ISSN 2949-2483

Volume 1 Number 3

JOURNAL OF DIGITAL TECHNOLOGIES AND LAW

2023

ELECTRONIC SCIENTIFIC AND PRACTICAL JOURNAL

JOURNAL OF DIGITAL TECHNOLOGIES AND LAW

Volume 1, № 3
2023

DOI: 10.21202/2949-2483.2023.3

ELECTRONIC SCIENTIFIC AND PRACTICAL JOURNAL

eISSN 2949-2483

Published since 2023, frequency – 4 issues a year. DOI: 10.21202/2949-2483

Editorial Board

Editorial

Head of the editorial office – Gulnaz Ya. Darchinova
Executive editor – Oksana A. Aymurzaeva
Executive secretary – Anastasiya D. Lapshina
Editor – Gulnara A. Tarasova
Technical editor – Svetlana A. Karimova
Designer – Gulnara I. Zagretdinova
Translator – Elena N. Belyaeva, PhD (Pedagogy), member of the Guild of Translators and Interpreters of the Republic of Tatarstan
Specialist in the promotion of the journal on the internet – Polina S. Gulyaeva

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, Russian Federation. Tel.: +7 (843) 231-92-90. Fax: +7 (843) 292-61-59. E-mail: info@ieml.ru. Website: https://ieml.ru

Date of signing the issue for publication: 2023, August 15. Hosted on the website https://www.lawjournal.digital: 2023, August 20.

JOURNAL OF DIGITAL TECHNOLOGIES AND LAW
Том 1, № 3
2023
DOI: 10.21202/2949-2483.2023.3
ELECTRONIC SCIENTIFIC AND PRACTICAL JOURNAL
eISSN 2949-2483

Content

Research article
DOI: https://doi.org/10.21202/jdtl.2023.25

Risks and Prospects of Creativity Tokenization

Ruslan A. Budnik

National Research University "Higher School of Economics"
Moscow, Russian Federation;
Shenzhen MSU-BIT University
Shenzhen, China

Keywords

Art,
blockchain,
creativity,
digital technologies,
law,
music,
NFT,
token,
tokenization,
work of art

Abstract

Objective: tokenization of creativity, alongside with cryptoeconomy and Web3 network infrastructure, is a notable trend in the development of modern society in the third decade of the 21st century. The objective of this article is to explore the risks and prospects emerging in the process of disposition of the creative labor results in the form of non-fungible tokens.

Methods: the research methodology is based on analysis of varied viewpoints on the problem, including diametrically opposing concepts. The opposing views of the observers manifest their attitude to tokenization of creative products as a speculative scheme, on the one hand, and a promising tool of creative industries development, on the other.

Results: the probable negative consequences of tokenization of intellectual activity results are identified; author's recommendations on managing these risks are given. Another result of this publication is analysis of economic-legal prospects stemming from tokenization of the objects of copyright and neighboring rights by the example of musical pieces.

Scientific novelty: it consists in presenting and substantiating a hypothesis that the relations formed in the musical industry under the modern sociocultural and technological realities will be reproduced in other creative industries. Also, scientific novelty consists in the analysis of prospects of tokenization of such results of intellectual activity as gaming artifacts, works of traditional and digital visual arts, patents and scientific achievements. The use of non-fungible tokens the ecosystem of network computer games will allow gamers

to buy and sell rights to game pieces autonomously from game publishers. Tokenization of industrial property objects and individualization means will ensure protection of intellectual rights of their authors while waiting for the issuance of a state protection document. In the modern society, there will be many of those wishing to become an owner of a token for a scientific work, as the popularity of science and innovations is constantly growing in developed countries. Ownership of a token for a scientific work will be regarded a moral investment, increasing the prestige and status of its owner. Tokens for scientific works have a high potential as a means of measuring value in a post-economic society.

Practical significance: it consists in the description of innovative means of using creative products and business models based on tokenization of the results of intellectual activity, ready to be implemented in practice.

For citation

Budnik, R. A. (2023). Risks and Prospects of Creativity Tokenization. *Journal of Digital Technologies and Law, 1*(3), 587–611. https://doi.org/10.21202/jdtl.2023.25

Contents

Introduction

One of the most notable trends of the third decade of the 21st century is shaping of cryptoeconomy and network infrastructure Web3 (Momtaz, 2022; Goel et al., 2022; Jelil, 2022).

Web3 is the next stage of the Internet development, aimed at implementing the functions, which earlier were not imposed on the global information-communication infrastructure (Murray et al., 2023). In particular, this is about reliable registration of property right, storing information on commercial transactions, legal status of things and nonmaterial objects in a decentralized distributed ledger with the degree

of reliability exceeding manifold the centralized and proprietary systems. Web3 reduces the possibility of external control and illegal use of users' private data, as they are stored in a decentralized network, not on centralized servers (Petcu et al., 2023). In practice, Web3 technologies are represented in the form of cryptocurrencies, non-fungible tokens (NFTs), decentralized applications and services, smart contracts, and metaverse prototypes.

Cryptoeconomy, just like Web3, is a multidimensional concept. On the one hand, cryptoeconomy is a branch of information science that solves the problems of coordination between participants in digital ecosystems through cryptography and economic incentives. On the other hand, cryptoeconomy is not a part of traditional economy but an integrity of post-economic institutions forming an ecosystem comprising the game theory, mathematical methods of modeling functions, mechanisms for designing and implementing useful services, virtual assets, game values and utilitarian digital rights (Yue et al., 2021). In addition, cryptoeconomy changes the purpose and meaning of fundamental economic institutions, such as money, assets, own and loan capital, corporate organization, production incentives, risk sharing and attitude to traditional financial tools (Chey, 2022). An example is relevant of blurring the boundaries between the concepts of debt and equity capital. Such financial technologies as convertible bonds, preferred shares, and total return swaps are something in between loan and equity means: they open new opportunities for attracting and using investments. Issuance of tokens for a present or future virtual asset or a startup idea provides funding which is neither loan nor equity capital but has certain features of both.

An important element of cryptoeconomy and Web3 infrastructure are non-fungible tokens (Wilson et al., 2022). A catchword "tokenization" refers to the process of transforming an asset into a digital token. This digital token is a small fragment of a program code recorded into a distributed ledger (blockchain) and serving as a title of perfection of the asset; it also contains technological attributes about its belonging to the system that supports transactions with it. A token may be transferred between users without intermediaries, i. e. it is an object of commercial turnover, the legal content of which are property rights to the tokenized asset registered by means of a smart contract.

One of the variants of using tokenization is real estate where the total value of property is divided and redistributed in tokens. These tokens allow investors to enter the market and to purchase specific plots of real estate quickly and cheaply (Far et al., 2022). In other words, tokenization lowers the entry barriers, eliminates intermediaries' fees and costs, and increases the asset liquidity, providing more flexibility and safety for investors. Besides real estate, tokenization can be applied to almost any assets, such as securities, shares, precious metals, intellectual property, licensing rights, selling tickets and visual arts (Kraizberg, 2023).

In this research, we focus on tokenized results of creative activity, as they most vividly highlight the positrive and negative aspects, as well as contradictions of this phenomenon. To obtain profit, right holders of copyright and neighbouring rights to tokenized objects acts in completely opposite ways in relation to traditional copyright mechanisms. In particular, the NFT market is contstructed in such a way that the price of a token for a work of art is based on a consensus value of the work of art, i. e. based on the perception of the creative product value by its target audience. Thus, users obtain an opportunity of unobstructed access and, as a minimum, noncommercial use of the work of art without paying money for the obtained privileges.

By present, the arsenal of token purchasers comprises a wide range of innovative ways of their monetization, not related to restricting access to the work of art (Okediji, 2017); however, they are usually collateral, not direct as a goods or an access code exchanged for money. They are sold in adjacent markets – those of attention, impressions, advertising, merch[1]; they require special skills – using the techniques of search optimization and digital marketing; creating unique resources – organization and development of thematic internet communities, or special conditions, such as forming an intra-group demand, outside of which they do not work (Colicev, 2023).

1. Methodology of researching tokenization of creativity

The methodology of this work is built on considering opposing opinions on creativity tokenization. The first group of observers is convinced that an NFT market is something similar to a financial pyramid, a scheme for deceiving people by selling them a nonexistent value through abuse of trust.

The second approach, on the contrary, postulates a positive effect of tokenization of creative industries. Proponents of this system of views analyze and construct promising business models and patterns of extracting profit from tokenized works of art to reward their authors and provide earnings to token holders. Proponents of such view argue that tokenization eliminates intermediaries between creators, users and right acquirers, reduces transaction costs and fees in this market, and strengthens relations between authors and their audience.

A detailed forecast of consequences of creativity tokenization was made based on music industry. It was noted that, due to the specificity of this art and, especially, its popular genres, it most vividly highlights the unfolding evolutionary processes, which are further implemented in other creative spheres as well (Henry, 2007). Also, the prospects of tokenization are considered regarding scientific works, patents to industrial property, pieces of analog and digital fine arts, artifacts of computer games industry and online gaming.

[1] "Merch" is a slang word for "merchandise" ("goods, attributes, trading"), which means official products with symbols of music bands, individual performers, sport teams, movies, etc.

2. NFT as a sociotechnical fraud

According to one of viewpoints, the market of non-fungible tokens for objects of digital art is a financial scheme of deceit using information-technical means, aimed at inflicting property harm in compliance with Article 165 of the Criminal Code of the Russian Federation[2] (further – CC RF) or fraud as defined by Article 159 CC RF[3], which may soon cease to exist (Walker, 2022; Scharfman, 2023).

According to this viewpoint, a buyer acts unreasonably buying NFT in a speculative unstructured market and will ultimately highly likely lose their money. To substantiate this position, more or less convincing arguments are given, which are worth considering in detail.

The first reason stated by NFT critics is the lacking material constituent of the goods, i. e. a token purchaser does not obtain a physical carrier with the object of copyright or neighboring rightsc. This argument seems shallow and unconvincing in the sense that the results of intellectual activity are all nonmaterial or intangible, which has not been impeding the development of the market of intellectual property rights for over three hundred years. During all this period, the doctrine is flawlessly working, which implies that the right to possessing the thing, in which the result of intellectual activity is expressed, is detached from the copyright to the work of art.

The second argument is that the possibility to copy works of art depreciates both the copies and the original. Dwelling upon this argument, one should add that, with the permission of the rights holder, there is a potential opportunity to make an infinite number of derivative works. Legitimately created derivative works obtain their own protection; thus, they actually decrease the rarity of the original, which, according to some analysts, depreciates the original as well (Hilko, 2021). This argument seems more consistent from the viewpoint of both the intellectual property rights and economics of material product, characteristic for the industrial period of civilization development, in which the resource value is a function of its rarity.

The third argument is of world-outlook character and, in our opinion, it should not be qualified as deceit or fraud. These are situations when a person joins or gets access to a certain social group, within which a specific system of values is functioning. Within such a community, a high artistic value and commercial value may belong to such works, while external observers may considered their virtues questionable and the price of rights to them obviously inflated. Nevertheless, people become imbued by the opinions of the group, make impulse purchases, and then regret about their actions, if the price of the token did not grow, as was forecasted by the “enlightened” community members,

---

2 Criminal Code of the Russian Federation No. 63-FZ of June 13, 1996 (1996). *Collection of legislation of the Russian Federation*, No. 25, Article 2954.

3 *Ibid*.

but fell. However, if we turn to the legal definition of fraud, we will see that there is no corpus delicti of fraud in the actions of the community members who made a promising estimation or recommended a neophyte to make the deal. This action can be compared to an unsuccessful stock market game using erroneous recommendations, which implies the risk of losses; a token purchaser should be aware of that and manifest reasonable diligence.

Below we give the examples of malicious acts using non-fungible tokens which may be qualified as theft of property, unlawful acquisition of rights to it, violation of copyright, and inflicting property harm by deceit or abuse of trust.

The first method of deceit can be characterized as fraud with a "dummy". Developers advertise and sell tokens for an object of digital art or a whole collection of such, but after getting money from investors or token purchasers reject their obligations and disappear without developing anything or launching to the market. Organizers of such scheme often use social networks to actively advertise their NFT project inside target groups, in order to gain trust and maximize the token price[4]. Having reached a high enough price of the token, which may be hundreds of thousands and even millions dollars, the founders disappear with the money obtained. A classic case of fraud with an NFT dummy is the Frosties NFT project, in which "exclusive" tokens for a game in a metaverse were sold. The project founders closed their website and accounts in social networks immediately after over US $1.3 million were invested into the project[5].

The second deceitful scheme using NFT is similar to a fraud with bankcards known as "phishing". Hackers use phishing to access an NFT account. To this end, they send fake links by e-mail or via popular social networks and forums, such as Twitter[6] and Discord. Clicking on the link and inserting details to enter launches malicious software, such as keyloggers and other spyware, accessing the user's account to steal money or compromise the account. Today, the number of fishing attacks using NFT is growing. For example, in February 2022 wrongdoers stole tokens worth almost $1.7 million during a fishing attack at a popular NFT platform OpenSea. As a campaign to update contract information, fraudsters copied a database and sent links to fraudulent websites to token owners[7].

---

4 For example, ten-fold – up to "ten X"; these are the so-called desirable "Xs" of the token price multiplier.

5 Kaaru, Steve. (2022, March 22). Frosties NFT: 2 charged in US over $1.3M rug pull. *CoinGeek*. https://coingeek.com/frosties-nft-2-charged-in-us-over-1-3m-rug-pull

6 The social network blocked in the territory of the Russian Federation.

7 Russell, B. (2022, February 20). $1.7 million in NFTs stolen in apparent phishing attack on OpenSea users. *The Verge*. https://www.theverge.com/2022/2/20/22943228/opensea-phishing-hack-smart-contract-bug-stolen-nft

The third example is related to selling a token in the secondary market. A fraudster places the highest stake on the lot, making the token owner sell it to this "best buyer". However, making use of the seller's inexperience in the market of cryptoassets, the wrongdoer changes currency without notifying the counteragent. For example, the fraudster offers 10 ETHs for a token for an object of digital art, which is now equivalent to almost US$ 15 thousand, but in the course of the deal, they manage to substitute the cryptocurrency for 10 TONs, which is now equal to about $10. To protect oneself against such a trick, one should thoroughly control the process of the deal, including the type of currency, and not agree to the price-reducing alternatives.

The fourth scheme is "pump and dump". A group of fraudsters disseminates deceitful information in order to increase the price of NFT, imitating a market character of this process. As soon as an investor is found, who invests into the project at an artificially pumped price, the fraudsters disappear with the money, leaving the buyers with useless assets. To create agitation around the project, both open and shadow manipulative advertising mechanisms in social networks are used, including support by celebrities. In addition, the wrongdoers imitate demand for the token using their own money, which actually move around their own accounts and wallets, attracting attention of active investors and not allowing them to ignore the asset. An example of such fraud is deceive the investors of Evil Ape project. An anonymous creator of the void collection disappeared with 798 ETHs worth over $2.7 million, and nothing has been heard of them since then[8].

The fifth scheme consists in appropriation of the authorship (plagiarism) of the work of art, in relation to which a token is issued, by a person not possessing the rights to it. In 2022, the management of OpenSea platform informed that over 80 % NFTs on this platform had been issued with violation of legal rightholders' rights[9]. Thus, the probability of purchasing a token for illegally appropriated copyright object is high today. If this fact is established, the price for such a token drops dramatically. For that reason, it is essential to check the rights to the work of art before making a deal.

Of utmost importance is the fact that the rules of platforms (for example, the currently most successful NFT resource – OpenSea) impose the obligation to check the rights to tokenized works onto the token purchaser. In the license agreement wording, the platform definitely and emphatically unambiguously rejects its liability for illegal actions of its users. The agreement states that the platform does not check the sellers' rights to a work of art, which token it creates and sells. The norms of the license agreement explicitly posit that the platform does not perform the so called clearance of rights, hence, the risks following from the sellers' illegal actions are fully and completely borne

8 Chalk, A. (2021, October 6). 'Evolved Apes' NFT creator Evil Ape disappears with $2.7M7. *PC Gamer*. https://www.pcgamer.com/evolved-apes-nft-creator-evil-ape-disappears-with-dollar27m

9 Volpicelli, Gian M. (2022, February 10). Why OpenSea's NFT Marketplace Can't Win. *WIRED*. https://www.wired.co.uk/article/opensea-nfts-twitter

by the buyer. The platform only serves as a marketplace, i. e. provides the location and tools for making a deal, but it is not a classic broker who guarantees to the parties the due diligence of the deal and mutual fulfilment of obligations. As a reasonable diligence, a token buyer must check the seller's authorities by asking for the правоустанавливающие документы – a license agreement for using the tokenized work of art. Alternatively, they must make certain of the authorship of the work of art creator, if they act without intermediaries, by examining their history and profile in social networks, thus reducing the risks of being involved into an illegal deal.

