorithm development, this bias can be due to several factors such as the depth of the neural network or the prior information required by the algorithm. As Yu. S. Kharitonova et al. (2021) noted, algorithmic bias exists even when the algorithm designer has no intention of discrimination, and even when the recommender system does not take demographic information as input;

3) representation bias, which occurs during data collection and is associated with uneven data collection that does not take into account outliers or anomalies. Representation bias can also occur when population diversity is not taken into account, for example, if not all demographic groups are included equally;

4) measurement bias manifests itself in unequal conclusions or errors in the construction of the training data set. These errors can lead to biased results for certain demographic groups[11].

In general, if a generative algorithm lacks quantity and quality on certain characteristics during data collection and processing, it will not be able to objectively reflect reality, leading to inevitable bias in algorithmic decisions and, consequently, to an unfair and possibly illegal decision by an employer to reject a more deserving candidate or, conversely, to hire a less qualified applicant.

1.3. Legal liability for the decision made by artificial intelligence to hire an employee

Current research contains opinions that applied AI management is already capable of showing whether the program will send its decisions to an employee (Ivanova et al., 2018). Another opinion is that current information-social changes are affecting and transforming the nature of labor relationships in such a way that personal communication will decline and person-to-person relationships will be replaced by those between workers in the digital environment (Lőrincz, 2018). These positions do not withstand criticism, because the very idea to recognize a system with AI as a subject of law contradicts such ideas about the subject of law as socio-legal value, dignity, autonomous legal will, and also comes into conflict with the composition of a legal relationship, the composition of an offense and is null and void within the institution of representation (Hisamova & Begishev, 2020).

[11] Roller, A. (2023, September 8). AI hiring bias: How HR can understand and mitigate potential pitfalls. https://clck.ru/3CVxwT

AI cannot be a participant of social relations, as it does not have the ability to establish interaction between subjects of law regarding the satisfaction of material or cultural needs. There is also no socially significant result that AI would like to achieve. AI can solely perform datafication of the subjects of law for specific algorithmic tasks set during programming and improved by machine learning. Therefore, recognizing AI as a legal entity is not possible based on the program property of its relationship with the external world. M. H. Jarrahi (2018) notes that AI and human decision-making should complement (not replace) each other and utilize their comparative advantages. AI is a means of automating the hiring of potential employees, a digital tool for interaction between the production system elements at the level of collecting, processing, analyzing and storing information.

Thus, AI can exist in the legal reality exclusively as an object of law. All decisions made by AI must be controlled and explained by a human (employer), who is responsible for their consequences. The final decision to hire or reject an applicant based on information received from AI can only be made by the employer or its authorized body.

2. Foreign practice of legal regulation of the use of artificial intelligence for hiring employees

Using AI technologies to optimize decision-making for hiring is attractive for employers, but, as we have seen, it creates significant legal problems that need to be solved at the legislative level. The possibility of adopting regulations in this area is still at the stage of academic discussions and conceptual developments in Russia, so we consider it relevant to turn to the study of best practices of foreign countries.

2.1. Legal regulation of the use of artificial intelligence for hiring employees in the USA

The greatest advance in the regulation of AI-assisted hiring relations is demonstrated by the USA, where the relevant state legal acts have been adopted.

Illinois was the first state to pass a law specifically regulating the use of AI by employers conducting interviews with potential employees. The Illinois Artificial Intelligence Video Interview Act went into effect in January 2020[12]. The law requires employers who are "considering candidates for positions located in Illinois"[13] to do all of the following: before asking candidates to submit video interviews, to notify job applicants that the employer

[12] Artificial Intelligence Video Interview Act (820 ILCS 42). https://clck.ru/3CVz5D

[13] Ibid.

may use AI to analyze the applicant's video interview and assess the applicant's suitability for the job; to provide the applicant with information about how AI works and the general characteristics it uses to evaluate applicants; to obtain the applicant's consent to be assessed by an AI. The law also stipulates that within 30 days of receiving a request from an applicant, an employer must delete the applicant's video interview and instruct any person who receives a copy of the video interview to do the same, including any electronically backed up copies.

In addition, on August 9, 2024, the State of Illinois enacted the Artificial Intelligence Employment Act (HB3773)[14]. The Act, effective January 1, 2026, amends the Illinois Human Rights Act and aims to prevent discriminatory effects of the use of AI in employment decision-making. The Act requires employers to provide notice of AI use for the following employment-related purposes: recruitment, hiring, promotion, renewal, selection for training or internships, termination, disciplinary action, and setting the term of an employment contract.

A Maryland law enacted in March 2020[15] requires employers to meet certain requirements in order to use facial recognition technology to interview job applicants. The law requires employers to obtain signed consent from job applicants before they can use facial recognition technology "for the purpose of creating a facial template" during an interview.

The New York City Council passed Local Law 144 on Automated Employment Decision Tools on December 11, 2021, which became effective on July 5, 2023. Under Law 144, an automated employment decision tool is any computational process based on machine learning, statistical modeling, data analysis, or AI that produces a simplified result, including a score, classification, or recommendation, used to substantially assist or replace discretionary hiring decisions that affect individuals. The Act requires employers to conduct a "bias check" of any automated employment decision-making tool prior to its use and to notify employees and candidates who reside in New York of the employer's using such tools in the assessment or evaluation for hiring or promotion, and of the job qualifications and characteristics to be evaluated by AI. Employers are also obliged to notify applicants ten days prior to using AI to make hiring decisions.

On May 17, 2024, the California Civil Rights Board published the Regulations to Protect Against Employment Discrimination in Automated Decision-Making Systems[16].

---

14 Illinois House Bill 3773 (2024, September 9). https://clck.ru/3DcoQm

15 Md. Code, Lab. & Empl. § 3-717. https://clck.ru/3CVzMD

16 Regulations to Protect Against Employment Discrimination in Automated Decision-Making Systems. (2024, May 17). https://goo.su/FwwU

The Regulations define an automated decision-making system as a computational process, including one based on machine learning, statistics or other data processing or AI techniques, that tests, evaluates, ranks, classifies, recommends or otherwise makes a decision or facilitates a human decision that affects employees or applicants. The Regulation emphasizes that the use of an automated decision-making system does not replace the required individual assessment of an applicant.

The Regulations also introduce a definition of an employer's agent, to include any person or third party who provides administration of automated decision-making systems used by an employer in making employment decisions that may result in denial of employment or otherwise adversely affect the terms, conditions, benefits, or privileges of employment. This means that employers are liable for the actions of third parties that the employer hires to operate decision-making systems if such systems have a discriminatory impact. In addition, the Regulations require employers and all other covered entities to retain any personnel or other employment records "related to any employment practice and affecting any employment benefits of any applicant or employee (including all applications, personnel, membership or referral records or files, and all machine learning data)" for four years.

On May 17, 2024, Colorado enacted a comprehensive AI regulation, the Consumer Protection for Artificial Intelligence Act[17], which includes labor standards. The law, which goes into effect on February 1, 2026, applies to both developers and organizations implementing AI in their operations, and requires "reasonable care" to avoid discriminatory algorithms. The law targets "high-risk AI systems", defined as any AI system that makes or is a significant factor in making a meaningful decision, including in employment. To comply with the law, employers must implement a risk management policy and program, conduct an annual impact assessment, notify employees or job applicants of the employer's use of AI if it is used to make a decision regarding an employee or applicant, and make a public statement summarizing the types of high-risk systems the employer uses. Employers must report a discovery of algorithmic discrimination to the Colorado Attorney General within 90 days of the discovery.

The Equal Employment Opportunity Commission (EEOC) has played an important role in promoting potential regulations on the AI-assisted hiring in the USA. On October 28, 2021, the EEOC launched the "AI and Algorithm Fairness Initiative"[18], in which it pointed out the need to examine the use of AI in hiring practices and to develop specific guidance for employers that should subsequently become the basis for legal regulation at the federal level.

---

17 Consumer Protections for Artificial Intelligence Act. (2024, May 17). https://clck.ru/3DcuBv

18 EEOC Artificial Intelligence and Algorithmic Fairness Initiative. (2021, October 28). https://clck.ru/3CVzfn

On May 12, 2022, the EEOC issued "The Americans with Disabilities Act and the Use of Software, Algorithms, and Artificial Intelligence to Assess Job Applicants and Employees"[19]. In this guidance, the EEOC identifies the three most common ways in which employers' use of AI may violate the rights of individuals with disabilities.

First, an employer may violate the rights of individuals with disabilities if it requires an applicant with a disability that prevents him or her from working with his or her hands to take a subject matter test that requires the use of a keyboard or trackpad without any accommodations or an alternative version of the test.

Second, an employer's algorithm may intentionally or unintentionally screen out a person with a disability, even if he or she is able to perform the job with reasonable accommodations. This could happen, for example, if interview software designed to analyze an applicant's problem-solving skills gives lower scores to a job applicant with a speech impediment that makes it difficult for the software to interpret his or her response according to the speech pattern that the software has been trained to recognize.

Third, the algorithmic decision-making tool that an employer uses to evaluate job candidates may violate the limitations of individuals with disabilities on disability-related questions and medical examinations. Such a violation could occur if the AI tool uses questions that either directly ask about the presence of a disability or could elicit a response that contains information about the individual's disability.

On May 18, 2023, the EEOC issued a document entitled "Selected Issues: Assessing Adverse Impact in Software, Algorithms, and Artificial Intelligence Used in Employment Selection Procedures"[20] in which it outlined its vision for further regulating the AI-assisted hiring.

First, an applicant selection process that uses AI may be found to be discriminatory if the selection rate of persons of a particular race, color, religion, sex or national origin, or combination of such characteristics (e.g., a combination of race and sex) is less than 80% of the unprotected group. This situation is similar to the above-mentioned case in Amazon, where the AI made candidate selections based on previous experience and favored predominantly male candidates.

Second, employers are responsible for any adverse impact caused by AI tools purchased or used by third-party AI vendors, and cannot rely on the AI vendors'

---

19 EEOC The Americans with Disabilities Act and the Use of Software, Algorithms, and Artificial Intelligence to Assess Job Applicants and Employees. (2022, May 12). https://clck.ru/3CVzk3

20 EEOC Select Issues: Assessing Adverse Impact in Software, Algorithms, and Artificial Intelligence Used in Employment Selection Procedures Under Title VII of the Civil Rights Act of 1964. (2023, May 18). https://clck.ru/3CVzoG

predictions or research about whether their AI tools will negatively impact job applicants. This supports the idea that AI lacks legal personality and places the responsibility for the algorithm's decisions on the employer.

Third, employers should systematically review AI tools to ensure that they are not discriminatory. If a probability exists that an AI tool produces an unequal impact, the employer must demonstrate that the use of the tool is job-related and consistent with business necessity and that there are no less discriminatory alternatives that are equally effective. This recommendation by the EEOC should help identify biased algorithms in AI-assisted hiring software.

On May 18, 2023, the Consumer Financial Protection Bureau (CFPB), the Department of Justice (DOJ), the Equal Employment Opportunity Commission (EEOC), and the Federal Trade Commission (FTC) issued a joint statement on discrimination and bias[21], which highlights three areas for regulating AI in hiring:

1) applying existing legal standards – the existing laws and regulations apply equally to the use of automated systems and new technologies, the agencies shall apply the existing legal frameworks to AI;

2) addressing harmful effects – AI can perpetuate unlawful bias, automate unlawful discrimination, and lead to other harmful effects, which highlights the need for vigilance in the use of AI in employment practices;

3) protection of individual rights – it is mandatory to protect individual rights from discriminatory AI practices.

On April 24, 2024, the U.S. Department of Labor (DOL) issued Guidance on how federal contractor employers should behave when using AI to hire workers (Artificial Intelligence and Equal Employment Opportunity for Federal Contractors)[22]. The Guidance obliges federal contractors to justify the need to use AI to hire workers; to analyze the extent to which the AI-assisted selection process is job-related; to monitor AI programs in use for biased algorithms; and to explore potentially less discriminatory alternative procedures for selecting applicants. The Guidance emphasizes that completely excluding humans from the process could result in violations of federal employment laws. A federal contractor is responsible for using third-party AI-enabled products and services to hire workers. The Guidance also sets forth a list of "promising practices" recommended for federal contractors to follow: to notice job applicants in advance about the use of AI

[21] Joint statement on enforcement efforts against discrimination and bias in automated systems. (2023, April 25). https://clck.ru/3CVzxw

[22] Artificial Intelligence and Equal Employment Opportunity for Federal Contractors (2024, April 24). https://clck.ru/3Dcv8d

in hiring; to transparently explain to job applicants the policy and procedure for using AI for hiring; to ensure that the AI system received from the vendor can be controlled and monitored; to test the AI system used for hiring and tailor it to certain protected groups; to monitor the use of AI in making hiring decisions; and to ensure that the AI system used for hiring is consistent with the federal employment laws.

2.2. Legal regulation of the use of artificial intelligence for hiring employees in the European Union

Unlike the US, where federal legislation still does not regulate the use of AI for hiring employees, the European Union adopted the EU Artificial Intelligence Act[23] on May 21, 2024, which provides for the creation of a common regulatory framework for the use of AI. This Regulation contains norms regulating the use of AI in labor relations, in particular in hiring employees.

The Regulation establishes three categories of AI software products (systems), divided by risk, according to which their use is regulated: prohibited systems (with unacceptable risk); systems with high risk; other AI systems (general purpose, general purpose with systemic risks). The latter category of AI software products are not covered by the Regulation at this stage and are not specifically regulated.

Unacceptable risk implies the prohibition of the use of emotional AI in employment (except for medical and security reasons), the targeted use of AI software to identify certain vulnerabilities (due to age, disability, specific social or economic situation of candidates), and the categorization of people based on biometric or personal data (by determining race, political views, trade union membership, religious, philosophical beliefs of applicants). Article 5 of the Regulation also refers to prohibited AI systems, in the context of hiring employees, those that use subconscious or manipulative techniques to distort a candidate's behavior by significantly impairing his or her ability to make informed decisions; perform scoring based on social behavior or known, perceived or predicted personal characteristics (e.g., making a prediction about the employee's possible dismissal based on their previous work experience); create or enhance facial recognition databases by inappropriately extracting facial images from the Internet or CCTV footage.

---

[23] 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 (Artificial Intelligence Act). https://clck.ru/3DdUr7

The Regulation classifies as high-risk AI systems software products used, inter alia, for recruiting and selecting people (placing targeted job advertisements, analyzing and filtering job applications, evaluating candidates), for making decisions affecting the terms and conditions of employment, promotion and termination of employment, for assigning tasks based on individual behavior, personality traits or characteristics, and for monitoring or evaluating people in employment relationships. According to the authors of the Regulation, these AI systems may have a significant impact on employees' career prospects, earnings and rights; they may perpetuate historical patterns of discrimination against, for example, of women, certain age groups, persons with disabilities, persons of a certain racial or ethnic origin, or violate their fundamental rights to personal data protection and privacy[24].

AI software products are not considered as high risk systems under Article 6 of the Regulation if they do not pose a significant risk of harm to the health, safety or fundamental rights of natural persons, including due to the lack of significant impact on the decision-making results, if one or more of the following criteria are met: a) the AI system is designed to perform a narrow procedural task; b) the AI system is designed to improve the outcome of an action previously performed by a human; c) the AI system is designed to identify decision-making patterns or deviations from previous decision-making patterns and is not intended to replace or influence a previously performed human assessment without proper human validation; d) the AI system is designed to perform a preparatory task for the assessment that is consistent with the purposes of the uses listed in Annex III to the Regulation (for example, pre-cataloging of applications from candidates using an AI algorithm).

The Regulation contains risk management methods for high-risk AI software products. These methods include: testing of the AI system (identification and analysis of foreseeable risks); risk assessment with and without the participation of a notified agency (throughout the life cycle of the AI system); development and adoption of appropriate and targeted risk management measures. Risk management is entrusted to the deployer – the person using the AI system in accordance with one's authority (unless the AI system is used for personal non-professional activities). A deployer can be either an employer or a person who, on behalf of an employer, uses an AI system for the purpose of selecting and recruiting employees.

The Regulation sets out the responsibilities of deployers of high-risk AI systems, which, among other things, should mitigate potential violations of applicants' rights. For example, deployers are required to provide sufficient transparency into the operation of the

24 Ibid.

high-risk AI system (i.e., the AI system must be designed and used in a manner that allows the output of the system to be interpreted and used appropriately); to inform applicants and employees that they will be subject to the high-risk AI system; and to ensure an appropriate level of accuracy, reliability, and cybersecurity of the high-risk AI system (high-risk AI systems must be resilient to unauthorized attempts by third parties to alter their algorithms, results or performance due to system vulnerabilities). When using high-risk AI systems, the Regulation recommends that automatically made decisions solely should not be relied on but human beings should be involved in their final verification or evaluation.

The algorithm results provided by high-risk AI systems when recruiting employees may be influenced by biases that tend to be progressively reinforced by machine learning and thus perpetuate and aggravate the existing discrimination, in particular against persons belonging to certain vulnerable groups. The Regulation therefore draws attention to the inadmissibility of biased algorithms in high-risk AI systems. In particular, big data sets in AI systems should take into account, to the extent required by their intended purpose, features, characteristics or elements specific to the particular geographical, contextual, behavioral or functional environment in which the AI system is intended to be used. High-risk AI systems that continue to learn after being deployed should be designed to eliminate or minimize the risk of potential bias and biased results affecting the baseline for future operations.

Thus, foreign experience demonstrates the main directions in the legal regulation of the AI use for hiring, which correspond to the previously identified legal problems in this area: the provisions concerning the AI use for hiring should contain requirements for transparency and consistency of information collection, processing and storage, unbiased algorithms and their periodic monitoring, the employer's responsibility for decisions made by AI when hiring.

Conclusions

The intensive introduction of AI in the field of labor management, in particular hiring of employees, creates both potential opportunities and significant risks. On the one hand, AI can significantly optimize and improve the efficiency of hiring procedures, but on the other hand, legal problems arise related to the violation of applicants' rights and employer's responsibility for algorithm errors.

Accordingly, taking into account the highlighted problems and the studied foreign experience, it is relevant for the Russian legislator to develop and include the following provisions into the labor legislation according to the three main directions of regulating the use of AI for hiring employees.

I. Transparency and consistency in the collection, processing and storage of information when using AI to hire employees.

Chapter 14 of the Labor Code of the Russian Federation sets forth the norms related to the employees' personal data protection, including those related to ensuring transparency and consistency in the collection, processing, storage and use of such data. It seems reasonable to extend the provisions of this chapter to job applicants and job entrants and supplement the relevant articles of Chapter 14 of the Labor Code of the Russian Federation with the following provisions: employers must notify job applicants in advance in writing that AI may be used to collect, process and analyze their personal data; employers must notify job applicants in advance in writing about the use of AI to conduct and analyze video interviews; employers must explain what AI software is used, how it works and what are the characteristics of the data used to assess job applicants; job applicants must give their written consent to be assessed by AI software; employers may not share video recordings of job applicants with other parties, including software developers; employers must delete data collected by AI about job applicants, including during video interviews, within 15 days of receiving a written request from the job applicant; employers may not use AI technology to hire a disabled person.

The list and scope of personal data that is permissible to be processed by AI in hiring should be regulated through a standardization mechanism. It should be noted that in 2020 the Federal Agency for Technical Regulation and Metrology developed the Perspective Program of Standardization in the priority area "Artificial Intelligence" for the period of 2021–2024. It provides for the development of 217 standards, among which there are no standards in the field of using AI for hiring. In this case, it is necessary to take into account the provisions of GOST R 59277-2020b of 03.01.2021, which approved the "National Standard of Artificial Intelligence Systems. Classification of artificial intelligence systems". The National Standard of AI systems classifies information depending on compliance with the following confidentiality classes: class 0 – open information; class 1 – internal information; class 2 – confidential information; class 3 – secret information. This classification can help to encode a clear list and admissible scope of applicants' information within the AI-assisted hiring systems.

II. Unbiased artificial intelligence algorithms for hiring employees.

It is crucial to code AI for hiring in a way that avoids biased algorithms and, as a result, discrimination and unjustified rejection. A tool to ensure unbiased AI algorithms for hiring can be mandatory certification of the relevant software.

Certification of software and AI algorithms is currently not mandatory in Russia, according to the RF Government Resolution No. 982 of 01.12.2009 "On approval of the unified list of products subject to compulsory certification and the unified list of products,

the conformity of which is confirmed in the form of declaration of conformity"[25]. It states that software is subject to confirmation of conformity with the manufacturer's declared specifications or state standards. However, the development of AI systems and the emergence of significant risks associated with the possible violation of labor rights of citizens requires the inclusion of AI and machine learning software in the list of products subject to mandatory certification based on developed state standards, as well as periodic monitoring. Therefore, employers should be required to conduct mandatory annual monitoring of the AI technology used for hiring and send a monitoring report to the certification center where the software used by the employer is certified.

It is also relevant to consider prohibiting employers from using AI scoring models for hiring, even with the applicant's consent, as these models have a significant risk of bias in predicting the applicant's labor behavior.

III. Liability of the employer for the decision made by artificial intelligence to hire employees.

AI cannot have legal personality and be responsible for the results of collecting, processing and analyzing applicants' data and making hiring decisions. Moreover, this position is already reflected in paragraph 6, part 1, of Article 86 of the current Labor Code of the Russian Federation, which stipulates that when making decisions affecting the interests of an employee, the employer has no right to base on the employee's personal data obtained solely as a result of their automated processing or electronic receipt. This norm should also be extended to job applicants and job entrants. That is, employers are liable for any negative impact caused by AI tools. In addition, employers are liable for the actions of third parties whom the employer hires to manage decision-making systems, including automated ones, if such decision-making systems have a discriminatory impact. It is also relevant to enshrine the latter provision in Article 90 of the Labor Code of the Russian Federation.

References

Basu, N., & Dave, R. (2024). Artificial intelligence and job sector – need for laws. *Educational Administration: Theory And Practice*, *30*(3), 690–701. https://doi.org/10.53555/kuey.v30i3.1337

Bigman, Y. E., Wilson, D., Arnestad, M. N., Waytz, A., & Gray, K. (2023). Algorithmic discrimination causes less moral outrage than human discrimination. *Journal of Experimental Psychology: General*, *152*(1), 4–27. https://doi.org/10.1037/xge0001250

Chen, L., Ma, R., Hannák, A. & Wilson, C. (2018). Investigating the impact of gender on rank in resume search engines. *Proceedings of the 2018 chi conference on human factors in computing systems*, *651*, 1–14. https://doi.org/10.1145/3173574.3174225

Chen, Z. (2023). Ethics and discrimination in artificial intelligence-enabled recruitment practices. *Humanities and Social Sciences Communications*, *10*. https://doi.org/10.1057/s41599-023-02079-x

De Stefano, V. (2019). "Negotiating the algorithm": automation, artificial intelligence and labor protection. *Comparative Labor Law & Policy Journal*, *41*(1), 15–46. https://doi.org/10.2139/ssrn.3178233

[25] Resolution of the Government of the Russian Federation dated 01.12.2009 No. 982. KonsultantPlyus. https://clck.ru/3EPpur

Estrada, G, Coronado, M., Soria, Y., Jiménez, S., Cristobal, J., Torres, E., Camargo, M., Taipe, M., Aparicio, S., Luis, J., & Briceño B. (2024). Inteligencia artificial en la gestión de los recursos humanos. R*evista de Climatolog´ıa Edici´on Especial Ciencias Sociales*, *24*, 2082–2092. (In Spanish).

Fedoseeva, O. V. (2021). On creating and developing emotional artificial intelligence. *Rossiya: tendencii i perspektivy razvitiya*, *16-1*, 674–676. (In Russ.).

Fuller, J., B. Raman M., Sage-Gavin, E., Hines, K. et al. (2021). *Hidden workers: untapped talent*. Harvard Business School Project on Managing the Future of Work and Accenture.

Ginu, G., Mary, T., Anusha, B., & Anson, M. (2021). A systematic review of artificial intelligence and hiring: Present Position and Future Research Areas. *Indian Journal of Economics and Business*, *20*(2), 57–70. http://dx.doi.org/10.5281/zenodo.5407602

Haenlein, M. & Kaplan, A. (2019). A brief history of artificial intelligence: On the past, present, and future of artificial intelligence. *California Management Review*, *61*(4), 5–14. https://doi.org/10.1177/0008125619864925

Hisamova, Z. I., & Begishev, I. R. (2020). The nature of artificial intelligence and the problem of legal personality determination. *Moscow Juridical Journal*, *2*, 96–106. (In Russ.). https://doi.org/10.18384/2310-6794-2020-2-96-106

Hunkenschroer, A. L., & Kriebitz, A. (2023). Is AI recruiting (un)ethical? A human rights perspective on the use of AI for hiring. *AI Ethics*, *3*, 199–213. https://doi.org/10.1007/s43681-022-00166-4

Ivanova, M., Bronowicka, J., Kocher, E., & Degner, A. (2018). *The App as a Boss? Control and Autonomy in Application-Based Management*: Working Paper. Europa-Universität Viadrina Frankfurt. https://doi.org/10.11584/arbeit-grenze-fluss.2

Jackson, M. (2021). Artificial intelligence & algorithmic bias: the issues with technology reflecting history & humans. *Journal of Business & Technology Law*, *16*(2), 299–316.

Jarrahi, M. H. (2018). Artificial intelligence and the future of work: Human-AI symbiosis in organizational decision making. *Business Horizons*, *61*(4), 577–586. https://doi.org/10.1016/j.bushor.2018.03.007

Kharitonova, Yu. S., Savina, V. S., & Pagnini, F. (2021). Artificial intelligence's algorithmic bias: ethical and legal Issues. Perm University Herald. *Juridical Sciences*, *53*, 488–515. (In Russ.). https://doi.org/10.17072/1995-4190-2021-53-488-515

Köchling, A., & Wehner, M. C. (2020). Discriminated by an algorithm: a systematic preview of discrimination and fairness by algorithmic decision-making in the context of HR recruitment and HR development. *Business Research*, *13*, 795–848. https://doi.org/10.1007/s40685-020-00134-w

Kuncel, N., Klieger, D., & Ones, D. (2014). In hiring, algorithms beat instinct. *Harvard Business Review*, *92*(5), 32.

Langer, M., Cornelius, J. K., & Andromachi, F. (2023). Information as a double-edged sword: the role of computer experience and information on applicant reactions towards novel technologies for personnel selection. *Computers in Human Behavior*, *81*, 19–30. https://doi.org/10.1016/j.chb.2017.11.036

Langer, M., König, C. J., Sanchez, D. R.-P., & Samadi, S. (2019). Highly automated interviews: applicant reactions and the organizational context. *Journal of Managerial Psychology*, *35*(4), 301–314. https://doi.org/10.1108/jmp-09-2018-0402

Lee, M. K. (2018). Understanding perception of algorithmic decisions: fairness, trust, and emotion in response to algorithmic management. *Big Data & Society*, *5*(1), 1–16. https://doi.org/10.1177/2053951718756684

Lőrincz, G. (2018). Kommentár a munka törvénykönyvéről szóló 2032. évi I. törvényhez: Munkajogi sci-fi. *Pécsi Munkajogi Közlemények*, *11*(1-2), 7–34. (In Hungarian)

Lukács, A., & Váradi S. (2023). GDPR-compliant AI-based automated decision-making in the world of work. *Computer Law & Security Review*, *50*, 105848. https://doi.org/10.1016/j.clsr.2023.105848

Novikov, D. A. (2023). Critical remarks on the liberal understanding in sociological and legal studies of the phenomenon of labour in the information society. *Russian Journal of Labour & Law*, *13*, 81–91. (In Russ.). https://doi.org/10.21638/spbu32.2023.105

Pradeep, T. (2024). Labour law in the era of artificial intelligence and automation. *International Journal For Multidisciplinary Research*, 6(2). https://doi.org/10.36948/ijfmr.2024.v06i02.16324

Reddy, S. (2022). The legal issues regarding the use of artificial intelligence to screen social media profiles for the hiring of prospective employees. *Obiter*, *43*(2), 113–131. https://doi.org/10.17159/obiter.v43i2.14254

Serova, A. V., & Shcherbakova, O. V. (2022). The employee's right to privacy transformation: digitalization challenges. *Kutafin Law Review*, *9*(3), 437–465. https://doi.org/10.17803/2713-0525.2022.3.21.437-465

Shcherbakova, O. V. (2021). The use of artificial intelligence programs when recruiting employees. *Electronic Supplement to the Russian Juridical Journal*, *3*, 72–76. (In Russ.). https://doi.org/10.34076/22196838_2021_3_72

Sivathanu, B., & Pillai, R. (2018). Smart HR 4.0 – how industry 4.0 is disrupting HR. *Human Resource Management International Digest*, *26*(4), 7–11. https://doi.org/10.1108/hrmid-04-2018-0059

Author information

Denis A. Novikov – Cand. Sci. (Law), Associate Professor, Department of Labor and Social Law, Saint Petersburg State University
Address: 7–9 Universitetskaya nab., 199034 Saint Petersburg, Russia
E-mail: d.novikov@spbu.ru
ORCID ID: https://orcid.org/0000-0003-2727-5357
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57218897105
WoS Researcher ID: https://www.webofscience.com/wos/author/record/CAA-7871-2022
Google Scholar ID: https://scholar.google.com/citations?user=gEjH4S4AAAAJ
RSCI Author ID: https://elibrary.ru/author_items.asp?authorid=1149154

Conflict of interests

The author declares no conflict of interests.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – August 6, 2023
Date of approval – August 22, 2023
Date of acceptance – September 25, 2024
Date of online placement – September 30, 2024

Научная статья
УДК 34:004:349.2:004.8
EDN: https://elibrary.ru/chpesp
DOI: https://doi.org/10.21202/jdtl.2024.31

Использование искусственного интеллекта при найме работников: проблемы и перспективы правового регулирования

Денис Александрович Новиков

Санкт-Петербургский государственный университет, Санкт-Петербург, Россия

Ключевые слова

алгоритм,
закон,
искусственный интеллект,
наем работника,
персональные данные,
право,
работник,
работодатель,
трудовое право,
цифровые технологии

Аннотация

Цель: определить правовые проблемы использования искусственного интеллекта при найме работников и обозначить основные направления их решения.

Методы: формально-юридический и сравнительно-правовой анализ, правовое прогнозирование, правовое моделирование, синтез, индукция, дедукция.

Результаты: выявлен ряд правовых проблем, возникающих при использовании искусственного интеллекта (ИИ) при найме работников, среди которых защита персональных данных соискателя, получаемых при применении искусственного интеллекта; дискриминация и необоснованный отказ в приеме на работу из-за предвзятости алгоритмов искусственного интеллекта; юридическая ответственность за принятое генеративным алгоритмом решение при найме работника. Автор полагает, что для оптимального решения указанных проблем необходимо обратить внимание на передовой опыт зарубежных стран, прежде всего на те страны, где приняты специальные законы о регулировании применения ИИ при найме работников и выработаны руководства для работодателей, применяющих генеративные алгоритмы в аналогичных целях. Кроме того, следует учесть законотворческую работу Европейского союза и США в сфере управления рисками, возникающими при использовании ИИ.

Научная новизна: в работе проведено комплексное исследование правовых проблем, возникающих при использовании ИИ при найме работников, зарубежного опыта их решения, что позволило автору выработать рекомендации по усовершенствованию российского законодательства в данной сфере. Проблему защиты персональных данных соискателей при использовании искусственного интеллекта для

найма автор предлагает решить путем дополнения трудового законодательства нормами, закрепляющими требования по прозрачности и согласованности сбора, обработки и хранения информации при применении генеративных алгоритмов. Перечень и объем допустимых для сбора персональных данных следует отобразить в специальном государственном стандарте. Решение проблемы дискриминации из-за предвзятости алгоритмов видится в обязательной сертификации и ежегодном мониторинге программ искусственного интеллекта для найма, а также запрете скоринговых инструментов оценки соискателей. Автор придерживается позиции, что искусственный интеллект не может «вершить судьбу» соискателя: ответственность за решения, принятые алгоритмом о найме, возлагается исключительно на работодателя, в том числе в случаях привлечениях третьих лиц для осуществления подбора работников.