Into the sixth category, we may include several other, not so popular but dangerous, types of deceit in the NFT market. Well-known is the scam with a "gratuitous distribution" of tokens, when the victim is promised to get a token as a gift for efforts to promote the collection. After the work is done, the scam organizers send a link for the executor to receive the prize into their electronic wallet, which requires inserting access details. However, the fraudsters only need the account details to appropriate the digital assets.

One more scam, known since the beginning of the informatization era, is fake support service. A wrongdoer communicates with the client allegedly to solve the problem with the account. Under the pretext of assisting the client, they send a link to a fake NFT platform, the algorithm of which requires inserting the personal e-wallet key, which is then read and used to steal the money.

In this section, we analyzed the currently known ways of deceit using NFT. This information is given to illustrate the thesis about a fraudulent character of relations in this market. Let us formulate several practical recommendations to enhance safety when working in this sphere and be protected against fraudulent schemes.

It should be noted that the proposed recommendations are typical measures of information-technological caution and self-protection techniques in the network environment. Do not click on suspicious links, as a wrongdoer may get the account details in such way. Never give anyone the password and/or access code to your account and e-wallet. It is worth using a two-factor authentication of the account to increase its protection. Before making a deal, check the identity and history of the token seller. Use a virtual private network (VPN) for cyphering and anonymization of the NFT traffic. In addition to an operative wallet to carry out transactions, it is expedient to have a so-called cold wallet, which is not used for transactions but is only used for storing digital assets in an autonomous and most safe mode.

Further, we will examine a diametrically opposite view at blockchain/NFT as a socially, culturally and technologically positive innovation, which may give new energy and open new ways to the development of creative industries in a technological society.

3. Result: NFT as a future of creative industries

According to the concept of the fine prospects of creative industries in a blockchain ecosystem, the technology of implementing the rights to works of art through tokens is a disruptive innovation, which may change the relations and rules of game in this sphere. One of the key advantages of blockchain platforms is the efficient implementation of legal and economic (in their inseparable synthesis – institutional) [10] relations (Hale, 1952), emerging around cryptocurrencies and tokens. Proponents of the institutional approach in scientific thought define the result of forming new legal-economic links due to the progressive achievements as an institutional environment of a higher order (Commons, 1959; Ayres, 1962). At that, the need for legal-economic innovations and their technological support is determined by the public demand for implementation of the newly formed relations, the nature of which we analyze in this article.

Today, a cohort of expert has been formed worldwide, whose opinion we take into account in the present work, who are united by the vision of the future progress of creative industries due to the use of blockchain/NFT tools. The experts, analyzing the transformation of creative activity and using its results in the specific spheres of intellectual domain under scientific-technical progress, emphasize that they are not specialists in blockchain, smart contracts or NFT minting, nor they have access to insider information or personal interests in NFT business. These circumstances are important to estimate the impartiality of the opinions expressed, as they sometimes look as overthrowing the established views on creativity as a sociocultural institution and on the economic models of commercialization of intellectual rights.

4. Tokenization of creativity by the example of music industry

One of the brightest researchers is Ted Gioia (Gioia, 2019), who systematically analyzes and forecasts how blockchain and NFT will influence music industry. His results are especially valuable due to several circumstances. Under the established remix culture, it is music, due to the specific restrictions of expressive means positively perceived by most listeners (Santiago, 2017), that vividly presents and largely determines the development trends of creative mechanics and the market of intellectual products in the technological era. Observations, conclusions and summarizations made in regard to musical pieces appear to be relevant for other domains of science and arts as well.

To join the world-outlook context, outside of which it would be difficult to perceive the researcher's way of thinking, we would like to cite his words: "I did spend many hours of my lost, wasted youth forecasting the evolution of emerging technologies in Silicon Valley for paying clients, as well as constructing schemes for the pricing, distribution,

[10] Institutional theory views law and economy as a legal-economic system of interdependences, not as autonomous subsystems.

and stakeholder incentivization of new products and services. (To be sure, that's a distinctly un-cool way of spending lost, wasted hours of youth—not with a bong, but an HP 15-C calculator in hand. But the truth is the truth, and those are the nerdy facts.)

And I do know a bit about music, not just as a critic and writer, but also with experience running a startup record label and advising various music tech startups over the years. I've also made pitches to VCs, raised money on Wall Street, guzzled expensive booze with investment bankers on private jets, etc. The whole kit, including the kaboodle.

In other words, I know enough to be dangerous"[11].

Gioia proposes a forecast of development of the NFT trend in music industry, which looks more and more paradoxical as we move forward along the list of expected effects.

First, a blockchain ensures linking a music file or any other digital work of art back to the original (the etalon digital file) of that work of art. Thus, each digital copy can be checked for authenticity and legality of using each digital copy. The question is whether it is useful and what legal-economic consequences it may have. One should remember in this regard, that creativity products are disseminated and used not solely in the Internet. A blockchain cannot stop their distribution outside the network. Any track, visual or audiovisual content, played on one medium can be recorded and played on another medium. The current level of technologies allows recording, copying and distributing any content with various devices, for example, recording an audiotrack of a TV- or radio program, make a photo of a picture in a museum, or a video recording in a cinema with a smart phone. Thus, bold statements that modern technologies will stop piracy are erroneous. Piracy will stay forever, especially if official copies of works of art, authenticated in blockchain, are as expensive as today.

Second, law-obedient citizens may use blockchain to ease identification of the rights holders of a recording and acquisition of a license for using it, for example in a movie, an advertisement, or an educational video. This is a legitimate solution to a genuine problem, it will not transform the industry or excite a common customer who does not often license music. Nevertheless, this would be a step forward.

The third innovation is authentication original files of unique music pieces and the possibility of selling the rights to them at a high price. In a new institutional environment, a music file will get a special status, "much like an original Picasso", and may become very expensive. However, this fundamentally changes the musician's relationship with the audience, and not for the better[12]. Instead of working for their fans, musicians will try to please an elite group of wealthy collectors, who purchase the "original" song as

---

11 Gioia, T. (2022, January 2). Eleven Wild Guesses on How Blockchain and NFTs Will Actually Impact Musicians and Songs. *The Honest Broker*. https://tedgioia.substack.com/p/eleven-wild-guesses-on-how-blockchain

12 *Ibid*.

a symbol of their status. Gioia wonders if it is right to build a "new music ecosystem on the whims of people like Martin Shkreli"[13]. Such things are already happening, but this "Shkrelitized approach represents only a tiny portion of the emerging NFT opportunity", which reduces the potential of more promising and large-scale business models in music industry.

The fourth prospect consists in using blockchain to strengthen the relationship between musicians and their audience. Tokenization of albums and songs is an effective means of implementing this momentous innovation. Imagine a new album is released with all cash flows from the music going to token-holders, while transactions are verified by a blockchain. In this scenario, the musician gets 50% of the tokens and the rest are sold to fans at a reasonable price, say, 1500 rubles, which is equivalent to 170 Yuan or $25. In addition, the tokens buyers receive a copy of the record, perhaps in the form of a compact disc, a vinyl album or a digital download, as well as and other gifts and bonuses. Some rights may further be transferable; others will belong to the participants in the initial offering only. Owners might hold the tokens as an investment tool or sell them, hence, the future cash flows to other fans. If the recording is very successful, the tokenized rights to it might be a profitable investment. One may imagine the situation like: "Hey, dude, I made a profit by reselling my Daft Punk token, and even got to keep the crappy album"[14]. In this case, record stores may become similar to "the New York Stock Exchange, with video screens displaying bid and ask prices for thousands of recording tokens"[15].

The fifth effect of the new model is transparency and honesty in paying royalties. Many musicians do not trust the royalty accounting and distribution system of recording companies. Gioia cites "a very famous jazz musician, with million-selling albums in his discography", who "had never received any payment from any record label in his entire career except for the initial advance when he signed a contract"[16]. The future royalties remained just a promise, regardless of the number of records sold. Blockchain/NFT technology may change this situation. It may transfer all revenues from selling the rights to a recording to an account that a record label or a band manager cannot access. The money will

---

13 Martin Shkreli is a well-known businessman from the USA, convicted of fraud in pharmaceutics. He purchased exclusive rights to an unpublished album of Wu-Tang Clan band for his personal collection. Later, the album was confiscated from Shkreli on account of debt repayment. At the moment of this writing, the album remains officially unpublished. See Sisario, B. (2021, October 20). Meet the New Owners of the Wu-Tang Clan's One-of-a-Kind Album. *The New York Times*. https://www.nytimes.com/2021/10/20/arts/music/wu-tang-clan-once-upon-a-time-in-shaolin.html

14 *Ibid*.

15 *Ibid*.

16 *Ibid*.

be distributed among authors, performers, other token owners and holders according to an Ethereum-regulated system of disbursements, for example. This algorithm does not ensure total honesty, but it will make stealing from artists more difficult.

The sixth forecast consists in that blockchain/NFT technology can make the results of creative activity an object of multilevel marketing[17], including the negative sides on this business model (Michalski et al., 2012). Under this scenario, a token buyer gets rewarded for finding new buyers. This "turbocharged" NFT model will incentivize the user to become a token distributor.

The seventh pattern is eccentric variations on the previous theme. Tokens may be structured by the terms met, for example, total sales. The results achieved are converted into authorities and are delegated down the organizational structure. For example, I am entitled to sell one hundred tokens of a top artist, and if you buy one, you can sell ten sub-tokens, etc. Another variants is that "platform" tokens can be issued that using the recording on a specific platform only. The music business may acquire a franchising model in the form of a structured network that maximizes cash flow due to the royalties received by each participant. Gioia suggests musicians should consider such opportunities, as the fans gain financially when a new piece or album becomes a hit; that could be much more effective than selling merch at concerts.

The eighth aspect is that tokenization of creativity creates the potential for various unethical practices and conflicts of interest: "Imagine if the radio deejay is a token holder? Or the playlist curator on the streaming service? Or the DJ at the college frat party? It's like payola on steroids"[18]. However, there is no offense or large-scale publicly dangerous deeds. Rewarding the fans after the musician's success seems rather just. One can imagine fans maintaining loyalty to an artist over many years because of, inter alia, an investment aspect: "I've been holding these tokens for years, and some day they're gonna pay off"[19].

[17] Multilevel marketing (MLM) is a concept of marketing goods and services via distribution agents, each building their own network and receiving interest from the sales of its members.

[18] Payola (from "pay" and "Victrola" – a brand of phonographs) – secret payoffs from record companies to radio stations and TV channels with a view of promoting music pieces belonging to them (broadcasting, imitation of the audience interest, promoting in ranking, charts, etc.). See Gioia, T. (2022, January 2). Eleven Wild Guesses on How Blockchain and NFTs Will Actually Impact Musicians and Songs. The Honest Broker. https://tedgioia.substack.com/p/eleven-wild-guesses-on-how-blockchain

[19] Gioia, T. (2022, January 2). Eleven Wild Guesses on How Blockchain and NFTs Will Actually Impact Musicians and Songs. *The Honest Broker*. https://tedgioia.substack.com/p/eleven-wild-guesses-on-how-blockchain

The ninth aspect is related to a well-known fact that the price for artist's works rockets after their death. This appeared to be true for music works too. A statistical study of 446 albums by 77 deceased musicians showed that a musician's recording revenues increase by an average of 54% after the artist's death[20]. This is not a trifle but a significant factor creating an incentive for fans and investors to purchase the tokens of aging artists. This source of funds may become a retirement plan for musicians. As they get older, their tokens rise in value and investors increase the portfolio. Just like a company issues more shares, an old musician might even issue more tokens to fund the cost of medical care and other late-in-life expenses.

The aspect number ten is that the course towards tokenization of at least a part of results of creative activity is taken rather firmly now, that is why the "major record labels ought to be setting up these token-based systems and marketplaces" for phonographic tokens. They may generate new business models and cash flows to increase their revenues and those of musicians and other rightholders. However, they "will do little or nothing to seize these opportunities, instead watching from the sidelines as tech startups implement every last one of them, and thus make the traditional record label increasingly irrelevant"[21] in this market. Given their extraordinary reliance on lawyers, one may predict that "old school music companies will file many lawsuits in a neo-luddite attempt to halt the advance of technology"[22]. This attempt will be as successful attempts to prevent Internet distribution of music twenty years ago.

Summarizing this review of the prospects of tokenization of musical business, it is worth reminding that it conclusions also refer to other domains of art and science, if their products and results are subject to digitalizing. The first conclusion is the following. Today's fascination of well-to-do customers with purchasing tokens of artistic works as trophies, displaying acts of status-driven consumption, buying artifacts of symbolic value, as well as opportunistic purchases of "digital fan-art" for speculations does not change much in creative industries. Thus situation vividly demonstrates a set of unfulfilled and lost opportunities. As Giaio puts it, "if all we get from the blockchain is a status-driven niche market for a few thousand collectors with deep pockets, we will have wasted most of the potential of these innovations"[23].

20 *Ibid*.

21 *Ibid*.

22 *Ibid*.

23 *Ibid*.

The above-described potential of using blockchain/NFT technologies may be truly transformative for creative industries. The result of its full-fledged application may be a new institutional model of the creative products market to "involve millions of music fans, who discover (to their delight) that the blockchain has enhanced their connections to artists, and even allows them to share in a song's success"[24], to invest and get revenues from the works of art, ensured high efficiency of transactions under the new legal and economic realities.

5. Critics of music industry tokenization

Critical approach to the above statements makes us doubt several aspects.

First, one may hardly unequivocally share the author's optimism about strengthening relations between a musician and an audience due to tokenization of the works of art. The problem is that occurrence of such effect has been forecast in relation to any innovation related to the Internet. This was expected of the Internet per se as a fundamental technology. This forecast rather reflects the author's desire then lists substantial reasons for its fulfillment. Where such a complex technology as blockchain/NFT appears, intermediaries always emerge, who simplify its use, and often these are completely new players in the market. For example, in music industry, major record labels were substituted by Spotify, Apple, and Google. One may assume that a wave of startups emerges, which is aimed at simplifying he work with NFTs for sellers and buyers for a commission.

The thesis that musical business may take up the franchising model as a network structure to maximize cash flow due to the royalties received by each participant is also doubtful. It looks like the number of people wishing to sink deep and do such things is vanishingly small. One may recall an attempt to organize a business model of micropayments for using content: 15 cents for listening to a song and 8 cents for access to a newspaper article. The model appeared to be unprofitable; no operator got interested in its implementation. As a result, a simpler and less selective model won in the market – the one of subscription to any content at a reasonable fixed price equivalent to about $10 a month[25].

The third objection is that only a minor share of artists has a really significant number of fans, thus, most of them cannot count on substantial royalty when selling tokens. Besides, the idea that fans support an artist for their own profits seems contradicting to the very essence of creativity.

---

24 *Ibid*.

25 Case, A. (2021). Who killed the micropayment? A history. *Medium*. https://caseorganic.medium.com/who-killed-the-micropayment-a-history-ec9e6eb39d05

6. Tokenization of gaming and cybersecurity

Jan Hartmann described the market of creative products created within electronic games today and gamificated metaverse tomorrow. The number of players reached 3.24 billion in 2022, and many of them face the problem of rights to original and derivative works of art which they create inside games and of legal disposition of these rights. The researcher marks the high potential of blockchain/NFT technology for solving this problem in the gaming market. In his opinion, game artifacts, such as personal belongings, weapons, skins and awards can and must be packed into NFTs and sell in the open market. A typical situation is that when a player wishes to buy accessories for their character, the only legitimate opportunity is to buy them from the game publisher. With the advent of legal-economical blockchain/NFT platform into the game ecosystem, gamers will be able to buy and sell the rights to gaming artifacts independently from a publisher. Such demonopolization is a dramatic shift in the industry structure towards the growth point of the market of tokens for gaming artifacts[26].