Практическая значимость: полученные результаты могут быть использованы для ускорения разработки и принятия правовых норм, правил, инструментов и стандартов в сфере использования ИИ для найма работников. Отсутствие надлежащего правового регулирования в данной сфере создает существенные риски как для прав человека, так и для развития отраслей экономики, в которых задействуются генеративные алгоритмы в целях найма работников.

Для цитирования

Новиков, Д. А. (2024). Использование искусственного интеллекта при найме работников: проблемы и перспективы правового регулирования. *Journal of Digital Technologies and Law*, *2*(3), 611–635. https://doi.org/10.21202/jdtl.2024.31

Список литературы

Новиков, Д. А. (2023). Критические замечания относительно либерального понимания в социологических и правовых исследованиях феномена труда в информационном обществе. *Ежегодник трудового права*, *13*, 81–91. https://doi.org/10.21638/spbu32.2023.105

Федосеева, О. В. (2021). К вопросу о создании и развитии эмоционального искусственного интеллекта. *Россия: тенденции и перспективы развития*, *16-1*, 674–676.

Харитонова, Ю. С., Савина, В. С., Паньини, Ф. (2021). Предвзятость алгоритмов искусственного интеллекта: вопросы этики и права. *Вестник Пермского университета. Юридические науки*, *53*, 488–515. https://doi.org/10.17072/1995-4190-2021-53-488-515

Хисамова, З. И., Бегишев, И. Р. (2020). Сущность искусственного интеллекта и проблема определения правосубъектности. *Московский юридический журнал*, *2*, 96–106. https://doi.org/10.18384/2310-6794-2020-2-96-106

Щербакова, О. В. (2021). Использование программ искусственного интеллекта при найме работников. *Электронное приложение к Российскому юридическому журналу*, *3*, 72–76. https://doi.org/10.34076/22196838_2021_3_72

Basu, N., & Dave, R. (2024). Artificial intelligence and job sector – need for laws. *Educational Administration: Theory And Practice*, *30*(3), 690–701. https://doi.org/10.53555/kuey.v30i3.1337

Bigman, Y. E., Wilson, D., Arnestad, M. N., Waytz, A., & Gray, K. (2023). Algorithmic discrimination causes less moral outrage than human discrimination. *Journal of Experimental Psychology: General*, *152*(1), 4–27. https://doi.org/10.1037/xge0001250

Chen, L., Ma, R., Hannák, A., & Wilson, C. (2018). Investigating the impact of gender on rank in resume search engines. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 651, 1–14. https://doi.org/10.1145/3173574.3174225

Chen, Z. (2023). Ethics and discrimination in artificial intelligence-enabled recruitment practices. *Humanities and Social Sciences Communications*, *10*, 567. https://doi.org/10.1057/s41599-023-02079-x

De Stefano, V. (2019). “Negotiating the algorithm”: automation, artificial intelligence and labor protection. *Comparative Labor Law & Policy Journal*, *41*(1), 15–46. https://doi.org/10.2139/ssrn.3178233

Estrada, G, Coronado, M., Soria, Y., Jiménez, S., Cristobal, J., Torres, E., Camargo, M., Taipe, M., Aparicio, S., Luis, J., & Briceño B. (2024). Inteligencia artificial en la gestión de los recursos humanos. R*evista de Climatolog´ıa Edici´on Especial Ciencias Sociales*, *24*, 2082–2092.

Fuller, J., B. Raman M., Sage-Gavin, E., Hines, K. et al. (2021). *Hidden workers: untapped talent*. Harvard Business School Project on Managing the Future of Work and Accenture.

Ginu, G., Mary, T., Anusha, B., & Anson, M. (2021). A systematic review of artificial intelligence and hiring: Present Position and Future Research Areas. *Indian Journal of Economics and Business*, *20*(2), 57–70. http://dx.doi.org/10.5281/zenodo.5407602

Haenlein, M., & Kaplan, A. (2019). A brief history of artificial intelligence: On the past, present, and future of artificial intelligence. *California Management Review*, *61*(4), 5–14. https://doi.org/10.1177/0008125619864925

Hunkenschroer, A. L., & Kriebitz, A. (2023). Is AI recruiting (un)ethical? A human rights perspective on the use of AI for hiring. *AI Ethics*, *3*, 199–213. https://doi.org/10.1007/s43681-022-00166-4

Ivanova, M., Bronowicka, J., Kocher, E., & Degner, A. (2018). *The App as a Boss? Control and Autonomy in Application-Based Management*: Working Paper. Europa-Universität Viadrina Frankfurt. https://doi.org/10.11584/arbeit-grenze-fluss.2

Jackson, M. (2021). Artificial intelligence & algorithmic bias: the issues with technology reflecting history & humans. *Journal of Business & Technology Law*, *16*(2), 299–316.

Jarrahi, M. H. (2018). Artificial intelligence and the future of work: Human-AI symbiosis in organizational decision making. *Business Horizons*, *61*(4), 577–586. https://doi.org/10.1016/j.bushor.2018.03.007

Köchling, A., & Wehner, M. C. (2020). Discriminated by an algorithm: a systematic preview of discrimination and fairness by algorithmic decision-making in the context of HR recruitment and HR development. *Business Research*, *13*, 795–848. https://doi.org/10.1007/s40685-020-00134-w

Kuncel, N., Klieger, D., & Ones, D. (2014). In hiring, algorithms beat instinct. *Harvard Business Review*, *92*(5), 32.

Langer, M., Cornelius, J. K., & Andromachi, F. (2023). Information as a double-edged sword: the role of computer experience and information on applicant reactions towards novel technologies for personnel selection. C*omputers in Human Behavior*, *81*, 19–30. https://doi.org/10.1016/j.chb.2017.11.036

Langer, M., König, C. J., Sanchez, D. R.-P., & Samadi, S. (2019). Highly automated interviews: applicant reactions and the organizational context. *Journal of Managerial Psychology*, *35*(4), 301–314. https://doi.org/10.1108/jmp-09-2018-0402

Lee, M. K. (2018). Understanding perception of algorithmic decisions: fairness, trust, and emotion in response to algorithmic management. *Big Data & Society*, *5*(1), 1–16. https://doi.org/10.1177/2053951718756684

Lőrincz, G. (2018). Kommentár a munka törvénykönyvéről szóló 2032. évi I. törvényhez: Munkajogi sci-fi. *Pécsi Munkajogi Közlemények*, *11*(1-2), 7–34.

Lukács, A., & Váradi S. (2023). GDPR-compliant AI-based automated decision-making in the world of work. *Computer Law & Security Review*, *50*, 105848. https://doi.org/10.1016/j.clsr.2023.105848

Pradeep, T. (2024). Labour law in the era of artificial intelligence and automation. *International Journal For Multidisciplinary Research*, 6(2). https://doi.org/10.36948/ijfmr.2024.v06i02.16324

Reddy, S. (2022). The legal issues regarding the use of artificial intelligence to screen social media profiles for the hiring of prospective employees. *Obiter*, *43*(2), 113–131. https://doi.org/10.17159/obiter.v43i2.14254

Serova, A. V., & Shcherbakova, O. V. (2022). The employee’s right to privacy transformation: digitalization challenges. *Kutafin Law Review*, *9*(3), 437–465. https://doi.org/10.17803/2713-0525.2022.3.21.437-465

Sivathanu, B., & Pillai, R. (2018). Smart HR 4.0 – how industry 4.0 is disrupting HR. *Human Resource Management International Digest*, *26*(4), 7–11. https://doi.org/10.1108/hrmid-04-2018-0059

Сведения об авторе

Новиков Денис Александрович – кандидат юридических наук, доцент, доцент кафедры трудового и социального права, Санкт-Петербургский государственный университет
Адрес: 199034, Россия, г. Санкт-Петербург, Университетская наб., 7–9
E-mail: d.novikov@spbu.ru
ORCID ID: https://orcid.org/0000-0003-2727-5357
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57218897105
WoS Researcher ID: https://www.webofscience.com/wos/author/record/CAA-7871-2022
Google Scholar ID: https://scholar.google.com/citations?user=gEjH4S4AAAAJ
РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=1149154

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.63.33 / Трудовые ресурсы. Трудоустройство
Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 6 августа 2023 г.
Дата одобрения после рецензирования – 22 августа 2023 г.
Дата принятия к опубликованию – 25 сентября 2024 г.
Дата онлайн-размещения – 30 сентября 2024 г.

Research article
UDC 34:004:349.2:004.8
EDN: https://elibrary.ru/mqtnqg
DOI: https://doi.org/10.21202/jdtl.2024.32

New Approaches to Researching AI Crime: Institutionalization of Digital Criminology

Fotios Spyropoulos

Philips University, Nicosia, Cyprus
Spyropoulos Law Firm, Athens, Greece

Keywords

artificial intelligence,
crime,
criminal deed,
cybercrime,
digital criminology,
digital society,
digital technologies,
ethics,
law,
technoethics

Abstract

Objective: the article deals with modern scientific approaches to the "digital society", identifies new criminological perspectives, such as that of digital criminology in an ever-changing hybrid world, in the scientific study of the potential use of AI by criminals, including what is referred to here as AI crime.

Methods: this article is an essay commonly used in humanities and social sciences, as the author aims to present provocative arguments to encourage readers to rethink AI issues in relation to criminality in the "hybrid world" based on a non-systematic literature review. The arguments should be supported by relevant references to "digital criminology" and its non-binary way of thinking in favour of a techno-social approach.

Results: the era of divided perspectives is coming to an end, and it's time for synergies, especially at the interdisciplinary level. The «mirror of artificial intelligence» can help identify flaws and solutions, ensuring the future of AI and human society is decided by the people. In a digital society, technology is integrated into people's lives, including crime, victimization, and justice. Digital technologies blur the boundaries between online and offline realities, creating a human-technological hybrid world where crimes occur in virtual networks. AI has potential for social good and Sustainable Development Goals, but concerns about human rights violations need to be addressed. Multidisciplinary approaches are needed to ensure safe use, address education inequalities, enhance justice, and identify online behavior as deviant or criminal. In the context of emerging technoethics, the idea that this unofficial norm, derived from a popular belief, will be the 'touchstone' for characterising online mediated behaviour as deviant/crimninal, is missing - or rather in the process of being formed.

Scientific novelty: the author aims to provide some insightful thoughts on formulating the right questions and interesting reflections from a technoethical perspective on the phenomenon of the use of information and communication technologies for criminal purposes under the catalytic influence of AI, recognising the social challenges arising from technological disruption (e.g. prediction and prevention through the transformation of policing, increased surveillance and criminal justice practises) in "digital society".

Practical significance: some of the initial ideas of this theoretical material can be used in the elaboration of proposals for amendements and additions to the current crime legislation, as well as in pedagogical activity, especially in the implementation of educational courses or modules on crime in the context of the digital transformation of society.

For citation

Spyropoulos, F. (2024). New Approaches to Researching AI Crime: Institutionalization of Digital Criminology. *Journal of Digital Technologies and Law, 2*(3), 636–656. https://doi.org/10.21202/jdtl.2024.32

Contents

Introduction

Let us begin by reflecting on the many and varied ways in which digital technologies have permeated everyday life in recent years, leading to the conclusion that nowadays "life is digital". "We are increasingly becoming digital data subjects, whether we like it or not, and whether we choose this or not" (Lupton, 2015).

Moreover, in the digital era, we witness the increasing use of technology and artificial intelligence (further – AI) to solve problems, while improving productivity and efficiency. For decades, computer scientists have been so captivated by the unlimited potential of new technologies that the negative effects of these systems have been probably downplayed or often ignored entirely (Hayward & Maas, 2020)[1]. Known as techno-

[1] Schneier, B. (2008, March 20). Inside the twisted mind of the security professional. Wired. https://clck.ru/3CzSKg

optimism (Danaher, 2022), this failure to effectively balance reward and risk was famously highlighted in "Don't be evil"[2], the former motto of the Google Code of Conduct.

But almost recently, scientists have been invigorated by a number of new research approaches that address how crime will be transformed by the impact of what Greenfield (2017) emphatically refers to as the "radical new technologies and AI of the networked era".

Technologists and criminologists are now realising that Artificial Intelligence systems will open up a plethora of new opportunities for serious criminal exploitation, in addition to enabling questionable policing practices (Hayward & Maas 2020; Ionescu et al., 2020; Broadhurst et al., 2019). Namely, the increase in the rate of crimes committed in the digital world, prove that the fast-evolving technology creates new opportunities for perpetrators while at the same time contributing to a rise in the levels and complexity of crime[3] (Lee & Chua, 2023; Di Nicola, 2022). It does so largely oblivious of the many social challenges posed by technological disruption (e.g. prediction and prevention by transforming policing, enhanced surveillance and criminal justice practices) (Brown, 2006a; Hayward, 2012; Holt & Bossler, 2014).

1. Artificial intelligence: problems of definition

Artificial intelligence can be an elusive concept - a phenomenon that is seemingly ubiquitous but at the same time strangely opaque. In popular culture and news reporting on AI, fanciful narratives often prevail, referring to iconic 'killer robots' or dystopian surveillance systems (Hayward & Maas, 2020). In people's everyday lives, however, AI operates on a much more prosaic level, controlling everything from smart TVs to language translation applications. According to K. Piper[4], "the conversation about AI is full of confusion, misinformation, and people talking past each other – in large part because we use the word 'A.I' to refer to so many things".

The borderline between what counts as AI proper and other forms of technology can be blurred. Moreover, the term 'intelligence' in the context of the AI paradigm is a loaded and deeply contested philosophical and scientific concept not mentioned when the philosophical and technical arguments converge in the debates about whether we will ever develop an AI that has consciousness and is complex enough in the right way to merit our moral concerns and protection (Boddington, 2017). Perhaps it is this generality and uncertainty that confuses people, not least because each supposed AI future raises its own set of concerns about safety, ethics, legality and liability.

---

2 Mayer, D. (2016). Why Google Was Smart To Drop Its 'Don't Be Evil' Motto. Fast Company.

3 Ife, C. C., Davies, T., Murdoch, S. J., & Stringhini, G. (2019). Bridging information security and environmental criminology research to better mitigate cybercrime. arXiv preprint arXiv:1910.06380. https://clck.ru/3CzSMo

4 Piper, K. (2018). The case for taking AI seriously as a threat to humanity, Vox. https://clck.ru/3CzSPd

The so-called "dual-use" aspect of technology is not an entirely new problem when it comes to cybercrime or (cyber-)security. While AI can be used to attack governments, it is also used by them to improve their capabilities. However, there are new vulnerabilities related to how AI can be abused and used maliciously. Systems for crime prevention and detection are among the many legitimate uses of AI (Dilek et al., 2015; Li et al., 2010; Lin et al., 2017; McClendon & Meghanathan, 2015). However, there is also a chance that the technology will be abused and used to further illegal activity (Kaloudi & Li, 2020; Sharif et al., 2016; Mielke & Chen, 2008; van der Wagen & Pieters, 2015). The critical issue is the ability of human attackers to use non-ASI (artificial superintelligence), systems to automate, enable and enhance cybercrime as we know it, as well as the ability to open totally new channels for cybercrime.

If society is to overcome this confusion, what is required are clear answers to straightforward questions: "What exactly is AI?" "What are its capabilities and limits?" & "What are the consequences of its proliferation and use in society, both as a tool for criminal or illegitimate ends, and as a means of security and social control?"

2. An approach to technoethics

The term 'technoethics' was coined in 1974 by the Argentine-Canadian philosopher Mario Bunge (1977) to refer to the special responsibilities of technologists and engineers for the development of ethics as a branch of technology.

"Ethics" can be defined as a code or set of principles by which people live. Ethics is about what is considered morally right and what is considered wrong. When people make moral judgements, they utter normative or prescriptive statements about what should be done, about moral duty and obligation, not descriptive statements about what is done. Ethical theory or moral philosophy, then, is the doctrine of the rules or principles underlying moral decisions, a justification for moral judgements. The application of ethical theory can help users, even to the point of determining how people should behave in various applications of technology.

Accordingly, technoethics is the interdisciplinary field that attempts to determine an appropriate standpoint or attitude or philosophy in the application of technology in real-life situations. Among several ethical theories, the most relevant to technological applications are consequentialism, deontologism and utilitarianism. Technoethics is concerned with the impact of ethics on technology, technological change, technological progress and its applications. This applies both to established areas such as bioethics, computer ethics or engineering ethics, as well as to new fields of research such as neuroethics (Heller, 2012).

Rocci Luppicini (2008) underlines the fact that, "...technoethics is based on the premise that it is crucial to promote dialogue aimed at determining the ethical use of technology, guarding against its misuse and devising thoughtful principles that help guide new technological advances for the benefit of society in a variety of social contexts and ethical dimensions".

To conclude with, technoethics is a rapidly developing area of ethics due to the rapid development of technologies and their integration into everyday life. It draws extensive knowledge from research fields such as information and communication, social sciences, technology and science studies, applied ethics and philosophy to discover the ethical benefits of technology, protect against its misuse and outline common principles that guide new advances in technological development and application for the benefit of society.

In answering the question of why we need technoethics and technological consciousness, there is no question that with the advancing technology of AI and ML we are confronted with technologies that are capable of learning and creating if they have a consciousness of their own. Therefore, we need to address the issues of technological consciousness and technoethics in order to find answers to the emerging moral dilemmas related to technology and to guide these advancing technologies in such a way that they benefit humanity, because after all, every single algorithm that promises a clear benefit can easily be misused to harm.

3. Ethical successes, failures and challenges in artificial intelligence

Technological progress has always been at the heart of the dynamics of the economic system, directly or indirectly affecting all economic and productive activities. The significant changes that are taking place are bringing about changes in a range of productive and economic activities. At the same time, they act as a powerful factor of imbalance and the creation or reproduction of new inequalities and inequities both at the level of the labour market, the structure of employment and the economy, and at the level of the socio-economic development of economies, sectors, regions and countries at the European and international levels.

The issues arising from technological developments and in particular from developments in the field of artificial intelligence are increasingly occupying scientific institutions, companies and public authorities. According to Dell Technologies' research department, which has studied future developments in collaboration with the Institute for the Future, one of the conclusions they have reached is that "people's dependence on machines will have evolved into a collaborative relationship, with people bringing skills such as creativity, passion and entrepreneurship"[5].

When we speak of ethical issues and challenges of technology and AI, there tends to be an implicit assumption that we are speaking of morally bad things. And, of course, most of the AI debate revolves around such morally problematic outcomes that need to be addressed. However, it is worth highlighting that technology and new advances in AI promises numerous benefits (Berendt, 2019)[6]. Many AI policy documents focus

5 Barbaschow, A. (2019, October 8). Machines as consumers: The future according to Dell Technologies. ZDNET.

6 Faggella, D. (2020). Everyday examples of artificial intelligence and machine learning. Boston, MA: Emerj. https://clck.ru/3CzSZw

on the economic benefits of AI that are expected to arise from higher levels of efficiency and productivity. These are ethical values insofar as they promise higher levels of wealth and wellbeing that will allow people to live better lives and can thus be conducive to or even necessary for human flourishing (see more EU's High-Level Expert Group on AI[7]).

But in contrary, the promise of improving efficiency, reducing costs and accelerate research and development has recently been tempered by concerns that these complex, opaque systems may do more harm than good to society. There are numerous accounts of the ethical issues of AI, mostly developments of a long-standing tradition of discussing ethics and AI in the literature (Coeckelbergh, 2019; Dignum, 2019; Müller, 2020), but increasingly also arising from a policy perspective[8]. The most common ethical issues indicatively are: a) Data privacy violations b) Sensitive information disclosure c) Misinformation and Deep Fakes˙ d) Lack of Oversight and Acceptance of Responsibility˙ e) Use of AI (facial recognition, replacement of jobs, health tracking, data provenance, amplification of existing bias in AI technology, lack of explainability and interpretability etc.

To sum up, it is important to underline that the legal and ethical issues that confront society due to Artificial Intelligence (AI) include privacy and surveillance, bias or discrimination, and potentially the philosophical challenge is the role of human judgment. Concerns about newer digital technologies becoming a new source of inaccuracy and data breaches have arisen as a result of its use. So, critical decisions have to be made to ensure we are protecting personal freedoms and using data appropriately.

Fears (justifiable or unjustifiable?) arise from the ever-increasing dominance of machines with artificial intelligence, characterised by 'superintelligence'. But the real danger is not the dominance of superintelligent machines, but of machines that are not yet 'intelligent' enough to cope with the tasks assigned to them. Machine intelligence will continue to improve, but it will fall far short of human intelligence, at least for the foreseeable future. This will reinforce the need for human skills and values to bridge the gap and mitigate the risk posed by powerful artificial intelligence in today's comprehensive and complex human societies. The key to addressing the above risks is to invest and enrich the human factor, but also to monitor artificial intelligence responsibly. In this way, it will be worthwhile to maintain development and societal trust in the technology. Human values are often missing in the moral values of machines with artificial intelligence. To reconcile them, citizens must achieve dominance over both by putting the former (machine values) in the service of the latter (human values). AI should not be used as a scapegoat for human moral failures. Through the "mirror of artificial intelligence", which is a very helpful

7 EU's High-Level Expert Group on Artificial Intelligence. (2019). Ethics guidelines for trustworthy AI. Brussels: European Commission. https://clck.ru/3CzSbj

8 Ibid.

diagnostic tool for society, people can learn as much as possible about its weaknesses and limitations, as well as about new insights and solutions it offers. The future of artificial intelligence and human society will not be decided for humans, but by humans. AI and the dominance of robots should not decide for humans, but humans must decide what is right and wrong.

The "digital society" has recently become popular in the social sciences and refers to a society characterised by information flowing through global networks at unprecedented speeds. But the most important feature of the digital society is it that recognises these technologies as an embedded part of the larger social entity and acknowledges the incorporation of digital technologies, media and networks into our daily lives (Lupton, 2015a, 2015b), including in the commission of crime, victimisation and justice. Namely Baym (2015) notes that the distinguishing features of digital technologies are the manner in which they have transformed how people engage with one another. This enmeshment of the digital and social has also been referred to as the digitalization of society in which 'technology is society, and society cannot be understood or represented without its technological tools' (Castells, 1996).

On the other hand, Digital criminology refers to the rapidly developing scientific field that applies criminological, social, cultural theory, the theory of technical systems and the corresponding research methods, in the study of crime, delinquent/deviant behavior and justice in the digital society (Stratton et al., 2017). Moreover, it renegotiates criminological theories in search of new scientific ideas that challenge the classical dichotomies – internet vs. physical world, virtual vs. real-both for the prevention and treatment of crimes in the digital environment, on the internet as well as more generally in the context of new technologies, in the context of the development of technoethics. So, in the field of digital criminology the boundaries of modern criminological theory and research are expanded and a broader and ongoing discussion of technology, sociality, crime, deviance and justice is fostered in new conceptual foundations and empirical directions in cyberspace and digital crime mapping.

4. Criminological challenges and perspectives in the "hybrid" world

Although more than fifteen years have passed since the dominance of social networks, the emergence of augmented reality and artificial intelligence, much of criminological research still traditionally focuses on information systems and internet technologies, viewing them either as targets of crime or as mere tools for the commission of otherwise traditional crimes (Hayward & Maas, 2020; Holt & Bossler, 2014). Moreover, many approaches are based on an inherent dualism, where cybercrime continues to be seen as a mirror or online version of its counterparts in the physical world, differing in means of commission and spatial extent, but not in essence and nature (Grabosky, 2001).

4.1. CrAIme terminology and typology

AI-based Cybercrime (Wang, 2020), AI cybercrime (Hoanca & Mock, 2020), AI Crime (further – AIC) (King et al., 2020), "harmful AI" (Hibbard, 2015; Johnson & Verdicchio, 2017), "malevolent AI"[9], malicious Use and abuse of AI (Blauth et al., 2022) and so on are some of the terms one comes across when reading the relevant academic literature and trying to find the position of AI in the criminological milieu.

For the majority of researchers, the use of AI can enable existing forms of crime ("cyber-enabled crime") or establish new forms of crime ("cyber-dependent crime") (Akdemir & Lawless, 2020; Grabosky, 2001). AI potentially enables attacks that are larger in scale and scope than previously possible with other technologies (Blauth, et al., 2022). Therefore, the term "AI-enabled crime" is preferred, as the possibilities exist both in the cybercrime domain (with overlaps with traditional cybersecurity terms) and in the rest of the world (some of these threats emerge as extensions of existing criminal activities, while others may be novel). The term "AI crime" proposed by King et al. (2020) to describe the situation in which AI technologies are repurposed to facilitate criminal acts by focusing on behaviours that are already defined as criminal in the respective legislation, on the other hand, is considered a term that is too limited to create a broad typology which is not limited to acts that constitute a crime in each state. For example, the creation and dissemination of misinformation/ false news may be harmful under certain national laws, but not necessarily a criminal offence. Therefore, the notion of "malicious use and misuse" of AI (King et al., 2020)[10] is seen as a very interesting alternative.

Within this vast range of possibilities, Hoanca & Mock (2020) classify AI cybercrime into three general and loosely overlapping areas: using AI to commit cybercrime online, using AI via new cybercrime channels that reach into physical space, and using AI or knowledge of AI to strike at the core of other AI systems, by corrupting data or algorithms. These are not three separated areas: they largely overlap, and the extent of their overlap will continue to increase. While, Hayward & Maas, (2020) in an attempt expand the criminological paradigm by taking into account the "tech-crime nexus" qualify the use of the term 'criminal uses of AI' and they identify three categories: (1) crimes with AI, (2) crimes on AI, and (3) crimes by AI. According to them, AI falls under

[9] Yampolskiy, R. V. (2016). Taxonomy of pathways to dangerous AI. arXiv:1511.03246v2, 143–148. https://clck.ru/3CzVKL

[10] Ciancaglini, V. (2020). Malicious uses and abuses of artificial intelligence. Trend Micro Research. United Nations Interregional Crime and Justice Research Institute (UNICRI); Europol's European Cybercrime Centre (EC3). https://clck.ru/3CzSmK

the first AIC category, where it can be a powerful instrument for "malicious" criminal use by introducing new threats or altering the intrinsic characteristics of already-existing ones. It is possible for current threats to spread in a physical setting[11]. Attacks that attempt to fool or "hypnotise" AI systems by taking advantage of and reverse-engineering system vulnerabilities fall under the second AIC category of crimes "on" AI. It has long been possible to "poison" the training data used by a system. Famously, after users fed the Microsoft Twitter[12] chatbot "Tay" a slurry of right-wing phrases, the chatbot turned racist within a day [13]. In the third AIC category, "Crimes by AI", the crucial aspect is the thorny issue of the legal status of AI – and its potential misuse as a "criminal shield/facilitator". A typical paradigm of such a case, according to Hayward & Maas (2020), is the case of a group of artists who published a random shopping bot on the dark web in 2015 – with the unsurprising result that it ended up buying drugs and was arrested by the Swiss police[14].

4.2. A Technoethics approach in the case of AI Crime

Efforts to reach an understanding of ethical aspects of different types of technology are challenged by the tendencies within academia to create information groups in separate fields and disciplines. Technoethics thus helps to connect separate knowledge bases around a common theme (technology, in our case AI). It is holistic in nature and provides an umbrella for all subfields of applied ethics that focus on technology-related areas of human activity, including economics, politics, globalisation, health and medicine, and research and development. Technoethics (further – TE) proposes that what should be changed is, strictly speaking, man's view of himself and his view of reality. Here lie the deepest reasons for the failure of the techno-scientific paradigm, which respects neither the nature of human beings nor the nature of beings in general. We must abandon techno-science, which implies the primacy of science over technology, and embrace a new relational paradigm that is gaining ground in postmodernity. Technoethics arose from the demand to stop the tendency inherent in much of technology to separate itself from freedom and instead to affirm technology as a spiritual activity, an outstanding product of the human spirit, and to recognise it as a driver and not as a mere recipient

11 See also Brundage, M., Avin, S., Clark, J. et al. (2018). The malicious use of artificial intelligence. https://clck.ru/3CzSuH

12 The social network blocked in the territory of the Russian Federation for disseminating unlawful information.

13 Gershgorn, D. (2016). Here's how we prevent the next racist chatbot. Popular Science. https://clck.ru/3CzSxm

14 See also Kasperkevic, J. (2015). Swiss police release robot that bought ecstasy online. The Guardian. https://clck.ru/3CzSzB

of theoretical developments in ethics. And one could say that its main contribution is to address new kinds of ethical questions. It is therefore not surprising that many of the current debates about technological progress are taken up by technoethics. They thus inevitably raise important questions about rights, privacy, responsibility and risks that need to be answered appropriately. Moreover, unlike traditional applied ethics, which emphasises ethical concern for living beings, TE is "biotechnocentric".

The scientific debates around AI-enabled future crime is mainly organized into three non-exclusive categories according to the relationship between crime and AI:

– Defeat to AI – e.g., breaking into devices secured by facial recognition.

– AI to prevent crime – e.g., spotting fraudulent trading on financial markets.

– AI to commit crime – e.g., blackmailing people with "deepfake" video (Caldwell et al., 2020).

And despite the fact that Artificial intelligence (AI) research and regulation seek to balance the benefits of innovation against any potential harms and disruption, one unintended consequence of the recent surge in AI research is the potential re-orientation of AI technologies to facilitate criminal acts, AI Crime (i.e. AIC is theoretically feasible thanks to published experiments in automating fraud targeted at social media users, as well as demonstrations of AI-driven manipulation of simulated markets)[15, 16] (Nguyen et al., 2015). The importance of AIC as a distinct phenomenon has not yet been acknowledged. The literature on AI's ethical and social implications focuses on regulating and controlling AI's civil uses and the AIC research that is available is scattered across disciplines, including socio-legal studies, computer science, psychology, and robotics etc. This lack of research focused on AI Crime undermines the scope for projections and solutions in this new area of potential criminal activity committed by AI, concerns the possibility of new crimes in the category of 'white collar crime' (LoPucki, 2017), but also raises questions about the legal personality of AI – as well as concerns about the use of such machines as "facilitators", their criminal liability, namely where the limits of liability models may undermine legal certainty, as it may be the case that agents, whether artificial or not, may engage in criminal acts or omissions without sufficiently matching the conditions of liability for a particular offence to constitute a (specifically) criminal offence (King at al., 2020; Bayern, 2016; Williams, 2017; McAllister, 2018).

[15] Huang, S., Papernot, N., Goodfellow, I., Duan, Y., & Abbeel, P. (2017). Adversarial attacks on neural network policies. arXiv preprint arXiv:1702.02284. https://clck.ru/3CzT6s

[16] Goodfellow, I. J., Shlens, J., & Szegedy, C. (2014). Explaining and harnessing adversarial examples. arXiv preprint arXiv:1412.6572. https://clck.ru/3CzT8m

A tecnoethical approach thus raises critical issues and questions to consider, especially concerns about destabilised concepts. The underlying concept of criminal law that is destabilised is the idea of criminal liability. AI as an "independent" criminal facilitator raises serious questions about basic legal norms such as the voluntarily committed offence (actus reus), criminal intent (mens rea) and various questions about the knowledge threshold. A second concept that seems to be shaken by this is the importance of social control, the idea of democratic values and the limits of the state's protection of human rights: scalable, comprehensive, inescapable surveillance and the potential use of AI and robotics for law enforcement[17] (Zardiashvili et al., 2019), including critical examinations of how to ensure democratic accountability for ML-based predictive policing technologies. The hidden state: ubiquitous yet tacit surveillance, AI drones and "smart-city" sensors creates new forms of "wide surveillance" that are ubiquitous, yet subtle, tacit, and deniable (Hayward & Maas, 2020). The oracle state: from detection and enforcement, to prediction and prevention with AI systems to be able to pick up on subtle patterns to offer (ostensibly) accurate predictions of future behaviour, including criminal conduct (Danaher, 2022).

However, the primary and exclusive focus on cyberspace, with direct and unambiguous reference to the Internet and "virtual or AI" technologies (categories of cybercrime that are easily and unambiguously distinguished from corresponding categories in "non-cyberspace"), also obscures the diverse and embedded nature of digital data and communication in modern societies (Jaishankar, 2008), where drift in the digital environment results from the dynamic intertwining between the characteristics of the technology and its use (Goldsmith & Brewer, 2014); the "desire for representation" of the deviant "virtual" self (Yar, 2012) is closely related to the broader trends of both self-created subjectivity through new communication platforms and artificial intelligence – the ability of machines to think, communicate and make decisions in ways that were previously only possible for humans (networked reality, networked portability and networked matter, etc.)[18].

S. Brown (2006a), in light of all these challenges, proposes a digital criminology that goes beyond the conventional framework and turns instead to "techno-social theories" (Latour, 1993; Lash, 2002; Haraway, 1987, 1991; Castells, 2001) because one feature of digital technologies is the way they have changed the way people interact with each other (Baym, 2015). Significantly, as she notes, analyses of cybercrime seem to be trapped in absolute distinctions between "virtual" and "embodied, real" crime,

[17] Interpol and UNICRI. (2019). Artificial Intelligence and Robotics for Law Enforcement. https://clck.ru/3CzTGP

[18] Institute for the Future (IFTF). (2019). Future of connected living – augmented humans in a networked world: Research Report. https://clck.ru/3CzTPY

with understandings of the "new" cybercrime relying almost exclusively on metaphors and the "translation" of "old" legal and theoretical frameworks (Aas, 2007; Hayward, 2012; Wood, 2016). In criminology, "nowhere is the vision of the criticality of the nature of the world as a human-technical hybrid..." in which all crimes occur in networks that differ only in the degree of virtuality/reality (embodiment) (Brown, 2006b). Consequently, criminologists today must understand crime and criminality at the blurred intersections of biology/technology, nature/society, object/acting subject and artificial/human. Rather than focusing the study of cybercrime on technology as a dissemination tool that has increased criminal opportunities and networks, it is now suggested that "digital/online (criminal) activities are best understood as processes, i.e., phenomena that are in constant dialogue and change with other phenomena/technologies within a human/technological hybrid world" (Brown, 2006a).

Conclusions

The era of divided perspectives and dichotomies may be coming to an end. Perhaps it is now time for synergies, especially at the interdisciplinary level. Why cling to dichotomies when we can harmonise approaches and perspectives? And all this in the context of the "digital society" that recognises technology as part of the wider social entity and accepts the integration of digital technologies, media and networks into people's lives, including the commission of crime, victimisation and justice.

Baym (2015) elaborates on the blurring of boundaries between online and offline realities, noting that the main characteristic of digital technologies is that they have transformed the way people interact with each other in a networked reality, in a world that is now perceived as a human-technological hybrid (Brown, 2006a) where all crimes occur in networks that differ only in the degree of virtuality/embodiment.

Moreover, all issues raised by the use of this technology are not purely technical but concern a wide range of scientific and non-scientific fields, and its safe use cannot be ensured without a multidisciplinary approach.

Artificial Intelligence has enormous potential to be used for social good and achievement of the Sustainable Development Goals. Even as it is being used to help address many of humanity's most critical social issues, its use is also raising concerns about infringement of human rights like the right to freedom of expression, right to privacy, data protection, and non-discrimination. AI-based technologies offer major opportunities if they are developed in respect of universal norms, ethics and standards, and if they are anchored in values based on human rights and sustainable development. For instance, reliable and transparent artificial intelligence can be an effective 'vehicle' for eliminating inequalities in the educational process, as it can be used to create programmes tailored to learning needs and improve the speed of learning.

Moreover, artificial intelligence can also play an important role in the field of justice by creating automated judicial systems, as well as in the field of jurisprudence in general. For example, in the criminal justice field, the use of AI systems for providing investigative assistance and automating decision-making processes is already in place in many judicial systems across the world.

In the context of emerging technoethics, the idea that this unofficial norm, derived from a popular belief, will be the 'touchstone' for characterising online mediated behaviour as deviant/crimninal, is missing - or rather in the process of being formed.

The moral values of machines with artificial intelligence too often lack the broader human values. To reconcile them, citizens must gain dominance over both and put the former (machine values) in the service of the latter (human values). AI should not be used as a scapegoat for human moral failings. Through the "mirror of artificial intelligence", which is a very helpful diagnostic tool for society, people can learn as much as possible about its flaws and limitations, as well as new insights and solutions it offers. The future of artificial intelligence and human society will not be decided for the people, but by the people.

References

Aas, K. F. (2007). Beyond the desert of the real: Crime control in a virtual(ised) reality. In Y. Jewkes (Ed.), *Crime Online* (pp. 160–177). Portland, Oregon: Willan Publishing.

Akdemir, N., & Lawless, C. J. (2020). Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: A lifestyle routine activities approach. *Internet Research*, *30*(6), 1665–1687. https://doi.org/10.1108/intr-10-2019-0400

Bayern, S. (2016). The implications of modern business–entity law for the regulation of autonomous systems. *European Journal of Risk Regulation*, *7*(1), 297–309. http://dx.doi.org/10.1017/S1867299X00005729

Baym, N. K. (2015). *Personal Connections in the Digital Age*. England: Polity, Cambridge.

Berendt, B. (2019). AI for the common good?! Pitfalls, challenges, and ethics pen-testing. *Paladyn, Journal of Behavioral Robotics*, *10*, 44–65. https://doi.org/10.1515/pjbr-2019-0004

Blauth, T. F., Gstrein, O. J., & Zwitter, A. (2022). Artificial intelligence crime: An overview of malicious use and abuse of AI. *IEEE Access*, *10*, 77110–77122. https://doi.org/10.1109/access.2022.3191790

Boddington, P. (2017). *Towards a Code of Ethics for Artificial Intelligence*. Oxford: Springer International Publishing.

Broadhurst, R., Maxim, D., Brown, P., Trivedi, H., & Wang, J. (2019). Artificial Intelligence and Crime. *SSRN Electronic Journal*. http://dx.doi.org/10.2139/ssrn.3407779

Brown, S. (2006a). The criminology of hybrids: Rethinking crime and law in technosocial networks. *Theoretical Criminology*, *10*(2), 223–244. https://doi.org/10.1177/1362480606063140

Brown, S. (2006b). Virtual criminology. In E. McLaughlin, & J. Muncie (Eds.), *The Sage Dictionary of Criminology* (pp. 224–258). London: Sage.

Bunge, M. (1977). Towards a Technoethics. *Monist*, *60*(1), 96–107.

Caldwell, M., Andrews, J. T., Tanay, T., & Griffin, L. D. (2020). AI-enabled future crime. *Crime Science*, *9*(1), 1–13. https://doi.org/10.1186/s40163-020-00123-8

Castells, M. (1996). *The Rise of the Network Society*. Oxford, England: Blackwell.

Castells, M. (2001). *The Internet Galaxy*. Oxford, England: Oxford University Press.

Coeckelbergh, M. (2019). Artificial Intelligence: some ethical issues and regulatory challenges. *Technology and regulation*, *2019*, 31–34. https://doi.org/10.26116/techreg.2019.003

Danaher, J. (2022). Techno-optimism: an analysis, an evaluation and a modest defence. *Philosophy & Technology*, *35*(54), 8. https://doi.org/10.1007/s13347-022-00550-2

Di Nicola, A. (2022). Towards digital organized crime and digital sociology of organized crime. *Trends in Organized Crime*. https://doi.org/10.1007/s12117-022-09457-y

Dignum, V. (2019). *Responsible artificial intelligence: how to develop and use AI in a responsible way*. Cham, Switzerland: Springer Nature Switzerland AG.
Dilek, S., Cakır, H., & Aydın, M. (2015). Applications of artificial intelligence techniques to combating cyber crimes: A review. *IJAIA*, *6*(1), 21–39. https://doi.org/10.5121/ijaia.2015.6102
Goldsmith, A., & Brewer, R. (2014). Digital drift and the criminal interaction order. *Theoretical Criminology*, *19*(1), 112–130. https://doi.org/10.1177/1362480614538645
Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles? *Social & Legal Studies*, *10*(2), 243–249. https://doi.org/10.1177/a017405
Greenfield, A. (2017). *Radical Technologies*. London: Verso.
Haraway, D. (1987). A manifesto for Cyborgs: Science, technology, and socialist feminism in the 1980s. *Australian Feminist Studies*, *2*(4), 1–42. https://doi.org/10.1080/08164649.1987.9961538
Haraway, D. (1991). *Simians, Cyborgs and Women: The Reinvention of Nature*. London: Free Association Books.
Hayward, K., & Maas, M. (2020). Artificial intelligence and crime: A primer for criminologists. *Crime Media & Culture*, *17*(2), 1–25. https://doi.org/10.1177/1741659020917434
Hayward, K. (2012). Five spaces of cultural criminology. *British Journal of Criminology*, *52*(3), 441–462. https://doi.org/10.1093/bjc/azs008
Heller, P. B. (2012). Technoethics: The Dilemma of Doing the Right Moral Thing in Technology Applications. *International Journal of Technoethics (IJT)*, *3*(1), 14–27. https://doi.org/10.4018/jte.2012010102
Hibbard, B. (2015). *Ethical Artificial Intelligence*. WI, USA: Madison.
Hoanca, B., & Mock, K. J. (2020). Artificial intelligence-based cybercrime. In *Encyclopedia of criminal activities and the deep web* (pp. 36–51). IGI Global.
Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior*, *35*(1), 20–40. https://doi.org/10.1080/01639625.2013.822209
Ionescu, B., Ghenescu, M., Răstoceanu, F., Roman, R., & Buric, M. (2020). Artificial intelligence fights crime and terrorism at a new level. *IEEE MultiMedia*, *27*(2), 55–61. https://doi.org/10.1109/mmul.2020.2994403
Jaishankar, K. (2008). Space transition theory of cybercrimes. In F. Schmallager, & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 283–301). New Jersey: Prentice Hall.
Johnson, D. G., & Verdicchio, M. (2017). Reframing AI discourse. *Minds and Machines*, *27*(4), 575–590. https://doi.org/10.1007/s11023-017-9417-6
Kaloudi, N., & Li, J. (2020). The AI-based cyber threat landscape. *ACM Computing Surveys*, *53*(1), 1–34. https://doi.org/10.1145/3372823
King, T. C., Aggarwal, N., Taddeo, M. & Floridi, L. (2020). Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions. *Science and Engineering Ethics*, *26*(1), 89–120. https://doi.org/10.1007/s11948-018-00081-0
Lash, S. (2002). *Critique of Information*. London: Sage.
Latour, B. (1993). *We Have Never Been Modern*. Cambridge, Massachusetts: Harvard University Press.
Lee, C. S., & Chua, Y. T. (2023). The Role of Cybersecurity Knowledge and Awareness in Cybersecurity Intention and Behavior in the United States. *Crime & Delinquency*, *70*(9), 2250–2277. https://doi.org/10.1177/00111287231180093
Li, S. T., Kuo, S. C., & Tsai, F. C. (2010). An intelligent decision-support model using FSOM and rule extraction for crime prevention. *Expert Systems with Applications*, *37*(10), 7108–7119. https://doi.org/10.1016/j.eswa.2010.03.004
Lin, Y. L., Chen, T. Y., & Yu, L. C. (2017). Using machine learning to assist crime prevention. *Proceedings of 6th IIAI International Congress on Advanced Applied Informatics (IIAI-AAI)*, 1029–1030. https://doi.org/10.1109/iiai-aai.2017.46
LoPucki, Lynn M. (2017, April 17). *Algorithmic Entities. Washington University Law Review (Forthcoming)*, 95. UCLA School of Law, Law-Econ Research Paper No. 17-09.
Luppicini, R. (2008). The Emerging Field of Technoethics. In R. Luppicini, & R. Adell (Eds.), *Handbook of Research on Technoethics*. IGI Global books. https://doi.org/10.4018/9781605660226.ch001
Lupton, D. (2015a). Quantified sex: a critical analysis of sexual and reproductive self-tracking using apps. *Culture, Health & Sexuality*, *17*(4), 440–453. https://doi.org/10.1080/13691058.2014.920528
Lupton, D. (2015b). *Digital Sociology*. 1st ed. London & New York: Routledge.
McAllister, A. (2018). Stranger than science fiction: the rise of A.I. interrogation in the dawn of autonomous robots and the need for an additional protocol to the U.N. convention against torture. *Minnesota Law Review*, *101*, 2527–2573.

McClendon, L., & Meghanathan, N. (2015). Using machine learning algorithms to analyze crime data. *MLAIJ*, *2*(1), 1–12. https://doi.org/10.5121/mlaij.2015.2101

Mielke, C. J., & Chen, H. (2008). Botnets, and the cybercriminal underground. *Proceedings of IEEE International Conference on Intelligence and Security Informatics (ISI 2008)*, 206–211. https://doi.org/10.1109/isi.2008.4565058

Müller, V. C. (2020). Ethics of artificial intelligence and robotics. In E. N. Zalta (Ed.), *The Stanford encyclopedia of philosophy*. Stanford, CA: Metaphysics Research Lab. Stanford University.

Nguyen, A., Yosinski, J., & Clune, J. (2015). Deep neural networks are easily fooled: high confidence predictions for unrecognizable images. *Proceedings of the IEEE conference on computer vision and pattern recognition,* 7–12 June, 427–436. https://doi.org/10.1109/cvpr.2015.7298640

Sharif, M., Bhagavatula, S., Bauer, L., & Reiter, M. K. (2016). Accessorize to a crime. *Proceedings of ACM SIGSAC Conference*, 1528–1540. https://doi.org/10.1145/2976749.2978392

Stratton, G., Powell, A., & Cameron, R. (2017). Crime and Justice in Digital Society: Towards a 'Digital Criminology'? *International Journal for Crime, Justice and Social Democracy*, *6*(2), 17–33. https://doi.org/10.5204/ijcjsd.v6i2.355

van der Wagen, W., & Pieters, W. (2015). From cybercrime to cyborg crime: botnets as hybrid criminal actor-networks. *British Journal of Criminology*, *55*(3), 578–595. https://doi.org/10.1093/bjc/azv009

Wang, X. (2020, April). Criminal law protection of cybersecurity considering AI-based cybercrime. *Journal of Physics: Conference Series*, *1533*(3), 032014. https://doi.org/10.1088/1742-6596/1533/3/032014

Williams, R. (2017). *Lords select committee, artificial intelligence committee, written evidence (AIC0206)*.

Wood, M. A. (2016). Antisocial media and algorithmic deviancy amplification: Analysing the id of Facebook's[19] technological unconscious. *Theoretical Criminology*, *21*(2), 1–18. https://doi.org/10.1177/1362480616643382

Yar, M. (2012). Crime, media and the will-to-representation: Reconsidering relationships in the new media age. *Crime, Media, Culture*, *8*(3), 245–260. https://doi.org/10.1177/1741659012443227

Zardiashvili, L., Bieger, J., Dechesne, F., & Dignum, V. (2019). AI ethics for law enforcement. *Delphi*, *2*(4), 179–185. https://doi.org/10.21552/delphi/2019/4/7

[19] The social network belongs to Meta, which is recognized as an extremist organization, its functioning is prohibited in the territory of the Russian Federation

Author information

Fotios Spyropoulos – PostDoc, PhD, Associate Professor of Criminal Law & Criminology, Faculty of Law, Philips University; Senior Partner of Spyropoulos Law Firm
Address: 4-6 Lamias Street, 2001, P.O. Box 28008, Nicosia, Cyprus; Alexandras Avenue 81, 11474, Athens, Greece
E-mail: fspyropoulos@gmail.com
ORCID ID: https://orcid.org/0000-0001-5950-3583
Google Scholar ID: https://scholar.google.com/citations?user=iKQYLWoAAAAJ

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – April 30, 2024
Date of approval – April 15, 2024
Date of acceptance – September 25, 2024
Date of online placement – September 30, 2024

Научная статья
УДК 34:004:349.2:004.8
EDN: https://elibrary.ru/mqtnqg
DOI: https://doi.org/10.21202/jdtl.2024.32

Новые подходы к исследованию ИИ-преступности: конституирование цифровой криминологии

Фотиос Спайропулос

Университет Филипс, Никосия, Кипр
Spyropoulos Law Firm, Афины, Греция

Ключевые слова

искусственный интеллект,
киберпреступность,
право,
преступление,
преступность,
техноэтика,
цифровая криминология,
цифровое общество,
цифровые технологии,
этика

Аннотация

Цель: опираясь на современные научные подходы к «цифровому обществу» и новые подходы в криминологии, выявить и определить цифровую криминологию, направленную на изучение возможных способов использования искусственного интеллекта преступниками, в том числе в рамках так называемой ИИ-преступности.

Методы: проблемы связи искусственного интеллекта с преступностью в «гибридном мире» переосмысливаются в статье преимущественно с учетом междисциплинарности, на уровне которой аргументы подкрепляются соответствующими отсылками к «цифровой криминологии» и ее небинарному образу мышления в рамках техносоциального подхода, несистематического обзора литературы.

Результаты: в исследовании отмечается, что в цифровом обществе технологии интегрируются в жизнь людей, включая сферы преступности, виктимизации и правосудия, стирая границы между онлайн- и офлайн-реальностью, создавая гибридный мир человека и технологий, где преступления происходят в виртуальных сетях. Показано, что искусственный интеллект обладает потенциалом для достижения целей социального благополучия и устойчивого развития, однако необходимо учитывать риски, связанные с нарушением прав человека. Обосновывается необходимость междисциплинарного подхода для обеспечения безопасного использования технологий, борьбы с неравенством в сфере образования, помощи в осуществлении правосудия и распознавании девиантного или преступного поведения в сети. Подчеркивается, что в контексте зарождающейся техноэтики пока отсутствует или, скорее, находится в процессе формирования идея о том, что эта неофициальная норма, основанная на обыденных представлениях, станет «опорным камнем» для характеристики опосредованного онлайн-поведения как девиантного или преступного.

Научная новизна: в статье с точки зрения техноэтики выдвигается ряд подходов к феномену использования информационно-коммуникационных технологий в преступных целях под влиянием искусственного интеллекта. При этом отмечены социальные вызовы, возникающие в результате технологических сбоев (например, прогнозирование и предотвращение преступлений путем трансформации деятельности органов охраны правопорядка, усиления наблюдения и практики уголовного правосудия) в «цифровом обществе».

Практическая значимость: идеи, лежащие в основе данного исследования, могут быть использованы при разработке предложений по внесению изменений и дополнений в действующее уголовное законодательство, а также в педагогической деятельности, особенно при реализации образовательных курсов или модулей по проблемам преступности в контексте цифровой трансформации общества.

Для цитирования

Спайропулос, Ф. (2024). Новые подходы к исследованию ИИ-преступности: конституирование цифровой криминологии. *Journal of Digital Technologies and Law*, *2*(3), 636–656. https://doi.org/10.21202/jdtl.2024.32

Список литературы

Aas, K. F. (2007). Beyond the desert of the real: Crime control in a virtual(ised) reality. In Y. Jewkes (Ed.), *Crime Online* (pp. 160–177). Portland, Oregon: Willan Publishing.

Akdemir, N., & Lawless, C. J. (2020). Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: A lifestyle routine activities approach. *Internet Research*, *30*(6), 1665–1687. https://doi.org/10.1108/intr-10-2019-0400

Bayern, S. (2016). The implications of modern business–entity law for the regulation of autonomous systems. *European Journal of Risk Regulation*, *7*(1), 297–309. http://dx.doi.org/10.1017/S1867299X00005729

Baym, N. K. (2015). *Personal Connections in the Digital Age*. England: Polity, Cambridge.

Berendt, B. (2019). AI for the common good?! Pitfalls, challenges, and ethics pen-testing. *Paladyn, Journal of Behavioral Robotics*, *10*, 44–65. https://doi.org/10.1515/pjbr-2019-0004

Blauth, T. F., Gstrein, O. J., & Zwitter, A. (2022). Artificial intelligence crime: An overview of malicious use and abuse of AI. *IEEE Access*, *10*, 77110–77122. https://doi.org/10.1109/access.2022.3191790

Boddington, P. (2017). *Towards a Code of Ethics for Artificial Intelligence*. Oxford: Springer International Publishing.

Broadhurst, R., Maxim, D., Brown, P., Trivedi, H., & Wang, J. (2019). Artificial Intelligence and Crime. *SSRN Electronic Journal*. http://dx.doi.org/10.2139/ssrn.3407779

Brown, S. (2006a). The criminology of hybrids: Rethinking crime and law in technosocial networks. *Theoretical Criminology*, *10*(2), 223–244. https://doi.org/10.1177/1362480606063140

Brown, S. (2006b). Virtual criminology. In E. McLaughlin, & J. Muncie (Eds.), *The Sage Dictionary of Criminology* (pp. 224–258). London: Sage.

Bunge, M. (1977). Towards a Technoethics. *Monist*, *60*(1), 96–107.

Caldwell, M., Andrews, J. T., Tanay, T., & Griffin, L. D. (2020). AI-enabled future crime. *Crime Science*, *9*(1), 1–13. https://doi.org/10.1186/s40163-020-00123-8

Castells, M. (1996). *The Rise of the Network Society*. Oxford, England: Blackwell.

Castells, M. (2001). *The Internet Galaxy*. Oxford, England: Oxford University Press.

Coeckelbergh, M. (2019). Artificial Intelligence: some ethical issues and regulatory challenges. *Technology and regulation*, *2019*, 31–34. https://doi.org/10.26116/techreg.2019.003

Danaher, J. (2022). Techno-optimism: an analysis, an evaluation and a modest defence. *Philosophy & Technology*, *35*(54), 8. https://doi.org/10.1007/s13347-022-00550-2

Di Nicola, A. (2022). Towards digital organized crime and digital sociology of organized crime. *Trends in Organized Crime*. https://doi.org/10.1007/s12117-022-09457-y

Dignum, V. (2019). *Responsible artificial intelligence: how to develop and use AI in a responsible way*. Cham, Switzerland: Springer Nature Switzerland AG.
Dilek, S., Cakır, H., & Aydın, M. (2015). Applications of artificial intelligence techniques to combating cyber crimes: A review. *IJAIA*, *6*(1), 21–39. https://doi.org/10.5121/ijaia.2015.6102
Goldsmith, A., & Brewer, R. (2014). Digital drift and the criminal interaction order. *Theoretical Criminology*, *19*(1), 112–130. https://doi.org/10.1177/1362480614538645
Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles? *Social & Legal Studies*, *10*(2), 243–249. https://doi.org/10.1177/a017405
Greenfield, A. (2017). *Radical Technologies*. London: Verso.
Haraway, D. (1987). A manifesto for Cyborgs: Science, technology, and socialist feminism in the 1980s. *Australian Feminist Studies*, *2*(4), 1–42. https://doi.org/10.1080/08164649.1987.9961538
Haraway, D. (1991). *Simians, Cyborgs and Women: The Reinvention of Nature*. London: Free Association Books.
Hayward, K., & Maas, M. (2020). Artificial intelligence and crime: A primer for criminologists. *Crime Media & Culture*, *17*(2), 1–25. https://doi.org/10.1177/1741659020917434
Hayward, K. (2012). Five spaces of cultural criminology. *British Journal of Criminology*, *52*(3), 441–462. https://doi.org/10.1093/bjc/azs008
Heller, P. B. (2012). Technoethics: The Dilemma of Doing the Right Moral Thing in Technology Applications. *International Journal of Technoethics (IJT)*, *3*(1), 14–27. https://doi.org/10.4018/jte.2012010102
Hibbard, B. (2015). *Ethical Artificial Intelligence*. WI, USA: Madison.
Hoanca, B., & Mock, K. J. (2020). Artificial intelligence-based cybercrime. In *Encyclopedia of criminal activities and the deep web* (pp. 36–51). IGI Global.
Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior*, *35*(1), 20–40. https://doi.org/10.1080/01639625.2013.822209
Ionescu, B., Ghenescu, M., Răstoceanu, F., Roman, R., & Buric, M. (2020). Artificial intelligence fights crime and terrorism at a new level. *IEEE MultiMedia*, *27*(2), 55–61. https://doi.org/10.1109/mmul.2020.2994403
Jaishankar, K. (2008). Space transition theory of cybercrimes. In F. Schmallager, & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 283–301). New Jersey: Prentice Hall.
Johnson, D. G., & Verdicchio, M. (2017). Reframing AI discourse. *Minds and Machines*, *27*(4), 575–590. https://doi.org/10.1007/s11023-017-9417-6
Kaloudi, N., & Li, J. (2020). The AI-based cyber threat landscape. *ACM Computing Surveys*, *53*(1), 1–34. https://doi.org/10.1145/3372823
King, T. C., Aggarwal, N., Taddeo, M. & Floridi, L. (2020). Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions. *Science and Engineering Ethics*, *26*(1), 89–120. https://doi.org/10.1007/s11948-018-00081-0
Lash, S. (2002). *Critique of Information*. London: Sage.
Latour, B. (1993). *We Have Never Been Modern*. Cambridge, Massachusetts: Harvard University Press.
Lee, C. S., & Chua, Y. T. (2023). The Role of Cybersecurity Knowledge and Awareness in Cybersecurity Intention and Behavior in the United States. *Crime & Delinquency*, *70*(9), 2250–2277. https://doi.org/10.1177/00111287231180093
Li, S. T., Kuo, S. C., & Tsai, F. C. (2010). An intelligent decision-support model using FSOM and rule extraction for crime prevention. *Expert Systems with Applications*, *37*(10), 7108–7119. https://doi.org/10.1016/j.eswa.2010.03.004
Lin, Y. L., Chen, T. Y., & Yu, L. C. (2017). Using machine learning to assist crime prevention. *Proceedings of 6th IIAI International Congress on Advanced Applied Informatics (IIAI-AAI)*, 1029–1030. https://doi.org/10.1109/iiai-aai.2017.46
LoPucki, Lynn M. (2017, April 17). *Algorithmic Entities. Washington University Law Review (Forthcoming)*, 95. UCLA School of Law, Law-Econ Research Paper No. 17-09.
Luppicini, R. (2008). The Emerging Field of Technoethics. In R. Luppicini, & R. Adell (Eds.), *Handbook of Research on Technoethics*. IGI Global books. https://doi.org/10.4018/9781605660226.ch001
Lupton, D. (2015a). Quantified sex: a critical analysis of sexual and reproductive self-tracking using apps. *Culture, Health & Sexuality*, *17*(4), 440–453. https://doi.org/10.1080/13691058.2014.920528
Lupton, D. (2015b). *Digital Sociology*. 1st ed. London & New York: Routledge.
McAllister, A. (2018). Stranger than science fiction: the rise of A.I. interrogation in the dawn of autonomous robots and the need for an additional protocol to the U.N. convention against torture. *Minnesota Law Review*, *101*, 2527–2573.
McClendon, L., & Meghanathan, N. (2015). Using machine learning algorithms to analyze crime data. *MLAIJ*, *2*(1), 1–12. https://doi.org/10.5121/mlaij.2015.2101

Mielke, C. J., & Chen, H. (2008). Botnets, and the cybercriminal underground. *Proceedings of IEEE International Conference on Intelligence and Security Informatics (ISI 2008)*, 206–211. https://doi.org/10.1109/isi.2008.4565058

Müller, V. C. (2020). Ethics of artificial intelligence and robotics. In E. N. Zalta (Ed.), *The Stanford encyclopedia of philosophy*. Stanford, CA: Metaphysics Research Lab. Stanford University.

Nguyen, A., Yosinski, J., & Clune, J. (2015). Deep neural networks are easily fooled: high confidence predictions for unrecognizable images. *Proceedings of the IEEE conference on computer vision and pattern recognition,* 7–12 June, 427–436. https://doi.org/10.1109/cvpr.2015.7298640

Sharif, M., Bhagavatula, S., Bauer, L., & Reiter, M. K. (2016). Accessorize to a crime. *Proceedings of ACM SIGSAC Conference*, 1528–1540. https://doi.org/10.1145/2976749.2978392

Stratton, G., Powell, A., & Cameron, R. (2017). Crime and Justice in Digital Society: Towards a 'Digital Criminology'? *International Journal for Crime, Justice and Social Democracy*, *6*(2), 17–33. https://doi.org/10.5204/ijcjsd.v6i2.355

van der Wagen, W., & Pieters, W. (2015). From cybercrime to cyborg crime: botnets as hybrid criminal actor-networks. *British Journal of Criminology*, *55*(3), 578–595. https://doi.org/10.1093/bjc/azv009

Wang, X. (2020, April). Criminal law protection of cybersecurity considering AI-based cybercrime. *Journal of Physics: Conference Series*, *1533*(3), 032014. https://doi.org/10.1088/1742-6596/1533/3/032014

Williams, R. (2017). *Lords select committee, artificial intelligence committee, written evidence (AIC0206)*.

Wood, M. A. (2016). Antisocial media and algorithmic deviancy amplification: Analysing the id of Facebook's[1] technological unconscious. *Theoretical Criminology*, *21*(2), 1–18. https://doi.org/10.1177/1362480616643382

Yar, M. (2012). Crime, media and the will-to-representation: Reconsidering relationships in the new media age. *Crime, Media, Culture*, *8*(3), 245–260. https://doi.org/10.1177/1741659012443227

Zardiashvili, L., Bieger, J., Dechesne, F., & Dignum, V. (2019). AI ethics for law enforcement. *Delphi*, *2*(4), 179–185. https://doi.org/10.21552/delphi/2019/4/7

[1] Социальная сеть принадлежит Meta, признанной экстремистской организацией, ее деятельность запрещена на территории Российской Федерации.

Сведения об авторе

Фотиос Спиропулос – научный сотрудник, PhD, доцент в области уголовного права и криминалистики, факультет права, Университет Филипс; старший партнер юридической компании Spyropoulos Law Firm
Адрес: Кипр, 28008, г. Никосия, ул. Ламиас, 4-6; Греция, 11474, г. Афины, Александрас авеню, 81
E-mail: fspyropoulos@gmail.com
ORCID ID: https://orcid.org/0000-0001-5950-3583
Google Scholar ID: https://scholar.google.com/citations?user=iKQYLWoAAAAJ

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.81 / Криминология
Специальность ВАК: 5.1.4 / Уголовно-правовые науки

История статьи

Дата поступления – 30 апреля 2024 г.
Дата одобрения после рецензирования – 15 мая 2024 г.
Дата принятия к опубликованию – 25 сентября 2024 г.
Дата онлайн-размещения – 30 сентября 2024 г.

Research article
UDC 34:004:343.9:004.4
EDN: https://elibrary.ru/ftkczu
DOI: https://doi.org/10.21202/jdtl.2024.33

Newsmaking Criminology in the 21st Century: Forming the Public Opinion under the New Reality

Valentina A. Babaeva

Moscow State Institute of International Relations (University) of the Ministry of Foreign Affairs of the Russian Federation, Moscow, Russia

Keywords

crime,
criminology,
digital society,
digital technologies,
Internet,
justice,
law enforcement agency,
law,
mass media,
news criminology

Abstract

Objective: to study the concept of newsmaking criminology and its relevance in the current conditions of mass media development.

Methods: the methodological basis of the work consists of general scientific, social, and special-legal methods of cognition. The conducted research is based on the dialectical method (in determining the general direction of the study), methods of formal logic (analysis, synthesis, induction, deduction, analogy), system method (in comparing and generalizing the information collected for the research).