Hartmann and other researchers pose the question about the usefulness of NFT beyond the market of digital art. In this context, products for digital identification and ensuring cybersecurity are mentioned. According to analysts, blockchain/NFT technology is effective for developing and supporting the decisions which provide users' confidentiality, authentification of information, identification of personality and a pseudonym, digital signature of transactions, ciphering messages and reliable data storage. The integrity of these solutions forms a common cybersecurity platform. Researchers conclude that the blockchain/NFT technology may become the basis of cybersecurity of a new generation.

7. Tokenization of classic and digital visual arts

Monty Preston agrees that blockchain/NFT technologies may help create new communication channels between artists and buyers of their works, broaden the opportunities for access to the world of art and democratize it, and form a new look at the values of art space. Dwelling upon the thesis of democratization, the analyst wrote that NFT provides artists with the opportunity to create and distribute works of art via online channels without traditional intermediaries, who for centuries dictated the rules of access to art and imposed their ideas about what art is and what cannot be considered as such. The effect of using the technology under study is that it is capable of involving into the art space the people who could not be represented in it full-fledged. These are artists from remote regions, women and underage artists. The legal-economic basis of blockchain/NFT provides them with the necessary tools to promote and earn from the results of creative activity, equaling the opportunities of these social groups.

---

[26] Hartmann, J. (2022, April, 19). Is there a future for the NFT beyond digital art? *Forkast*. https://forkast.news/is-there-future-for-nft-beyond-digital-art

The analyst also thinks that this technology will change the relations in the sphere of supporting artists and art in general. As transactions in blockchain are indirect and are not mediated by a third party, collectors and fans will be able to support artists directly. As NFT allows shared and fractional ownership, rightholders and collectors will be able to share the revenues from using artists' works. In a specialized poll of current artists, such features of the NFT model of creativity monetization as getting royalty without intermediaries and in lieu of future sales were listed among the most demanded. If blockchain/NFT innovations in the sphere of fine arts are implemented, the future of artists may be filled with more freedom and autonomy from corporate sponsorship, megacollectors and pretentious curators[27].

8. Tokenization of patents

A research group of scientists headed by Professor Qiang Qu from Shenzhen Institute of Advanced Technology, Chinese Academy of Sciences, and Professor Seyed Mojtaba Hosseini Bamakan from Yazd University (Iran) proposed a multilevel architecture of patent management system based on NFT (Bamakan et al., 2022).

To substantiate their project, the researchers list the following arguments. Patenting an invention, a useful model, an industrial sample, or registering a trademark is a lengthy, labor consuming and expensive process. The procedure of getting a protection document takes many months and even years. The researchers believe that the unique features of non-fungible tokens may accelerate this process, as well as increase the level of protection of rights to tokenized industrial property objects and individualization means.

According to the researchers, the project does not aim at substituting or ousting the state registration of industrial property objects and individualization means, but may provide protection of intellectual rights when waiting for the issuance of the state protection document. Besides, tokenization of patents and trademarks is aimed at simplifying the licensing of patent rights for inventors, commercial companies and universities through legal-economic mechanisms of blockchain/NFT technology. As every transaction is fixed in blockchain, it will be easier to trace the changes in property rights to patents. By improving the licensing of eights to the use of protected solutions, tokenization of patents will facilitate the increase of the rightholders' revenues. The researchers also believe that such legal-economic NFT tool as an automatically executed smart contract, which fixes the terms and price of using the patented solution, may support the efficiency of the market of intellectual rights. This result may be achieved, inter alia, due to automation of collecting license fees for using the solutions of rightholders. Patent tokens may be both used

[27] Preston, M. (2020, March 16). Curators Inside The Industry. *Art Plugged*. https://artplugged.co.uk/monty-preston-curators-inside-the-industry

individually and combined into a commercial portfolio of solutions for a certain domain, with subsequent distribution of royalties among the patent authors and rightholders.

Developers propose the following algorithm of creating and working with patent tokens. Inventors register their technical solution on a blockchain platform in order to patent it. Further, they upload the information which consists of the patent content and the intellectual property belonging to them. A built-in mechanism provides checking the data to prevent their dubbing and other manipulations. Here one should mark that the model constructors do not disclose an important aspect related to the formal and essential expertise of the application, as well as the mechanism of its further conversion into a patent or a rejection of its issuance. Based on the current level of technology, one may assume that solution of these tasks is imposed on artificial intelligence means built into the platform. Further, if the patent is issued it becomes visible to all users of the blockchain.

The potential consumers who need access to the patent content, after registering in the network, apply to the rightholders. As a result if communication between the parties, a smart contract is composed, with the terms of using the patent, which comes into effect after payment by one of the available means: fiat money, cryptocurrency or unique tokens. Additionally, a non-disclosure agreement (NDA) is generated and signed by the parties. The smart contract mechanism controls the parties' consent with the deal terms and its further execution.

At the application level, if a buyer agrees with the open terms of using the patent, stated by its rightholder, they may make payment and immediately unblock the rights to its exploitation without additional interaction between the parties. While patent systems of the world are of national or regional character (for example, Eurasian patent system), tokenization of patents will help to eliminate geographical barriers between them through the mechanism of search enquiry in a distributed ledger. Simple and cheap search, automated licensing, speedy transactions for obtaining and paying for the rights to using patents scattered around the world will help the interested persons to facilitate implementing innovative solutions. The proposed system may also be used for alienating patents and tracing information about rightholders. The system architecture includes adjudicatory module for dispute resolution, the functions of processing claims, supporting confidential information exchange, checking and proving authorship, transfer of rights, creation and placement of protection publications.

Feasibility and potential of the project of patent rights and copyright tokenization is confirmed by the partnership between IBM and IPwe corporation, aimed at stimulating patent transactions using the IBM blockchain platform. They claim at IBM Services that the patent NFTs they develop are simplified smart contracts for intellectual assets with

an accessible supply chain[28]. This said, patent tokenization is still seen as a matter of the future, unlike tokenization of the objects of copyright and neighboring rights, which has launched the market turnover of respective tokens in today's reality.

9. Tokenization of scientific works

Above, we have discussed the NFT trend in relation to works of art and solutions of technical problems, but tokenization of scientific works seems rather promising, too. One should remember that the amount of transferred rights is determined by the author as the original rightholder of the work created and the potential seller of a token for a scientific work. According to the intellectual rights doctrine, the author completely and irreversibly keeps personal rights, including the right to the name, the right to be called the author of the work, the right to protection of the work against distortion and other rights of this type; at the same time, the author may dispose of property rights or a part of them to their own advantage and without harm to their reputation, by issuing a token for a scientific work.

We believe that in the modern society there may be many of those wishing to become an owner of a token for a scientific work, as the positive effect of the results of scientific research can be observed daily, and the popularity of science and innovations is constantly growing in developed countries. For this reason, owning a token for a scientific work will increase prestige and status of its rightholder. Besides, tokens for scientific works have a high potential as a means of value measuring in the post-economic society and a tool for its accumulation. Due to global integration and inclusion into the branch "scientific clubs", the academic community is fully ready for efficient application of the mechanisms of consensual elaboration of the value of scientific works for their subsequent tokenization and, hence, logging on to a completely new source of means for rewarding researchers and funding academic work.

Conclusions

This article analyzes the hypothesis and a set of supporting arguments stating that non-fungible tokens for objects of digital art are a technology for extracting means from the asses that have no real value, through deceiving their purchasers. To justify this position, its proponents list the absence of material component of the goods; the presence of unrestricted possibilities to create additional digital copies of the work, devaluating the original and the replicas; and the fact that non-fungible tokens have value only in narrowly specialized limited communities, but not in the broad market.

---

[28] Berman, B. (2021). IBM-IPwe Partnership Hopes to Increase Patent Efficiency, Propel Transactions. *IPWatchdog*. https://www.ipwatchdog.com/2021/06/07/ibm-ipwe-partnership-hopes-increase-patent-efficiency-propel-transactions/id=134326

The article presents a description of the techniques of unlawful enrichment using NFT via misappropriation of someone else's property, unlawful acquisition of rights to it, violation of copyright, and inflicting harm by fraud or abuse of trust. Recommendations are proposed to prevent and eliminate the described risks.

Positive prospects of tokenization of creative products are demonstrated in detail by the example of music industry. Eleven models of innovative use of musical recordings are described. Positive and negative aspects of these approaches are analyzed, as well as their impact on social relations in the sphere of music creation and consumption. A conclusion is made that, under the realities of remix culture formed as a result of broad dissemination of content creation, use and transformation technologies, the relations and development trends formed in the music industry will be spread to other spheres of science and art.

In conclusion, we have considered the deductions of researchers about tokenization of other results of intellectual activity. Among them are computer gaming artifacts, results of classical and digital visual arts, patents for inventions, useful models and industrial samples, as well as an original view of the expediency of scientific works tokenization.

References

Ayres, C. E. (1962). *The Theory of Economic Progress: a Study of the Fundamentals of Economic Development and Cultural Change*. Schocken Books.

Bamakan, S. M. H., Nezhadsistani, N., Bodaghi, O., & Qu, Q. (2022). Patents and intellectual property assets as non-fungible tokens; key technologies and challenges. *Sci Rep*, *12*, 2178. https://doi.org/10.1038/s41598-022-05920-6

Chey, H.-K. (2022). Cryptocurrencies and the IPE of money: an agenda for research. R*eview of International Political Economy*, 1–16. https://doi.org/10.1080/09692290.2022.2109188

Colicev, A. (2023). How can non-fungible tokens bring value to brands. *International Journal of Research in Marketing*, *40*(1), 30–37. https://doi.org/10.1016/j.ijresmar.2022.07.003

Commons, J. R. (1959). *Institutional economics: its place in political economy*. Madison: University of Wisconsin Press.

Far, S. B., Bamakan, S. M. H., Qu, Q., & Jiang, Q. (2022). A Review of Non-fungible Tokens Applications in the Real-world and Metaverse. *Procedia Computer Science*, *214*, 755–762. https://doi.org/10.1016/j.procs.2022.11.238

Gioia, T. (2019). *Music: a subversive history*. Basic Books.

Goel, A. K., Bakshi, R., & Agrawal, K. K. (2022). Web 3.0 and decentralized applications. *Materials Proceedings*, *10*(1), 8. https://doi.org/10.3390/materproc2022010008

Hale, R. L. (1952). F*reedom Through Law. Public Control of Private Governing Power*. Columbia University Press.

Henry, C. (Ed.). (2007). *Entrepreneurship in the creative industries: An international perspective*. Edward Elgar Publishing.

Hilko, M. R. (2021). *Disrupting Copyright. How Disruptive Innovations and Social Norms are Challenging IP Law*. Taylor & Francis.

Jelil, S. N. (2022). *Non-Fungible Tokens, Crypto-Assets and Web3: What's in It for Conservation Science?* http://dx.doi.org/10.2139/ssrn.4282312

Kraizberg, E. (2023). Non-fungible tokens: a bubble or the end of an era of intellectual property rights. *Financial Innovation*, *9*, 32.

Michalski, R., Jankowski, J., & Kazienko, P. (2012, November). Negative effects of incentivised viral campaigns for activity in social networks. In *2012 Second International Conference on Cloud and Green Computing Xiangtan*, China (pp. 391–398). https://doi.org/10.1109/CGC.2012.95

Momtaz, P. P. (2022). Some very simple economics of Web3 and the Metaverse. *FinTech*, *1*(3), 225–234. https://doi.org/10.3390/fintech1030018

Murray, A., Kim, D., & Combs, J. (2023). The promise of a decentralized internet: What is Web3 and how can firms prepare? *Business Horizons*, *66*(2), 191–202. https://doi.org/10.1016/j.bushor.2022.06.002

Okediji, R. L. (Ed.). (2017). *Copyright law in an age of limitations and exceptions*. Cambridge University Press.

Petcu, A., Pahontu, B., Frunzete, M., & Stoichescu, D. A. (2023). A Secure and Decentralized Authentication Mechanism Based on Web 3.0 and Ethereum Blockchain Technology. *Applied Sciences*, *13*(4), 2231. https://doi.org/10.3390/app13042231

Santiago, J. M. (2017). The «Blurred Lines» of Copyright Law: Setting a New Standard for Copyright Infringement in Music. *Brooklyn Law Review*, *83*(1). https://brooklynworks.brooklaw.edu/blr/vol83/iss1/18/

Scharfman, J. (2023). *The Cryptocurrency and Digital Asset Fraud Casebook*. Springer International Publishing.

Walker, W. (2022). *The Definitive Guide to NFT Investing. Learn to Profit From the NFT, Metaverse, and Crypto Gaming Connection*. PublishDrive.

Wilson, K. B., Karg, A., & Ghaderi, H. (2022). Prospecting non-fungible tokens in the digital economy: Stakeholders and ecosystem, risk and opportunity. *Business Horizons*, *65*(5), 657–670. https://doi.org/10.1016/j.bushor.2021.10.007

Yue, Y., Li, X., Zhang, D., & Wang, S. (2021). How cryptocurrency affects economy? A network analysis using bibliometric methods. *International Review of Financial Analysis*, *77*, 101869. https://doi.org/10.1016/j.irfa.2021.101869

Author information

Ruslan A. Budnik – Doctor of Juridical Sciences, Professor, Deputy Director of International scientific-educational center "UNESCO Chair of Copyright, Neighboring, Cultural and Information Rights", National Research University "Higher School of Economics"; Professor at Russian-Chinese Center for comparative legal science, Shenzhen MSU-BIT University
Address: 3 Bolshoy Trekhsvyatitelskiy pereulok, 436, 101000 Moscow, Russian Federation;
No. 1, International University Park Road, Dayun New Town, Longgang District, Shenzhen, Guangdong Province, PRC, 518172, China
E-mail: rbudnik@hse.ru
ORCID ID: https://orcid.org/0000-0001-8076-1560
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=43760909700
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/record/1299111
Google Scholar ID: https://scholar.google.com/citations?user=Z9tacXwAAAAJ
RSCI Author ID: https://www.elibrary.ru/author_items.asp?authorid=822805

Conflict of interest

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
ASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – February 16, 2023
Date of approval – May 1, 2023
Date of acceptance – August 15, 2023
Date of online placement – August 20, 2023

Научная статья
УДК 34:347.211:75:78:808.1:004
EDN: https://elibrary.ru/xhasaw
DOI: https://doi.org/10.21202/jdtl.2023.25

Риски и перспективы токенизации творчества

Руслан Александрович Будник

Национальный исследовательский университет «Высшая школа экономики»
г. Москва, Российская Федерация;
Университет «МГУ-ППИ в Шэньчжэне»
г. Шэньчжэнь, Китайская Народная Республика

Ключевые слова

NFT,
блокчейн,
искусство,
музыка,
право,
произведение,
творчество,
токен,
токенизация,
цифровые технологии

Аннотация

Цель: токенизация творчества в одном ряду с криптоэкономикой и сетевой инфраструктурой Web3 представляет собой заметный тренд развития современного общества в третьем десятилетии двадцать первого века. Цель настоящей статьи заключается в исследовании рисков и перспектив, возникающих в процессе распоряжения результатами творческого труда в виде невзаимозаменяемых токенов.

Методы: методика настоящей работы построена на анализе различных точек зрения ученых на эту проблему, включая диаметрально противоположные концепции. Полярные позиции наблюдателей характеризуют их отношение к токенизации творческих продуктов как к спекулятивной схеме, с одной стороны, и перспективному инструменту развития творческих индустрий – с другой.

Результаты: выявлены возможные негативные последствия токенизации результатов интеллектуальной деятельности, а также авторские рекомендации по управлению этими рисками. Еще одним результатом настоящей публикации выступает анализ экономико-правовых перспектив, вытекающих из токенизации объектов авторских и смежных прав на примере музыкальных произведений.