Results: the functions of newsmaking criminology in its classical manifestation, as well as its additional functions in the study of mass media in the Internet, were revealed. It is suggested that with the emergence of the World Wide Web, the relevance of newsmaking criminology has increased: social networks, blogs and video hosting as alternative media have a strong influence on public opinion, while an unlimited number of people have access to content generation, contrary to traditional media. Many states understand the importance of interaction between mass media and law enforcement agencies and are actively implementing their methods of promoting newsmaking criminology online. This article points out the risks that arise in media coverage of law enforcement and crime. One of such risks is the cancel culture, which is spontaneous, unpredictable in nature, and may jeopardize the quality of life of the victim or business reputation and activity of organizations.

Scientific novelty: the functions performed by newsmaking criminology in the study of traditional and alternative media were identified. So far, such doctrine has not been sufficiently researched taking into account modern forms of mass communication. Examples of interaction between law enforcement agencies of different states and the media were analyzed.

Practical significance: the study contributes to understanding the correlation between criminological phenomena and modern media platforms. The Internet and social networks provide new channels of information exchange that differ significantly from traditional media such as printed media or television.

For citation

Babaeva, V. A. (2024). Newsmaking Criminology in the 21st Century: Forming the Public Opinion under the New Reality. *Journal of Digital Technologies and Law, 2*(3), 657–673. https://doi.org/10.21202/jdtl.2024.33

Contents

Introduction

Interaction between law enforcement officers and mass media (hereinafter – the media) has an ambivalent nature. It is of particular interest to researchers of the nature of such a relationship from the viewpoint of criminology. The media have a tremendous influence on public opinion, which can both reduce the level of citizens' trust in law enforcement agencies or contribute to stereotypes about a certain criminal phenomenon, and do the opposite. Through cooperation, law enforcement agencies and the media can provide the public with accurate and reliable information on incidents, investigations and law enforcement activities, inform about public safety issues, and raise awareness of crime prevention strategies. Such cooperation is key to ensuring public safety, establishing trust, and facilitating effective communication with the public. This potentially enhances positive law enforcement-public relations while ensuring the dissemination of accurate and timely information.

The term "newsmaking criminology" was first introduced by Gregg Barak in 1988. This scientific doctrine studies the peculiarities of interaction between law enforcement agencies and the media, the influence of the media on public opinion about law enforcement

officers and the criminogenic situation in the country. Newsmaking criminology is a subset of so-called public criminology, a special approach to criminology, in which scholars disseminate the results of their research in this field beyond academia to a wider audience.

This article examines the concept of newsmaking criminology through the prism of modern legal realities. The era of digitalization encompasses all spheres of society, including the media. The author of this concept viewed newsmaking criminology considering traditional media like radio, television, newspapers, etc. The community formed in the World Wide Web has become a new form of media, interaction with which has become a much more complex process than the interaction with traditional media was supposed to be. Social processes on the Internet are more spontaneous and unpredictable, which bears a number of risks.

1. Classical newsmaking criminology

Criminologists often criticize the media for the emotional narrative, distortion of facts and oversimplification they bring to crime and justice issues. This phenomenon is caused by the social and technological advances of the media: their ability to reproduce and create content and their influence on many aspects of social and cultural life. The media are capable of creating public opinion, determining the views of individuals and entire social groups (Sysoev, 2007). From this perspective, powerful forms of communication create unrealistic images of criminality and avoid rational reflection on these phenomena. Central to this critique is the concept of media as a communication process and the notions underlying it (Arrigo & Bersot, 2015; Stout & Clamp, 2015; Gore et al., 2020, De Melo Bandeira, 2013; Cotee, 2004).

Newsmaking criminology is the deliberate activity of criminologists examining media representations of crime and criminal justice and working with media representatives to shape “newsworthy” stories about crime and justice (Barak, 1988).

Despite the similarities between the terms “newsmaking criminology” and “media criminology”, there are some differences between the two concepts. Mass communication (media) criminology is a concept aimed at analyzing the causes and patterns of crime in multiple mass communications and information exchange in general (Gorshenkov, 2003). Thus, newsmaking criminology can be called a subtype of media criminology.

Newsmaking criminology encompasses the issues in media coverage of the administration of justice, thus directly affecting citizens’ perceptions of law enforcement or crime in general. The originator of this concept points to the insufficiency of adequate education among participants in educational programs. For example, programs on economics and politics invite experts in these scientific fields, while criminology programs lack relevant specialists (Barak, 2007). The deficit of expert opinion in such materials can be explained by time constraints and their infotainment nature: few experts can take the discussion of the issue beyond “soundbites” or “talking points” within the

narrative (Frost & Phillips, 2011). Newsmaking criminology is driven by a moral and political motivation to inform media audiences and dispel misconceptions about crime and justice (Richards et al., 2020).

The relationships between the criminal justice system and the media system has been the subject of research, speculation and commentary throughout the 20th century. These relationships can be described as symbiotic: the criminal justice system is a valuable resource for the media system, as information about recent crimes and their prosecution is sought after by audiences. In search of new material, the media monitor the latest trends in society for real and potential threats to individual and collective well-being. Many journalistic investigations and exposés contribute to the detection of latent offenses, and timely publicized information can prevent upcoming crimes (Shamaev, 2018). The interaction between the media and law enforcement agencies is a strategic remedy towards crime, and its result affects several spheres at once. Thus, newsmaking criminology has a number of functions (Ozkan, 2019).

First, the analytical function of newsmaking criminology is to study the representation of crime and criminal justice administration in the media. It analyzes the content, framing, and possible bias in the news, helping to identify patterns and trends in media coverage of crime.

Second, newsmaking criminology examines the formation of public opinion and the target audience's perception of crime and the criminal justice process. Newsmaking criminology examines how media narratives influence public opinion, shape fear or stereotypes about particular phenomena or criminogenic factors. It also examines the broader social implications of crime and criminal justice representations, such as how the media affect public trust in certain social institutions and the stigmatization of certain groups and communities.

Third, newsmaking criminology looks at the ethical implications of media practices in reporting crime. This function looks at aspects such as misinformation, incomplete coverage of all the facts of a criminal case, etc. Gregg Barak emphasized the media's representation of crime in a one-dimensional and distorted format. For example, only the most "interesting" stories, which, in theory, should attract a large audience and generate profits for TV news channels or newspapers, are presented to the public, while other social issues may be ignored or distorted.

Fourth, newsmaking criminology has an educational function. The specificity of the concept of newsmaking criminology lies not only in the interaction of criminologists and law enforcement officials with the media, but also in taking the ideas of criminology as a science beyond academia and making them more accessible for study. The aim of the educational function is to create a deeper understanding of criminal problems, to debunk myths and misconceptions about the administration

of criminal justice and to promote media literacy, which in turn contributes to the reduction of crime.

The media have a direct influence on public consciousness, which can contribute to both the reduction and increase of crime (Matskevich, 2013). For example, the representation of law enforcement officers in the media as competent specialists gives citizens a sense of security and motivates them to cooperate with law enforcement agencies (Gaidai & Grozin, 2020). Materials published by the media may contain so-called criminally repulsive triggers – audiovisual materials causing a chain of feelings in a person that may suppress criminal motivation (Tokarev & Bodrov, 2012). Such triggers can be stories that remind a potential offender of the inevitability of punishment. Establishing cooperation between law enforcement agencies and the media is one of the methods of creating a positive perception of law enforcement among citizens (Glukhova et al., 2017).

The ability of the media system to reach a wide audience positions it as an important resource for the criminal justice system and all related judicial and law enforcement agencies. For the criminal justice system to work effectively, it must achieve credibility based on people's willingness to give it legitimacy, and media narratives can influence this process.

The entertainment media have also been studied and criticized for their influence on public opinions about the people and institutions that make up the criminal justice system. A large number of television programs (e.g., comedies, detective stories, dramas, biographies, documentaries) focus in one way or another on police, lawyers, judges, criminals, and crime victims. The impact of these images on public attitudes and behavior has received considerable attention of researchers. Journalists can enhance the overall legitimacy of the justice system by reporting on its activities. Public trust and confidence that law enforcement officials are working properly can be maintained through the coverage of crime in news sources.

2. Newsmaking criminology in the 21st century

In the pre-Internet era, the media had a stricter system of censorship. With the advent of the World Wide Web, particularly social media, it became more difficult to censor the exponentially growing flow of information. The concept of newsmaking criminology was developed in the 1980s; consequently, in that period, researchers focused on the features of the representation of the criminal justice administration in traditional media, particularly radio, television, and newspapers. In the broad sense of the term "mass media", the Internet can also be called a kind of mass media (Sukhodolov & Bychkova, 2017). The so-called alternative media (also known as social media), video hostings, blogs and social networks are a more chaotic system with a global reach to audience. Any user can share their subjective opinion, which, depending on how the algorithms work, can find a wide response among other users from all over the world. One and the same judgment

acquires different meanings and has a different impact on public opinion depending on the author personality. This exacerbates the relevance of newsmaking criminology. Such new cyberspace phenomena as cancel culture, cyberbullying, information wars, etc., draw the attention of the scientific community to the need to update the doctrine of newsmaking criminology.

In the case of classical media, several people work on the content production in order to improve its quality; the source material is aimed at an audience within a single state or region. Consequently, the techniques developed by newsmaking criminologists when interacting with traditional forms of media can still be applied on the Internet, but their effectiveness has become much lower. This indicates the need to find new approaches to interaction.

According to statistics, in recent years there have been serious changes in preferences regarding sources of information. For example, in 2010 in the Russian Federation 89 % of respondents preferred television as the main source of news, 13 % received information from news sites on the Internet, 21 % – from printed newspapers and magazines, 19 % learned news on the radio and only 4 % of respondents learned news from blogs, websites and social networks. As of 2023, it can be seen that in 13 years the dynamics of viewers' preference has changed in favor of alternative media. In 2023, the percentage of Russians receiving information from television was 62 %, from news sites – 42 %, from blogs and social networks – 23 %. Indicators of preference for radio and printed press decreased to 8 and 7 % respectively[1].

At the same time, the trust rating for news sources has also changed: the level of trust in television was 43 % in 2023 with 63 % in 2010. During this period, the trust level for forums, blogs and social networks increased from 4 % to 13 %.

With the advent of the Internet and alternative media, newsmaking criminology is gaining additional functions. For example, now it is also tasked with studying Internet communities and subcultures, formation of these communities and their impact on crime rates. This field focuses on the representation of the law enforcement officer image in the online community and among different subcultures. Newsmaking criminologists can examine how information circulates in these spaces and how it correlates with the behavior of online communities' participants in real life.

Genre features of an Internet communication are blurred. On the one hand, it has features of a personal diary entry; on the other hand, such a record is aimed at being read by a wide range of users (Aleksandrova, 2008). One person's subjective opinion, based on emotions and speculative assessment, rarely supported by facts, can find a wide response among other users and lead to public resonance. This suggests the

[1] Sources of information: preferences of the Russians. (2023, February 14). "Obshchestvennoye mneniye" Fund. https://clck.ru/3CgYy3

personalization of alternative media, in which the basis of public opinion on the Internet can be formed not only by a blogger, a politician or another media personality, but also by any user of the Web (Bykov & Akhmedova, 2021).

In this feature of alternative media lies another new function of newsmaking criminology: modern conditions allow law enforcement and criminologists to create blogs and news pages without having to interact with representatives of traditional media. As mentioned above, law enforcement agencies and representatives of traditional media often pursue different goals, therefore the result of such interaction can negatively affect the quality and content of the material that news criminologists originally wanted to convey. For example, when studying the criminology of mass communications, D. A. Shestakov identified several methods of influencing public opinion used by traditional media, such as direct falsification of facts, creating the illusion of open discussion, and dosing information (Shestakov). The specificity of alternative media is that newsmaking criminologists can interact with the audience on the Web directly and choose content for enlightenment without needing to interact with other persons, as in the case of traditional media.

In this aspect, of interest are the approaches of some BRICS member states to the interaction between law enforcement agencies and the media within states. For example, India considers it undesirable for law enforcement agencies to interact with news channels to cover news about criminal cases that are under investigation or where no court decision has been announced, as the information may potentially cause moral damage to the defense or prosecution[2]. India's approach is also interesting because of an unusual experiment on the part of law enforcement agencies where regional police stations are setting up blogs and social media accounts[3]. For example, the Mumbai police blog has 4 million subscribers. In such blogs, police officers share news about the crime situation in the region and also offer a feedback system. For example, citizens can report suspicious incidents to law enforcement officers using Twitter[4] or WhatsApp.

In the case of Brazil, its Internet segment faces a confrontation between organized crime and law enforcement because criminals use social media to intimidate the public and promote their illegal businesses[5]. Brazilian law enforcement agencies stick

2 Narendran, A. (2022, June 14). Police-Media relations: Should they be regulated? The Probe. https://clck.ru/3CgZ4q

3 Chaturvedi, A. (2019, July 27). Law enforcement agencies turn to social media for better outreach. The Economic Times. https://clck.ru/3CgZ93

4 The social network blocked in the territory of the Russian Federation for disseminating unlawful information.

5 Muggah, R. (2015, August 21). Gangsta's Paradise: How Brazil's Criminals (and Police) Use Social Media. Instituto Igarapé. https://goo.su/lRgf

to a strategy similar to Indian and use social media to increase their public profile and streamline obtaining information.

Newsmaking criminologists from South Africa emphasize that their situation regarding the image of law enforcement officers is similar to that of the UK and the US (Motsepe, 2020). Information reported in the alternative media makes the South African Police Service (SAPS) appear incompetent and unprofessional. The image of the body has been tarnished by a number of mediated uproars involving actions by officers such as institutional racism, incompetent investigation of crimes (murders), and recurrent corruption. Historically, the media in South Africa has played a significant role in exposing police abuse and misconduct (Potgieter, 2013). Thus, the level of public trust in the police in South Africa is very low.

3. Cancel culture as a criminological phenomenon

Another factor that reinforces the relevance of alternative media influence on citizens' opinions about law enforcement is the emergence and development of the "cancel culture" phenomenon. The reason for such a cancelation can be a public statement that is considered unacceptable from the viewpoint of certain groups. The exponential speed of spreading negative reactions to the statement can have irreparable consequences for the future career of its author. Not only individuals, but also private institutions, public bodies and even states with their cultural heritage and citizens can be subjected to "cancelling".

The cancel culture developed in 2015-2020. To date, this phenomenon is most widespread in English-speaking countries such as the United States and the United Kingdom. However, the trends of cancel culture were also noticed in other countries, such as France, South Korea, and the Russian Federation. Recently, the Russian Federation, its culture and citizens have become the objects of cancellation in foreign traditional and alternative media[6]. In Russian society, the cancel culture has only recently emerged and there are currently only a few known cases of media personalities and CEOs being "canceled". Unlike in the West, at the moment, the effects of the cancel culture in Russia do not have such a grave impact on the career or life of the persons exposed to it.

Cancel culture is a form of ostracism in which an individual who has committed an act contrary to the ideas of good and evil of certain groups is expelled from social or professional circles. One of the reasons for the emergence and development of cancel culture is the sharp refusal of Web users to compromise with those whose worldview

[6] Akopov, P. (2022). Cancelling Russia has got to a universe level. RIA Novosti. https://clck.ru/3CgZS4

goes against their ideals, as well as the desire to ward off unpleasant concepts as much as possible (Lukianoff & Haidt, 2019). Anyone, despite limited access to the facts, can decide and publicly state whether or not they believe a person is guilty, and then demand that the person be "cancelled". "Cancelling" entails dismissal, inciting widespread hatred against the person, the organization, or even the community. The public organizations behind the initiation of "cancelling" may also seek criminal prosecution of the person, depending on the nature of the "cancel" victim's actions. The widespread public outcry caused by the "cancelling" of a person in the media undermines the principle of objectivity and impartiality of the court, a vivid example of which is the Harvey Weinstein trial (Borzunova et al., 2020). By dictating the judicial process, a broad public actually becomes judge and jury for the "cancelling" victim (Baranova, 2021).

Cancel culture has four characteristic features in all cases of this phenomenon: (1) public condemnation of unacceptable behavior; (2) retroactivity, i.e., an action that is permissible at one time may be grounds for cancelling years later; (3) failure to support the victim of cancelling, and (4) a desire to see the victim suffer consequences or punishment, such as loss of employment and profits, imprisonment, and even suicide.

A reason for canceling a person can be either an act that goes against the general view of morality and ethics (e.g., fraud, sexual assault, etc.) or an act or statement that is inconsistent with the life stance and political views of a particular group. The trend of "canceling" acquires the character of a snowball, as a result of which the victim is canceled by citizens and institutions that do not belong to the offended social group. For example, the uproar that followed Joanne K. Rowling's statement about the absurdity of the gender reassignment concept forced many companies that have nothing to do with the LGBT community[7] to cancel contracts with the writer and refuse to cooperate with her.

Returning to media coverage of law enforcement forming a positive public opinion, it is worth noting that newsmaking criminology faces complexities that were not foreseen by its author Gregg Barak. This is due to the subjectivity of assessing the situation in the materials posted online and the difficulty of predicting their impact on the public. For example, as part of the uproar related to the killing of George Floyd in 2020, an uncontrollable wave of negative judgments about the U.S. police in general emerged on the Internet, which subsequently led to mass riots. Given the unpredictability of sociocultural phenomena on the Internet, in the long term, similar cases may be repeated in other states.

According to the U.S. National Center for Health Statistics, in 2020, the annual increase in homicides was the largest since 1905[8]. In 2020, there were seven to eight homicides

7 In the Russian Federation, it is forbidden to propagate nontraditional sexual relations.

8 Crude death rates for all causes: United States, 2020-Quarter 3. (2020) National Center for Health Statistics. https://clck.ru/3CgZcE

for every 100,000 people in the USA, up from six homicides per 100,000 people a year earlier. The increase in the nation's homicide rate in 2020 far exceeded the 20 percent increase measured in 2001, which was caused by the September 11 terrorist attacks. One of the reasons for the increase in US homicides in 2020 is believed to be changes in relations between police and the public following the murder of George Floyd in Minnesota[9].

Incidents similar to the story of G. Floyd have previously occurred in the criminal practice of the United States. However, the police activity of this country has never been subjected to such an acute public stigmatization due to a single officer behavior. The reason for such a strong reaction was the widespread publicity of the incident in the media. For example, articles calling for the complete isolation of the police from society appeared in serious US newspapers, such as The New York Times. The author of one such article suggests that abolishing the police altogether and redirecting funding to other public sectors, such as education, could not only reduce crime but eliminate it in principle, thus rendering the police irrelevant and obsolete as a social institution[10].

Another effect of media coverage of crime that has received considerable attention from researchers is the effect of pre-trial publicity on juries. It has been observed that most crime coverage is prejudicial to the defendant. A variety of experimental and quasi-experimental studies have shown consistent support for the hypothesis that at least a moderate bias against the defendant may result from the impact of pretrial publicity.

Bruschke and Loges (2003) found that the conviction rates of federal murder defendants whose cases received little press coverage did not differ significantly from the conviction rates of defendants whose cases received extensive press coverage. They found that the highest conviction rates were among those defendants whose cases received between one and five articles in the media. Defendants who received the most publicity received significantly longer prison sentences than those with little or no media exposure.

Although the said study was conducted in 2004, it is still relevant now that the adoption of Internet media has become a massive phenomenon. The media, by influencing public opinion, contributes to the development of bias in potential jurors, which contradicts the basic rights of the accused in court. Hence, legal scholars have to look for ways to ensure the right to an impartial trial, taking into account the modern reality (Brown, 2013). The personalization of internet media is a new aspect

9 Gramlich, J. (2021, October 27). What we know about the increase in US murders in 2020. https://clck.ru/3CgZgE

10 Kaba, M. (2020, June 12). Yes, we mean literally abolish the police because reform won't happen. The New York Times. https://clck.ru/3CgZkz

of contemporary life and newsmaking criminology needs to adapt to it. Negative manifestations of modern media such as cancel culture have enormous implications for the criminal justice system. Cancel culture is a form of cyberbullying with the stigmatization of individuals, institutions, and even states with their cultural heritage.

Conclusions

Newsmaking criminology, developed in the 1980s, has not lost its relevance. The emergence of the World Wide Web and new forms of media indicates the need for new research within this subfield of criminology. Forms of interaction with traditional media are not effective in relation to Internet media. The emergence of complex social phenomena such as cancel culture exacerbate the importance of developing countermeasures to influence public opinion. If the paradigms discrediting law enforcement are entrenched in the digital community, suggesting that a common user is more effective in struggling against crime, they become a potential criminogenic factor in which such struggle may extend beyond cyberspace into everyday life.

References

Aleksandrova, I. B. (2008). Moblogs and blogs: alternative mass media? *Vestnik Moskovskogo universiteta. Ser. 10. Zhurnalistika*, *4*, 68–79. (In Russ.).

Arrigo, B. A., & Bersot, H. Y. (2015). Critical criminology. In *International Encyclopedia of the Social & Behavioral Sciences* (2d Ed., pp. 244–250). https://doi.org/10.1016/b978-0-08-097086-8.45053-1

Barak, G. (1988). Newsmaking criminology: Reflections of the media, intellectuals, and crime. *Justice Quarterly*, *5*(4), 565–587. https://doi.org/10.1080/07418828800089891

Barak, G. (2007). Doing newsmaking criminology from within the academy. *Theoretical Criminology*, *11*(2), 191–207. https://doi.org/10.1177/1362480607075847

Baranova, M. V. (2021). Cancel culture as an innovative legal and cultural phenomenon. *Juridical Techniques*, *15*, 123–128. (In Russ.).

Borzunova, N. Yu., Maksimova, K. L., & Tsechoev, A. M. (2020). The Principle of Presumption of Innocence in Criminal Proceedings and Problems of Its Implementation. *Sociology and Law*, *4*, 86–91. (In Russ.). https://doi.org/10.35854/2219-6242-2020-4-86-91

Brown, K. R. (2013). Somebody poisoned the jury pool: Social media's effect on jury impartiality. *Texas Wesleyan Law Review*, *19*, 809. https://doi.org/10.37419/twlr.v19.i3.6

Bruschke, J., & Loges, W. E. (2003). *Free press vs. fair trials: Examining publicity's role in trial outcomes*. Routledge.

Bykov, I. A., & Akhmedova, Yu. D. (2021). Cancel culture in the political discourse of modern Russia. *Vestnik Kabardino-Balkarskogo gosudarstvennogo universiteta: Zhurnalistika. Obrazovaniye. Slovesnost*, *1*(1), 14–26. (In Russ.). https://doi.org/10.24334/KBSU.2021.1.1.002

Cottee, S. (2004). The idea of a critical criminology: irony, scepticism and commitment. *International Journal of the Sociology of Law*, *32*(4), 363–376. https://doi.org/10.1016/j.ijsl.2004.08.001

De Melo Bandeira, G. C. S. (2013). "Corruption" and social and economic criminal law: Criminology, criminal policy, political science and law & economics – A new idea about criminal liability of legal entities. *Tékhne*, *11*(2), 105–113. https://doi.org/10.1016/j.tekhne.2013.10.002

Frost, N. A., & Phillips, N. D. (2011). Talking heads: Crime reporting on cable news. *Justice Quarterly*, *28*(1), 87–112. https://doi.org/10.1080/07418820903173336

Gaidai, M. K., & Grozin, S. Yu. (2020). The role of the media in police performance assessment. *Yurist-Pravoved*, *3*(94), 195–198. (In Russ.).

Glukhova, A. A., Iudin, A. A., & Shpilev, D. A. (2017). Assessment by citizens of the level of confidence of police and protection from criminal entry. *Actual Problems of Economics and Law*, *11*(3), 56–80. (In Russ.) https://doi.org/10.21202/1993-047X.11.2017.3.56-80

Gore, M. L., Hübschle, A., Botha, A. J., Coverdale, B. M., Garbett, R., Harrell, R. M., Krüger, S. C., Mullinax, J. M., Olson, L. J., Ottinger, M. A., Smit-Robinson, H., Shaffer, L. J., Thompson, L. J., Van Den Heever, L., & Bowerman, W. W. (2020). A conservation criminology-based desk assessment of vulture poisoning in the Great Limpopo Transfrontier Conservation Area. *Global Ecology and Conservation*, *23*, e01076. https://doi.org/10.1016/j.gecco.2020.e01076

Gorshenkov, G. N. (2003). *Criminology of mass communications*. (In Russ.).

Lukianoff, G., & Haidt, J. (2019). *The coddling of the American mind: How good intentions and bad ideas are setting up a generation for failure*. Penguin.

Matskevich, I. M. (2013). Mass consciousness and crime. *Schriften zum deutschen und russischen Strafrecht*, *3*, 167–178. (In German).

Motsepe, L. L. (2020). The impact of news media on the SAPS's public image: 30 years in democratic policing. In *Proceedings of the 11th International Conference on Social Sciences* (pp. 167–181).

Ozkan, T. (2019). Criminology in the age of data explosion: New directions. *The Social Science Journal*, *56*(2), 208–219. https://doi.org/10.1016/j.soscij.2018.10.010

Potgieter, P. J. (2013). Exploring the public image of the police in a post-apartheid South Africa. *Acta Criminologica: African Journal of Criminology & Victimology*, *26*(2), 147–169.

Richards, I., Wood, M. A., & Iliadis, M. (2020). Newsmaking criminology in the twenty-first century: an analysis of criminologists' news media engagement in seven countries. *Current Issues in Criminal Justice*, *32*(2), 125–145. https://doi.org/10.1080/10345329.2019.1696442

Shamaev, A. V. (2018). Criminology. The role of mass media in preventing crime in Russia. *Problems of Science*, *12*(36), 69–71. (In Russ.).

Shestakov, D. A. (2013). Legal journalism and criminology of mass communication. *Platon*, *1*, 40–41. (In Russ.).

Stout, B., & Clamp, K. (2015). Applied Criminology and Criminal Justice. In *International Encyclopedia of the Social & Behavioral Sciences* (2d Ed., pp. 832–838). https://doi.org/10.1016/b978-0-08-097086-8.10512-4

Sukhodolov, A. P., Bychkova, A. M. (2017). On the role of mass media in countering the propaganda of suicide in social networks. *Evroaziatskoe sotrudnichestvo: gumanitarnye aspekty*, *1*, 111–127. (In Russ.).

Sysoyev, A. M. (2007). Influence of mass media on formation of criminogenic attitude. *Ugolovno-ispolnitel`noe pravo*, *2*, 32–34 (In Russ.).

Tokarev, A. A., & Bodrov, N. F. (2012). Criminological and forensic approaches to the study of mass-media publications which provoke deviant behavior. *Actual Problems of Russian Law*, *2*, 214–223. (In Russ.).

Author information

Valentina A. Babaeva – post-graduate student, Department of Criminal Law, Criminal Procedure and Criminology, Moscow State Institute of International Relations (University) of the Ministry of Foreign Affairs of the Russian Federation
Address: 76 prospekt Vernadskogo, 119454 Moscow, Russia
E-mail: tina.babaeva.a@gmail.com
ORCID ID: https://orcid.org/0000-0001-8298-4960
RSCI Author ID: https://elibrary.ru/author_items.asp?authorid=1162866

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – February 29, 2024
Date of approval – Март 20, 2024
Date of acceptance – September 25, 2024
Date of online placement – September 30, 2024

Научная статья
УДК 34:004:343.9:004.4
EDN: https://elibrary.ru/ftkczu
DOI: https://doi.org/10.21202/jdtl.2024.33

Новостная криминология в XXI веке: формирование общественного мнения в новых реалиях

Валентина Андреевна Бабаева

Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации, Москва, Россия

Ключевые слова

дискриминация,
Интернет,
культура отмены,
новостная криминология,
общественные отношения,
право,
преступность,
социальная сеть,
средство массовой информации,
цифровые технологии

Аннотация

Цель: исследование концепции новостной криминологии и ее актуальности в современных условиях развития средств массовой информации.

Методы: методологическую основу работы составляют общенаучные, социальные, специально-юридические методы познания. Проведенное исследование основано на диалектическом методе (при определении общего направления исследования), методах формальной логики (анализ, синтез, индукция, дедукция, аналогия), системном методе (при сопоставлении и обобщении информации, собранной в процессе исследовательской деятельности).

Результаты: выявлены функции новостной криминологии в классическом ее проявлении, а также ее дополнительные функции при изучении медиа в интернет-пространстве. Высказано предположение, что с появлением Всемирной сети актуальность новостной криминологии повысилась: социальные сети, блоги и видеохостинги как альтернативные средства массовой информации имеют сильное влияние на общественное мнение, при этом в отличие от традиционных средств массовой информации доступ к генерации контента имеет неограниченный круг лиц. Многие государства понимают важность взаимодействия средств массовой информации и правоохранительных органов и активно внедряют свои методы реализации новостной криминологии в сети. Автор статьи указывает на риски, возникающие при освещении материалов о правоохранительных органах и преступности в СМИ. Одним из таких рисков является культура отмены, которая носит стихийный, непредсказуемый характер, при котором может пострадать качество жизни жертвы или деловая репутация и деятельность организаций.

Научная новизна: определены функции, выполняемые новостной криминологией при изучении традиционных и альтернативных медиа. До настоящего времени такая доктрина не была исследована в достаточной мере с учетом современных форм массовой коммуникации. Проведен анализ примеров взаимодействия правоохранительных органов разных государств и средств массовой информации.

Практическая значимость: исследование вносит вклад в область понимания корреляции между криминологическими явлениями и современными медийными платформами. Интернет и социальные сети предоставляют новые каналы информационного обмена, которые существенно отличаются от традиционных средств массовой информации, таких как печать или телевидение.

Для цитирования

Бабаева, В. А. (2024). Новостная криминология в XXI веке: формирование общественного мнения в новых реалиях. *Journal of Digital Technologies and Law*, *2*(3), 657–673. https://doi.org/10.21202/jdtl.2024.33

Список литературы

Александрова, И. Б. (2008). Моблоги и блоги: альтернативные СМИ? *Вестник Московского университета. Серия 10. Журналистика*, *4*, 68–79. https://elibrary.ru/jvvror

Баранова, М. В. (2021). Канселинг (cancel culture) как инновационный правокультурный феномен. *Юридическая техника*, *15*, 123–128. https://elibrary.ru/mjkmnp

Борзунова, Н. Ю., Максимова, К. Л., Цечоев, А. М. (2020). Принцип презумпции невиновности в уголовном судопроизводстве и проблемы его реализации. *Социология и право*, *4*, 86–91. https://doi.org/10.35854/2219-6242-2020-4-86-91

Быков, И. А., Ахмедова, Ю. Д. (2021). Культура отмены и персонификация политического дискурса. *Вестник Кабардино-Балкарского государственного университета: Журналистика. Образование. Словесность*, *1*(1), 14–26. https://doi.org/10.24334/KBSU.2021.1.1.002

Гайдай, М. К., Грозин, С. Ю. (2020). Роль СМИ в оценке деятельности полиции. *Юристъ-Правоведъ*, *3*(94), 195–198. https://elibrary.ru/bnfjvu

Глухова, А. А., Иудин, А. А., Шпилев, Д. А. (2017). Оценка гражданами уровня доверия полиции и защищенности от преступных посягательств. *Russian Journal of Economics and Law*, *3*(43), 56–80. EDN: https://elibrary.ru/zfnfbp. DOI: https://doi.org/10.21202/1993-047X.11.2017.3.56-80

Горшенков, Г. Н. (2003). *Криминология массовых коммуникаций*. Н. Новгород. https://elibrary.ru/qvxufj

Мацкевич, И. М. (2013). Общественное сознание и преступность. *Schriften Zum Deutschen und Russischen Strafrecht*, *3*, 167–178. (на нем.). https://elibrary.ru/ozdolh

Суходолов, А. П., Бычкова, А. М. (2017). К вопросу о роли средств массовой информации в противодействии пропаганде суицида в социальных сетях. *Евроазиатское сотрудничество: гуманитарные аспекты*, *1*, 111–127. https://elibrary.ru/yrofay

Сысоев, А. М. (2007). Влияние средств массовой информации на формирование криминогенных установок. *Уголовно-исполнительное право*, *2*, 32–34. https://elibrary.ru/jxdzvn

Токарев, А. Л., Бодров, Н. Ф. (2012). Криминологический и судебно-экспертный подходы к изучению публикаций СМИ, стимулирующих антиобщественное поведение. *Актуальные проблемы российского права*, *2*, 214–223. https://elibrary.ru/zkpxqk

Шамаев, А. В. (2018). Криминология. Роль средств массовой информации в предупреждении преступности в России. *Проблемы науки*, *12*(36), 69–71.

Шестаков, Д. А. (2013). Правовая журналистика и криминология массовой коммуникации. *Платон*, *1*, 40–41. https://elibrary.ru/ywylwh

Arrigo, B. A., & Bersot, H. Y. (2015). Critical criminology. In *International Encyclopedia of the Social & Behavioral Sciences* (2d Ed., pp. 244–250). https://doi.org/10.1016/b978-0-08-097086-8.45053-1

Barak, G. (1988). Newsmaking criminology: Reflections of the media, intellectuals, and crime. *Justice Quarterly*, *5*(4), 565–587. https://doi.org/10.1080/07418828800089891

Barak, G. (2007). Doing newsmaking criminology from within the academy. *Theoretical Criminology*, *11*(2), 191–207. https://doi.org/10.1177/1362480607075847

Brown, K. R. (2013). Somebody poisoned the jury pool: Social media's effect on jury impartiality. *Texas Wesleyan Law Review*, *19*, 809. https://doi.org/10.37419/twlr.v19.i3.6

Bruschke, J., & Loges, W. E. (2003). *Free press vs. fair trials: Examining publicity's role in trial outcomes*. Routledge.

Cottee, S. (2004). The idea of a critical criminology: irony, scepticism and commitment. *International Journal of the Sociology of Law*, *32*(4), 363–376. https://doi.org/10.1016/j.ijsl.2004.08.001

De Melo Bandeira, G. C. S. (2013). "Corruption" and social and economic criminal law: Criminology, criminal policy, political science and law & economics – A new idea about criminal liability of legal entities. *Tékhne*, *11*(2), 105–113. https://doi.org/10.1016/j.tekhne.2013.10.002

Frost, N. A., & Phillips, N. D. (2011). Talking heads: Crime reporting on cable news. *Justice Quarterly*, *28*(1), 87–112. https://doi.org/10.1080/07418820903173336

Gore, M. L., Hübschle, A., Botha, A. J., Coverdale, B. M., Garbett, R., Harrell, R. M., Krüger, S. C., Mullinax, J. M., Olson, L. J., Ottinger, M. A., Smit-Robinson, H., Shaffer, L. J., Thompson, L. J., Van Den Heever, L., & Bowerman, W. W. (2020). A conservation criminology-based desk assessment of vulture poisoning in the Great Limpopo Transfrontier Conservation Area. *Global Ecology and Conservation*, *23*, e01076. https://doi.org/10.1016/j.gecco.2020.e01076

Lukianoff, G., & Haidt, J. (2019). *The coddling of the American mind: How good intentions and bad ideas are setting up a generation for failure*. Penguin.

Motsepe, L. L. (2020). The impact of news media on the SAPS's public image: 30 years in democratic policing. In *Proceddings of the 11th International Conference on Social Sciences* (pp. 167–181).

Ozkan, T. (2019). Criminology in the age of data explosion: New directions. *The Social Science Journal*, *56*(2), 208–219. https://doi.org/10.1016/j.soscij.2018.10.010

Potgieter, P. J. (2013). Exploring the public image of the police in a post-apartheid South Africa. *Acta Criminologica: African Journal of Criminology & Victimology*, *26*(2), 147–169.

Richards, I., Wood, M. A., & Iliadis, M. (2020). Newsmaking criminology in the twenty-first century: an analysis of criminologists' news media engagement in seven countries. *Current Issues in Criminal Justice*, *32*(2), 125–145. https://doi.org/10.1080/10345329.2019.1696442

Stout, B., & Clamp, K. (2015). Applied Criminology and Criminal Justice. In *International Encyclopedia of the Social & Behavioral Sciences* (2d Ed., pp. 832–838). https://doi.org/10.1016/b978-0-08-097086-8.10512-4

Сведения об авторе

Бабаева Валентина Андреевна – аспирант кафедры уголовного права, уголовного процесса и криминалистики, Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации
Адрес: 119454, Россия, г. Москва, проспект Вернадского, 76
E-mail: tina.babaeva.a@gmail.com
ORCID ID: https://orcid.org/0000-0001-8298-4960
РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=1162866

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.81 / Криминология
Специальность ВАК: 5.1.4 / Уголовно-правовые науки

История статьи

Дата поступления – 29 февраля 2024 г.
Дата одобрения после рецензирования – 20 марта 2024 г.
Дата принятия к опубликованию – 25 сентября 2024 г.
Дата онлайн-размещения – 30 сентября 2024 г.

Research article
UDC 34:004:341:004.8
EDN: https://elibrary.ru/nbizuv
DOI: https://doi.org/10.21202/jdtl.2024.34

Violation of the Airspace of Countries by Unmanned Aerial Vehicles (Drones) from the Perspective of International Law

Milad Kashi Kamijani
University of Qom, Qom, Iran

Keywords

airspace,
armed conflict,
digital technologies,
drone,
human rights,
humanitarian law,
international convention,
international law,
law,
unmanned aerial vehicle

Abstract

Objective: to illustrate the challenges to international law and the shortcomings of current regulation caused by the rapid development of drone technology, by the example of using unmanned aerial vehicles (drones) in airspace.

Methods: the study is based primarily on a set of methods for interpreting the provisions of international law, which allow analyzing the provisions in the field of using unmanned aerial vehicles (drones).

Results: based on international air law and humanitarian law, the article examines the issues of unmanned aerial vehicles (drones) using airspace. The main sources of law in this area are analyzed, including the provisions of international air law, especially the Paris, Madrid, Havana and Chicago Conventions. An attempt is made to answer the questions arising from the development of unmanned technologies as to which rules of international law apply to their use and whether existing international law is capable of responding effectively to them. The article shows the current understanding of the legal status of airspace over the territory of a state. The author puts forward the question whether the sphere of unmanned aerial vehicles, automatic and autonomous weapons, which combines scientific and military achievements with new technologies, is exceptional. In this regard, the problem of using unmanned aerial vehicles as a universal weapon in international conflicts is touched upon. A conclusion is made that the use of intelligent, guided and robotic weapons capable of automatic

decision-making, such as drones, requires the revision of existing conventions or the establishment of new legal standards for these weapons. It is proposed to consider such drones as military aircraft of a special type.

Scientific novelty: international legal responsibility of states for the military use of drones has not received an unambiguous assessment in the doctrine. However, much in this issue depends on the legal interpretation of the most important international legal categories. Further development of this issue is directly related to the issues of international responsibility and the concept of state sovereignty over airspace.

Practical significance: the development of unmanned aviation at the present stage demonstrates the imperfection of the existing legal framework, which is designed to regulate these relations. With regard to the study of the global trend in the current international law, the identification of the shortcomings in the provisions of the latter is important primarily for their further modernization, taking into account modern scientific achievements and the development of the concept of a state sovereignty over its airspace.

For citation

Kamijani, M. K. (2024). Violation of the Airspace of Countries by Unmanned Aerial Vehicles (Drones) from the Perspective of International Law. *Journal of Digital Technologies and Law*, *2*(3), 674–689. https://doi.org/10.21202/jdtl.2024.34

Contents

Introduction

Some thinkers are of the opinion that new digital technologies in general and drones in particular have challenged the current international law and the current international law has emerged in the face of new technologies and new weapons; faced with this type of technology, it has reached its lowest level; as a result, active international

law has not been able to respond to the needs arising from new technologies, hence, new laws must be formulated in accordance with such technologies to control them (Bace et al., 2024).

Today, the initiative in many wars belongs to countries with air superiority. To a large extent, the aggression of superpowers against weaker countries is done through air strikes, because these expensive and strategic weapons are simpler and more reliable than others (Niu et al., 2024; Ambos, 2008).

Regarding drones, Gilley states that «unmanned aerial vehicles are capable of meeting current legal standards»[1] and compares the authorization of a drone attack to the authorization of a manned aircraft. He concludes that if an attack by a piloted aircraft is impermissible, it is also impermissible by a drone (unmanned aerial vehicle, UAV). Over time, the use of UAVs has expanded in several civilian and military applications (Siddiqi et al., 2022).

As a result, the pilot does not determine the law, so there is no need for a new regulation for the use of drones, and the current law will respond to the new needs. Gill continues that «the law is the law»[2] regardless of «platform», and no new law is needed for drones[3].

By using the current international law and the existing rules, it is possible to take steps within the humanitarian law and the law of armed conflict, as well as by using soft law, to develop appropriate rules in the field of new technologies and new weapons without the need to change the existing ones. It is appropriate either to create a new law, or to consider the current international law ineffective and ignore it (Majd et al., 2021).

Therefore, we can examine the export production and the use of new technologies in the field of new weapons with the existing rules and find a solution to get out of the deadlock of «no restrictions in the field of new weapons» (Ishiwatari, 2024).

1. Sovereign airspace and status of unmanned aerial vehicles (drones)

The complete and exclusive sovereignty of the state in its airspace is embodied in Article 1 of the Chicago Convention, and according to Article 2 of the Convention, the air sovereignty of the state includes the space above the land and the waters of the territory adjacent to its sovereignty, which this type of sovereignty is defined and officially recognize by the Chicago Convention (Clarke, 2014; Ishiwatari, 2024).

It seems necessary to pay attention to the fact that in the discussion of the relationship between UAVs and the Chicago Convention, the subject of the UAV is mostly addressed

1 EU-OSHA. (2023, September 11). Unmanned aerial vehicles: implications for occupational safety and health. https://clck.ru/3EGYKv

2 Ibid.

3 Ibid.

and other issues such as sovereignty are not mentioned. This is because by default the government using the drone has received the consent of the territorial government and has not necessarily violated the principles of non-interference and non-use of weapons, or it is based on the country's request for help. So, the use of drones is allowed based on the country's territorial consent or the country's request (Clarke & Moses, 2014).

Sovereignty here refers to the independence of the air and space of each country independent of other countries. Article 1 of the Chicago Convention states that «the contracting state has complete and exclusive sovereignty over the airspace above its territory»[4], while Article 8 of the Chicago Convention explicitly prohibits the flight of drones without the prior consent of other states.

It should also be noted that the future of drones largely depends on how they are used by governments. It means that the status of a drone is not certain in advance and is determined by what the government has planned for it. A drone may be used for a military operation and at another time for humanitarian aid (Tatsidou et al., 2019), so the nature of the flight is important in the law and regulations that govern it. Drones are not subject to any absolute and special prohibition in law (Abeyratne, 2010).

2. The Chicago Convention and its role in the organization of air traffic of aircraft

For the first time, the 1919 Paris Convention on Aviation provided a definition of an airplane, according to which «an aircraft is any device capable of taking off or moving in the air»[5] at the International Civil Aviation Conference in 1944 in Chicago. More than 50 countries were present in that conference, invited by the United States to create a legal institution for the development of national aircraft after World War II.

The direct involvement of the pilot's human factor in flying an aircraft is not the definition criterion. As a result, drones correspond to the definition by the Paris Convention and the 1967 ICAO definition, and their regulations include drones to a certain extent (Ishiwatari, 2024).

The ICAO member states under the Chicago Convention agreed to accept its principles. The first and most important principle is the full sovereignty of the member states over the airspace of their territory. There is no doubt that the government's sovereignty over its airspace is one of the most important properties of contemporary international law. Violation of the airspace of countries by foreign planes is against international law and has caused significant accidents (Vogel, 2011).

---

4 International Civil Aviation Organization. (2000). Convention on International Civil Aviation (8th Ed.). https://clck.ru/3EGYe5

5 The 1919 Paris Convention: The starting point for the regulation of air navigation. The postal history of icao. https://clck.ru/3EGfbC

Article 8 of the Convention is the only article that has a passing reference to unmanned aircraft and considers their flight subject to the special permission of the country over which the drone is flying. Therefore, the drone, as a flying device, has been under the legal regime of the Chicago Convention to some extent, and the permission to operate in the territory of other countries is subject to obtaining the consent of those countries.

Article 3 of the Convention separates national and state aircraft. It states that none of the state aircraft of the treaty member countries has the right to fly over or land in another country without obtaining permission. However, it seems that the mandatory power of these two articles is not enough to legalize the plurality of drone activities. Other regulations are needed, especially regarding airspace violations, violations of the sovereignty of states, and violations of humanitarian and human rights standards (Vogel, 2011).

3. International airspace regime and responsibility for its violation

The General Assembly approved the definition of aggression on December 14, 1974, in meeting No. 2319, without voting and according to the consensus of the members. This resolution has an approval document and an appendix defining encroachment as follows.

According to Article 1, aggression means the use of armed force by a government against the sovereignty, territorial integrity or political independence of another government or its use in other ways contrary to the United Nations Charter. Article 2 on the preemption of a government in the use of armed forces says that the Security Council has the authority to, according to the United Nations Charter, confirm the occurrence of violation for reasons such as insufficient intensity of the measures taken or not accepting their results (Vogel, 2011).

The Paris Convention as the first international document in the field of air rights stipulates that each of the signatories of the Convention will recognize the complete and exclusive sovereignty of states over the airspace above their territory.

This general statement of governments has been repeated and specified in subsequent treaties and conventions. The 1926 Madrid Convention, the 1928 Havan Convention and, most importantly, the 1944 Chicago Convention all emphasize the exclusive jurisdiction of states over the airspace above their territory. It seems that even before the outbreak of the First World War, this perception of the legal status of the airspace above the land was common among governments. For example, we can point to the reaction of the Dutch government in the years before the start of the war, protesting against the German planes passing over the territory of that country without obtaining prior permission.

Such violations have a major difference with other crimes within the jurisdiction of the International Criminal Court, namely genocide, crimes against humanity, and war crimes, and provide a suitable basis for committing the aforementioned crimes.

There are permanent members of the Security Council who can make various flights and violate sovereign territories easily and by using the right of veto, allowing this type of aircraft in the space of other countries, despite their displeasure.

In the case of unmanned aircraft, serving as an automatic weapon or with a documented remote control, in principle there is no pilot to judge and bear the responsibility for the violation. In general, the ground controller is responsible and the human element of this situation is considered (Nelson & Gorichanaz, 2019; Bassi, 2019).

Therefore, according to the international regulations, the executive agents of Hedayad Behbad and their related human chain are responsible for all events. Because they are thousands of kilometers away from the battlefield, the agents of the drones will be exempted from the responsibilities such as the necessary forecasts in the attacks and the guarantee of separation and proportionality (Vogel, 2011).

4. Concept and principle of a state's sovereignty over its airspace

Regarding the rights of airspace and air rights, the most prominent universalist was Yu. Kolosov who in 1977 in Prague put forward the concept of identifying the exclusive and complete sovereignty of any country over the airspace of that country's territory[6]. The concept defines a country's airspace as the air layer above its land and water territory, which continues as long as there is an atmosphere, and after that a zone beyond the atmosphere, or space, begins.

Article 1 of Paris Convention dated October 13, 1919 confirmed the absolute and exclusive sovereignty of the states over their territorial airspace and territorial waters. The Chicago Convention dated December 7, 1944 also confirms this principle. Article 2 of the 1958 Convention Geneva also stipulates that the said sovereignty includes the upper space of the territorial sea and its bottom. According to Article 3 of the Civil Aviation Law approved in 1338 Hijri Shamsi, government has absolute and exclusive sovereignty over the coastal waters.

If drones enter a country's airspace without permission, such aircraft can be intercepted for identification purposes, forced to leave the airspace through a designated air route, and directed to land for investigation or prosecution. Therefore, none of the government planes have the right to fly over or land on the territory of another country without obtaining permission through a contract, etc., and not complying with its terms and conditions. There can be other serious violations of international law.

According to international air law, every country has the right to restrict or prohibit the flight of other countries' aircraft in a part of its territory for military or security reasons. Also, countries should respect the sovereignty of other countries if they use photography equipment. Each contracting state can prohibit or restrict the use of photographic equipment over its territory (Vogel, 2011).

These principles, by comparison of priority, prove the prohibition of using spy planes over the territories and countries and confirm the illegality and immorality of this action.

---

6 Proceedings of the Workshop on Space Law in the Twenty-first Century. https://clck.ru/3EPvCk

Therefore, the fact that these illegal acts are more frequent than before shows their insolence and heinousness.

According to the Article 8 of Chicago Convention, the flight of unmanned aircraft that are capable of flying independently without a pilot is not allowed over the territory of any country without obtaining a special permit and observing the provisions contained in the said permit. Each of the countries has agreed to fly drones in the areas declared free for national planes and put under the necessary control and supervision to prevent possible dangers for national planes. According to this Article, the violation of the Iranian territory by the American drone is condemned.

5. Using armed drones and issues of international humanitarian law

Originally, drones were designed as reconnaissance aircraft. In this case, the discussions of humanitarian and human rights were less explored and investigated. At some point, however, missiles began to be joined and utilized with unmanned systems (Sopha et al., 2024; Rainer, 2014).

Since then, discussions of humanitarian rights became more seriously than before, in addition to the existence of laws and regulations in the use of new technologies. Discussions are going on concerning the humanitarian consequences of such technologies; the position of international law, especially international humanitarian law, is highlighted in the face of using new technologies, including drones (Sopha et al., 2024).

The use of armed drones has caused serious questions in the field of international law, specifically international humanitarian law, human rights and the use of force. If it is concluded that governments in certain circumstances fulfill their obligations but they violate their international law, the issue of the government is also raised. Therefore, the need to pay attention to the main principles and foundations of humanitarian rights in this field is felt more and more, while these drones attack people without any declaration of war or without an armed conflict. If there is such a conflict, drones are used against people.

The use of drones in the line of armed ammunition should be also limited in non-combat situations in parallel with humanitarian rights under the control of human rights regulations. Regarding the legitimacy of using drones, some points should be checked. Firstly, drones are considered a weapon, an important tool for launching missiles and bombs; so, they should comply with human rights standards.

Today, it is accepted that humanitarian and human rights must be implemented during armed conflicts. As a result, not only the Geneva Conventions, but also the standards of human rights must be respected, and any resort to force, even by drones, must be done with respect and guarantee of minimum human standards.

6. International responsibility of countries committing violations

The International Court of Justice in various cases relied on the principle of not resorting to force as a mandatory rule in international law. The most important source

in determining cases of aggression is the relevant resolution by the United Nations General Assembly. According to this resolution, the mere entry of military equipment into a country is considered aggression and violates the principle of non-use of force. According to Article 51 of the United Nations Charter, recourse to defense is legitimate only against armed attack as one of the examples of aggression, and legitimate defense against other forms of aggression is not recognized (Sopha et al., 2024).

Drones are neither among state aircraft nor among civil state aircraft, but they can be considered as military aircraft of a special nature. According to the Chicago Convention, the unauthorized entry of these drones into the airspace of a country will be an example of aggression and the international responsibility of the states will follow.

Before an armed attack by a drone, resorting to legitimate defense is not relevant and armed attack is basically not the use of spy drones; hence, legitimate defense against spy drones will not be raised.

On the other hand, the victim state can reciprocate by confiscating the UAV in peacetime or confiscating it in wartime. In this case, the international responsibility will not be towards the victim state. Spying on countries, including the United States, with the help of military drones, in addition to violating some principles of the Chicago Convention, is also contrary to principles such as the prohibition of interference in the country's internal affairs and the non-use of force. The responsibility of the countries from whose territory this action took place is also clear from the viewpoint of international law, because the silence of the governments indicates their satisfaction (Chen & Wang, 2009).

Filing lawsuits against states in relation to the country's international violations caused by sending spy drones to another country's airspace is a matter that does not have sufficient legal and expedient grounds (Wang et al., 2024).

It seems that the best way to compensate for the intrusion of foreign drones is to stop and confiscate them, which has been achieved so far thanks to modern information technologies. In addition to these actions, ICAO also recommended to file a complaint at the United Nations Secretariat, the Civil Aviation Security Council (Askerbekov et al., 2024; Wang et al., 2024; Dolata & Schwabe, 2023).

The main international authority for grievances and lawsuits to prevent threats and acts of aggression is the Security Council, and the aggrieved government must take legal action by filing a complaint with the Security Council regarding the penetration and infiltration of the hostile country's military drones (Li & Dang, 2024).

Regarding the judicial proceedings, it should be said that in the first case of stopping the drones, no international judicial body has the authority to deal with this matter. Only if the parties' consent to judicial proceedings, the International Court of Justice can deal with the case, which is very unlikely to happen due to the current situation. Since the aerial vehicles are considered to be governmental and not state, they do not refer to the Chicago Convention. The dispute resolution mechanisms and facilities of this convention do not apply to them (Dolata & Schwabe, 2023).

The International Court of Justice is the authority to deal with legal claims between countries, not on issues such as encroachment and so on. Of course, it would be useful if the Security Council allowed this and resolved the political part by itself. But if the UN Security Council delays dealing with the issue legally, it is natural that the government will do it through the International Court of Justice (Zègre-Hemsey et al., 2024).

But only the legal aspect of this issue can be examined in court. This issue has two dimensions, one is political and the other is legal; the International Court of Justice can only deal with the legal aspect. Undoubtedly, the matter is rather complicated, but at the same time, the satisfaction of the other party must be taken into account. It is not possible to refer the case to the International Court of Justice without the parties to the dispute giving their consent or declaring their confirmation of the court jurisdiction. Unless the governments have already accepted this jurisdiction during the course of events, the two parties or parties involved in the dispute must agree that the matter should be referred to the court. Therefore, filing a lawsuit in the International Court of Justice is subject to the consent of the parties to the lawsuit. In any case, violating the airspace of countries is considered a threat to peace and security, and the threatened government can refer to the UN Security Council.

Conclusion

The use of unmanned aircraft in international conflicts as all-use weapons is a very complex issue. Though unmanned aircraft are weapons, the provisions governing arms control are not applied to them. As a result, in the context of the law of hostilities, these planes are used as means or in line with the method of war.

For this reason, the international community insists that the use of drones must be accepted in accordance with the provisions of the United Nations Charter and international law. The use of this type of aircraft should be carried out in accordance with the main and fundamental provisions of international humanitarian law, including the principle of separation, the principle of pride, the principle of proportionality and the principle of caution. The issues of territorial integrity, sovereignty of governments and airspace of countries should also be taken into account.

In this article, we examined the violation of the airspace of countries by drones from the perspective of international law. We considered international air law, especially referring to the Chicago Convention, international humanitarian law and its very important provisions, such as the prohibition of useless sacrifice and proportionality. Also, multilateral export control measures and restrictions governing drones in the fields of their application (international air law and the relationship between sovereign governments and international humanitarian law and protection of civilians) were

examined so that a better lesson could be learned from the current position of the UAV in international law.

The use of intelligent, guided and automatic decision-making robot weapons such as drones is a complex issue, due to the ambiguity in observing the principle of separation and proportionality. It is necessary to revise the existing conventions or to establish new legal standards regarding this type of weapons.

The topic of individual criminal responsibility in case of committing international crimes is not as easy as for classical weapons. This is due to the presence of multiple controllers of these types of weapons. In any case, executive agents and remote control operators, in the entire human chain of directing these types of weapons, are responsible for the created situations.

References

Abeyratne, R. I. (2010). *Aviation Security Law*. Springer Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-11703-9

Ambos, K. (December 14, 2011). Article 25: *Individual Criminal Responsibility: Commentary on the Rome statute of the International Criminal Court*, Second edition (pp. 743–770), O. Triffterer, ed., München, 2008.

Askerbekov, D., Garza-Reyes, J. A., Ghatak, R. R., Joshi, R., Kandasamy, J., & De Mattos Nascimento, D. L. (2024). Embracing drones and the Internet of drones systems in manufacturing – An exploration of obstacles. *Technology in Society*, *78*, 102648. https://doi.org/10.1016/j.techsoc.2024.102648

Bace, B., Gökce, Y., & Tatar, U. (2024). Law in orbit: International legal perspectives on cyberattacks targeting space systems. *Telecommunications Policy*, *48*(4), 102739. https://doi.org/10.1016/j.telpol.2024.102739

Bassi, E. (2019). European drones regulation: today's legal challenges. In *International Conference on Unmanned Aircraft Systems (ICUAS)* (pp. 443–450). https://doi.org/10.1109/icuas.2019.8798173

Chen, H., & Wang, Y. Li (2009). A survey of autonomous control for UAV. In *International Conference on Artificial Intelligence and Computational Intelligence*, Shanghai, China. 2009 (pp. 267–271). https://doi.org/10.1109/AICI.2009.147

Clarke, R. (2014). The regulation of civilian drones' impacts on behavioural privacy. *Computer Law & Security Report*, *30*(3), 286–305. https://doi.org/10.1016/j.clsr.2014.03.005

Clarke, R., & Moses, L. B. (2014). The regulation of civilian drones' impacts on public safety. *Computer Law & Security Report*, *30*(3), 263–285. https://doi.org/10.1016/j.clsr.2014.03.007

Dolata, M., & Schwabe, G. (2023). Moving beyond privacy and airspace safety: Guidelines for just drones in policing. *Government Information Quarterly*, *40*(4), 101874. https://doi.org/10.1016/j.giq.2023.101874

Ishiwatari, M. (2024). Leveraging drones for effective disaster management: A comprehensive analysis of the 2024 Noto Peninsula earthquake case in Japan. *Progress in Disaster Science*, *23*, 100348. https://doi.org/10.1016/j.pdisas.2024.100348

Li, X., & Dang, A. (2024). Spatial Patterns of Drone Adoption: Insights from Communities in Southern California. *Technological Forecasting & Social Change*, *203*, 123391. https://doi.org/10.1016/j.techfore.2024.123391

Majd, N., Savari, H., & Fakheri, N. (2021). Legal Rules Governing the Flying of Drones in Air Warfare from the Perspective of International Law. *Public Law Studies Quarterly*, *51*(3), 1203–1221. https://doi.org/10.22059/jplsq.2019.283487.2042

Nelson, J., & Gorichanaz, T. (2019). Trust as an ethical value in emerging technology governance: The case of drone regulation. *Technology in Society*, *59*, 101131. https://doi.org/10.1016/j.techsoc.2019.04.007

Niu, B., Zhang, J., & Xie, F. (2024). Drone logistics' resilient development: impacts of consumer choice, competition, and regulation. *Transportation Research. Part A: Policy and Practice*, *185*, 104126. https://doi.org/10.1016/j.tra.2024.104126

Rainer, D. (2014). Rules, regulations and codes for drones, unmanned aerial vehicle, NextGen Air Transportation, unmanned air systems. *Journal of Chemical Health & Safety*, *21*(6), 34–35. https://doi.org/10.1016/j.jchas.2014.09.003

Siddiqi, M. A., Iwendi, C., Jaroslava, K., & Anumbe, N. (2022). Analysis on security-related concerns of unmanned aerial vehicle: attacks, limitations, and recommendations. *Mathematical Biosciences and Engineering*, *19*(3), 2641–2670. https://doi.org/10.3934/mbe.2022121

Sopha, B. M., Asih, A. M. S., & Agriawan, J. I. (2024). Adopters and non-adopters of drones in humanitarian operations: An empirical evidence from a developing country. *Progress in Disaster Science*, *21*, 100314. https://doi.org/10.1016/j.pdisas.2024.100314

Tatsidou, E., Tsiamis, C., Karamagioli, E., Boudouris, G., Pikoulis, A., Kakalou, E., & Pikoulis, E. (2019). Reflecting upon the humanitarian use of unmanned aerial vehicles (drones). *Swiss Medical Weekly*, *149*(1314), w20065. https://doi.org/10.4414/smw.2019.20065

Vogel, R. J. (2011). Drone Warfare and the Law of Armed Conflict. *Denver Journal of International Law and Policy*, *39*(1), 101–138.

Wang, S., Zheng, C., & Wandelt, S. (2024). Policy challenges for coordinated delivery of trucks and drones. *Journal of the Air Transport Research Society*, *2*, 100001. https://doi.org/10.1016/j.jatrs.2024.100001

Zègre-Hemsey, J. K., Cheskes, S., Johnson, A. M., Rosamond, W. D., Cunningham, C. J., Arnold, E., Schierbeck, S., & Claesson, A. (2024). Challenges & barriers for real-time integration of drones in emergency cardiac care: Lessons from the United States, Sweden, & Canada. *Resuscitation Plus*, *17*, 100554. https://doi.org/10.1016/j.resplu.2024.100554

Author information

Milad Kashi Kamijani – Master of Public Law, Faculty of Law, University of Qom
Address: Al-Ghadir Boulevard, after Quds Town, 3716146611 Qom, Iran
E-mail: Mkk1377@gmail.com
ORCID ID: https://orcid.org/0009-0008-1640-3230
WoS Researcher ID: https://www.webofscience.com/wos/author/record/ISU-4107-2023
Google Scholar ID: https://scholar.google.com/citations?user=zsEAxXoAAAAJ

Conflict of interests

The author declares no conflict of interests.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – October 13, 2023
Date of approval – November 1, 2023
Date of acceptance – September 25, 2024
Date of online placement – September 30, 2024

Научная статья
УДК 34:004:341:004.8
EDN: https://elibrary.ru/nbizuv
DOI: https://doi.org/10.21202/jdtl.2024.34

Нарушение воздушного пространства страны беспилотными летательными аппаратами (дронами) с точки зрения международного права

Милад Каши Камиджани

Университет Кума, Кум, Иран

Ключевые слова

беспилотный летательный аппарат,
воздушное пространство,
вооруженный конфликт,
дрон,
международная конвенция,
международное гуманитарное право,
международное право,
права человека,
право,
цифровые технологии

Аннотация

Цель: на примере использования беспилотными летательными аппаратами (дронами) воздушного пространства показать вызовы международному праву и недостатки действующего регулирования, обусловленные стремительным развитием беспилотных технологий.

Метод: исследование построено прежде всего на совокупности способов толкования положений международного права, позволяющих проанализировать положения в области использования беспилотных летательных аппаратов (дронов).

Результаты: в статье на основе международного воздушного и гуманитарного права рассматриваются вопросы использования беспилотными летательными аппаратами (дронами) воздушного пространства. Проводится анализ основных источников права в этой сфере, которыми служат, в частности, положения международного воздушного права, особенно Парижской, Мадридской, Гаванской и Чикагской конвенций. Предпринимается попытка ответить на возникающие в связи с развитием беспилотных технологий вопросы о том, какие нормы международного права распространяются на их использование и способно ли действующее международное право на них эффективно реагировать. Показано современное представление о правовом статусе воздушного пространства над территорией государства. Автор задается вопросом, не является ли исключительной область беспилотных летательных аппаратов, автоматических и автономных видов вооружений, объединяющей научные и военные достижения с новыми технологиями. В этой связи затрагивается проблема использования беспилотных летательных аппаратов в международных конфликтах в качестве универсального оружия. Делается вывод о том, что при использовании интеллектуального, управляемого и роботизированного оружия,

способного автоматически принимать решения, такого как беспилотники, необходимо пересмотреть существующие конвенции или установить новые правовые стандарты в отношении этого вида оружия. Такие беспилотники предлагается рассматривать как военные воздушные суда особого типа.

Научная новизна: международно-правовая ответственность государств за военное применение беспилотных летательных аппаратов не получила в доктрине однозначной оценки, вместе с тем многое в данном вопросе зависит от юридического толкования важнейших международно-правовых категорий, а дальнейшая разработка данной проблематики непосредственно связана с развитием вопросов международной ответственности и концепцией суверенитета государства над воздушным пространством.