Научная новизна: состоит в выдвижении и обосновании гипотезы о том, что отношения, сформировавшиеся в музыкальной индустрии в современных социокультурных и технологических реалиях, будут воспроизводиться в других творческих индустриях. Кроме того, научная новизна также заключается в анализе перспектив токенизации таких результатов интеллектуальной деятельности, как игровые артефакты, произведения художественного и цифрового изотворчества, патентов и достижений науки. Применение невзаимозаменяемых токенов в экосистеме сетевых компьютерных игр позволит геймерам покупать

и продавать права на игровые произведения независимо от издателя. Токенизация объектов промышленной собственности и средств индивидуализации обеспечит защиту интеллектуальных прав их авторов в период ожидания выдачи государственного охранного документа. В современном обществе найдется немало желающих стать собственником токена на научное произведение, поскольку популярность науки и инноваций непрерывно растет в развитых странах. Владение токеном на научное произведение будет считаться моральной инвестицией, повышать престиж и статус его правообладателя. Токены на произведения науки имеют высокий потенциал в качестве средства измерения ценности в постэкономическом обществе.

Практическая значимость: практическая значимость исследования состоит в описании инновационных способов использования творческих продуктов и бизнес-моделей, основанных на токенизации результатов интеллектуальной деятельности, готовых к воплощению на практике.

Для цитирования

Будник, Р. А. (2023). Риски и перспективы токенизации творчества. *Journal of Digital Technologies and Law*, *1*(3), 587–611. https://doi.org/10.21202/jdtl.2023.25

Список литературы

Ayres, C. E. (1962). *The Theory of Economic Progress: a Study of the Fundamentals of Economic Development and Cultural Change*. Schocken Books.

Bamakan, S. M. H., Nezhadsistani, N., Bodaghi, O., & Qu, Q. (2022). Patents and intellectual property assets as non-fungible tokens; key technologies and challenges. *Sci Rep*, *12*, 2178. https://doi.org/10.1038/s41598-022-05920-6

Chey, H.-K. (2022). Cryptocurrencies and the IPE of money: an agenda for research. R*eview of International Political Economy*, 1–16. https://doi.org/10.1080/09692290.2022.2109188

Colicev, A. (2023). How can non-fungible tokens bring value to brands. *International Journal of Research in Marketing*, *40*(1), 30–37. https://doi.org/10.1016/j.ijresmar.2022.07.003

Commons, J. R. (1959). *Institutional economics: its place in political economy*. Madison: University of Wisconsin Press.

Far, S. B., Bamakan, S. M. H., Qu, Q., & Jiang, Q. (2022). A Review of Non-fungible Tokens Applications in the Real-world and Metaverse. *Procedia Computer Science*, *214*, 755–762. https://doi.org/10.1016/j.procs.2022.11.238

Gioia, T. (2019). *Music: a subversive history*. Basic Books.

Goel, A. K., Bakshi, R., & Agrawal, K. K. (2022). Web 3.0 and decentralized applications. *Materials Proceedings*, *10*(1), 8. https://doi.org/10.3390/materproc2022010008

Hale, R. L. (1952). F*reedom Through Law. Public Control of Private Governing Power*. Columbia University Press.

Henry, C. (Ed.). (2007). *Entrepreneurship in the creative industries: An international perspective*. Edward Elgar Publishing.

Hilko, M. R. (2021). *Disrupting Copyright. How Disruptive Innovations and Social Norms are Challenging IP Law*. Taylor & Francis.

Jelil, S. N. (2022). *Non-Fungible Tokens, Crypto-Assets and Web3: What's in It for Conservation Science?* http://dx.doi.org/10.2139/ssrn.4282312

Kraizberg, E. (2023). Non-fungible tokens: a bubble or the end of an era of intellectual property rights. *Financial Innovation*, *9*, 32.

Michalski, R., Jankowski, J., & Kazienko, P. (2012, November). Negative effects of incentivised viral campaigns for activity in social networks. In *2012 Second International Conference on Cloud and Green Computing Xiangtan*, China (pp. 391–398). https://doi.org/10.1109/CGC.2012.95

Momtaz, P. P. (2022). Some very simple economics of Web3 and the Metaverse. *FinTech*, *1*(3), 225–234. https://doi.org/10.3390/fintech1030018

Murray, A., Kim, D., & Combs, J. (2023). The promise of a decentralized internet: What is Web3 and how can firms prepare? *Business Horizons*, *66*(2), 191–202. https://doi.org/10.1016/j.bushor.2022.06.002

Okediji, R. L. (Ed.). (2017). *Copyright law in an age of limitations and exceptions*. Cambridge University Press.

Petcu, A., Pahontu, B., Frunzete, M., & Stoichescu, D. A. (2023). A Secure and Decentralized Authentication Mechanism Based on Web 3.0 and Ethereum Blockchain Technology. *Applied Sciences*, *13*(4), 2231. https://doi.org/10.3390/app13042231

Santiago, J. M. (2017). The «Blurred Lines» of Copyright Law: Setting a New Standard for Copyright Infringement in Music. *Brooklyn Law Review*, *83*(1). https://brooklynworks.brooklaw.edu/blr/vol83/iss1/18/

Scharfman, J. (2023). *The Cryptocurrency and Digital Asset Fraud Casebook*. Springer International Publishing.

Walker, W. (2022). *The Definitive Guide to NFT Investing. Learn to Profit From the NFT, Metaverse, and Crypto Gaming Connection*. PublishDrive.

Wilson, K. B., Karg, A., & Ghaderi, H. (2022). Prospecting non-fungible tokens in the digital economy: Stakeholders and ecosystem, risk and opportunity. *Business Horizons*, *65*(5), 657–670. https://doi.org/10.1016/j.bushor.2021.10.007

Yue, Y., Li, X., Zhang, D., & Wang, S. (2021). How cryptocurrency affects economy? A network analysis using bibliometric methods. *International Review of Financial Analysis*, *77*, 101869. https://doi.org/10.1016/j.irfa.2021.101869

Сведения об авторе

Будник Руслан Александрович – доктор юридических наук, профессор, заместитель директора Международного научно-образовательного центра «Кафедра ЮНЕСКО по авторскому праву, смежным, культурным и информационным правам», Национальный исследовательский университет «Высшая школа экономики»; профессор Российско-китайского центра сравнительного правоведения, Университет «МГУ-ППИ в Шэньчжэне».
Адрес: 101000, Российская Федерация, г. Москва, Большой Трехсвятительский переулок 3, 436;
518172, Китайская Народная Республика, провинция Гуандун, г. Шэньчжэнь, район Лунган, Даюньсиньчэн, ул. Гоцзидасюэюань, 1.
E-mail: rbudnik@hse.ru
ORCID ID: https://orcid.org/0000-0001-8076-1560
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=43760909700
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/record/1299111
Google Scholar ID: https://scholar.google.com/citations?user=Z9tacXwAAAAJ
РИНЦ Author ID: https://www.elibrary.ru/author_items.asp?authorid=822805

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: 10.41.26 / Личные неимущественные права авторов и исполнителей
Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 16 февраля 2023 г.
Дата одобрения после рецензирования – 1 мая 2023 г.
Дата принятия к опубликованию – 15 августа 2023 г.
Дата онлайн-размещения – 20 августа 2023 г.

Research article
DOI: https://doi.org/10.21202/jdtl.2023.26

"Pure Rat Country" – Reflections on Case Decision 2022-001-FB-UA of Facebook Oversight Board (Knin Cartoon Case)

Gergely Ferenc Lendvai

Pázmány Péter Catholic University
Budapest, Hungary

Keywords

Digital technologies,
Facebook*,
freedom of expression,
hate speech,
human rights,
knin cartoon,
law,
Meta*,
oversight board,
regulation

Abstract

Objective: the present paper aims to analyse Case Decision 2022-001-FB-UA of Facebook* Oversight Board, also known as the Knin cartoon case and attempts to put the case as well as its procedure in a historical and cultural context to set out a critical approach concerning Facebook's* content moderation.

Methods: the paper uses desk research as the primary source of method. The paper's resource background builds upon comparative case studies and case analysis as well. The paper uses resources from various disciplines: legal philosophy, international law, media law, platform regulation, history.

Results: the paper presents the context of the Knin cartoon case as well as the key findings of the Oversight Board and the reasoning behind its decision. Furthermore, this paper aims to reflect on the idea of hate speech as interpreted by the Oversight Board and makes a tentative to contextualise and introduce the main problems and possible solutions regarding Meta's content moderation in the scope of the present case.

Scientific novelty: the Knin case has not been analysed in such historical and contextual depth before as the case decision was issued in 2022. Only a few analyses from merely legal standpoints were published thus far.

Practical significance: the findings regarding the Knin case may be of importance of three main aspects: (1) it could be used for further critical analyses on Facebook's* content moderation, (2) it could serve as a recommendation regarding platform regulation and guideline development and (3) it presents the paramount relevance and significance of the holistic interpretational perspectives when determining hate speech. As for the latter the present paper argues that the historical, cultural, societal and symbolic interpretation and understanding of hate speech determination is not only instrumental, but the only viable method to understand, determine and judge upon alleged hate speech cases.

For citation

Lendvai, G. F. (2023). "Pure Rat Country" – Reflections on Case Decision 2022-001-FB-UA of Facebook Oversight Board (Knin Cartoon Case). *Journal of Digital Technologies and Law, 1*(3), 612–628. https://doi.org/10.21202/jdtl.2023.26

Contents

Introduction

Harvard Law School professor Noah Feldman coined the idea of a quasi-Supreme Court in late 2018[1] and later approved by Meta (Facebook* at the time) CEO Mark Zuckerberg (Klonick, 2020; Douek, 2021). Despite certain criticism concerning possible monitoring and objectivity issues (Sale, 2022), the Board was created as an independent, legitimate and authoritative (Bayer, 2022) self-regulation institution (Bayer, 2022; Klonick, 2020), in order to ensure that Facebook* promotes freedom of expression via balancing concurring values (free speech, safety, privacy to name a few) (Pickup, 2021). As for self-regulation, Medzini proposes the usage of the expression "enhance self-regulation" so as to emphasise the delegation of regulatory responsibilities in addition to the classic intermediation mechanisms (Medzini, 2022). The identification of the Oversight Board as a Supreme Court (Cowls & Dominiquo-Schramm, 2022) is a rather grandiose or even naïve narrative

[1] Klonick, K.: Inside the making of Facebook's Supreme Court. *The New Yorker*. https://www.newyorker.com/tech/annals-of-technology/inside-the-making-of-facebooks-supreme-court

(Schultz, 2021), however, as this independent body established by Meta uses the Community Standards of Facebook* (Pickup, 2021) as well as international human rights law and decisions (e.g. international human right principles) (Vukčević, 2021; Benesch, 2020; Helfer & Land, 2022), the relevance and importance to understand, interpret and review the Oversight Board's decisions seem more current than ever before. One has to consider that despite the contractual nature between users and Facebook* (Schultz, 2021; Bayer, 2022), the power structure of freedom of expression, as Schultz rightly said (Shultz, 2021), has drastically changed via the introduction of the Oversight Board. Though the Oversight Board's decisions aim to hold accountable Meta and its decisions and policymaking (O'Kane, 2022), and are therefore solely binding on Facebook* (Wong & Floridi, 2022), this authority is unique extent-wise, despite Facebook's* critical position regarding online expression and communication globally (Wong & Floridi, 2022). As Schultz acknowledged (Shultz, 2021): "The members of the OB (the Oversight Board) are not only "judges": they are also partly in charge of their own legislation. This is a unique concentration of power over access to freedom of expression to billions of people. At no time in human history have so few people exercised this much control over so many other people's possibility to be heard." This immense power over people's lives (Chander, 2012) and authority of human rights also come with expectations from the public – is the Oversight Board, for example, capable of solving the polemic presented by the digitalisation of communication, such as online hate speech or cyberbullying (Pongó, 2020)[2]? The answer thus far seems ambiguous as the Oversight Board tends to follow a more conservative approach concerning issues like the above: a minuscule number of cases are even presented before the Board (Wong & Floridi, 2022; Nunziato, 2022), and the legal argumentations are often theoretical. They are based on abstract or general principles (Kulick, 2022). Though the Board (henceforth: "the OB") often takes on culturally fundamental and controversial issues (Takhshid, 2021) (see for example the Zwarte Piet decision as a quasi-landmark case on the issue of blackface[3] or the decision on misinformation concerning COVID-19[4]), the majority of the cases are tackling hate speech-related problems (Wong & Floridi, 2022) and Facebook's* reaction thereto. In the present writing, the so-called Knin cartoon case

[2] Klonick, K. (2019, October 28). Does Facebook's Oversight Board Finally Solve the Problem of Online Speech. *CIGI*. https://www.cigionline.org/articles/does-facebooks-oversight-board-finally-solve-problem-online-speech/

[3] Oversight Board decision no. 2021-002-FB-UA. https://oversightboard.com/sr/decision/2021/002/public-comments

[4] Oversight Board decision no. 2020-006-FB-FBR. https://oversightboard.com/sr/decision/006/public-comments

will be discussed[5], a relatively new case that was selected to be brought before the OB in March 2022[6] after a Facebook* user appealed the removal of a video where a Disney cartoon was edited so that it depicted Serbians as rats[7].

1. The details and Knin cartoon case

The case was selected to be discussed by the OB in March 2022 after a user appeal. In accordance with the official communication on the announcement of the selection of three cases to be brought before the OB, the problematic post concerned a video posted on a Croatian public Facebook* page (pretjerivač). As the video was captioned in Croatian, Meta used translation to understand the meaning behind the main post. According to Meta's translation, the caption said, "The Player from Čavoglave and the rats from Knin". Before diving into the case's details, I propose a contextual interpretation of the fundamental factors of the case. Čavoglave is a relatively small village in the Dalmatian Hinterland south of Croatia. As per the 2020 Croatian census, Čavoglave has 190 inhabitants[8].

Croatians took great pride in the village of Čavoglave as a Thompson (Croatian rock band led by frontman Marko Perković Thompson) wrote a patriotic (deemed by some as an ideological call (Robionek, 2017)) and Croatian-nationalist fight song about the town[9]. A Croatian symbol (Robionek, 2017), the Thompson song is of crucial importance as it was the leading factor that led to the nationwide acknowledgment and popularization of it (Melichárek, 2015). Knin is a city with a population of around 8.000–10.000 inhabitants near Čavoglave in the south of Croatia. Historical sight, the city has been an important centre during medieval times and is a relatively well-known city for being the fortress of Serbs during the abovementioned war. Knin was also, for a short time, the capital of the unrecognised Serbian military region, the Republic of Serbian Krajina, in 1991 (Leutloff-Grandits, 2008). Serbs have historically inhabited Knin. In the years leading up to the war, around 80% of the population claimed to be Serbian. This Serbian majority drastically changed after the war, as in 2021, only 21.42 % of the population claimed to be Serbian (Leutloff-Grandits, 2008; Douek, 2020). Knin is not a city free from nationalist controversies. On 5 August 2011, Croatian state officials celebrated the 16th anniversary of "Operation Storm", carried out by Croatian armed forces between August and November 1995 in the Krajina region of Croatia in Knin[10]. Operation Storm is understood as a massive offensive military action against Croatian Serbians (Banjeglav, 2015). Thousands of Serbians

5 Oversight Board decision no. 2022-001-FB-UA. https://oversightboard.com/news/1629549600777906-oversight-board-overturns-meta-s-original-decision-in-knin-cartoon-case-2022-001-fb-ua/

6 Oversight Board, Announcing the Board's next cases. https://oversightboard.com/news/175638774325447-announcing-the-oversight-board-s-next-cases/

7 Oversight Board Selects a Case Regarding a Video of an Edited Cartoon Depicting a Croatian City. *Facebook Transparency Center*. https://transparency.fb.com/hu-hu/oversight/oversight-board-cases/cartoon-case/

8 Opcina Ruzic. *Čavoglave*. https://www.opcina-ruzic.hr/index.php/naselja/cavoglave

9 Thompson-Cavoglave. https://www.youtube.com/watch?v=tVaYgPBYnOQ

10 Amnesty International Public Statement, Croatia: Praise for "Operation Storm" creates climate of impunity. Index: EUR 64/010/2011. https://www.amnesty.eu/wp-content/uploads/2018/10/AIR12-Report-English.pdf

had to flee during the operation, and a multitude of Serbians faced inhuman treatment from the Croatian Army (Banjeglav, 2015). Amnesty International expressed concerns about glorifying war criminals and called on Croatia to commence dealing with the legacy of war (Banjeglav, 2015). To pour oil on the already burning "cultural" fire, many crimes were not prosecuted later, including the ones committed in Knin, as it was not a priority for the Croatian judiciary, as per Vesna Terselic, head of Documenta, a Human Rights Committee in Croatia[11]. Though ex-mayor Marko Jelić attempted to smooth the somewhat bitter liaison between Serbian and Croatians[12], the relation, even to this day, is incredibly vivid and a foundation for many conflicts (recently, for example, the Croatian Ministry of Foreign and European Affairs demanded a public apology from the Serbian delegation who visited Knin for referring to the city "as Serbian and occupied"[13]). Given the above and in full accordance with the Overarching Criteria for Case Selection of the OB[14], the Knin cartoon was rightly selected as it concerned hate speech in the context of a long-lasting nationalist conflict between Serbians and Croatians and it concerned two towns that are equally relevant both historically and culturally.

Drifting back to the shores of the Knin cartoon case, it is essential to lay down the case details[15]. The "infamous" video was an edit of Disney's "The Pied Piper" cartoon. The original cartoon is the cartoon interpretation of a renowned German/Saxon folk tale, the Pied Piper of Hamelin (in German: "der Rattenfänger von Hameln"), whose main figure is the pied piper, a man – who is a rat catcher – luring away the rats invading the town of Hamelin with his magic flute. Researchers suggest that the tale of Pied Piper served as a figure of rodent control or as safeguard against infection (Singleton et al., 2003). The cartoon scene, which was edited, depicts the city of Hamelin originally being overrun by a pack of rats. The Croatian narration of the video describes that the rats wished to live in a "pure rat country". Therefore, the rats continuously aimed to push out the people from the city. In the first part of the video, a clear provocation can be observed as well – above the gates of the city, a clear and well-readable "Knin" title can be read. The word "Knin" is montaged via an intentional edit of the original video. Though Facebook's* search engine does not display the Knin cartoon, the original version is available and watchable on Youtube; the above part is the video's opening scene[16]. As the video progresses, viewers can see a multitude of rats running around the city

11 *Operation Storm Anniversary Highlights Croatia and Serbia's Bitter Mistrust*. https://balkaninsight.com/2022/08/03/operation-storm-anniversary-highlights-croatia-and-serbias-bitter-mistrust/

12 Mayor of Knin: I will invite Serbs to return, this is their city too. *RTRS*. https://dijasporars.com/en/gradonacelnik-knina-pozvacu-srbe-da-se-vrate-ovo-je-i-njihov-grad/

13 Hina. (2021, January 29). *Croatia demands apology from Serbia for calling Knin "Serbian occupied town"*. № 1. https://rs.n1info.com/english/news/croatia-demands-apology-from-serbia-for-calling-knin-serbian-occupied-town/

14 Oversight Board. *Overarching Criteria for Case Selection*, 2.

15 Decision no. 2022-001-FB-UA.

16 *Nestanak Srba iz Knina*. https://www.youtube.com/watch?v=5nQjwH9vHTU

of Knin. People are trying to harass the animals by hitting them with brooms and sticks, and the video also portrays a scene where rats are devouring a tremendous amount of food in an instant. The hectic circumstances change as the pied piper from Čavoglave appears. First, the rats ignored the pied piper. In a particular scene, the rats are sticking their tongues out as a reaction to the piper appearing in town (the narrator also says that the "great rat aggression" continued). In accordance with the original folklore and the visual presentation, the pied piper starts to play a melody on his magic flute. The rats commence amassing, forming a gigantic crowd of rats, and start to dance harmoniously, standing on two legs, singing their favourite song and following the piper, who leads the "rat mass" out of Knin.

One of the most controversial parts of the video is the audio content which is used to represent the rats' favourite song as it is a song which intends to commemorate Momčilo Đujić. Momčilo Đujić was a Serbian Orthodox priest and a Chetnik military warlord (also known as a vojvoda). Đujić played a crucial role in leading the Serbian resistance during World War II. However, Đujić's reputation from a Croatian perspective is not as heroic, as he and the Chetniks he led were enemies of the Croatian state (Ramet, 2011). The Dinara Chetnik Division, led by Momčilo Đujić, is accountable for initiating tens and thousands of violent actions committed against Croatian civilians at the end of 1944. The actions included pillaging villages, murdering people, raping women and robbing inhabitants of their belongings[17]. Author and historian Mihael Sobolevski deems the inhuman terror committed by Chetniks as one of the most egregious tragedies in the Krivi Put community during World War II.

When the last rat left the town of Knin, the people cheered in joy. As the story continues, the cartoon pans over the pied piper leading the rats when a tractor appears in the back of the horizon. The piper herds the rats into the tractor, which then disappears. The pied piper then happily bids farewell to the tractor (a magical tractor, as the narrator sarcastically put it) full of rats, and the narrator ends the video by saying that rats "disappeared forever from the lands" and "everyone lived happily ever after". The tractor as a form of leaving the town is also historically symbolic. During Operation Storm, a polemic and highly controversial Croatian military action, many of the 200.000 ethnic Serbians who had to flee from Croatia in 1995 used trucks and tractors to leave the region[18]. The fleeing was an "epic scene of chaos" as Associated Press reporter Julijana Mojsilovic told the Los Angeles Times in 1995[19]. Mojsilovic described the scenes in more detail: "Disoriented people were fleeing with any possessions they could grab aboard tractors, cars, horse-driven carts, bicycles – just

17 Sobolevski, M. *Robbery and terror of Dinara Četnik division in the Krivi Put region on 28th and 29th December 1944*. https://hrcak.srce.hr/clanak/27653

18 McLaughlin, D. (2015, August 5). Croatia celebration of 1995 military victory alienates ethnic Serbs. *Al Jazeera*. http://america.aljazeera.com/articles/2015/8/5/croatia-celebration-of-1995-military-victory-alienates-and-angers-serbs1.html

19 Croatia Captures Rebel Serb City; Thousands Flee : Balkans: Takeover of Knin sends refugees on panicked flight to Serb-held areas of Bosnia. U.N. officer tells of bodies lying in the streets. Two more peacekeepers killed. https://www.latimes.com/archives/la-xpm-1995-08-06-mn-32175-story.html

about anything that could carry them"[20]. Reports also reported that roads were filled with anxious people stressfully taking flight with tractors. In Topusko, Serbs and Muslims were jammed into vehicles (mainly tractors, buses and trucks) even to have an opportunity to get out of Croatia[21]. Concluding the above, the tractor is a historical metaphor for the suffering, terror and inhuman circumstances that Serbs had to endure during the end of the war.

As for the extent of the content, the page had, at the time, over 50.000 followers. The post was viewed over 380.000 times, and despite the 397 user reports (362 reports concerning hate speech), Meta* opted not to take down the post and remove the content. The keep-up[22] decision was appealed to the OB, after which Meta* conducted an additional review (human review) to determine whether the content in question violated the Community Standards or the Hate Speech policy. Meta* has decided not to remove the content after the human review has been conducted. Interestingly, after the case was announced to be the subject of a full review by the OB, Meta* made two significant changes to the content moderation of the Knin cartoon. It is worth highlighting that the decision on the full review has concluded in January 2022, so the Knin cartoon has already been up and available on the platform for weeks. Meta* first decided that the Knin cartoon did not violate the Hate Speech policy per letter but per spirit[23] (quoting directly from the decision: "Meta* explained that a"spirit of the policy" decision is made when the policy rationale section of one the Community Standards makes clear that the policy is meant to address a given scenario that the language of the policy itself does not address directly") then later decided again that the offensive cartoon violated the Hate Speech policy per letter as well[24]. Meta* also concluded that all previous reviews were in error, meaning all three decisions on the keep-up decision were erroneous. To stir some confusion regarding the already – diplomatically – premature proceeding of the taking down-keeping up polemics, Meta* failed to inform the users of the modification and amendments to the decision after having informed them that the content did not violate Meta's* policies. The user who reported the content before the OB argued that: "[t]he Pied Piper symbolises the Croatian Army, which, in 1995, conducted an expulsion of Croatia's Serbs, portrayed here as rats".

---

20 Mojsilovic, J. (1995, August 6). Shelling of Knin Causes disbelief, panic, flight. https://www.washingtonpost.com/archive/politics/1995/08/06/shelling-of-knin-causes-disbelief-panic-flight/5cdb41ed-39c1-4c7f-a8f5-ab012c097039/

21 Pomfret, J. (1995, August 7). Thousands of Serb refugees flee Croatian army advance. *The Washington Post*. https://www.washingtonpost.com/archive/politics/1995/08/07/thousands-of-serb-refugees-flee-croatian-army-advance/2912317d-a965-449e-9c97-62ca900dc6a6/

22 Klonick, K. (2021, February 12). Inside the making of Facebook's Supreme Court. https://www.newyorker.com/tech/annals-of-technology/inside-the-making-of-facebooks-supreme-court

23 Oversight Board Case of Knin Cartoon. *Global Freedom of Expression*. https://globalfreedomofexpression.columbia.edu/cases/oversight-board-case-of-knin-cartoon/

24 Oversight Board Selects a Case Regarding a Video of an Edited Cartoon Depicting a Croatian City. https://transparency.fb.com/hu-hu/oversight/oversight-board-cases/cartoon-case/

2. The Oversight Board's decision

The OB overturned Meta's* decision to leave up the Knin cartoon on the platform. After a standard proceeding, the OB found that the video violated Facebook's* Hate Speech and Violence and Incitement Community Standards. The aim of said Community Standards is to prevent potential offline harm related to Facebook* content. When using this document, Facebook* intends to pay close attention to language and context to find the critical cultural, contextual, linguistic and other perspectives that can guide the moderators to interfere with someone's freedom of expression as the content that the user in question has published constitutes a credible threat to the public or personal safety. The Hate Speech policy also prohibits attacks against people based on protected characteristics, including ethnicity[25]. The OB found that portraying Serbians as rats is "dehumanising and hateful". The Board also concluded that the video constitutes a celebration of past acts of discriminatory treatment.

The OB rightly realises the deep historical and contextual connotations: Replacing the name "Hamelin" with the Croatian city of "Knin", the identification of the piper with the Croatian village of Čavoglave (a reference to the anti-Serb song "Bojna Čavoglave" by the band 'Thompson' whose lead singer is from Čavoglave) and the image of rats fleeing on tractors are all references to Croatian military's «Operation Storm." This 1995 operation reportedly resulted in the displacement, execution, and forcible disappearance of ethnic Serb civilians. The comments on the post confirm that this connection was clear to people who viewed the content[26].

Rooted in the issues above, the OB found that the post violated Dignity and Safety, two internal and core values/standards of Meta*.

As it turned out from the review of the OB, 40 Croatian-speaking moderators have worked on this issue, and none of them deemed the content a violation of Facebook* standards. However, the above is problematic from another aspect as well – as the OB correctly assumed, the hateful video, containing numerous deep discriminatory symbols and comparisons, can be an incitement to violence. Ergo, Meta* and the moderators not only failed to comply with the Hate Speech policies, but they did fail to comply with their own Violence and Incitement Community Standards.

The OB has raised awareness of two key issues in its decision. Firstly, the escalation of the moderation and the specialised moderation team has failed to encompass and understand the video's implicit and culturally undeniable meanings. As mentioned above, contextual and cultural distinctions should be highly emphasised when determining hate speech on Meta*, according to their hate speech policies. Secondly, the OB proposed two

[25] Oversight Board decision no. 2021-002-FB-UA. https://oversightboard.com/sr/decision/2021/002/public-comments

[26] Oversight Board overturns Meta's original decision in 'Knin cartoon' case (2022-001-FB-UA). https://oversightboard.com/news/1629549600777906-oversight-board-overturns-meta-s-original-decision-in-knin-cartoon-case-2022-001-fb-ua/

recommendations to Meta*: (1) the clarification of the Hate Speech Community Standard with a specialised guideline to understanding implicit references and (2) amendment to the modification system in accordance with the changes of Meta's determination of the case in question[27].

Conclusions

The OB aimed to involve public opinion on the Knin cartoon issue; therefore, the decision-making process was accompanied by the institution of a public commenting platform where third parties were capable of sharing their views on the case. In the Public Comment Appendix[28], the OB collected and shared 13 comments without sharing the identity of the authors of the comments. Interestingly, out of the 13 comments, only two originated from Europe, which is highly questionable and raises questions on the contextual and cultural interpretation dilemma. Even more curiously, in the Appendix, only two comments are available to be read.

Meta's* answer to the issues raised by the OB regarding the fact that the post may be categorised as a form of incitement is also to be examined critically. Meta* claimed that a violent threat must be supported or accompanied by exclusion or expulsion – ergo, something physically and forcibly violent[29]. This, however, raises a crucial question on the applicability of the Violence and Incitement Community Standard. According to Meta, the rat references, as well as their "fleeing" from the Knin cartoon, can not be undeniably and unmistakably construed as references to a possible violent threat with regard to the displacement of Serbians[30]. This explanation suggests a highly high threshold of the applicability of the abovementioned community standard. Although, naturally, arguing that the Knin cartoon case is an easy-to-decide case would be rather difficult, the threat is undoubtedly present because of the aforementioned historical references clearly and undisguisedly targeting Serbians and the visible and unfiltered mocking of the pain, suffering and loss of Serbians in 1995. In this context, it is also to be underlined that the narrator supposes that Knin lives happily only after every single rat has left the city, which can easily be interpreted even as a call for action.

A number of international legal texts were used, such as the International Covenant on Civil and Political Rights, the International Convention on the Elimination of All Forms of Racial Discrimination, the Office of the United Nations High Commissioner for Human

---

27 Oversight Board decision no. 2021-002-FB-UA. https://oversightboard.com/sr/decision/2021/002/public-comments

28 Oversight Board Public Comment Appendix for Knin Cartoon. https://oversightboard.com/news/1629549600777906-oversight-board-overturns-meta-s-original-decision-in-knin-cartoon-case-2022-001-fb-ua/

29 Oversight Board Case of Knin Cartoon. *Global Freedom of Expression*. https://globalfreedomofexpression.columbia.edu/cases/oversight-board-case-of-knin-cartoon/

30 *Ibid*.

Rights' Rabat Plan of Action or United Nations Human Rights Council Comm., General Comment No. 34, which is not unusual for the OB as it often relies on the principles laid down in these documents during decision-making (Bayer, 2021). These documents' usage further proves the OB's significant ambition to use and apply international principles to the cases brought before it (which is also supported by the fact the numerous judges came from a background based on international law expertise[31]). As Article 19 of the ICCPR was used to examine the interference with the post author's freedom of expression, the OB proposed a more concrete, academic and practical legal point of view. The most crucial part of the 3-part test in the present case is the question of legality. As the OB proposed, the idea, the usage and the application, or even the general understanding of the hate speech stipulations of Meta* are standing on a weak foot if 40 moderators failed to assume or understand the video posted as hate speech correctly. The proposal for a guideline cannot be constituted as a recommendation, and it is a warning sign for Meta* that the doctrines and the lack of applicability guides are a systematic problem which lets a hateful, offensive, and profoundly discriminatory post be present despite nearly 400 reports. Secondly, Meta* should invest more in the more profound appreciation and realisation of linguistic, ethnic, historical and cultural differences. The Board had even mentioned the linguistic aspect before in the Armenians in Azerbaijan case in 2020[32]. The answers of Meta* seemed to lack the abovementioned aspects, and moderators clearly failed to be cognizant of obvious references, which, again, is not a set of continuous individual mistakes but an inherent, implicit, ingrained and structural one rooted in the community standards. Meta*, thus far, has not issued a clearer guidebook on either hate speech or violent threats or the detection thereof. A third solution can be viewed as the most radical one. The OB currently does not have the power to directly influence or establish stipulations on policies set forth by Meta*, and the "house rules" (Goldman & Miers, 2021), therefore, may remain as untouched as ever, including the problematic algorithms that often fail to identify illegal content (Frazier, 2021). Though addressing speech policies is based on the constitutional non-delegation doctrine (Elkin-Koren & Perel, 2020; Cowls & Dominiquo-Schramm, 2022), the task of governing online spaces and platforms cannot be wholly and exclusively executed by public authorities and Facebook's* initiative to oversee moderation is certainly favourable in developing a conjoint mechanism (Balkin, 2018; Arun 2021). Alas, it would be more than interesting to see a recommendation that has a binding power on the policy development of Meta*[33], which would serve as a "multi-edged sword": (1) it would undoubtedly inspire Meta to improve the

31 What Kind of Oversight Board Have You Given Us? The University of Chicago Law Review Online. https://lawreviewblog.uchicago.edu/2020/05/11/fb-oversight-board-edouek/

32 Oversight Board decision no. 2021-002-FB-UA. https://oversightboard.com/sr/decision/2021/002/public-comments

33 Facebook Releases an Update on Its Oversight Board: Many Questions, Few Answers. https://www.lawfareblog.com/facebook-releases-update-its-oversight-board-many-questions-few-answers

standards, implement guidelines and generally ameliorate content moderation (Douek, 2019) and set standards for the platform (Bayer, 2021) and (2) a more user-based experience could be achieved as Meta* would be obligated to implement and create policies, standards and mechanisms that better represent user's interests (Klonick, 2020) and Meta* would evade concerns over "overmoderation" (Rogoff, 2019), and (3) the better implementation of international principles[34] would be more promptly applied to the right to freedom of expression on Facebook* (Dvoskin, 2022; Helfer & Land, 2022). In conclusion, a more formalised (Douek, 2022) and, at the same time, highly contextualised content moderation guideline system is recommended to provide an adaptable solution (Douek, 2022) to problems like the ones observed in the Knin cartoon case. A firm-specific proposal like the above could evolve the OB to play an even larger and more substantial role regarding Facebook's* moderation (Gorwa, 2019).