Практическая значимость: развитие на современном этапе беспилотной авиации демонстрирует несовершенство сформированной правовой базы, которая призвана регулировать указанные отношения. В связи с исследованием общемировой тенденции в контексте действующего международного права, выявление недостатков положений последнего имеет значение прежде всего для дальнейшей их модернизации с учетом современных достижений науки и развития концепции суверенитета страны над ее воздушным пространством.

Для цитирования

Камиджани, М. К. (2024). Нарушение воздушного пространства страны беспилотными летательными аппаратами (дронами) с точки зрения международного права. *Journal of Digital Technologies and Law*, *2*(3), 674–689. https://doi.org/10.21202/jdtl.2024.34

Список литературы

Abeyratne, R. I. (2010). *Aviation Security Law*. Springer Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-11703-9

Ambos, K. (December 14, 2011). Article 25: *Individual Criminal Responsibility: Commentary on the Rome statute of the International Criminal Court*, Second edition (pp. 743–770), O. Triffterer, ed., München, 2008.

Askerbekov, D., Garza-Reyes, J. A., Ghatak, R. R., Joshi, R., Kandasamy, J., & De Mattos Nascimento, D. L. (2024). Embracing drones and the Internet of drones systems in manufacturing – An exploration of obstacles. *Technology in Society*, *78*, 102648. https://doi.org/10.1016/j.techsoc.2024.102648

Bace, B., Gökce, Y., & Tatar, U. (2024). Law in orbit: International legal perspectives on cyberattacks targeting space systems. *Telecommunications Policy*, *48*(4), 102739. https://doi.org/10.1016/j.telpol.2024.102739

Bassi, E. (2019). European drones regulation: today's legal challenges. In *International Conference on Unmanned Aircraft Systems (ICUAS)* (pp. 443–450). https://doi.org/10.1109/icuas.2019.8798173

Chen, H., & Wang, Y. Li (2009). A survey of autonomous control for UAV. In *International Conference on Artificial Intelligence and Computational Intelligence*, Shanghai, China. 2009 (pp. 267–271). https://doi.org/10.1109/AICI.2009.147

Clarke, R. (2014). The regulation of civilian drones' impacts on behavioural privacy. *Computer Law & Security Report*, *30*(3), 286–305. https://doi.org/10.1016/j.clsr.2014.03.005

Clarke, R., & Moses, L. B. (2014). The regulation of civilian drones' impacts on public safety. *Computer Law & Security Report*, *30*(3), 263–285. https://doi.org/10.1016/j.clsr.2014.03.007

Dolata, M., & Schwabe, G. (2023). Moving beyond privacy and airspace safety: Guidelines for just drones in policing. *Government Information Quarterly*, *40*(4), 101874. https://doi.org/10.1016/j.giq.2023.101874

Ishiwatari, M. (2024). Leveraging drones for effective disaster management: A comprehensive analysis of the 2024 Noto Peninsula earthquake case in Japan. *Progress in Disaster Science*, *23*, 100348. https://doi.org/10.1016/j.pdisas.2024.100348

Li, X., & Dang, A. (2024). Spatial Patterns of Drone Adoption: Insights from Communities in Southern California. *Technological Forecasting & Social Change*, *203*, 123391. https://doi.org/10.1016/j.techfore.2024.123391

Majd, N., Savari, H., & Fakheri, N. (2021). Legal Rules Governing the Flying of Drones in Air Warfare from the Perspective of International Law. *Public Law Studies Quarterly*, *51*(3), 1203–1221. https://doi.org/10.22059/jplsq.2019.283487.2042

Nelson, J., & Gorichanaz, T. (2019). Trust as an ethical value in emerging technology governance: The case of drone regulation. *Technology in Society*, *59*, 101131. https://doi.org/10.1016/j.techsoc.2019.04.007

Niu, B., Zhang, J., & Xie, F. (2024). Drone logistics' resilient development: impacts of consumer choice, competition, and regulation. *Transportation Research. Part A: Policy and Practice*, *185*, 104126. https://doi.org/10.1016/j.tra.2024.104126

Rainer, D. (2014). Rules, regulations and codes for drones, unmanned aerial vehicle, NextGen Air Transportation, unmanned air systems. *Journal of Chemical Health & Safety*, *21*(6), 34–35. https://doi.org/10.1016/j.jchas.2014.09.003

Siddiqi, M. A., Iwendi, C., Jaroslava, K., & Anumbe, N. (2022). Analysis on security-related concerns of unmanned aerial vehicle: attacks, limitations, and recommendations. *Mathematical Biosciences and Engineering*, *19*(3), 2641–2670. https://doi.org/10.3934/mbe.2022121

Sopha, B. M., Asih, A. M. S., & Agriawan, J. I. (2024). Adopters and non-adopters of drones in humanitarian operations: An empirical evidence from a developing country. *Progress in Disaster Science*, *21*, 100314. https://doi.org/10.1016/j.pdisas.2024.100314

Tatsidou, E., Tsiamis, C., Karamagioli, E., Boudouris, G., Pikoulis, A., Kakalou, E., & Pikoulis, E. (2019). Reflecting upon the humanitarian use of unmanned aerial vehicles (drones). *Swiss Medical Weekly*, *149*(1314), w20065. https://doi.org/10.4414/smw.2019.20065

Vogel, R. J. (2011). Drone Warfare and the Law of Armed Conflict. *Denver Journal of International Law and Policy*, *39*(1), 101–138.

Wang, S., Zheng, C., & Wandelt, S. (2024). Policy challenges for coordinated delivery of trucks and drones. *Journal of the Air Transport Research Society*, *2*, 100001. https://doi.org/10.1016/j.jatrs.2024.100001

Zègre-Hemsey, J. K., Cheskes, S., Johnson, A. M., Rosamond, W. D., Cunningham, C. J., Arnold, E., Schierbeck, S., & Claesson, A. (2024). Challenges & barriers for real-time integration of drones in emergency cardiac care: Lessons from the United States, Sweden, & Canada. *Resuscitation Plus*, *17*, 100554. https://doi.org/10.1016/j.resplu.2024.100554

Сведения об авторе

Милад Каши Камиджани – магистр в области публичного права, факультет права, Университет Кума
Адрес: Иран, 3716146611, г. Кум, бульвар Аль-Гадир
E-mail: Mkk1377@gmail.com
ORCID ID: https://orcid.org/0009-0008-1640-3230
WoS Researcher ID: https://www.webofscience.com/wos/author/record/ISU-4107-2023
Google Scholar ID: https://scholar.google.com/citations?user=zsEAxXoAAAAJ

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.87 / Международное право
Специальность ВАК: 5.1.5 / Международно-правовые науки

История статьи

Дата поступления – 13 октября 2023 г.
Дата одобрения после рецензирования – 1 ноября 2023 г.
Дата принятия к опубликованию – 25 сентября 2024 г.
Дата онлайн-размещения – 30 сентября 2024 г.

Research article
UDC 34:004:341:004.4
EDN: https://elibrary.ru/tedarm
DOI: https://doi.org/10.21202/jdtl.2024.35

Prospects of Handling Digital Technology Disputes by Courts of Integration Associations

Valentina P. Talimonchik

Russian State University of Justice, Saint Petersburg, Russia

Keywords

Court of the Eurasian Economic Union,
court,
digital technologies,
dispute resolution,
dispute,
integration associations,
international law,
judge,
justice,
law

Abstract

Objective: to analyze the competence and procedure of case handling by the courts of integration associations, allowing them to resolve disputes related to information technologies, and to identify the prospects of handling of this category of disputes by the courts of integration associations.

Methods: the main research methods were analysis, synthesis, and problem-theoretical method.

Results: the article identified the main features of the "disputes related to digital technologies" category in relation to resolving disputes involving individuals by the courts of integration associations. It reveals opportunities for some courts of integration associations to resolve disputes related to information technologies. The said opportunities are provided by the courts competence, allowing the appeal of individuals, as well as by the dispute resolution procedure involving experts. By analyzing international treaties and practice of courts of integration associations, the author proves that the changes in the category of "disputes related to digital technologies" are related not only to technologies, but also to information and communication systems. By own judgments, the author reveals the content of disputes related to digital technologies in the courts of integration associations.

Scientific novelty: the paper reveals the peculiarities of the category "disputes related to digital technologies" in relation to the courts of integration associations and the prospects of resolving disputes related to information technologies by the courts of integration associations.

Practical significance: the conclusions provided in the article can be used to improve the practice of courts of integration associations.

For citation

Talimonchik, V. P. (2024). Prospects of Handling Digital Technology Disputes by Courts of Integration Associations. *Journal of Digital Technologies and Law, 2*(3), 690–710. https://doi.org/10.21202/jdtl.2024.35

Contents

Introduction

Traditionally, the issue of technology disputes resolution has been the responsibility of the United Nations Commission on International Trade Law (hereinafter – UNCITRAL). The 79th session of UNCITRAL Working Group II was held in New York on February 12–16, 2024[1].

An outcome document is also submitted to the 80th session, scheduled for September 30–October 4, 2024 in Vienna[2]. UNCITRAL has already achieved certain results with respect to international commercial arbitration.

[1] The UN Commission on International Trade Law (UNCITRAL) Working Group II on Dispute Settlement adopted the document "Technology Dispute Settlement and Adjudication: Model Exceptions and Explanatory Texts".

[2] Draft UNCITRAL Model Exceptions on Express Dispute Settlement Based on Expert Opinion (SpecialEOS).

First, a category of technology-related dispute was developed. It includes a wide variety of categories arising from "high" technologies across industries and services. Information technologies are not identified separately.

Second, common model exceptions were developed. For example, the arbitration exception contains the application of the UNCITRAL Expedited Arbitration Rules, with modifications for expedited appointment of the arbitrator by the appointing institution, expedited consultation with the parties, and convenient venue and language of the proceedings.

Third, an expert opinion exception is being worked on. An exception on the appointment of independent technical consultants is proposed. To select the technical consultant, the tribunal shall consult on the area of specialization and terms of reference for the expert. The parties are entitled to comment on the clarifications provided by the technical consultant.

In general, UNCITRAL is close to finalizing a system for the resolution of technology-related disputes arising from international transactions.

Since 2021, the World Intellectual Property Organization (further – WIPO) turns to advanced technologies[3]. The WIPO Arbitration and Mediation Center handles ICT-related disputes and has the potential to resolve issues relating to information and communication systems. Unlike UNCITRAL, which handles technology-related disputes by international commercial arbitration, the WIPO Center has offered effective pre-trial resolution of these types of disputes.

As of July 1, 2021, a new version of the WIPO Expert Opinion Rules is in force. An opinion is understood as a judgment rendered by an expert in accordance with Article 17 of the Rules on a matter referred to expert examination. Article 17 of the Rules provides that the expert may make a decision based on, without limitation: 1) any information provided by the parties; 2) the expert's competence; 3) any other information that the expert considers relevant to the case. The expert may, after consultation with the parties, make an interim or partial decision.

The competence of UNCITRAL and WIPO cannot refer to international judicial institutions. International judicial institutions have a separate legal framework for their activities, are characterized by narrow competence and do not constitute a system.

International judicial institutions are currently active in resolving disputes between states and individuals. The courts of various integration associations potentially may handle technology-related disputes.

[3] They cover digital technologies (Internet of Things (IoT), blockchain, metaverse, artificial intelligence (AI) including generative AI (GenAI), big data and cloud computing), as well as physical technologies (autonomous driving, 3D printing and hardware innovations).

The courts of integration associations on the African continent are numerous[4]. The judicial practice of integration associations may use UNCITRAL's Technology Related Dispute Indicators[5].

Disputes related to information technologies, handled in the integration associations, have been poorly researched. The practice of the EU Court of Justice was studied by Thomas Shaw (2016).

Fundamental studies on information technology law by Chris Reed and John Angel (2007), Andrew Murray (2010), Thomas Smedinghoff (2000), Diana Rowland and Elisabeth Macdonald (2005), Rowland et al. (2017) contain sections on commercial domain disputes.

A thorough analysis of the judicial practice, mainly national, can be found in (Armstrong et al., 2021).

A research by F. F. Wang (2014) devotes a special section to electronic commercial disputes.

Works on legal regulation of advanced technologies by T. Hoeren & B. Kolany (2018), M. Burri (2021), S-Y. Peng, C-F. Lin and T. Streinz (2021), S. Chesterman (2021), M. Compagnucci (2020), M. Kovac (2020), and N. Rebe (2021) do not touch upon courts of integration associations.

The rather extensive academic literature on the legal aspects of blockchain also does not address the problem of technology-related dispute resolution by courts of integration associations, as integration policies in this area are just emerging (Cappiello & Carullo, 2021; Herian, 2018; Stabile & Prior, 2020; Bambara & Allen, 2018; Fox & Green, 2019; Barker, 2020).

As the practice of the EU Court of Justice, including that related to digital technologies, is always subject to rigorous doctrinal analysis, this study will focus on integration associations in Africa and South America. The analysis will focus on two questions: 1) whether the competence of the courts of the integration associations allows them to handle digital technology disputes; and 2) whether the procedural rules of the courts of the integration associations take into account the specific features of this type of disputes, namely shortened procedural time limits and the participation of experts.

---

4 Court of Justice of the Common Market for Eastern and Southern Africa; Court of Justice of the East African Community; Court of Justice of the Central African Economic and Monetary Community; Court of Justice of the West African Economic and Monetary Community; Tribunal of the South African Development Community.

5 UNCITRAL's Draft Provisions on Technology Dispute Settlement provide examples of disputes arising in various industries: aerospace, audio, automotive or mobility means, artificial intelligence, biotechnology, computer manufacturing, electronics, information technology, medical devices, military/defense nanotechnology, nuclear physics, photonics, robotics, semiconductors, telecommunications, pharmaceuticals and financial technology. All these disputes are inextricably linked to economic integration.

1. Prospects for handling digital technology disputes by the courts of integration associations on the African continent

1.1. Prospects for handling digital technology disputes by the Court of Justice of the Common Market for Eastern and Southern Africa

1.1.1. Peculiarities of the competence of the Court of Justice of the Common Market for Eastern and Southern Africa

The competence of the Court of Justice of the Common Market for Eastern and Southern Africa (hereinafter referred to as the COMESA Court) to handle a certain category of disputes is determined by COMESA Treaty[6]. Also, to determine the competence of the COMESA Court to handle disputes related to digital technologies, the category of "digital technologies" should be defined.

At present, the term "technologies" in relation to digital technologies is a conventional term. In addition to the well-established term "information and communication technologies" (ICT), it should include information and communication systems[7].

Characteristically, ICT and information and communication systems are developed by private actors who enter into various kinds of contractual relationships.

ICTs accompany information throughout its "life cycle", which involves a variety of disputes. When information is created, disputes relate to intellectual property rights[8]. When ICTs are put into circulation, various service contracts are concluded (for implementation or technical support)[9]. Disputes may be related not only to contracts, but also to the use of ICTs without the developer's authorization.

Information and communication systems are also characterized by the concept of life cycle[10]. As with ICT, the use of information and communication systems is mediated through various contracts. At the phases of researching, designing and

---

6 Treaty establishing the Common market for Eastern and Southern Africa. https://clck.ru/3DsBHS

7 Artificial Intelligence, big data, neural networks, distributed ledgers and other systems that are relatively autonomous from a human.

8 If the software, database, or technology in the form of a trade secret is custom-built.

9 ICTs as a tool are used to search, obtain, disseminate, transfer, store, transform, systematize, destroy information and access to it, for which purpose the operator of a search engine, the owner of a website, the person with whom the information is linked, enter into legal relations, about which disputes may arise.

10 The Resolution of the General Conference of the United Nations Educational, Scientific and Cultural Organization (UNESCO) "Recommendation on the Ethical Aspects of Artificial Intelligence", adopted at its 41st session held in Paris from November 9 to 24, 2021, defines the notion of the life cycle of an artificial intelligent system as follows: the entire set of phases, from the research, design and development phases through to the deployment and utilization phases, which include maintenance, operation, marketing, financing, monitoring and evaluation, performance control, decommissioning, dismantling and disposal.

developing an information and communications technology system, these are labor and contracting agreements, and also investment ones. The deployment of an information and communications technology system may require agents and distributors. The use of an information and communications technology system involves various service contracts[11]. Various types of torts, including unfair competition, may occur after the deployment of an information and communications technology system.

It should be stated that disputes related to digital technologies arise mainly in the field of private international law. They are "transferred" to the public law sphere if: 1) public international law allows private parties to appeal to an international judicial institution; 2) an international treaty defining the terms of reference of an international judicial institution touches upon issues related to ICT and information and communication systems.

An analysis of Section 5 of the COMESA Treaty allows us to distinguish the categories of cases in which individuals may bring cases before the COMESA Court. First, any person having residence or domicile in a Member State may apply to the COMESA Court of Justice to appeal against acts of COMESA bodies when national remedies have been exhausted. Second, the COMESA Court also performs the function of arbitrating private contracts.

The COMESA Treaty defines the general[12] and specific aims and objectives of the Common Market. The specific objectives are formulated for specific areas of cooperation. In the field of communications, the objective is to promote cooperation that would facilitate the production of goods, trade in goods and services, and the movement of people. In the field of industry, the objectives are to eliminate rigidity in production structures in order to ensure high quality goods and services competitive in the Common Market and to create appropriate favorable conditions for the private sector to participate in economic development and cooperation within the Common Market, to cooperate in the field of industrial development. Cooperation in the information field is not separately identified. Issues of support for advanced technologies can be addressed within the framework of industrial development.

11 Contracts on the services of maintenance, operation provision, monitoring and evaluation, performance control, as well as decommissioning, dismantling and disposal.

12 The general goals include, inter alia: (1) to achieve sustainable growth and development of member States by promoting a more balanced and harmonious development of their production and marketing structures; (2) to promote joint development in all areas of economic activity and joint adoption of macroeconomic policies and programs to improve the living standards of their peoples and strengthen closer relations among their member States; (3) to cooperate in creating a favorable environment for foreign, cross-border, and domestic investment, including jointly promoting research for development; 4) to strengthen relations between the Common Market and the rest of the world and to develop common positions in international forums. These objectives are so broadly formulated that they do not require adaptation to the needs of information and communication systems development.

1.1.2. Peculiarities of the procedure of the COMESA Court of Justice for resolving digital technology disputes

The COMESA Court's 2016 Rules of Procedure[13] take into account the possibility of an expert's participation in the proceedings. They provide for a special request by the applicant for the appointment of an expert. A special rule is provided for the expert questioning: if the expert notifies the Registrar of the Court at least fifteen days before the hearing that he or she is unable to communicate adequately in one of the languages of the COMESA Court, the Court may permit the expert to give his or her evidence in English or another language and interpretation must be provided. If a person is called to testify as an expert, the Registrar may appoint a reasonable fee for the time spent both in testifying and in performing any work on the case. Characteristically, the examination procedure is not separately regulated; the status of an expert is similar to that of a witness.

The COMESA Court's 2016 Rules of Procedure cannot objectively take into account the shortened time limits for proceedings in disputes related to information technology, as they do not separately distinguish this category of disputes[14]. In general, the volume of cases heard by the COMESA Court involving legal persons is insignificant.

1.2. Prospects for handling digital technology disputes by East African Court of Justice

1.2.1. Analysis of the competence of East African Court of Justice to handle digital technology disputes

Section 8 of the 1999 East African Community Treaty[15] governs the status of the East African Community Court of Justice. The East African Community Court of Justice is the judicial body that enforces the law in interpreting, applying and enforcing the provisions of the 1999 Treaty.

In relation to private parties, the East African Community Court of Justice hears the following appeals: 1) by private parties on the validity of any act of a Member State on the ground that it violates the Treaty; 2) by parties to commercial contracts where their agreements contain an arbitration exception conferring jurisdiction on the Court.

The Community's objective is to develop policies and programs aimed at broadening and deepening cooperation between Member States in the political, economic, social and cultural fields, research and technology, defense, security, as well as in the legal and judicial spheres for their mutual benefit. Thus, research and technology is singled out as a separate area of cooperation.

---

13 COMESA Court of Justice. https://clck.ru/3DsBdr

14 Examples of cases involving legal persons handled by COMESA Court are: Malawi Mobile Limited vs COMESA; Malawi Mobile Limited Vs Government of the Republic of Malawi & Malawi Communication Regulatory Authority.

15 East African Court of Justice. (1999). The Treaty. https://clck.ru/3DsBez

In order to achieve the common objective, the Community shall, inter alia, ensure: (1) sustainable growth and development of the region; (2) mainstreaming gender in all its endeavors and enhancing the role of women in cultural, social, political, economic and technological development; (3) strengthening partnerships with the private sector and civil society to achieve sustainable socio-economic and political development. The East African Community is characterized by a clear orientation towards development, which contributes to the expansion of competencies of the Court of Justice of this integration association.

1.2.2. Peculiarities of the procedure of East African Court of Justice for resolving digital technology disputes

The Court of Justice of the East African Community is very active. The panel of the first instance has so far heard 179 cases, while the appeal panel has heard 53 cases, of which the most frequent are cases involving appeals by individuals and legal entities. For example, the case Chester House Limited v. the Attorney General of the Republic of Uganda & 3 others dealt with the protection of foreign investment.

The 1999 Treaty and the Rules of Procedure 2019[16] of the East African Community Court of Justice set certain rules for appeals by individuals.

The 1999 Treaty sets a short time limit for appeals by private parties: proceedings must be commenced within two months of the entry into force, publication, directive, decision or action complained of, or from the date on which the complainant became aware of it. The parties may be represented by a lawyer entitled to appear before the Supreme Court of any of the Member States.

Chapters VII and XII of the Rules of Procedure set out the procedure for handling cases. Expert participation is provided for. The parties may examine the expert's report at the Registry and obtain copies at their own expense. In the case of any person called by the Court to testify as an expert, the Registrar may appoint a reasonable fee for the time spent both in giving evidence and in carrying out any work on the case. The procedure for engaging an expert is not regulated in detail. The expert is not engaged by the Court, but by the parties concerned.

1.3. Prospects for handling digital technology disputes by the Court of Justice of the West African Economic and Monetary Union

1.3.1. Analysis of the competence of the Court of Justice of the West African Economic and Monetary Union to handle digital technology disputes

The Court of Justice of the West African Economic and Monetary Union (hereinafter referred to as the ECOWAS Court of Justice) has been handling individual complaints since 2005.

---

[16] East African Court of Justice. (2019). Rules of procedures 2019. https://clck.ru/3DsBoz

The 1975 Treaty on the Economic Community of West African States (ECOWAS)[17] included a mandate for the Community Court of Justice to handle disputes relating to the Treaty interpretation and operation. The rules for the Court functioning were established by the 1991 Protocol on the Community Court of Justice. The Court became operational in December 2000.

The ECOWAS Additional Protocol of 2005[18] established the rules for admissibility of complaints to include disputes between individuals and their own member states. The ECOWAS Court of Justice included the following divisions: the ECOWAS Administrative Tribunal, the Court of Human Rights, the Court of Arbitration, and the Inter-State Dispute Resolution Tribunal.

According to Article 4 of the 2005 Protocol, individuals and legal entities have the right to appeal to the ECOWAS Court of Justice. There is no need to exhaust domestic remedies to approach the ECOWAS Court of Justice.

The ECOWAS Treaty defines the overall objective of the association without specifying it[19]. It also defines the means of achieving the objective, which may contribute to the development of information and communication systems in the region[20].

ECOWAS focuses on economic integration but emphasizes information as a separate area of cooperation.

1.3.2. Peculiarities of the procedure of the ECOWAS Court of Justice for resolving digital technology disputes

According to the Rules of Procedure of the ECOWAS Court of Justice, in force since January 1, 2022[21], the Court may use an expert opinion. The order appointing the expert must define his or her task and set a time limit within which he or she must prepare his or her opinion.

---

17 ECOWAS. https://clck.ru/3DsBxo

18 Supplementary Protocol A/SP.1/01/05 amending the preamble and Articles 1, 2, 9 AND 30 of Protocol A/P.1/7/91 relating to the community Court of Justice and Article 4 paragraph 1 of the English version of the said Protocol. https://clck.ru/3DsByp

19 The ECOWAS objective is to promote cooperation and integration leading to an economic union in West Africa in order to improve the living standards of its peoples and to maintain and consolidate economic stability, strengthen relations among member States and contribute to the progress and development of the African continent.

20 The means of achieving the objective include: 1) harmonization and coordination of national policies and promotion of integration programs, projects and activities, including in the fields of industry and communications, as well as information, science, and technology; 2) promotion of joint production enterprises; 3) elimination of obstacles to the free movement of people, services and capital between the member States; 4) establishment of an economic union; 5) promotion of joint ventures by private enterprises and other economic operators; 6) harmonization of standards; 7) promotion of information dissemination, especially among rural populations, women's and youth organizations and socio-professional associations such as media associations, business men and women, workers and trade unions.

21 Community Court of Justice, ECOWAS (The Economic Community of West African States) rules of the Community Court of Justice of the Economic Community of West African States (ECOWAS). https://clck.ru/3DsBzs

The expert shall receive a copy of the Court's order, together with all the documents necessary for the examination. He or she shall be supervised by the judge-rapporteur, who may be present during the examination and who shall be informed of the task progress. The court may require the parties or one of them to deposit security for the costs of the expert's opinion. After the expert has given his or her opinion, the Court may order to interrogate him or her, having first notified the parties of the need for his or her presence. Before performing the task, the expert shall take the following oath in writing or in court: "I swear or affirm that I will perform my task faithfully and impartially". If either party objects to the expert on the ground that he or she is not a competent or proper person to act as an expert, or for any other reason, or if the expert refuses to testify, take an oath, the matter shall be resolved by the court.

Thus, the Rules of Procedure of the ECOWAS Court of Justice, in force since January 1, 2022, best reflect the specificity of digital technology disputes.

1.4. Possibility of resolving digital technology disputes by the courts of other integration associations on the African continent

1.4.1. Problem of resolvability of digital technology disputes by the South African Development Community Tribunal

The SADC Tribunal was established under Article 9 of the SADC Treaty[22]. Previously, the SADC Tribunal had dealt with disputes involving private persons. Cases brought before the SADC Tribunal involved expropriation of private property by states. In Mike Campbell (Pvt) LTD and Others v. Zimbabwe (Case No. SADC (T) 2/2007, Main Decision of November 28, 2008), the applicant's rights were violated by the expropriation of his private property without compensation. In handling the case, the SADC Tribunal was guided by principles of international human rights law rather than applying any specific human rights treaty.

Following its decisions against the Government of Zimbabwe in this and related cases, the Tribunal functioning was suspended. A process of reviewing its competence followed. The new 2014 Protocol on the Tribunal sought to revise the Tribunal's mandate by limiting it to handling disputes involving states only. As a consequence, the SADC Tribunal was prevented from handling digital technology disputes involving private actors.

22 Southern African Development Community. (2021). SADC Treaty. https://clck.ru/3DsFEk

1.4.2. Problem of resolvability of digital technology disputes by the Court of Justice of the Economic and Monetary Union of Central Africa

Article 5 of the 1994 Treaty establishing the Central African Economic and Monetary Community (CEMAC)[23] stipulates that the judicial chamber of the CEMAC Court of Justice shall provide for the interpretation of the CEMAC Treaty and subsequent conventions.

With regard to the potential to resolve disputes involving private parties, the Court ensures the validity of decisions, directives and regulations of the Community institutions. Appeals by private parties are not separately identified.

The power to handle other disputes may be conferred on the Court by decisions adopted by the Conference of Heads of State and Government.

2. Prospects for handling digital technology disputes by the courts of the South American integration associations

2.1. Prospects for handling digital technology disputes by the Court of Justice of the Andean Community

2.1.1. Analysis of the competence of the Court of Justice of the Andean Community to handle digital technology disputes

The competence of the Court of Justice of the Andean Community is defined by the 1996 Agreement establishing the Court of Justice of the Andean Community[24] It includes disputes involving private persons[25].

An action to invalidate an Andean Community act must be brought within two years from the date of its entry into force. If this period has expired, any of the parties to the proceedings referred to the national courts may petition the national court to declare the decision of the Andean Community authority inapplicable to the particular case.

The 1969 Cartagena Agreement[26] defined the general objective of the Andean Community[27]. Mechanisms and measures were provided to achieve the integration objective, including: (1) adoption of joint programs, implementation of industrial programs and means of industrial integration; (2) implementation of services programs

---

23 Traite instituant la Communaute Économique et Monetaire de l'Afrique Centrale (Texte authentique). https://clck.ru/3DsFJE

24 Treaty creating the Court of Justice of the Andean community. https://clck.ru/3DsFL7

25 Natural or legal persons may bring an action to invalidate decisions adopted by the Andean Council of Ministers of Foreign Affairs or the Andean Community Commission, resolutions of the General Secretariat or agreements that affect their subjective rights or legitimate interests.

26 Andean Subregional Integration Agreement (Cartagena Agreement). https://clck.ru/3DsFMs

27 To promote the balanced and harmonious development of the member States on equal terms through integration and socio-economic cooperation; to accelerate their economic growth; and to promote their participation in the regional integration process, with the prospect of the gradual formation of a Latin American Common Market.

and liberalization of intra-regional trade in services; and (3) adoption and implementation of programs to promote scientific and technological development. The latter measure allows the Andean Community to function under advanced technology development.

2.1.2. Features of the procedure of the Court of Justice of the Andean Community for handling digital technology disputes

The Statute of the Court of Justice of the Andean Community regulates the involvement of experts in a very limited manner[28]. The parties, with the Tribunal's prior authorization, may participate in a hearing through experts only to clarify technical issues. During the hearing, the Chairperson and the judges may question the experts. Thus, experts are engaged by the parties.

However, the Andean Community established a regional system for the protection of intellectual property, which led to the active work of the Andean Community Court of Justice in resolving such disputes. The WIPO Lex database contains 117 decisions of the Andean Community Court of Justice on intellectual property issues. For example, in 2024, the Andean Community Court of Justice acted as the final instance in the copyright disputes Carlos Alberto Massó Vasco vs Caracol Televisión S.A., Entidad de Gestión Colectiva de Derechos de Productores Audiovisuales de Colombia vs IA TRIP S.A.S. (propietaria del establecimiento hotelero Hotel Picasso Inn). Given the experience of the Andean Community Court of Justice with respect to "traditional" telecommunications, disputes in the area of intellectual property and advanced technologies are unlikely to cause significant difficulties.

2.2. Problem of resolvability of digital technology disputes within other South American integration associations

2.2.1. Problem of resolvability of digital technology disputes by the Caribbean Court of Justice

The 1973 Treaty Establishing the Caribbean Community (hereinafter – CARICOM)[29] did not provide for the establishment of the Community Court of Justice. Later, the Treaty was revised.

Established in 2001, The Caribbean Community Court of Justice has both first instance and appellate jurisdiction. In its appellate jurisdiction, the Court acts as a court of the final instance in civil and criminal cases for those states that have recognized its appellate jurisdiction. As a court of first instance, it applies international law to the interpretation and application of the Revised Treaty of Chaguaramas. The 2001 Agreement establishing the Caribbean Court[30] does not provide for appeals by individuals, but the Caribbean Community

---

28 Estatuto del Tribunal de Justicia de la Comunidad Andina. https://clck.ru/3DsFTt

29 Treaty establishing the Caribbean Community. https://clck.ru/3DsFVu

30 Agreement establishing the Caribbean Court of Justice. https://clck.ru/3DsFXT

Court of Justice recognized such jurisdiction in 2008 in the case of two entities against Guyana.