* The organization is recognized as extremist, its activity is prohibited in the territory of the Russian Federation.

References

Arun, Ch. (2021). Facebook's Faces. *Harvard Law Review Forum*, *135*, 22–37.

Balkin, J. M. (2018). Free Speech is a Triangle. *Columbia Law Review*, *118*, 12–20.

Banjeglav, T. (2015). A Storm of Memory in Post-War Croatia. *Cultures of History Forum*, *4*, 34–39.

Bayer, J. (2021). Rights and Duties of Online Platforms. In J. Bayer, B. Holznagel, P. Korpisaari, L. Woods (Eds.). *Perspectives on Platform Regulation: Concepts and Models of Social Media Governance Across the Globe*. Baden-Baden, Nomos–Digitalization and the Law. https://doi.org/10.1002/poi3.298

Bayer, J. (2022). A Facebook Ellenőrző Bizottság mint alternatív vitarendező szerv. *Fundamentum*, *3*, 5–16.

Benesch, S. (2020). But Facebook's Not a Country: How to Interpret Human Rights Law for Social Media Companies. *Yale Journal on Regulation Online Bulletin*, *38*, 71–86.

Chander, A. (2012). Facebookistan. *North Carolina Law Review*, *90*(5), 56–61.

Cowls, J-D., & Dominiquo-Schramm, M. (2022). Constitutional Metaphors: Facebook's 'Supreme Court' and the Legitimation of Platform Governance. *New Media & Society*, *3*, 23346. https://doi.org/10.1177/14614448221085559

Douek, E. (2019). Facebook's, Oversight Board: Move Fast with Stable Infrastructure and Humility. *North Carolina Journal of Law and Technology*, *21*, 123–130.

Douek, E. (2020). What Kind of Oversight Board Have You Given Us. *The University of Chicago Law Review Online*, *23*, 45–59.

Douek, E. (2021). Governing Online Speech. *Columbia Law Review*, *121*(3), 34456.

Douek, E. (2022). The Siren Call of Content Moderation Formalism. In L. Bollinger, G. Stone (Eds.). *Social Media, Freedom of Speech, and the Future of our Democracy*. Oxford, Oxford University Press. https://doi.org/10.1093/oso/9780197621080.003.0009

Dvoskin, B. (2022). Expert Governance of Online Speech. *Harvard International Law Journal*, *63*, forthcoming.

Elkin-Koren, N., & Perel, M. (2020). Separation of Functions for AI: Restraining Speech Regulation by Online Platforms. *Lewis & Clark Law Review*, *24*(3), n.pag. https://doi.org/10.2139/SSRN.3439261

Frazier, K. (2021). Why Meta Users Need a Public Advocate: a Modest Means to Address the Shortcomings of the Oversight Board. *Richmond Journal of Law & Technology*, *XXVIII*(3), 596–622.

Goldman, E., & Miers, J. (2021). Online Account Terminations/Content Removals and the Benefits of Internet Services Enforcing Their House Rules. *Journal of Free Speech Law*, *1*, 192–225.

[34] The Oversight Board: Operationalizing the UN Guiding Principles on Business and Human Rights. https://www.wbcsd.org/contentwbc/download/2248/28541

Gorwa, R. (2019). The platform governance triangle: conceptualising the informal regulation of online content. *Internet Policy Review*, *8*, 1–22. https://doi.org/10.14763/2019.2.1407

Helfer, L. R., & Land, M. K. (2022). The Facebook Oversight Board's Human Rights Future. *Cardozo Law Review*, *44*(6), 1–70.

Klonick, K. (2020). The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression. *The Yale Law Journal*, *129*, 2418.

Kulick, A. (2022). Corporations as Interpreters and Adjudicators of International Human Rights Norms – Meta's Oversight Board and Beyond. *The Law and Practice of International Courts and Tribunals*, *5*, 8–17.

Leutloff-Grandits, C. (2008). Claiming in Postwar Croatia: The Dynamics of Property Relations and Ethnic Conflict in the Knin Region. *Journal of Refugee Studies*, *21*(1), 34–45. https://doi.org/10.1093/jrs/fen004

Medzini, R. (2022). Enhanced self-regulation: The case of Facebook's content governance. *New Media & Society*, *24*(10), 1–29. https://doi.org/10.1177/1461444821989352

Melichárek, M. (2015). Národná symbolika a mýtus v srbských vojenských piesňach z obdobia r. 1991–1995. *Porta Balkanica*, *7*(2), 25–34.

Nunziato, D. C. (2022). Protecting Free Speech and Due Process Values on Dominant Social Media Platforms. *Hastings Law Journal*, *73*(5), 1255.

O'Kane, R. (2022). Meta's Private Speech Governance and the Role of the Oversight Board: Lessons from the Board's First Decisions. *Stanford Technology Law Review*, *25*(2), 167–209.

Pickup, E. L. (2021). The Oversight Board's Dormant Power to Review Facebook's Algorithms. *Yale Journal on Regulation Bulletin*, *39*(1), 2–21.

Pongó, T. (2020). Új Korszak Az Online Véleménynyilvánítás Korlátozásában? Gondolatok a Facebook Oversight Board működéséről. *Iustum Aequum Salutare*, *XVI*(4), 147–162.

Ramet, S. P. (2011). Serbia and the Serbs in World War Two. Berlin, Springer. https://doi.org/10.1057/9780230347816

Robionek, B. (2017). Musik als Transportmittel für Ideologie. In K., Bozay, D. Borstel (Eds.). *Ungleichwertigkeitsideologien in der Einwanderungsgesellschaft*. Wiesbaden, Springer. https://doi.org/10.1007/978-3-658-14245-2_14

Rogoff, Z. (2019). Five Free Expression Safeguards from a Facebook User's Perspective. *TPRC47: Research Conference on Communications, Information and Internet Policy*. http://dx.doi.org/10.2139/ssrn.3428062

Sale, H. A. (2022). Monitoring Facebook. *Harvard Business Law Review*, *12*. https://ssrn.com/abstract=4213540

Schultz, M. (2021). Six Problems with Facebook's Oversight Board. In J. Bayer, B. Holznagel, P. Korpisaari, & L. Woods (Eds.), *Perspectives on Platform Regulation: Concepts and Models of Social Media Governance Across the Globe*. Baden-Baden, Nomos. https://doi.org/10.5771/9783748929789-145

Singleton, F. Hinds, L. A., Krebs, Ch., & Spratt, D. M. (2003). R*ats, mice and people: rodent biology and management*. Canberra, Australian Centre for International Agricultural Research.

Takhshid, Z. (2021). Regulating Social Media in the Global South. *Vanderbilt Journal of Entertainment & Technology Law*, *24*(1), 1–55.

Vukčević, I. (2021). Facebook Oversight Board's Decision on the Indefinite Suspension of Donald Trump's Account. *Pravni Zapisi*, *12*(1), 295–311. https://doi.org/10.5937/pravzap0-32521

Wong, D., & Floridi, L. (2022). Meta's Oversight Board: A Review and Critical Assessment, Minds and Machines. https://doi.org/10.1007/s11023-022-09613-x

Author information

Gergely Ferenc Lendvai – Juris Doctor, dr. and Pázmány Péter Catholic University (PhD candidate)
Address: Hattyú utca 17, Budapest, Hungary
E-mail: lendvaigergely@me.com
ORCID ID: https://orcid.org/0000-0003-3298-8087
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/record/ISU-4560-2023
Google Scholar ID: https://scholar.google.com/citations?user=CVKzt1AAAAAJ

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

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

Article history

Date of receipt – December 20, 2022
Date of approval – May 1, 2023
Date of acceptance – August 15, 2023
Date of online placement – August 20, 2023

Научная статья
УДК 34:34.096:7.091.5:7.097:004
EDN: https://elibrary.ru/xoftaw
DOI: https://doi.org/10.21202/jdtl.2023.26

«Чисто крысиная страна» – размышления о решении по делу 2022-001-FB-UA Наблюдательного совета Фейсбука (Дело мультфильма о городе Книн)

Гергели Ференц Лендваи

Католический университет Петера Пазманя
Будапешт, Венгрия

Ключевые слова

Мета*,
мультфильм о городе Книн,
Наблюдательный совет,
права человека,
право,
регулирование,
свобода выражения мнения,
Фейсбук*,
цифровые технологии,
язык ненависти

Аннотация

Цель: в работе представлен анализ решения Наблюдательного совета Фейсбука* по делу 2022-001-FB-UA, известному как «Дело мультфильма о городе Книн». Цель исследования – определение места данного дела в историческом и культурном контексте и выработка критического подхода к проблеме модерирования контента в компании «Фейсбук»*.

Методы: основным методом, используемым в работе, является изучение источников. Исследование опирается на сравнительное изучение и анализ кейсов. Использованы положения различных дисциплин, таких как философия права, международное право, право в области средств массовой информации, регулирование деятельности платформ, история.

Результаты: в работе представлен контекст дела мультфильма о городе Книн и основные решения Наблюдательного совета Фейсбука* с их обоснованиями. Кроме того, отражена концепция языка ненависти в понимании Наблюдательного совета и сделана попытка показать контекст и описать основные проблемы и возможные решения в области модерирования контента в компании Мета* на примере данного дела.

Научная новизна: с момента опубликования решения по делу мультфильма о городе Книн в 2022 г. он не подвергался глубокому историческому и контекстуальному анализу. До настоящего времени вышли лишь несколько работ, анализирующих его с юридической точки зрения.

Практическая значимость: полученные результаты важны в трех основных аспектах: (1) они могут быть использованы для дальнейшего критического анализа модерирования контента в компании «Фейсбук»*, (2) они могут служить в качестве рекомендаций в области регулирования деятельности платформ и разработки инструкций и (3) они показывают исключительную актуальность и важность целостного подхода к определению языка ненависти. В рамках последнего аспекта работа доказывает, что историческая, культурная, общественная и символическая интерпретация и понимание проблемы определения языка ненависти является не только практически применимым, но и единственным целесообразным методом для распознавания, определения и вынесения суждения о предполагаемом использовании языка ненависти.

Для цитирования

Лендваи, Г. Ф. (2023). «Чисто крысиная страна» – размышления о решении 2022-001-FB-UA Наблюдательного совета Фейсбука (Дело мультфильма о городе Книн). *Journal of Digital Technologies and Law*, *1*(3), 612–628. https://doi.org/10.21202/jdtl.2023.26

Список литературы

Arun, Ch. (2021). Facebook's Faces. *Harvard Law Review Forum*, *135*, 22–37.

Balkin, J. M. (2018). Free Speech is a Triangle. *Columbia Law Review*, *118*, 12–20.

Banjeglav, T. (2015). A Storm of Memory in Post-War Croatia. *Cultures of History Forum*, *4*, 34–39.

Bayer, J. (2021). Rights and Duties of Online Platforms. In J. Bayer, B. Holznagel, P. Korpisaari, L. Woods (Eds.). *Perspectives on Platform Regulation: Concepts and Models of Social Media Governance Across the Globe*. Baden-Baden, Nomos–Digitalization and the Law. https://doi.org/10.1002/poi3.298

Bayer, J. (2022). A Facebook Ellenőrző Bizottság mint alternatív vitarendező szerv. *Fundamentum*, *3*, 5–16.

Benesch, S. (2020). But Facebook's Not a Country: How to Interpret Human Rights Law for Social Media Companies. *Yale Journal on Regulation Online Bulletin*, *38*, 71–86.

Chander, A. (2012). Facebookistan. *North Carolina Law Review*, *90*(5), 56–61.

Cowls, J-D., & Dominiquo-Schramm, M. (2022). Constitutional Metaphors: Facebook's 'Supreme Court' and the Legitimation of Platform Governance. *New Media & Society*, *3*, 23346. https://doi.org/10.1177/14614448221085559

Douek, E. (2019). Facebook's, Oversight Board: Move Fast with Stable Infrastructure and Humility. *North Carolina Journal of Law and Technology*, *21*, 123–130.

Douek, E. (2020). What Kind of Oversight Board Have You Given Us. *The University of Chicago Law Review Online*, *23*, 45–59.

Douek, E. (2021). Governing Online Speech. *Columbia Law Review*, *121*(3), 34456.

Douek, E. (2022). The Siren Call of Content Moderation Formalism. In L. Bollinger, G. Stone (Eds.). *Social Media, Freedom of Speech, and the Future of our Democracy*. Oxford, Oxford University Press. https://doi.org/10.1093/oso/9780197621080.003.0009

Dvoskin, B. (2022). Expert Governance of Online Speech. *Harvard International Law Journal*, *63*, forthcoming.

Elkin-Koren, N., & Perel, M. (2020). Separation of Functions for AI: Restraining Speech Regulation by Online Platforms. *Lewis & Clark Law Review*, *24*(3), n.pag. https://doi.org/10.2139/SSRN.3439261

Frazier, K. (2021). Why Meta Users Need a Public Advocate: a Modest Means to Address the Shortcomings of the Oversight Board. *Richmond Journal of Law & Technology*, *XXVIII*(3), 596–622.

Goldman, E., & Miers, J. (2021). Online Account Terminations/Content Removals and the Benefits of Internet Services Enforcing Their House Rules. *Journal of Free Speech Law*, *1*, 192–225.

Gorwa, R. (2019). The platform governance triangle: conceptualising the informal regulation of online content. *Internet Policy Review*, *8*, 1–22. https://doi.org/10.14763/2019.2.1407

Helfer, L. R., & Land, M. K. (2022). The Facebook Oversight Board's Human Rights Future. *Cardozo Law Review*, *44*(6), 1–70.

Klonick, K. (2020). The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression. *The Yale Law Journal*, *129*, 2418.

Kulick, A. (2022). Corporations as Interpreters and Adjudicators of International Human Rights Norms – Meta's Oversight Board and Beyond. *The Law and Practice of International Courts and Tribunals*, *5*, 8–17.

Leutloff-Grandits, C. (2008). Claiming in Postwar Croatia: The Dynamics of Property Relations and Ethnic Conflict in the Knin Region. *Journal of Refugee Studies*, *21*(1), 34–45. https://doi.org/10.1093/jrs/fen004

Medzini, R. (2022). Enhanced self-regulation: The case of Facebook's content governance. *New Media & Society*, *24*(10), 1–29. https://doi.org/10.1177/1461444821989352

Melichárek, M. (2015). Národná symbolika a mýtus v srbských vojenských piesňach z obdobia r. 1991–1995. *Porta Balkanica*, *7*(2), 25–34.

Nunziato, D. C. (2022). Protecting Free Speech and Due Process Values on Dominant Social Media Platforms. *Hastings Law Journal*, *73*(5), 1255.

O'Kane, R. (2022). Meta's Private Speech Governance and the Role of the Oversight Board: Lessons from the Board's First Decisions. *Stanford Technology Law Review*, *25*(2), 167–209.

Pickup, E. L. (2021). The Oversight Board's Dormant Power to Review Facebook's Algorithms. *Yale Journal on Regulation Bulletin*, *39*(1), 2–21.

Pongó, T. (2020). Új Korszak Az Online Véleménynyilvánítás Korlátozásában? Gondolatok a Facebook Oversight Board működéséről. *Iustum Aequum Salutare*, *XVI*(4), 147–162.

Ramet, S. P. (2011). Serbia and the Serbs in World War Two. Berlin, Springer. https://doi.org/10.1057/9780230347816

Robionek, B. (2017). Musik als Transportmittel für Ideologie. In K., Bozay, D. Borstel (Eds.). *Ungleichwertigkeitsideologien in der Einwanderungsgesellschaft*. Wiesbaden, Springer. https://doi.org/10.1007/978-3-658-14245-2_14

Rogoff, Z. (2019). Five Free Expression Safeguards from a Facebook User's Perspective. *TPRC47: Research Conference on Communications, Information and Internet Policy*. http://dx.doi.org/10.2139/ssrn.3428062

Sale, H. A. (2022). Monitoring Facebook. *Harvard Business Law Review*, *12*. https://ssrn.com/abstract=4213540

Schultz, M. (2021). Six Problems with Facebook's Oversight Board. In J. Bayer, B. Holznagel, P. Korpisaari, & L. Woods (Eds.), *Perspectives on Platform Regulation: Concepts and Models of Social Media Governance Across the Globe*. Baden-Baden, Nomos. https://doi.org/10.5771/9783748929789-145

Singleton, F. Hinds, L. A., Krebs, Ch., & Spratt, D. M. (2003). R*ats, mice and people: rodent biology and management*. Canberra, Australian Centre for International Agricultural Research.

Takhshid, Z. (2021). Regulating Social Media in the Global South. *Vanderbilt Journal of Entertainment & Technology Law*, *24*(1), 1–55.

Vukčević, I. (2021). Facebook Oversight Board's Decision on the Indefinite Suspension of Donald Trump's Account. *Pravni Zapisi*, *12*(1), 295–311. https://doi.org/10.5937/pravzap0-32521

Wong, D., & Floridi, L. (2022). Meta's Oversight Board: A Review and Critical Assessment, Minds and Machines. https://doi.org/10.1007/s11023-022-09613-x

Информация об авторе

Гергели Ференц Лендваи – доктор права, докторант, Католический университет Петера Пазманя
Адрес: Венгрия, г. Будапешт, улица Хаттью, 17
E-mail: lendvaigergely@me.com
ORCID ID: https://orcid.org/0000-0003-3298-8087
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/record/ISU-4560-2023
Google Scholar ID: https://scholar.google.com/citations?user=CVKzt1AAAAAJ

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: 10.19.65 / Правонарушения в области информатики. Ответственность в информационном праве
Специальность ВАК: 5.1.2 / Публично-правовые (государственно-правовые) науки

История статьи

Дата поступления – 20 декабря 2022 г.
Дата одобрения после рецензирования – 1 мая 2023 г.
Дата принятия к опубликованию – 15 августа 2023 г.
Дата онлайн-размещения – 20 августа 2023 г.

Research article
DOI: https://doi.org/10.21202/jdtl.2023.27

Intelligent Transport Systems as the Basis of de Lege Ferenda of the Transport System of the Russian Federation

Maria A. Bazhina

V. F. Yakovlev Ural State Law University
Yekaterinburg, Russian Federation

Keywords

Artificial intelligence,
digital technologies,
highly automated vehicle,
intelligent transport system,
law,
legal regulation,
Safety,
transport infrastructure,
transport legislation,
unmanned vehicle

Abstract

Objective: to research the trends of legal regulation of using intelligent transport systems under digital transformation of the transport sector of economy, namely, the growing importance of intelligent transport systems in the future transport system of the Russian Federation.

Methods: systemic-structural method is the basis for researching intelligent transport systems. It enables to study the architecture of intelligent transport systems as a complex structural unity. Also, comparative-legal method was used, aimed at illustrating the differences and similarities in the legal regulation of intelligent transport systems. Methods of legal modeling and forecasting, as well as formal-logic method, served as secondary methods to comprehensively study the legal regulation of intelligent transport systems.

Results: the article presents conceptual approaches to defining the notion of "intelligent transport systems" and outlining the hierarchy of intelligent transport systems, which play a fundamental role in building the transport sector. Based on the analysis, conclusions are made about the vectors of forming transport legislation, aimed at regulating the use of intelligent transport systems.

Scientific novelty: the article provides a conceptual approach to forming the legal regulation of intelligent transport systems. To this end, the issue is considered about the essential content of the notion

of “intelligent transport systems” at legal and scientific levels; the current terminological problems in building the legal regulation are shown. Analysis of the architecture of intelligent transport systems allowed for the first time to formulate the basic approaches to shaping the legal regulation of its individual elements (including highly automated and fully automated transport means, “smart” infrastructure, etc.) not in isolation but as constituent parts of the whole matter.

Practical significance: the presented materials and conclusions facilitate the development of legal regulation of transport industry under digital transformation. The article accentuates the legal regulation of intelligent transport systems taking into account their technical and technological features. It is the intelligent transport systems that are de lege ferenda of the transport system, which determines the vector of transformation of transport legislation. In turn, development of the legal bases allows broadening the geography of introducing technical novelties and making their application much more large-scale.

For citation

Bazhina, M. A. (2023). Intelligent Transport Systems as the Basis of de Lege Ferenda of the Transport System of the Russian Federation. *Journal of Digital Technologies and Law, 1*(3), 629–649. https://doi.org/10.21202/jdtl.2023.27

Contents

Introduction

The modern national and global transport system is characterized by constantly growing numbers of transport means participating in carrying cargo and passengers. This trend has the following negative consequences:

1) the growing number of transport accidents, the immediate cause of which is the human factor, in most cases;

2) harmful impact on the environment (Bagreeva et al., 2019);

3) overload of transportation routes, which leads to problems with coordination of logistic chains and decreasing the speed of cargo delivery (Du et al., 2023);

4) lack of transparency of the transportation process;

5) lack of a "seamless" transportation corridor for carrying cargo and passengers (underdeveloped multimodal transportation).

At the same time, the stable development of the Russian economy (in particular, the effective functioning of distribution chains and other economy segments) requires accelerating the cargo turnover on the premise of the increased safety of transportation process, quality of the transportation operations performed, ensuring their reliability and transparency. In other words, it is necessary to create an integrated and continuous multimodal system of sustainable and intelligent transport mobility[1].

To solve the above tasks for all modes of transport, certain measures are taken, associated with the increased automation of certain transport operations, emergence of digital services for the participants of transportation process, development of interfaces to implement projects controlling parking lots and stands, traffic regulation, automated identification of vehicles, etc. The current changes, touching upon all modes of transport, require creating a legal system, which is nowadays is being formed through issuing individual normative-legal acts. Examples include the following. In aviation industry, the Complex program of aviation sector development in the Russian Federation up to 2030[2] was adopted. In the maritime sphere, the Naval doctrine of the Russian Federation[3] was adopted. In railroad sector, changes will come into force since September 2023 referring to transporting passengers, luggage, and cargo using automated systems[4].

However, the largest number of changes is related to the legal regulation of automobile transportation. This is due to the fact that, on the basis of the 78th session of the Global forum on road safety held in Geneva on March 25–29, 2019, a resolution was adopted[5], according to which highly- and fully automated vehicles are introduced into road traffic. This document became the basis for further development of legal regulation of the use of automated vehicles in various countries. For example, the Russian Federation adopted the Concept of ensuring road safety on general purpose automobile roads using unmanned

1 This task seems relevant not only within one state but at the international level as well (decision of the European Commission of December 3, 2021, establishing the Multimodal forum for passenger mobility).

2 Executive Order of the Government of the Russian Federation No. 1693-r of 25.06.2022. (2022). *Collection of legislation of the Russian Federation*, *27*, Article 4877.

3 Decree of the President of the Russian Federation No. 512 of July 31, 2022 (2022). *Collection of legislation of the Russian Federation*, *31*, Article 5699.

4 Order of the Ministry of Transportation of the Russian Federation No. 352 of September 5, 2022 (2022). *Official Internet-portal of legal information*. www.pravo.gov.ru, # 0001202210270033.

5 *Report of the Global forum on road safety on the work of its 78th session*. https://unece.org/DAM/trans/doc/2019/wp1/ECE-TRANS-WP1-167r.pdf

vehicles[6] (further – the Concept of ensuring road safety). Besides, the Russian government adopted new rules of transporting cargo by automobile vehicles[7].

Foreign countries also develop legislation in this field. For example, Japan adopted the Public-Private ITS Concept Roadmap 2018[8]. On June 7, 2019, the plan was reviewed, but no conceptual changes were introduced (Public-Private ITS Concept Roadmap 2019)[9].

The mentioned measures are a serious step towards creating and functioning of an integrated transportation system in the country. However, it is obvious that they are not sufficient for implementation of the set task, as the current digitalization measures are discrete. This local character exists not only in technical but also in legal terms. Isolation of the technical component consists in automation being implemented only in certain segments of the transportation process. Each segment functions in isolation, without the required interconnections between them. Besides, digitalization of transport industry is performed separately by modes of transport. From the viewpoint of legal regulation, the adopted normative-legal acts aimed at regulating transport relations (in particular, the use of intelligent transport systems) are explicitly pro-automobile. The lack of a common legal regulation stipulating the universal rules with regard to all modes of transport[10] is an obstacle for creating a national interactive transport system, as was indicated in the Transport strategy of the Russian Federation up to 2030 with a forecast up to 2035[11], which would serve as the basis for solving the above problems (Zhihan & Shang, 2022). Also, locality in the legal aspect implies the lack of international regulation but the predominance of the national legislation.

The above testifies to the fact that in the Russian Federation there is still no transportation system as an integral structure, providing transportation accessibility, mobility, transparence, safety of transportation services, and a common legal regulation of transportation system. Under digitalization, such separation of the elements of transportation system becomes even more obvious.

---

6 Executive Order of the Government of the Russian Federation No. 724-r of March 25, 2020 (2020). *Collection of legislation of the Russian Federation*, 13, Article 1995.

7 Decree of the Government of the Russian Federation No. 2200 of December 21, 2020 (2020). *Collection of legislation of the Russian Federation*, 52(part II), Article 8877.

8 Public-Private ITS Concept Roadmap 2018. https://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20180615/siryou9.pdf

9 Public-Private ITS Concept Roadmap 2019. https://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20190607/siryou9.pdf

10 In this case, there may be exceptions from the universal approach in legal regulation, due to technical features of a specific kind of transport and the transportation process associated with it.

11 Executive Order of the Government of the Russian Federation No. 3363-r of November 27, 2021 (2021). *Collection of legislation of the Russian Federation*, 50 (part IV), Article 8613.

Thus, the transportation industry faces the need to create a single transport environment, providing the multimodal technological interaction of various modes of transport, participants of the transportation process and infrastructure both within one state and at international level. The sustainable and inclusive mobility can be only provided by increasing connectedness and coordination between all processes taking place in the transport activity.

Emergence of end-to-end digital technologies (artificial intelligence, Internet of Things, cloud and fog computing, robotics, big data processing[12]) became the necessary tool (Gromova & Ivanc, 2020) which enabled to solve the set tasks in transport industry. The use of digital technologies makes it possible to speak of creating intelligent transport systems, intended for synchronization and coordination of all its elements, on the one hand, and integration of information-communication technologies into the country's transport complex, on the other hand. It is intelligent transport system that forms a potential for developing the transport system in Russia. This important role of intelligent transport systems is due to the fact that, on the basis of collecting, processing and analyzing the data from all sources, the valuable information is formed, which is then used for control and decision making on transport. Due to the said characteristics, intelligent transport systems can meet the challenges indicated in the Strategic direction in the sphere of digital transformation of transport industry of the Russian Federation up to 2030[13].

Despite the high significance of intelligent transport systems, their legal regulation is currently still being formed. This is due to formation of the essential content of the notion "intelligent transport systems" and building the structure of intelligent transport systems.

1. Ontology of the notion of "intelligent transport systems"

Legal regulation of various public relations is based on the conceptual apparatus (Bazhina, 2022), the syntagmatic unit (Fomenko, 1970) of which is a notion. The essential content of notions determines the very direction of legal regulation. Efficiency of legal regulation depends on the accurate wording of the notion content and construction of logical interconnections between the notions. That is why establishing the content of the notion of "intelligent transport systems" seems to be a primary tasks in the study of legal regulation of using intelligent transport systems.

---

12 Clause 36 of the Strategy of information society development in the Russian Federation, adopted by the Decree of the President of the Russian Federation of May 9, 2017 No. 203.

13 Executive Order of the Government of the Russian Federation No. 3744-r of December 21, 2021. (2021). *Collection of legislation of the Russian Federation*, 1 (part IV), Article 264.

In the 1980s–1990s, some countries researched the issues of transport flows coordination. One example is a Munich project COMFORT, aimed at optimizing the transport flow in a city center taking into account the planning of highway network in the neighboring towns[14].

In 1994, an international congress was for the first time held in Paris, devoted to intelligent transport systems, namely, intelligent automobile highway transport systems[15]. In 1995, the congress was held in Yokohama, Japan. This event became the basis for creating a project called the "Extensive plan for development of intelligent transport systems". Thus, Japan is considered to be the country where the intelligent transport systems originated.

Currently, many countries of the world carry out developments in this sphere. In this regard, it is important to define the essential content of intelligent transport systems.

In a broad sense, an intelligent transport system is interpreted as a system ensuring mobility using digital technologies. However, various countries provide their own definitions of the notion of "intelligent transport systems", which differ in certain aspects. Notably, some documents offer no definitions but focus on the importance of intelligent transport systems for the transport sector of economy.

Below we consider several approaches to defining the notion of "intelligent transport systems".

1. Essential component of the notion "intelligent transport systems" is defined by indicating their direct purpose.

The Japanese Society of Automotive Engineers issued a special document called "Standardization of intelligent transport systems. Activity of ISO/TS 204"[16] (further – Standardization of ITS adopted by the Japanese Society of Automotive Engineers); it points out that intelligent transport systems are specially created to rapidly increase traffic safety, transportation efficiency and comfort, energy saving and environment protection (Hasegawa, 2013).

2. Intelligent transport system is interpreted as a system of transportation.

The UNECE Road Map on Intelligent Transport Systems for 2021–2025, issued by the UN Economic Commission for Europe in December 2020[17] (further – the UNECE Road Map on Intelligent Transport Systems), intelligent transport system is understood as a system of internal transport to which information-communication technologies (further – ICT) with a view of providing mobility.

---

14 Zhankazieva S. V., & Vorobyeva T. V. (2013). World experience of formation and development of regional ITS. *Vestnik GLONASS*. http://vestnik-glonass.ru/stati/mirovoy_opyt_stanovleniya_i_razvitiya_regionalnykh_its/

15 European Commission. (1995). "Towards an intelligent transport system". Community Research and Development Information Service.

16 https://www.jsae.or.jp/01info/org/its/its_2019_en.pdf

17 *Draft revision of the UNECE Road Map on Intelligent Transport Systems*. UNECE. https://unece.org/sites/default/files/2021-01/ECE-TRANS-2021-15r.pdf

3. Intelligent transport systems are a set of applications or technologies. Such approach is used in the Preamble of the Directive 2010/40/EU of the European Parliament and of the Council of July 7, 2010, "on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport"[18] (further – EU Directive 2010). These applications are aimed at provision of innovative services related to various modes of transport. They help various users to be better informed about the condition of transport network. Thus, the use of transport networks becomes safer, more coordinated and 'smarter'. In the legislation of Canada, intelligent transportation system is defined as the advanced and emerging technology (including computers, sensors, control, communications, and electronic devices) in transportation to save lives, time, money, energy and the environment[19].