Although there are no clear treaty provisions establishing the jurisdiction of the Caribbean Community Court of Justice to handle digital technology disputes, its rules are highly adapted to handling this type of dispute. In particular, the Caribbean Court of Justice Original Jurisdiction Rules 2021[31] regulate a number of expertise issues: the essential duty of the expert before the Court to assist the Court to decide impartially the issues relevant to the expert's competence; the order in which that duty is to be exercised; the content of the expert's report; the expert's right to apply to the Court for instructions; the Court's power to limit expert opinion; the Court's power to appoint a single expert; and the consequences of failure to provide the expert's opinion. In general, such detailed regulation of expert involvement not only contributes to the resolution of information technology disputes, but could be taken into account in UNCITRAL's work on this topic.

2.2.2. Problem of resolvability of digital technology disputes within Mercosur

The 1991 Treaty establishing the Common Market between the Argentine Republic, the Federative Republic of Brazil, the Republic of Paraguay and the Eastern Republic of Uruguay (Treaty of Asunción)[32] did not provide for the possibility of private participation in the Mercosur dispute settlement mechanism. By concluding the Treaty of Asunción, the member states decided to establish a Common Market by December 31, 1994. The Common Market was to include, among other things, the free movement of services, coordination of macroeconomic and sectoral policies of the participating states in the fields of industry, services and any other areas that may be agreed upon. As a consequence, the sphere of information, telecommunications, including ICTs, was not singled out in the structure of the Common Market and was not regulated separately.

The Brazilian and Olivos Protocols established procedures for the resolution of disputes concerning the interpretation, application or non-compliance with the Asunción Treaty or any of its protocols, and decisions of Mercosur bodies. However, no mechanism was developed for handling appeals from legal entities and individuals. Individuals can only file complaints with the National Offices of the Common Market Group of the participating state in which they reside. The lack of a unified dispute resolution mechanism within Mercosur hinders the resolution of disputes related to information technologies.

---

31 Caribbean Court of Justice. Original Jurisdiction Rules 2021. https://clck.ru/3DsFdd

32 Treaty establishing a Common Market between the Argentine Republic, the Federal Republic of Brazil, the Republic of Paraguay and the Eastern Republic of Uruguay (Treaty of Asuncion). https://clck.ru/3DsFdd

3. Prospects for handling digital technology disputes by the Court of the Eurasian Economic Union

3.1. Analysis of the competence of the Court of the Eurasian Economic Union for handling digital technology-related disputes

The Court of the Eurasian Economic Union (hereinafter – the EAEU Court) has the competence to resolve disputes involving private persons – economic entities in relation to the acts of the ECE, which, among other things, may be related to information technologies.

The possibility of handling information technology disputes is determined by the specificity of the ECE competence[33]. The potential to resolve disputes related to information and communication systems derives from a number of EAEU acts[34].

In addition, a number of "information society services" have been included in the list of sectors in which free movement of services and uniform policies are ensured[35]. Potentially, disputes related to these categories of services could be resolved by the EAEU Court of Justice.

Special types of services are governed by the general provisions on the single market for services (Advisory Opinion of the EAEU Court of Justice of July 10, 2020). There are no special rules on "information society services" in the EAEU legislation.

3.2. Peculiarities of the procedure of the Court of the Eurasian Economic Union for resolving digital technologies disputes

The Statute of the EAEU Court provides for Specialized Expert Groups only for the resolution of disputes relating to support of agriculture, industrial subsidies, and special trade measures. Disputes related to digital technologies are not singled out as a separate category of disputes requiring the establishment of Specialized Groups.

For these three categories of disputes, the requirements for experts are highlighted: 1) high qualification, knowledge and experience in relation to the subject matter of the dispute; 2) independence; 3) no conflict of interest.

---

33 In particular, the Commission carries out activities in the following areas: 1) competition policy; 2) mutual trade in services and investment; and 3) intellectual property. In all of these areas, issues related to the use of information technology may arise.

34 Artificial intelligence technologies are included in the List of priority economic activities for industrial cooperation of EAEU member states, approved by the Decision of the Eurasian Intergovernmental Council of November 27, 2018, No. 9, as well as the List of "industries of the future", approved by the Order of the Eurasian Intergovernmental Council of March 7, 2017, No. 2.

35 According to the Decision of the Supreme Eurasian Economic Council of December 23, 2014 No. 110, the list of sectors of the common market of services, in particular, includes: 1) services related to databases, including the provision of information on websites; provision of services of searching for data and other information from information resources; 2) services of providing assistance in keeping computer systems in working condition, their maintenance, and improvement of programs.

At the same time, the rules of proceedings in the EAEU Court allow participation of experts, including experts of Specialized Groups, as well as specialists. But only experts of Specialized Groups are granted immunities.

An expert or specialist has a number of rights[36]. They shall submit a written opinion on the issues raised. An expert or specialist may not participate in handling a dispute in which they previously participated in another capacity.

The general deadline for a decision in the EAEU Court is not later than 90 days from the date of the claim receipt, so the EAEU Court can promptly resolve disputes related to digital technologies.

Conclusions

The following conclusions can be drawn based on the study results.

The term "digital technology disputes" is complex and encompasses not only ICT-related disputes, but also disputes related to information and communication systems in general.

This category of disputes includes digital technology disputes arising from international contracts and non-contractual relations between private actors, handled by national courts under the rules of international jurisdiction, as well as international commercial arbitrations, and disputes handled by international judicial institutions to which private parties may be a party. Digital technology disputes can potentially arise in inter-state relations.

Courts in a number of integration associations (except the South African Development Community Tribunal, the Court of Justice of the Central African Economic and Monetary Community, and Mercosur) have the potential to handle digital technology disputes, and the Andean Community Court of Justice has been active in intellectual property disputes, including in relation to ICTs. The possibility of handling digital technology disputes by the courts of integration associations is ensured by the specifics of their competence, which allows for private parties, as well as by the dispute resolution procedure, which includes the involvement of experts. However, the principle of transparency of their activities does not allow for the confidentiality of such proceedings, and the problem of shortening the terms of handling of digital technology disputes can only be resolved in the very distant future.

References

Armstrong, D., McCombie, F., & Davis, C. (2021). *Cyber Litigation: The Legal Principles*. New York: Bloomsbury Professional Ltd.

Bambara, J., & Allen, P. (2018). *Blockchain: A Practical Guide to Developing Business, Law, and Technology Solutions*. McGraw-Hill Education.

[36] Familiarize oneself with the case materials related to the subject matter of the expertise; ask questions to other persons involved in the dispute; request additional materials to provide an opinion.

Barker, R. (Ed.) (2020). *The Law and Governance of Decentralised Business Models: Between Hierarchies and Markets*. London: Routledge.

Burri, M. (2021). *Big Data and Global Trade Law*. Cambridge: Cambridge University Press. https://doi.org/10.1017/9781108919234

Cappiello, B., & Carullo, G. (Eds.) (2021). *Blockchain, Law and Governance*. London: Springer. https://doi.org/10.1007/978-3-030-52722-8

Chesterman, S. (2021). *We, the Robots?: Regulating Artificial Intelligence and the Limits of the Law.* Cambridge: Cambridge University Press. https://doi.org/10.1017/9781009047081

Compagnucci, M. C. (2020). *Big Data, Databases and "Ownership" Rights in the Cloud*. London: Springer. https://doi.org/10.1007/978-981-15-0349-8

Fox, D., & Green, S. (Eds.) (2019). *Cryptocurrencies in Public and Private Law*. Oxford: Oxford University Press.

Herian, R. (2018). *Regulating Blockchain: Law, Technology and the Ethics of Political Economy*. London: Routledge. https://doi.org/10.4324/9780429489815

Hoeren, T., & Kolany, B. (Eds.) (2018). *Big Data in Context Legal, Social and Technological Insights*. London: Springer. https://doi.org/10.1007/978-3-319-62461-7

Kovac, M. (2020). *Judgement-Proof Robots and Artificial Intelligence A Comparative Law and Economics Approach*. London: Springer/Palgrave Macmillan. https://doi.org/10.1007/978-3-030-53644-2

Murray, A. (2010). *Information Technology Law: the law and society*. Oxford: Oxford University Press.

Peng, S-Y., Lin, C-F., & Streinz, T. (Eds.) (2021). *Artificial Intelligence and International Economic Law: Disruption, Regulation, and Reconfiguration*. Cambridge: Cambridge University Press. https://doi.org/10.1017/9781108954006

Rebe, N. (2021). *Artificial Intelligence: Robot Law, Policy and Ethics*. Leiden: Brill – Nijhoff. https://doi.org/10.1163/9789004458109

Reed, C., & Angel, J. (Eds.) (2007). *Computer Law: the Law and Regulation of Information Technology*. Oxford: Oxford University Press.

Rowland, D., Kohl, U., & Charlesworth, A. (2017). *Information Technology Law* (5th ed.). London: Routledge.

Rowland, D., & Macdonald, E. (2005). *Information technology law* (3rd ed.). Abingdon: Cavendish Publishing Ltd.

Shaw, T. J. (2016). *Information and Internet Law: Global Practice*. Createspace Independent Publishing Platform.

Smedinghoff, T. J. (2000). *Online Law.* New York: Pearson Education Corporation.

Stabile, D., & Prior, K. (2020). *Digital Assets and Blockchain Technology: U.S. Law and Regulation*. Cheltenham: Edward Elgar Publishing Limited.

Wang, F. F. (2014). *Law of Electronic Commercial Transactions. Contemporary Issues in the EU, US and China.* New York: Routledge. https://doi.org/10.4324/9780203628812

Author information

Valentina P. Talimonchik – Dr. Sci. (Law), Associate Professor, Professor of the Department of General Theoretical Legal Disciplines, North-West branch of the Russian State University of Justice
Address: 5 Aleksandrovskiy park, 197046 Saint Petersburg, Russia
E-mail: talim2008@yandex.ru
ORCID ID: https://orcid.org/0000-0002-5302-460X
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57190001688
WoS Researcher ID: https://www.webofscience.com/wos/author/record/H-1253-2013
Google Scholar ID: https://scholar.google.com/citations?user=7EluYwgAAAAJ
RSCI Author ID: https://elibrary.ru/author_items.asp?authorid=447740

Conflict of interests

The author is a member of the Editorial Board of the Journal; the article has been reviewed on general terms.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – June 10, 2024
Date of approval – July 1, 2024
Date of acceptance – September 25, 2024
Date of online placement – September 30, 2024

Научная статья
УДК 34:004:341:004.4
EDN: https://elibrary.ru/tedarm
DOI: https://doi.org/10.21202/jdtl.2024.35

Перспективы рассмотрения споров, связанных с цифровыми технологиями, судами интеграционных объединений

Валентина Петровна Талимончик

Российский государственный университет правосудия, Санкт-Петербург, Россия

Ключевые слова

интеграционные объединения,
международное право,
право,
правосудие,
разрешение споров,
спор,
суд,
Суд Евразийского экономического союза,
судья,
цифровые технологии

Аннотация

Цель: проведение анализа компетенции и процедуры рассмотрения дел судами интеграционных объединений, позволяющих им разрешать споры, связанные с информационными технологиями, и определение перспектив рассмотрения этой категории споров судами интеграционных объединений.

Методы: использованы основные методы исследования – анализ, синтез и проблемно-теоретический метод.

Результаты: выявлены основные особенности категории «споры, связанные с цифровыми технологиями» применительно к специфике разрешения споров с участием частных лиц судами интеграционных объединений, а также потенциальные возможности для ряда судов интеграционных объединений разрешать споры, связанные с информационными технологиями, которые обеспечиваются особенностями компетенции судов, допускающей обращение частных лиц, а также процедуры разрешения споров, включающей привлечение экспертов. Доказано изменение категории «споры, связанные с цифровыми технологиями» как связанной не только с технологиями, но и информационно-коммуникационными системами, посредством анализа международных договоров и практики судов интеграционных объединений; в результате собственных суждений автора выявлено содержание споров, связанных с цифровыми технологиями, в отношении судов интеграционных объединений.

Научная новизна: в работе выявлены особенности категории «споры, связанные с цифровыми технологиями» в отношении судов интеграционных объединений и перспективы разрешения споров, связанных с информационными технологиями, судами интеграционных объединений.

Практическая значимость: выводы, данные в статье, могут быть использованы при совершенствовании практики судов интеграционных объединений.

Для цитирования

Талимончик, В. П. (2024). Перспективы рассмотрения споров, связанных с цифровыми технологиями, судами интеграционных объединений. *Journal of Digital Technologies and Law*, *2*(3), 690–710. https://doi.org/10.21202/jdtl.2024.35

Список литературы

Armstrong, D., McCombie, F., & Davis, C. (2021). *Cyber Litigation: The Legal Principles*. New York: Bloomsbury Professional Ltd.

Bambara, J., & Allen, P. (2018). *Blockchain: A Practical Guide to Developing Business, Law, and Technology Solutions*. McGraw-Hill Education.

Barker, R. (Ed.) (2020). *The Law and Governance of Decentralised Business Models: Between Hierarchies and Markets*. London: Routledge.

Burri, M. (2021). *Big Data and Global Trade Law*. Cambridge: Cambridge University Press. https://doi.org/10.1017/9781108919234

Cappiello, B., & Carullo, G. (Eds.) (2021). *Blockchain, Law and Governance*. London: Springer. https://doi.org/10.1007/978-3-030-52722-8

Chesterman, S. (2021). *We, the Robots?: Regulating Artificial Intelligence and the Limits of the Law.* Cambridge: Cambridge University Press. https://doi.org/10.1017/9781009047081

Compagnucci, M. C. (2020). *Big Data, Databases and "Ownership" Rights in the Cloud*. London: Springer. https://doi.org/10.1007/978-981-15-0349-8

Fox, D., & Green, S. (Eds.) (2019). *Cryptocurrencies in Public and Private Law*. Oxford: Oxford University Press.

Herian, R. (2018). *Regulating Blockchain: Law, Technology and the Ethics of Political Economy*. London: Routledge. https://doi.org/10.4324/9780429489815

Hoeren, T., & Kolany, B. (Eds.) (2018). *Big Data in Context Legal, Social and Technological Insights*. London: Springer. https://doi.org/10.1007/978-3-319-62461-7

Kovac, M. (2020). *Judgement-Proof Robots and Artificial Intelligence A Comparative Law and Economics Approach*. London: Springer/Palgrave Macmillan. https://doi.org/10.1007/978-3-030-53644-2

Murray, A. (2010). *Information Technology Law: the law and society*. Oxford: Oxford University Press.

Peng, S-Y., Lin, C-F., & Streinz, T. (Eds.) (2021). *Artificial Intelligence and International Economic Law: Disruption, Regulation, and Reconfiguration*. Cambridge: Cambridge University Press. https://doi.org/10.1017/9781108954006

Rebe, N. (2021). *Artificial Intelligence: Robot Law, Policy and Ethics*. Leiden: Brill – Nijhoff. https://doi.org/10.1163/9789004458109

Reed, C., & Angel, J. (Eds.) (2007). *Computer Law: the Law and Regulation of Information Technology*. Oxford: Oxford University Press.

Rowland, D., Kohl, U., & Charlesworth, A. (2017). *Information Technology Law* (5th ed.). London: Routledge.

Rowland, D., & Macdonald, E. (2005). *Information technology law* (3rd ed.). Abingdon: Cavendish Publishing Ltd.

Shaw, T. J. (2016). *Information and Internet Law: Global Practice*. Createspace Independent Publishing Platform.

Smedinghoff, T. J. (2000). *Online Law.* New York: Pearson Education Corporation.

Stabile, D., & Prior, K. (2020). *Digital Assets and Blockchain Technology: U.S. Law and Regulation*. Cheltenham: Edward Elgar Publishing Limited.

Wang, F. F. (2014). *Law of Electronic Commercial Transactions. Contemporary Issues in the EU, US and China.* New York: Routledge. https://doi.org/10.4324/9780203628812

Сведения об авторе

Талимончик Валентина Петровна – доктор юридических наук, доцент, профессор кафедры общетеоретических правовых дисциплин, Северо-Западный филиал Российского государственного университета правосудия
Адрес: 197046, Россия, г. Санкт-Петербург, Александровский парк, 5
E-mail: talim2008@yandex.ru
ORCID ID: https://orcid.org/0000-0002-5302-460X
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57190001688
WoS Researcher ID: https://www.webofscience.com/wos/author/record/H-1253-2013
Google Scholar ID: https://scholar.google.com/citations?user=7EluYwgAAAAJ
РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=447740

Конфликт интересов

Автор является членом редакционной коллегии журнала, статья прошла рецензирование на общих основаниях.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.87 / Международное право
Специальность ВАК: 5.1.5 / Международно-правовые науки

История статьи

Дата поступления – 10 июня 2024 г.
Дата одобрения после рецензирования – 1 июля 2024 г.
Дата принятия к опубликованию – 25 сентября 2024 г.
Дата онлайн-размещения – 30 сентября 2024 г.

Review
UDC 34:004:347.211:004.383.8.032.26
EDN: https://elibrary.ru/sperfj
DOI: https://doi.org/10.21202/jdtl.2024.36

Neurorights, Neurotechnologies and Personal Data: Review of the Challenges of Mental Autonomy

Yan Cornejo
Independent Researcher, Guayaquil, Ecuador

Keywords

digital technologies,
ethics,
human rights,
law,
legislation,
mental autonomy,
neurorights,
neurotechnologies,
personal data,
privacy

Abstract

Objective: to present the results of a systematic review of research on the impact of neurotechnology on legal concepts and regulatory frameworks, addressing ethical and social issues related to the protection of individual rights, privacy and mental autonomy.

Methods: The systematic literature review was based on the methodology proposed by a renowned British scholar, a professor emerita of computer science at Keele University Barbara Kitchenham, chosen for its flexibility and effectiveness in obtaining results for publication. Thorough searches were carried out with the search terms “neurotechnology”, “personal data”, “mental privacy”, “neuro-rights”, “neurotechnological interventions”, and “neurotechnological discrimination” on both English and Spanish sites, using search engines like Google Scholar and Redib as well as databases including Scielo, Dialnet, Redalyc, Lilacs, Scopus, Medline, and Pubmed. The focus of this research is bibliometric data and its design is non-experimental with a cross-sectional and descriptive, using content analysis based on PRISMA model.

Results: the study emphasizes the need to establish clear ethical principles to protect individual rights and promote responsible use of neurotechnologies; a number of problems of mental autonomy were identified, such as improper handling of information, lack of legal security guarantees, violation of rights and freedoms in the medical sphere. The author shows the need to adapt the existing regulatory legal framework to address the ethical and social problems arising from the new neurotechnologies. It is noted that a broad study of neurotechnology issues will contribute to the protection of human rights.

Scientific novelty: an expanded understanding of the five neurorights within the Universal Declaration of Human Rights is proposed; neurorights are viewed as a new category of rights aimed at protecting mental integrity against the misuse of neurotechnologies. The author justifies the adoption of such technocratic principles as personal identity, free will, mental privacy, equal access and protection against bias.

Practical significance: the obtained results are relevant for understanding modern legal concepts related to neurorights and for adapting the existing normative legal acts to solve ethical and social problems arising from the emergence of new technologies, protection of human neurorights and liability for their violation. The study of these issues is key for provision of further responsible development and use of neurotechnologies.

For citation

Cornejo, Ya. (2024). Neurorights and Personal Data: Challenges and Mental Autonomy. *Journal of Digital Technologies and Law, 2*(3), 711–728. https://doi.org/10.21202/jdtl.2024.36

Contents

Introduction

The rapid advancement of neurotechnologies has opened up unprecedented possibilities for understanding and enhancing the functioning of the human brain. However, this progress has also posed significant ethical and social challenges related to the protection of individual rights, privacy, and mental autonomy.

In this context, there arises the need to establish a conceptual and practical framework to guide the responsible development and application of these technologies. Neurorights, as defined by Moisés Barrio, are the digital rights of citizens that can be exercised with the same effectiveness both within and outside the digital environment (Arellano, 2024; Parlatino, 2023; Fukushi, 2024).

In Spain, the Digital Rights Charter stands out as a fundamental element in recognizing rights in this environment, without replacing fundamental rights also known as human rights or individual guarantees. It is important to note that neurorights do not seek to create new fundamental rights, but rather to describe and specify the changing nature of the digital environment, thus proposing the recognition of new human rights to adapt to these changes (González, 2021; Hsu, 2024).

In the ethical and legal sphere, Goering et al. (2021) defines neurorights as "a conceptual and practical framework to guide the responsible development and application of neurotechnologies", emphasizing the need to establish clear ethical principles that protect individual rights and promote the responsible use of these technologies (Gómez, 2021).

Meanwhile, Filipova (2022) describes them as "an emerging field that explores the ethical and legal challenges related to the development and application of neurotechnologies", highlighting the importance of a solid regulatory framework to ensure the responsible development and application of these technologies (Cáceres & López, 2022).

Concerns about the potential ethical risks associated with neurotechnologies are shared by several authors. The creation of the Brain Activity Map (BAP) has sparked debates about mental privacy, the responsibility of our actions, and advances in neurotechnology, as well as issues of stigmatization and discrimination related to neurological measures. In this context, artificial intelligence, algorithmic biases, and neuroscientific evidence are relevant in legal and judicial domains (Fernández, 2023; López-Silva & Madrid, 2022; Cáceres et al., 2021; Clausen et al., 2017; Cornejo-Plaza et al., 2024).

Neurotechnologies have opened a world of possibilities for understanding and enhancing the functioning of the human brain, while posing ethical and social challenges related to the protection of individual rights, privacy, and mental autonomy. Hence, the research question arises: How can existing regulatory frameworks adapt to address the ethical and social challenges posed by emerging neurotechnologies? This question is pivotal to ensure the responsible development and application of neurotechnologies for the benefit of society.

The aim of this research is to conduct a bibliometric analysis of the effects of regulatory frameworks concerning the ethical and social challenges posed by emerging neurotechnologies for the betterment of humanity.

1. Neurorights, neurotechnologies and its legal and ethical implications

1.1. Neurorights

The field of neuro-rights emerges in response to the rapid development of neurotechnologies, which have the potential to transform how we understand and address the human brain. However, these technologies also pose significant ethical and social challenges related to the protection of individual rights, privacy, and mental autonomy (Moreu, 2022).

The earliest debates on neuro-rights trace back to the 1990s, with authors like Judy Illes, who began exploring the ethical implications of new brain technologies (Borbón & Borbón, 2022). In 2002, the United Nations Educational, Scientific and Cultural Organization (UNESCO) convened a conference on neuroethics, discussing the challenges and opportunities of neurotechnologies and proposing the need to develop an ethical framework for their development and application.

In this context, neuro-rights emerge as a conceptual and practical framework to address these challenges. The term "neuro-rights" constitutes a new category of rights aimed at protecting mental integrity from the misuse of neurotechnologies[1].

Nonetheless, it is troubling that there isn't a special international regulation in place to handle possible abuses of life, integrity, and freedom of speech resulting from multinational corporations trading in neurotechnologies (Parlatino, 2023).

López-Silva and Madrid (2022) are among the authors who demonstrate a strong connection between the terms "mental" and "psychic", connecting them to the term "psychological". Additionally, they suggest that "cerebral" be used in place of "neuronal," given the strong connection between the two terms. In this sense, "mental" is closely linked to "mental privacy," which is commonly used to refer to the confidentiality of neural information. But it's crucial to understand that, depending on the application domain and the historical-cultural context of each scenario, the intricacy of this problem could evoke varied responses.

According to Parlatino (2023), neuro-rights, also known as brain rights, are a new international legal framework that emphasizes the protection of the brain and its functions in addition to the already established human rights. These rights include the right to one's own identity, mental privacy, and individuality. Additionally, they incorporate materials with legally mandated safeguards to address the increasing hazards associated with the advancement and use of neurotechnologies in people (Moreu, 2022).

Neuroscientific research, therapeutic practice, and technology advancement are only a few of the many domains in which neuro-rights are applicable (Parlatino, 2023).

---

[1] Universidad Santiago de Chile. (2021). Cambalache, 4. (In Spain). https://clck.ru/3Ct9Wi

1.2. Neurotechnologies

Neurotechnologies refer to those technologies focused on the study of the improvement of the nervous system. Towards those parts that need rehabilitation or assistance due to loss of functions, that is, rehabilitation on motor disorders allows progress achieved in research and development in its most basic functions (Barrios et al., 2017).

Experts mention that neurotechnologies are related to a wide variety of methods and instruments that work in conjunction with the brain and nervous system in a general way and that monitor passively or alter the activity if it is active (Andorno, 2023).

Furthermore, report states that the benefits of neurotechnology are being explored in relation to the work environment by transcribing thoughts to screens without using keyboards, however, he is concerned about the implicit risks that may violate privacy, free will and human dignity.

UNESCO carried out a study where neurotechnology is only investigated in 10 Latin American countries, a situation that causes concern due to the possibility of little equitable access to knowledge and disparity in health care, research and innovation for the benefit of human beings[2].

Neurotechnological research focused on the brain involves important challenges because it promotes the protection of neurorights aimed at legal reforms (Ruiz & Cayón, 2021) because methods and instruments are used to connect with the nervous system.

The use of neurotechnologies not only considers their therapeutic use but also their ability to stimulate the empowerment capabilities of human beings (Reguera & Cayón, 2021), the main concern of neurotechnology is its integration with AI because it can challenge the essence of the human being.

Likewise, neurotechnology exposes the intimacy of thoughts, emotions, subconscious as well as neuronal activity (Reguera & Cayón, 2021), but the concern of respect for human dignity, rights and fundamental freedoms, the latter due to the law on the protection of personal data, reoccurs. regulation already implemented in most countries around the world, as well as the confidentiality of mental data, personal identity, freedom of thought.

In fact, neurotechnologies related to neurorights are approached from two aspects: mental privacy and the right to privacy where the individuality of people is emphasized, which is why it is crucial that they be addressed by public powers at a regional and international level (Andorno, 2023).

In this way, neurotechnologies go beyond the medical field because they show us the opportunities and challenges in cognitive processes, being able to develop preventive and therapeutic diagnoses, and in that sense neurotechnologies have taken off at the level

[2] UNESCO. (2021). Report of the International Bioethics Comittee of UNESCO (IBC) on ethical issues of neurotechnology. https://clck.ru/3Ct9sj

of Latam and the Caribbean where UNESCO has developed a series of studies that include the human genome together with artificial intelligence

Lately, neurotechnologies have made great advances because, due to big data, large volumes of data have been processed and, together with AI, results are obtained in a short time, allowing the identification of patterns of neural activity or thought reading, where the ethical and legal approach combines two categories: brain images (neuroimaging) and brain-computer interfaces (ICC, BCI) (Andorno, 2023).

1.3. Ethical and legal issues

The objective of neurotechnologies is to investigate neurological mechanisms of mental activity and human behavior to influence them, which leads to ethical and legal situations where they can be regulated according to values and principles of certain disciplines (Andorno, 2023), and for this reason, UNESCO expresses its concern about those groups that request the creation of new neurorights and that undermine the existing ones.

To understand these neurorights a little better, they are mentioned: mental privacy. Mental integrity, personal identity and cognitive freedom.

1.3.1. Mental Privacy

This right is closer to access to mental data that gives rise to neurotechnologies where an attempt is made to protect non-consensual access to your brain data by third parties, as well as the dissemination of the same, whether by advertising companies, insurers, employers, government companies, etc.

This respect is mentioned by international human rights standards that include the confidentiality of personal data, which states that there will be no arbitrary interference in the private life, family, home, honor or reputation of any person (art. 12), as well as supported by the American Convention on Human Rights of 1969 (known as the Pact of San José de Costa Rica) (Andorno, 2023).

However, there is concern that the protection of mental data due to a legal interpretation not provided for in the laws, which is why these regulations need to be clarified to ensure the privacy of said data and thus avoid dichotomies in the opinions of jurists (Reguera & Cayón, 2021; Hertz, 2022; Makin et al., 2020).

Finally, this mental information is of concern because it can be used as biometric data that identifies a person and can be used in the future for mental health issues and cognitive abilities for discrimination purposes (Arellano, 2024).

1.3.2. Mental Integrity

The confidentiality of mental data associated with neurotechnology applications can affect mental integrity due to the damage that could be caused to the psychological dimension of the person, due to the possible ease or access to intentionally alter the electrical stimulation parameters that can cause manipulating brain-computer interface devices. (Hertz, 2022; Alharbi, 2023).

Just as there are negative implications, there are also positive contributions in its use because the so-called "memory engineering" is used to treat diseases such as Alzheimer's or post-traumatic stress, where they can erase memories that justify their disappearance for better mental health of the patient.

1.3.3. Personal Identity

Personal identity is related to the psychological continuity of an individual, whose own characteristics remain over time, being able to recognize themselves and differentiate themselves from others, that is, preserve their essence (Hertz, 2022).

When treatment therapies or procedures are performed that can alter your mental states, they could have consequences in possible changes in your behavior, this due to inappropriate or abusive use of brain stimulation devices, because we are subjects of rights that are protected by international standards.

1.3.4. Cognitive freedom

It is related to mental self-determination, that is, choosing and exercising control over one's own mental states that can be altered or conditioned by third parties without their consent (Hertz, 2022).

The term freedom was used by Wrye Sententia in 2004 (Sententia, 2004), who explains that right and freedom are determined by one's own conscience and thoughts, although Bublitz (Bublitz, 2013) explains that the right to alter and enhance one's own mental states as well as to refuse the use of devices that can manipulate their mental states (Parlatino, 2023, Hertz, 2022).

Cognitive freedom is related to the freedom of thought recognized in Human Rights and it is imperative that it be clarified that said freedom also includes the internal dimension of mental activity (Andorno, 2023; Hertz, 2022).

2. Research methodology

The goal of the current study is to analyze the ethical and social issues surrounding neuro-rights in upcoming neurotechnologies through a thorough evaluation of the literature. Thorough searches were carried out using search engines like Google Scholar and Redib as well as databases including Scielo, Dialnet, Redalyc, Lilacs, Scopus, Medline, and Pubmed.

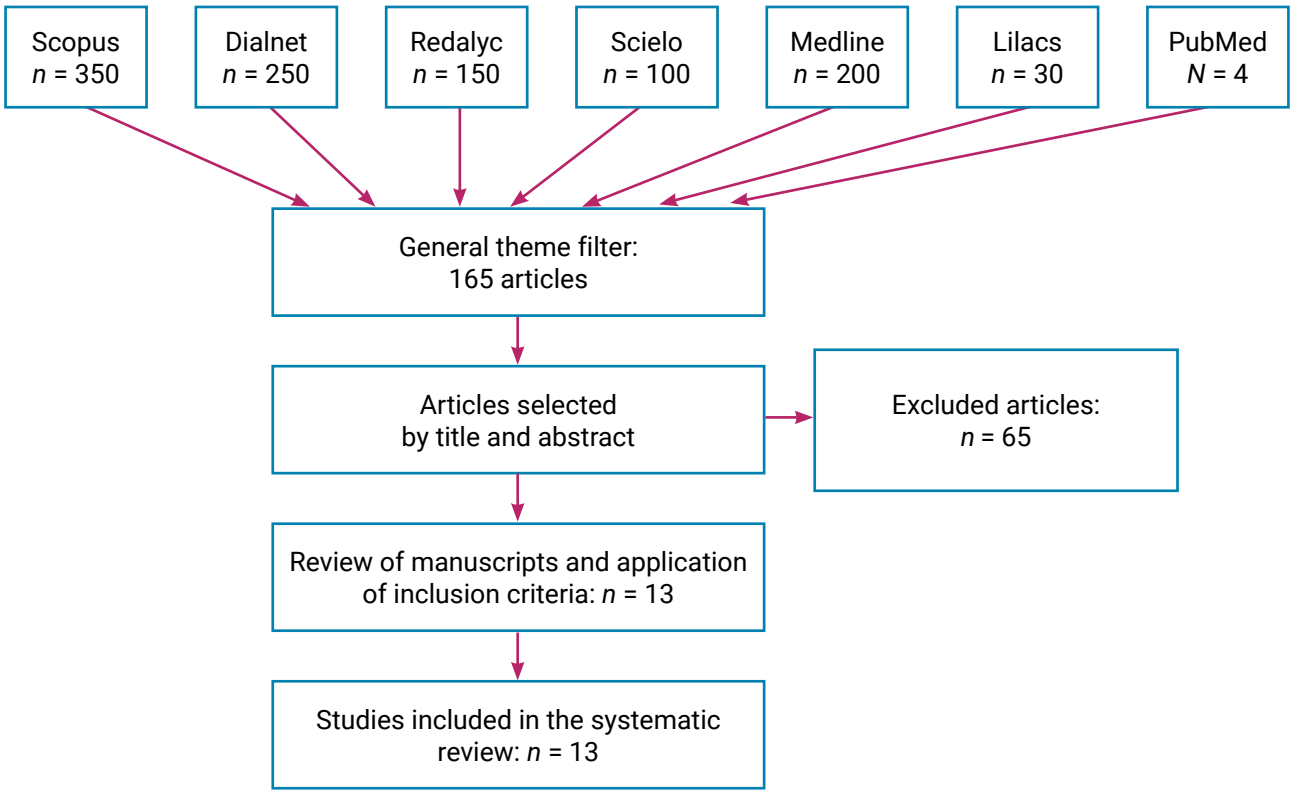


Fig. 1. Own elaboration based on PRISMA-COCHRANE model

Among the search terms were "neurotechnology," "personal data," "mental privacy," "neuro-rights," "neurotechnological interventions," and "neurotechnological discrimination," and they were used to find both English and Spanish sites. The systematic literature review was based on the methodology proposed by a renowned British scholar, a professor emerita of computer science at Keele University Barbara Kitchenham[3], chosen for its flexibility and effectiveness in obtaining results for publication.

2.1. Inclusion and Exclusion criteria

To assess the quality of evidence, only articles and reviews written in English or Spanish (see Table 1) involving institutions, researchers, and personnel related to neuro-rights were considered. Content analysis technique was applied to answer the research question. Duplicate articles, editorial comments, press releases, news, opinions, and clinical recommendations were excluded. Articles were filtered to select the most relevant ones, and full research papers related to neuro-rights in patients were reviewed.

2.2. Population and Sample

The population analyzed was based on the selected research articles that met the inclusion and exclusion criteria established in the design phase, as shown in Table 1.

[3] https://goo.su/PmZdwxj

Table 1 Research on neurorights and neurotechnologies

N	Autor	Theme	Year
1	E. Cáceres, J. Diez, E. García	Neuroethics and neurorights	2021
2	A. R. González	"Neurorights", evidences of neuroscience and guarantees of judicial independence	2021
3	M. Ienca	On Neurorights	2021
4	M. Ienca, R. Andorno	Approaches to new human rights in the era of neuroscience and neurotechnology	2021
5	S. Ruiz, V. Ramos, R. Concha, et al., C. Caneo	Negative effcets of the Law 20.584 and the discussed Law on neurorights for scientific research and medical practice in Chili: urgent need to learn on mistakes	2021
6	Y. V. Bastidas Cid	Neurotechnology: the brain-computer interface and the protection of brain- or neurodata in the context of personal data processing in the European Union	2022
7	C. López, N. Cáceres	Neuroright as a new sphere of human rights protection	2022
8	R. Orias	Neurorights. New frontier in human rights	2022
9	V. E. Rocha Martínez	Neuroright as a new sphere of human rights protection	2022
10	H. Fernández	Neurorights, neurotechnologies and risk management in modernity. Historical analysis, dialectics and holistic approach	2023
11	P. López-Silva, R. Madrid	Protecting the mind: analysis of the concept of the mental in the Law on neurorights	2023
12	J. I. Murillo	On the possibility of mind-reading or the external control of behavior: Contribution of Aquinas to the Neurorights discussion	2023
13	W. Arellano	Neurorights and their regulation	2024

3. Research results

Table 1 shows the number of selected primary studies evidencing the authors' studies and research in the field of neuro-rights and neurotechnology. These studies reflect opinions or criteria regarding the inappropriate handling of patient information, lack of legal security guarantees, and susceptibility to being undervalued, which may potentially result in misuse behaviors and mishandling of information (Borbón et al., 2020).

3.1. Data collection and Analysis

To facilitate and summarize the contents of the selected articles according to the inclusion and exclusion criteria, a Systematic Literature Review was employed. This tool outlines an open and understandable procedure for gathering and choosing various articles and information sources.

Initially, the following search phrases were used in the aforementioned databases: "neuro-rights," "personal data," "mental privacy," "neurotechnological discrimination," and "access to neuroscientific data." 1084 articles in all were acquired. 165 articles that satisfied the selection criteria were selected after the titles and abstracts were reviewed. Following a thorough reading of all the articles, 13 were chosen for the final review.

The literature study made it possible to identify the following rights and issues at the nexus of neuro-rights and personal data:

Challenges:

– Mental Privacy: People's mental privacy may be threatened by the gathering and processing of neuroscientific data.

– Neurotechnological Discrimination: There's a chance that people will be singled out for special treatment because of their unique neurobiological traits.

– Access to Neuroscientific Data: Maintaining the privacy of individuals is as important as advancing scientific research when it comes to access to neuroscientific data.

Rights:

– Right to Mental Privacy: People are entitled to decide how their neuroscientific data is gathered, used, and shared.

– Right to Neurotechnological Non-Discrimination: People are entitled to be treated equally regardless of their neurobiological traits.

– Right to Access Neuroscientific Data: People are entitled to view the neuroscientific data that pertains to them as well as the data that is used to inform judgments about them.

– Right to Mental Identity: The idea of the self in which a person chooses and maintains their personal identity.

– Right to Free Will: The ability to choose for oneself.

3.2. Discussion of the results

Table 2 outlines moral practices that should be taken into account when providing medical care in the area of neuro-rights in order to preserve and uphold patients' liberties and rights.

Table 2 Main principles of rendering medical assistance in the sphere of neurorights

No	Behaviors
A	Honesty
B	Free access
C	Equity
D	Justice
E	Professional secret
F	Information Privacy
G	Integrity
H	Transparency
I	Informed Consent
J	Responsibility

The company FasterCapital[4] highlights the advancements of neurotechnologies in various sectors, such as education and healthcare, driving innovation and improving

[4] Neurotech Startups and the Future of Human Enhancement. URL: https://clck.ru/3DvQTJ

the quality of life for individuals with conditions like ALS, mental health disorders, and communication difficulties. However, it is important to delve into aspects related to privacy, consent, and equitable access to these technologies by service-providing companies. Figure 2 demonstrates the potential for enhancement in human capabilities, based on data provided by FasterCapital.

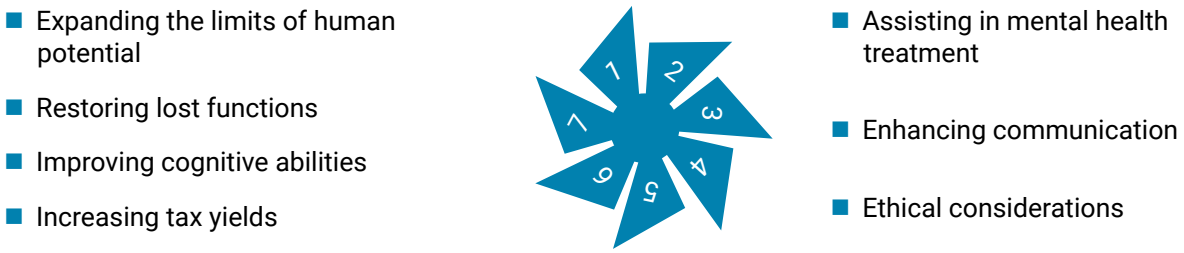


Fig. 2. Understanding the potential of neurotechnologies to improve human capabilities

The systematic review provides scientific evidence of the positive impact of neurotechnologies in treating diseases such as Parkinson's, Alzheimer's, psychosis, dementia, and sensory and motor functions of the central nervous system, as well as in pain medicine. Neurotechnological interventions may represent an effective treatment option for individuals with mental disorders who do not respond to traditional treatments. However, further research is needed to confirm these results and assess the long-term safety and efficacy of such interventions (Andorno, 2023; Ruiz et al., 2021).

The results obtained from the Systematic Literature Review underscore the need to ethically address the challenges posed by neurotechnologies in the realm of regulations, as mentioned in each of the studies included in this research. There is a call for expanding the literature related to neurotechnologies to protect individual rights (Andorno, 2023; Arellano, 2024; Cid, 2022; Borbón et al., 2020; Cáceres et al., 2021; Fernández, 2023; Goering et al., 2021; Baselga-Garriga et al., 2022).

Additionally, several authors propose basic deontological principles that incorporate respect and assistance to others, thereby promoting ethics in the use of neurotechnologies. In this regard, the Organization of American States (OAS) develops an educational program centered on values that fosters the socialization of attitudes and norms to create new constructs that promote harmony among all involved parties.

Conclusions

In conclusion, existing regulatory frameworks must adapt to address the ethical and social challenges posed by emerging neurotechnologies. Ensuring the preservation of individual rights, privacy, and mental autonomy requires the establishment of policies and regulations.

Moreover, increased cooperation between organizations, scientists, and businesses is necessary for the responsible development and use of neurotechnologies. This entails encouraging openness, informed permission, and fairness in the use of these technologies.

Evidence of the potential advantages of neurotechnologies in treating a range of illnesses and mental health issues may be found in the systematic literature review. Nonetheless, more investigation is required to assess their long-term efficacy and safety.

The significance of enlightening the public about the moral and legal implications of neurotechnologies is also emphasized. In the area of applied neuroscience, this entails advancing deontological ideas that support the respect and defense of human rights.

In conclusion, as new neurotechnologies arise, regulatory frameworks must adapt to meet the ever-changing moral and societal issues they raise. To guarantee that these technologies be used morally and responsibly for the good of society, multidisciplinary cooperation and a proactive attitude are needed.

References

Alharbi, H. (2023). Identifying thematics in a brain-computer interface research. *Computational Intelligence and Neuroscience*, *4*, 2793211. https://doi.org/10.1155/2023/2793211

Andorno, R. (2023). *Neurotecnologías Y Derechos Humanos En América Latina Y El Caribe: Desafíos Y Propuestas De Política Pública*. University of Zurich; UNESCO. (In Spain). https://doi.org/10.5167/uzh-237729

Arellano, W. (2024). Los Neuroderechos y su Regulación. *Inteligencia Artificial*, *27*(73), 4–13. (In Spain). https://doi.org/10.4114/intartif.vol27iss73pp4-13

Barrios, L., Minguillón, J., Perales, F., Ron-angevin, R., Solé, J., & Mañanas, M. (2017). Estado del Arte en Neurotecnologías para la asistencia y la Rehabilitación en España: Tecnologías Auxiliares, Transferencia Tecnológica y Aplicación Clínica. *Revista Iberoamericana de Automática e Informática Industrial RIAI*, *14*(4) 355–361. (In Spain). https://doi.org/10.1016/j.riai.2017.06.004

Cid, Ya. V. B. (2022). Neurotecnología: Interfaz cerebro-computador y protección de datos cerebrales o neurodatos en el contexto del tratamiento de datos personales en la Unión Europea. *Informática y Derecho*, *11*. (In Spain).

Baselga-Garriga, C., Rodriguez, P., & Yuste, R. (2022). Neuro Rights: A Human Rights Solution to Ethical Issues of Neurotechnologies. In P. López-Silva, & L. Valera (Eds.), *Protecting the Mind. Ethics of Science and Technology Assessment* (Vol. 49). Springer, Cham. https://doi.org/10.1007/978-3-030-94032-4_13

Bastidas Cid, Y. V. (2022). Neurotecnología: Interfaz cerebro-computador y protección de datos cerebrales o neurodatos en el contexto del tratamiento de datos personales en la Unión Europea. *Informática Y Derecho. Revista Iberoamericana De Derecho Informático (2.ª época)*, *11*, 101–182.

Borbón, D., & Borbón, L. (2022). NeuroDerechos Humanos y Neuroabolicionismo Penal. *Cuestiones Constitucionales*, *1*(46), 29–64. (In Spain). https://doi.org/10.22201/iij.24484881e.2022.46.17047

Borbón, D., Borbón, L., & Laverde, J. (2020). Análisis crítico de los NeuroDerechos Humanos al libre albedrío y al acceso equitativo a tecnologías de mejora. *Ius Et Scientia*, *6*(2), 135–161. (In Spain). https://doi.org/10.12795/ietscientia.2020.i02.10

Bublitz J-C. (2013). My Mind is Mine!? Cognitive Liberty as a Legal Concept. In: Hildt E., & Franke A. (Eds.), *Cognitive Enhancement. An Interdisciplinary Perspective* (pp. 233–264). Dordrecht: Springer.

Cáceres, E., Diez, J., & García, E. (2021). Neuroética y NeuroDerechos. *Revista del Posgrado en Derecho de la UNAM*, *1*, 37–86. (In Spain). https://doi.org/10.22201/ppd.26831783e.2021.15.179

Cáceres, E. & López, C. (2022). El neuroderecho como un nuevo ámbito de protección de los derechos humanos. *Cuestiones Constitucionales*, *1*(46), 65–92. (In Spain). https://doi.org/10.22201/iij.24484881e.2022.46.17048

Clausen, J. E., Fetz, J., Donoghue, J., Ushiba, J., Spörhase, U., Chandler, J., Birbaumer, N., & Soekadar, S. R. (2017). Help, hope, and hype: Ethical dimensions of neuroprosthetics. Accountability, responsibility, privacy, and security are key. *Science*, *356*(6345), 1338–1339. https://doi.org/10.1126/science.aam7731

Cornejo-Plaza, M. I., Cippitani, R., & Pasquino, V. (2024). Chilean Supreme Court ruling on the protection of brain activity: neurorights, personal data protection, and neurodata. *Frontiers in Psychology*, *15*. https://doi.org/10.3389/fpsyg.2024.1330439

Filipova, I. A. (2022). Neurotechnologies in law and law enforcement: past, present and future. *Law Enforcement Review*, *6*(2), 32–49. https://doi.org/10.52468/2542-1514.2022.6(2).32-49

Fernández, H. (2023). Neuroderechos, neurotecnologías y administración de riesgos en la modernidad, Análisis histórico, dialéctica Holismo. *Tzhoen*, *15*(1), 99–112. (In Spain). https://doi.org/10.26495/tzh.v15i1.2457

Fukushi, T. (2024). East Asian perspective of responsible research and innovation in neurotechnology. *IBRO Neuroscience Reports*, *16*, 582–597. https://doi.org/10.1016/j.ibneur.2024.04.009

Goering, S., Klein, E., Specker Sullivan, L. et al. (2021). Recommendations for Responsible Development and Application of Neurotechnologies. *Neuroethics*, *14*, 365–386. https://doi.org/10.1007/s12152-021-09468-6

Gómez, R. M. (2021). Inteligencia artificial y neuroderechos. Retos y perspectivas. *Cuestiones Constitucionales*, *1*(46), 93–119. (In Spain). https://doi.org/10.22201/iij.24484881e.2022.46.17049

González, A. R. (2021). "Neuroderechos", prueba neurocientífica y garantía de independencia judicial. *Derecho & Sociedad*, *57*, 1–26. (In Spain). https://doi.org/10.18800/dys.202102.007

Hertz, N. (2022). Neurorights – Do we Need New Human Rights? A Reconsideration of the Right to Freedom of Thought. *Neuroethics*, *16*, 5. https://doi.org/10.1007/s12152-022-09511-0

Hsu, J. (2024). Privacy concerns over brain monitors. *The New Scientist*, *262*(3490), 10. https://doi.org/10.1016/s0262-4079(24)00850-9

Ienca, M. (2021). On Neurorights. *Frontiers in Human Neuroscience*, *15*, 701258. https://doi.org/10.3389/fnhum.2021.701258

Ienca, M., & Andorno, R. (2021). Hacia nuevos derechos humanos en la era de la neurociencia y la neurotecnología. *Análisis Filosófico*, *41*(1), 141–185. (In Spain). https://doi.org/10.36446/af.2021.386

López, C., & Cáceres, E. (2022). El neuroderecho como un nuevo ámbito de protección de los derechos humanos. *Cuestiones Constitucionales*, *46*. (In Spain). https://doi.org/10.22201/iij.24484881e.2022.46.17048

López-Silva, P., & Madrid, R. (2022). Protecting the Mind: An Analysis of the Concept of the Mental in the Neurorights Law. *Revista De Humanidades De Valparaíso*, *20*, 101–117. http://dx.doi.org/10.22370/rhv2022iss20pp101-117

Makin, J. G., Moses, D. A., & Chang, E. F. (2020). Machine translation of cortical activity to text with an encoder-decoder framework. *Nature Neuroscince*, *23*, 575–582. https://doi.org/10.1038/s41593-020-0608-8

Moreu, C. E. (2022). La Reulación de los neuroderechos. *Revista General de Legislación y Jurisprudencia*, *1*, 69–98. (In Spain). https://doi.org/10.30462/rglj-2022-01-04-840

Murillo, J. I. (2023). On the possibility of mind-reading or the external control of behavior: Contribution of Aquinas to the Neurorights discussion. *Scientia et Fides*, *11*(2), 87–105. https://doi.org/10.12775/SetF.2023.017.

Orias, R. (2022). Los neuroderechos. Una nueva frontera para los derechos humanos. *Agenda Internacional*, *XXIX*(40), 211–227. (In Spain). https://doi.org/10.18800/agenda.202201.009

Parlatino. (2023). *Ley modelo de Neuroderechos para América Latina y el Caribe*. (In Spain).

Reguera, A. M., & Cayón, J. (2021). La Garantía de los Neuroderechos: A propósito de las iniciativas emprendidas para su reconocimiento. *Derecho y salud*, *31*(1), 213–222. (In Spain).

Rocha Martínez, V. E. (2022). Nuevos derechos del ser humano. *Cuestiones Constitucionales. Revista Mexicana De Derecho Constitucional*, *1*(46), 251–277. https://doi.org/10.22201/iij.24484881e.2022.46.17055

Ruiz, S., Ramos, P., & et al, Caneo, C. (2021). Efectos negativos en la investigación y el quehacer médico en Chile de la Ley 20.584 y la Ley de Neuroderechos en discusión: la urgente necesidad de aprender de nuestros errores. *Revista médica de Chile*, *149*(3). (In Spain). http://dx.doi.org/10.4067/s0034-98872021000300439

Sententia, W. (2004). Neuroethical Considerations: cognitive liberty and converging technologies for improving human cognition. Annals of the New York Academy of Sciences, 1013(1), 221–228. https://doi.org/10.1196/annals.1305.014

Author information

Yan Cornejo – Magister, CEO of Academia Cibers, Private Consultant Data Privacy, Independent Researcher
Address: La Fae mz 32 villa 18, Guayaquil, Ecuador
E-mail: yancornejo@yahoo.com
ORCID ID: https://orcid.org/0000-0003-0373-1581
WoS Researcher ID: https://www.webofscience.com/wos/author/record/KWU-8753-2024
Google Scholar ID: https://scholar.google.com/citations?user=clFiXCsAAAAJ

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – May 9, 2024
Date of approval – May 29, 2024
Date of acceptance – September 25, 2024
Date of online placement – September 30, 2024

Научный обзор
УДК 34:004:347.211:004.383.8.032.26
EDN: https://elibrary.ru/sperfj
DOI: https://doi.org/10.21202/jdtl.2024.36

Нейроправа, нейротехнологии и персональные данные: обзор проблем психологической автономии

Ян Корнехо

Независимый исследователь, Гуаякиль, Эквадор

Ключевые слова

законодательство,
нейроправа,
нейротехнологии,
неприкосновенность частной жизни,
персональные данные,
права человека,
право,
психологическая автономия,
цифровые технологии,
этика

Аннотация

Цель: представить результаты проведенного систематического обзора исследований влияния нейротехнологий на юридические концепции и нормативную правовую базу, направленные на решение этических и социальных проблем, связанных с защитой индивидуальных прав, неприкосновенности частной жизни и психологической автономии.

Методы: систематический обзор литературы проводился по методологии, предложенной известным британским ученым – почетным профессором Университета Кила Барбарой Китченхэм, отличающейся гибкостью и эффективностью в получении результатов. Поиск осуществлялся на англо- и испаноязычных сайтах по ключевым словам («нейротехнологии», «персональные данные», «психологическая конфиденциальность», «нейроправа», «нейротехнологические вмешательства» и «нейротехнологическая дискриминация») с использованием таких поисковых систем, как Google Scholar и Redib, а также баз данных Scielo, Dialnet, Redalyc, Lilacs, Scopus, Medline и Pubmed. Фокус данного исследования – библиометрические данные — характеризуется как неэкспериментальный, кросс-секционный и описательный с применением контент-анализа на основе модели PRISMA.

Результаты: в представленном исследовании подчеркивается необходимость установления четких этических принципов, защищающих права личности и способствующих ответственному использованию нейротехнологий; выявлен ряд проблем психологической автономии, таких как ненадлежащее обращение с информацией, отсутствие гарантий юридической безопасности, нарушение прав и свобод на примере отношений в медицинской сфере. Исследование показывает необходимость адаптации существующей нормативной правовой базы для решения этических и социальных проблем, возникающих в связи с появлением новых нейротехнологий. Отмечается, что широкое исследование вопросов в сфере нейротехнологий будет способствовать защите прав человека.

Научная новизна: предложено расширенное понимание пяти нейроправ в рамках Всеобщей декларации прав человека; нейроправа представлены как новая категория прав, направленных на защиту психологической целостности от неправомерного использования нейротехнологий; обосновано принятие таких принципов технократии, как личная идентичность, свобода воли, психологическая конфиденциальность, равноправный доступ и защита от предвзятости.

Практическая значимость: полученные результаты имеют значение для понимания современных юридических концепций, связанных с нейроправами, адаптации существующих нормативных правовых актов для решения этических и социальных проблем, возникающих в связи с появлением новых технологий, защиты нейроправ человека и ответственности за их нарушение. Исследование данной проблемы имеет ключевое значение для обеспечения дальнейшего ответственного развития и применения нейротехнологий.

Для цитирования

Корнехо, Я. (2024). Нейроправа, нейротехнологии и персональные данные: обзор проблем психологической автономии. *Journal of Digital Technologies and Law*, *2*(3), 711–728. https://doi.org/10.21202/jdtl.2024.36

Список литературы

Alharbi, H. (2023). Identifying thematics in a brain-computer interface research. *Computational Intelligence and Neuroscience*, *4*, 2793211. https://doi.org/10.1155/2023/2793211

Andorno, R. (2023). *Neurotecnologías Y Derechos Humanos En América Latina Y El Caribe: Desafíos Y Propuestas De Política Pública*. University of Zurich; UNESCO. https://doi.org/10.5167/uzh-237729

Arellano, W. (2024). Los Neuroderechos y su Regulación. *Inteligencia Artificial*, *27*(73), 4–13. https://doi.org/10.4114/intartif.vol27iss73pp4-13

Barrios, L., Minguillón, J., Perales, F., Ron-angevin, R., Solé, J., & Mañanas, M. (2017). Estado del Arte en Neurotecnologías para la asistencia y la Rehabilitación en España: Tecnologías Auxiliares, Transferencia Tecnológica y Aplicación Clínica. *Revista Iberoamericana de Automática e Informática Industrial RIAI*, *14*(4) 355–361. https://doi.org/10.1016/j.riai.2017.06.004

Cid, Ya. V. B. (2022). Neurotecnología: Interfaz cerebro-computador y protección de datos cerebrales o neurodatos en el contexto del tratamiento de datos personales en la Unión Europea. *Informática y Derecho*, *11*.

Baselga-Garriga, C., Rodriguez, P., & Yuste, R. (2022). Neuro Rights: A Human Rights Solution to Ethical Issues of Neurotechnologies. In P. López-Silva, & L. Valera (Eds.), *Protecting the Mind. Ethics of Science and Technology Assessment* (Vol. 49). Springer, Cham. https://doi.org/10.1007/978-3-030-94032-4_13

Bastidas Cid, Y. V. (2022). Neurotecnología: Interfaz cerebro-computador y protección de datos cerebrales o neurodatos en el contexto del tratamiento de datos personales en la Unión Europea. *Informática Y Derecho. Revista Iberoamericana De Derecho Informático (2.ª época)*, *11*, 101–182.

Borbón, D., & Borbón, L. (2022). NeuroDerechos Humanos y Neuroabolicionismo Penal. *Cuestiones Constitucionales*, *1*(46), 29–64. https://doi.org/10.22201/iij.24484881e.2022.46.17047

Borbón, D., Borbón, L., & Laverde, J. (2020). Análisis crítico de los NeuroDerechos Humanos al libre albedrío y al acceso equitativo a tecnologías de mejora. *Ius Et Scientia*, *6*(2), 135–161. https://doi.org/10.12795/ietscientia.2020.i02.10

Bublitz J-C. (2013). My Mind is Mine!? Cognitive Liberty as a Legal Concept. In: Hildt E., & Franke A. (Eds.), *Cognitive Enhancement. An Interdisciplinary Perspective* (pp. 233–264). Dordrecht: Springer.

Cáceres, E., Diez, J., & García, E. (2021). Neuroética y NeuroDerechos. *Revista del Posgrado en Derecho de la UNAM*, *15*, 37–86. https://doi.org/10.22201/ppd.26831783e.2021.15.179

Cáceres, E. & López, C. (2022). El neuroderecho como un nuevo ámbito de protección de los derechos humanos. *Cuestiones Constitucionales*, *1*(46), 65–92. https://doi.org/10.22201/iij.24484881e.2022.46.17048

Clausen, J. E., Fetz, J., Donoghue, J., Ushiba, J., Spörhase, U., Chandler, J., Birbaumer, N., & Soekadar, S. R. (2017). Help, hope, and hype: Ethical dimensions of neuroprosthetics. Accountability, responsibility, privacy, and security are key. *Science*, *356*(6345), 1338–1339. https://doi.org/10.1126/science.aam7731

Cornejo-Plaza, M. I., Cippitani, R., & Pasquino, V. (2024). Chilean Supreme Court ruling on the protection of brain activity: neurorights, personal data protection, and neurodata. *Frontiers in Psychology*, *15*. https://doi.org/10.3389/fpsyg.2024.1330439

Filipova, I. A. (2022). Neurotechnologies in law and law enforcement: past, present and future. *Law Enforcement Review*, *6*(2), 32–49. https://doi.org/10.52468/2542-1514.2022.6(2).32-49

Fernández, H. (2023). Neuroderechos, neurotecnologías y administración de riesgos en la modernidad, Análisis histórico, dialéctica Holismo. *Tzhoen*, *15*(1), 99–112. https://doi.org/10.26495/tzh.v15i1.2457

Fukushi, T. (2024). East Asian perspective of responsible research and innovation in neurotechnology. *IBRO Neuroscience Reports*, *16*, 582–597. https://doi.org/10.1016/j.ibneur.2024.04.009

Goering, S., Klein, E., Specker Sullivan, L. et al. (2021). Recommendations for Responsible Development and Application of Neurotechnologies. *Neuroethics*, *14*, 365–386. https://doi.org/10.1007/s12152-021-09468-6

Gómez, R. M. (2021). Inteligencia artificial y neuroderechos. Retos y perspectivas. *Cuestiones Constitucionales*, *1*(46), 93–119. https://doi.org/10.22201/iij.24484881e.2022.46.17049

González, A. R. (2021). "Neuroderechos", prueba neurocientífica y garantía de independencia judicial. *Derecho & Sociedad*, *57*, 1–26. https://doi.org/10.18800/dys.202102.007

Hertz, N. (2022). Neurorights – Do we Need New Human Rights? A Reconsideration of the Right to Freedom of Thought. *Neuroethics*, *16*, 5. https://doi.org/10.1007/s12152-022-09511-0

Hsu, J. (2024). Privacy concerns over brain monitors. *The New Scientist*, *262*(3490), 10. https://doi.org/10.1016/s0262-4079(24)00850-9

Ienca, M. (2021). On Neurorights. *Frontiers in Human Neuroscience*, *15*, 701258. https://doi.org/10.3389/fnhum.2021.701258

Ienca, M., & Andorno, R. (2021). Hacia nuevos derechos humanos en la era de la neurociencia y la neurotecnología. *Análisis Filosófico*, *41*(1), 141–185. https://doi.org/10.36446/af.2021.386

López, C., & Cáceres, E. (2022). El neuroderecho como un nuevo ámbito de protección de los derechos humanos. *Cuestiones Constitucionales*, *46*. https://doi.org/10.22201/iij.24484881e.2022.46.17048

López-Silva, P., & Madrid, R. (2022). Protecting the Mind: An Analysis of the Concept of the Mental in the Neurorights Law. *RHV*, *20*, 101–117. http://dx.doi.org/10.22370/rhv2022iss20pp101-117

Makin, J. G., Moses, D. A., & Chang, E. F. (2020). Machine translation of cortical activity to text with an encoder-decoder framework. *Nature Neuroscince*, *23*, 575–582. https://doi.org/10.1038/s41593-020-0608-8

Moreu, C. E. (2022). La Reulación de los neuroderechos. *Revista General de Legislación y Jurisprudencia*, *1*, 69–98. https://doi.org/10.30462/rglj-2022-01-04-840

Murillo, J. I. (2023). On the possibility of mind-reading or the external control of behavior: Contribution of Aquinas to the Neurorights discussion. *Scientia et Fides*, *11*(2), 87–105. https://doi.org/10.12775/SetF.2023.017.

Orias, R. (2022). Los neuroderechos. Una nueva frontera para los derechos humanos. *Agenda Internacional*, *XXIX*(40), 211–227. https://doi.org/10.18800/agenda.202201.009

Parlatino. (2023). *Ley modelo de Neuroderechos para América Latina y el Caribe*. (In Spain).

Reguera, A. M., & Cayón, J. (2021). La Garantía de los Neuroderechos: A propósito de las iniciativas emprendidas para su reconocimiento. *Derecho y salud*, *31*(1), 213–222.

Rocha Martínez, V. E. (2022). Nuevos derechos del ser humano. *Cuestiones Constitucionales. Revista Mexicana De Derecho Constitucional*, *1*(46), 251–277. https://doi.org/10.22201/iij.24484881e.2022.46.17055

Ruiz, S., Ramos, P., & et al, Caneo, C. (2021). Efectos negativos en la investigación y el quehacer médico en Chile de la Ley 20.584 y la Ley de Neuroderechos en discusión: la urgente necesidad de aprender de nuestros errores. *Revista médica de Chile*, *149*(3). https://dx.doi.org/10.4067/s0034-98872021000300439

Sententia, W. (2004). Neuroethical Considerations: cognitive liberty and converging technologies for improving human cognition. Annals of the New York Academy of Sciences, 1013(1), 221–228. https://doi.org/10.1196/annals.1305.014

Сведения об авторе

Ян Корнехо – магистр, генеральный директор компании Academia Cibers, консультант по проблемам персональных данных, независимый исследователь
Адрес: Эквадор, г. Гуаякиль, ул. Ла Фае зм 32, 18
E-mail: yancornejo@yahoo.com
ORCID ID: https://orcid.org/0000-0003-0373-1581
WoS Researcher ID: https://www.webofscience.com/wos/author/record/KWU-8753-2024
Google Scholar ID: https://scholar.google.com/citations?user=clFiXCsAAAAJ

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.07.45 / Право и научно-технический прогресс
Специальность ВАК: 5.1.2 / Публично-правовые (государственно-правовые) науки

История статьи

Дата поступления – 9 мая 2024 г.
Дата одобрения после рецензирования – 29 мая 2024 г.
Дата принятия к опубликованию – 25 сентября 2024 г.
Дата онлайн-размещения – 30 сентября 2024 г.