The Standards of International Standardization Organization ISO/TS14812:2022 Intelligent transport systems – Vocabulary in clause 3.1.2.4 define intelligent transport systems by listing their constituent elements. These are various technologies, namely: information, communication, sensor, and control technologies, intended for use in the interests of ground transport system.

4. Intelligent transport system is interpreted as a system of transport complex management. This approach underlies regulation of intelligent transport systems in Russia. The notion of "intelligent transport systems" is stipulated in the Russian national standard of the same title. It is understood as "the management system integrating modern information and telematic technologies and intended for automated search and acceptance for implementation of the maximally effective scenarios of managing a regional transport-road complex, a specific vehicle or group of vehicles, with a view of providing the set mobility of the population, maximizing the indicators of road network exploitation, increasing safety and efficiency of the transportation process, comfort of the drivers and users of transport"[20].

This notion is fully repeated in several normative-legal acts, namely: the Concept for providing safety of road traffic with participation of unmanned vehicles on general purpose automobile roads[21], as well as the general provisions of the Concept for creating and functioning of the national network of intelligent transport systems

---

18 European Parliament. https://www.europarl.europa.eu/legislative-train/theme-resilient-energy-union-with-a-climate-change-policy/file-electronic-freight-transport-information

19 *ITS Canada*. https://www.itscanada.ca/about

20 *GOST R 56829-2015 "National standard of the Russian Federation. Intelligent transport systems. Terms and definitions"*. https://docs.cntd.ru/document/1200128315?section=text

21 Executive Order of the Government of the Russian Federation No. 724-r of March 25, 2020 (2020). *Collection of legislation of the Russian Federation*, 13, Article 1995.

on general purpose automobile roads[22] (further – Concept for creating intelligent transport systems).

Scientific literature also supports the above concept in terms of the essence of intelligent transport systems. An intelligent transport system is integration of management, information and communication technologies with transport infrastructure (Sladkowski & Pamula, 2016).

The presented concepts illustrate the overall pattern of the development of legal regulation with regard to intelligent transport systems. As was justly noted in the UNECE Road Map on Intelligent Transport Systems, due to the differences in economic priorities each state may interpret the content of the notion "intelligent transport systems" in its own way[23]. From the viewpoint of legal regulation of the use of intelligent transport systems, such inconsistency may cause "confusion at international level"[24]. This seems to be an obstacle for the global introduction and use of intelligent transport systems. Accordingly, an important step in overcoming the said difficulties may become the development of the general, interstate guidelines and rules which would allow determining the order of technical and technological compatibility of intelligent transport systems used in each state.

The presented definitions have certain common features which can be identified.

First, intelligent transport systems are the basis of the contemporary transport system.

Second, intelligent transport systems are directly connected with digital technologies with the help of which they function.

Third, the key purpose of using intelligent transport systems consists in automation of transport operations with a view of creating a competitive transport system.

However, none of the mentioned deterministic approaches is comprehensive. This is due to the fact that the elements of an intelligent transport system are not comprehensively considered in the presented definitions. Meanwhile, structural elements are significant for determining the essential content of a notion, as well as for building logical links with other notions and forming the conceptual apparatus underlying any legal regulation. It is this aspect that served as the basis for considering the architecture (structure) of intelligent transport systems.

---

22 Order of the Ministry of Transportation of the Russian Federation No. AK-247-r of 30.09.2022. (2022). *Transport of Russia*, 49, 05.12.2022–11.12.2022.

23 *Status of the implementation of the ECE Road Map on Intelligent Transport Systems.* UN Economic Commission for Europe. https://unece.org/sites/default/files/2023-01/ECE_TRANS_2023_19_Rev1R.docx

24 *Ibid*.

2. Architecture (structure) of intelligent transport systems

When considering the issue of the architecture of intelligent transport systems, one should specify several conceptual aspects.

First, considering the issue of the architecture of intelligent transport systems seems strategically important to reflect the essence of intelligent transport systems and their definite purpose in the evolution of transport activity. It is through the architecture of intelligent transport systems that integration into the very idea of creating the intelligent transport systems takes place and its emergence is determined. Building the architecture of intelligent transport systems is pivotal for developing an adequate legal regulation of the use of intelligent transport systems.

Second, the architecture of intelligent transport systems is currently developed with regard to road transport network. Other components of transport system (other modes of transport) are not considered in the documents devoted to automobile transport. This determines the specified elements of the architecture of intelligent transport systems.

Many documents, including normative legal acts, use the notion of "the architecture of intelligent transport systems". According to the Russian preliminary national standard on intelligent transport systems, "the architecture is understood as fundamental concepts or properties of the system in its own environment, embodied in elements, relations, and structure"[25]. In other words, the term "architecture" denotes a certain structure, forming the intelligent transport system as a system consisting of various elements. It is used to emphasize the complexity and multifunctionality of intelligent transport systems.

Various sources, both normative and academic, call these components differently, namely: levels, subsystems, etc. The grounds for specifying such elements also differ.

The Concept for creating intelligent transport systems indicates that their architecture must consist of certain levels, namely: integration platform, complex subsystem, instrumental subsystem, peripheral equipment, telecommunication infrastructure, and solutions (including hardware-software) in the sphere of information security and failure safety.

Another approach to defining the levels is described in a book devoted to intelligent transport systems in road traffic, published by Radiocommunication Bureau (Switzerland)[26]. According to it, the criterion for specifying the levels of intelligent transport systems are their users, divided into three groups. The first group is road operators, i. e. an organization managing roads for local purposes, as a rule, to maintain the traffic and react

---

[25] *PNST RF 636-2022 «Intelligent transport systems. Commercial transportation. Control over automobile transportation in a supply chain. Part 1. Architecture and definitions of data".* (2022). Moscow: FGBU RST.

[26] *Intelligent transport systems: Handbook on Land Mobile (including Wireless Access)* (Vol. 4. 2021 edition). https://www.itu.int/dms_pub/itu-r/opb/hdb/R-HDB-49-2021-PDF-E.pdf

to road accidents. They control the traffic situation and provide information to the traffic participants. The road operator plays an important role in rendering various services of intelligent transport systems. One exception is the systems for providing safety between vehicles. The second group of users consists of vehicle drivers. This group is the final user of many services of intelligent transport systems and an indirect supplier of a large amount of data about the road characteristics (either through remote testing or through information collection by a vehicle and providing it to a third party). The third group of users is travelers or pedestrians who use intelligent transport systems to obtain information about the road situation, to plan trips, use transit services or require for emergency assistance.

According to the definition of "intelligent transport system"[27] by the division of the US Department of Transportation – Research and Innovative Technology Administration (RITA)[28], it consists of 26 types of technology-based systems. These systems can be divided into two large categories: smart infrastructure and smart vehicles.

Another viewpoint is that intelligent transport systems consist of the following elements: road signals management systems, road traffic management systems, highway management systems, transit management systems, accident management systems, traveler information services, emergency management services, extended analytics of road traffic, electronic payment systems, public transport management systems, connected cars infrastructure, road network productivity monitoring, safety systems on railway crossings, and commercial transport management systems (Abduljabbar et al, 2019).

Similar to this is the concept according to which intelligent transport systems include a smart system of public transport, a smart system of road infrastructure, a smart system of parking lots, a smart system of road management and control, safety and emergency management, a smart system of pavement management (Lakshmi Shankar Iyer, 2021).

The hierarchical analysis of intelligent transport systems shows the lack of a common approach to specify the components of intelligent transport systems. Accordingly, the components indicated in a system differ from each other based on the grounds for their specification. This feature determines the development of legal regulation of the use of intelligent transport systems.

---

27 *Intelligent Transportation Systems Joint Program Office. Strategic Plan 2020–2025*. www.ITS.DOT.GOV/STRATPLAN2020

28 This division of the US Department of Transportation was created in 2005 in order to improve coordination of transport research, develop transport studies, technologies, and analysis.

3. Prospects of development of legal regulation and use of intelligent transport systems

The above analysis of the essential content of the "intelligent transport systems" notion and the hierarchical structure of the intelligent transport systems allows making certain conclusions regarding the legal regulation of the use of intelligent transport systems. Below we consider them in more detail.

1. The current trend in forming the national legislation regarding the use of intelligent transport systems does not fully reflect the needs of modern economy. This is due to the fact that the development of all spheres of activity is oriented towards international exchange of goods. Besides, the development of intelligent transport systems testifies to the emergence of interstate issues related to providing cybersecurity. Thus, information-communication technologies, so to say, blur the existing territorial boundaries between the states and a threat to digital security of a state occurs (Kutyur & Toupin, 2020). Solving these problems at a self-contained national level cannot be effective. An interstate approach is demanded in developing the legal regulation of intelligent transport systems.

2. Specifying the above listed elements as components of the integral entity is only oriented towards automobile transport. This does not comply with the conceptual approach stipulated by the program documents devoted to reforming the transport industry. Mobility in transport sphere implies not only the possibility to seamlessly deliver cargo from one point to another (including using various modes of transport), but also transparency of the whole transportation process (including the document flow).

3. The hierarchy of intelligent transport system determines the directions of legal regulation development in the transport sphere. The described approaches to specifying the structural components are built on the basis of the tasks faced by the transport sector of economy. These include: transport management, safety provision, "smart" vehicles and transport infrastructure. Legal regulation of these directions is currently imperfect (Zemlin, 2022). It is fragmentary and does not allow building a systemic approach in legal regulation. As an example, we consider the sphere of transport management.

Transport management is the key sphere, as it is through management that "the process of orderly impact of a subject onto an object" is implemented (Kharitonova, 2011). Without going deep into the approaches to researching the category of "management" (Ananyeva, 2015), we have to point out that management is understood in several meanings in the transport industry. On the one hand, the state implements management of various transport processes by introducing digital technologies (for example, using the artificial intelligence technologies[29]). Thus, between the state represented by its bodies and subjects of transport activity public relations occur consisting in observance

[29] Passport of the Strategy of digital transformation of transport industry of the Russian Federation. *SPS KonsultantPlyus*.

of the established rules and requirements. On the other hand, management in the sphere of transport is carried out by the subjects of transport activity themselves. It occurs within civil-legal relations when the subjects of transport activity render transport services to their clients. As an example, one may mention the relations of servicing highly automated vehicles, including control over movement of such vehicles. The most relevant actor is this situation is the operator. However, the prepared draft law and some provisions of the current legislation in the sphere of legal regulation of highly automated vehicles consider the operator as a physical person performing certain actions.

The draft law "On highly automated vehicles and on amendments in certain legislative acts of the Russian Federation"[30] introduces the notion of "an operator of a highly automated vehicle" which is understood as a physical person situated outside the highly automated vehicle, performing monitoring over its motion via remote access, having an opportunity of remote interference into strategic management of the highly automated vehicle, and possessing the knowledge of remote interference into the functioning of such vehicles. The Decree of the Government of the Russian Federation of December 29, 2022, No. 2495 "On establishing an experimental legal regime in the sphere of digital innovations and adopting the Program of experimental legal regime in the sphere of digital innovations in rendering transport services using highly automated vehicles in the territories of certain subjects of the Russian Federation"[31] uses the notion "operator", who is a physical person not being a test driver and situated outside the highly automated vehicle of the 2nd category, performing routing and supervisory control of the highly automated vehicle of the 2nd category (determining and changing the route of movement, activation and deactivation).

In the cited extracts from law, an operator is not a subject of transport activity. Stemming from the analysis of norms, one may suggest that their status is closer to a subcontractor – a physical person in civil-legal contractor agreement or an employee in labor relations, when a physical person has a labor function in the form of a list of certain actions or inactions.

Such approach seems fragmentary, not suitable from the viewpoint of hierarchy of intelligent transport system, where management is the key element for the functioning of the whole intelligent transport system. We believe such activity should be licensed and subject to state control in order to have an opportunity for regulation.

---

30 Draft Federal Law "On highly automated vehicles and on amendments in certain legislative acts of the Russian Federation" of June 8, 2021, No. 02/04/06-21/00116763. http://regulation.gov.ru/p/116763

31 Decree of the Government of the Russian Federation No. 2495 of December 29, 2022 (2022). *Collection of legislation of the Russian Federation*, 1 (part II), Article 300.

Given the existing experience of stipulating such actors in the current legislation devoted to digitalization, one may draw an analogy with an operator of an information system (Article 5 of Federal Law of July 31, 2020, No. 259-FZ "On digital financial assets, digital currency and on amendments in certain legislative acts of the Russian Federation"[32]), as well as with an operator of an investment platform (Chapter 2 of Federal Law of August 2, 2019, No. 259-FZ "On attracting investments using investment platforms and on amendments in certain legislative acts of the Russian Federation"[33]).

Another example of targeted legal regulation is development of legislation on "smart" vehicles as one of the elements of intelligent transport system. A "smart" vehicle should be understood as highly automated or fully automated vehicle. It is important to point out a terminological confusion which is due to the fact that both the academic community and the national and international legislations lack a single notion meaning a vehicle that is managed by itself through an automated driving system built into the vehicle.

For example, the Concept of traffic safety contains a terminological paradox. On the one hand, the document title includes the notion of "unmanned vehicle". On the other hand, this document points out the priority of using the notions of "highly automated vehicle" and "fully automated vehicle". These notions were also recommended by the Resolution of the Global Forum on traffic safety. Another document – the Program of experimental legal regime using highly automated vehicles – uses solely the notion of "highly automated vehicle". However, these highly automated vehicles are divided into two categories.

As the legal level shows no terminological accuracy, academic literature also uses different terms. Each author denotes the examined objects by a term they consider to be more appropriate. For example, some author use the term "unmanned vehicle" (Ananenko, 2020; Begishev, 2021; Korobeev, Chuchaev, 2019; Stepanyan, 2019; Begishev, Bersei, Sherbakova et al., 2022). Others consider the term "highly automated vehicle" to be more appropriate (Yudkina, 2022; Evstigneev, 2019; Takeyoshi Imai, 2019; Begishev, Bersei, Amvrosova et al., 2022).

Each of the presented viewpoints regarding the naming of such smart vehicles deserves attention. However, in order to avoid discrepancies in the future legal regulation, it is necessary to elaborate a common approach to naming such vehicles. In this regard, we believe it appropriate to pay attention to the following.

---

32 Federal Law No. 259-FZ of July 31, 2020 (2020). *Collection of legislation of the Russian Federation*, 31 (part I), Article 5018.

33 Federal Law No. 259-FZ of August 2, 2019. (2019). *Collection of legislation of the Russian Federation,* 31, Article 4418.

First, the notion "unmanned" is used in various acts to denote a vehicle which can manage movement without a human inside. This notion is largely used in the acts devoted to air transport. For example, GOST R 56122-2014 "National standard of the Russian Federation. Air transport. Unmanned aviation systems. General requirements"[34] and Regulation No. 428/2009 of the European Council[35] use the term "unmanned aerial vehicle". Clause 5 of Article 32 of the Aviation Code of the Russian Federation[36] interpret unmanned aerial vehicle as a vessel managed or controlled by an external pilot, i. e. a person situated beyond the board of the vessel.

Thus, the term "unmanned" means only that the person controlling the vehicle is not situated inside the vehicle (Sipetas et al, 2023; O'Hern, & St. Louis, 2023).

Second, the notion of "automated vehicle" is used with regard to road transport in normative-legal regulation, including international one. For example, the classification of automation levels[37] (further – SAE classification), developed by the Society of automotive engineers (SAE), the notion of "automated vehicle" includes the vehicles of levels 3–5:

– level 3 – conditional automation, i. e. control over the vehicle requires the presence of a driver, who may not constantly trace the road situation but must be ready to take control over the vehicle;

– level 4 – high automation, i. e. the vehicle is equipped to move without a driver under certain conditions;

– level 5 – full automation, i. e. a driver is not required to control the vehicle (Schubert, 2015).

Besides, other national systems also use the notions "highly automated vehicle" and "fully automated vehicle". For example, in a German law devoted to regulation of road traffic (Straßen verkehrs gesetz (StVG)) one of the first articles (clause 1a) is called "Kraftfahrzeuge mit hoch- oder voll automatsierter Fahrfunktion", meaning "Motor vehicles with highly or fully automated driving function"[38].

---

34 GOST R 56122-2014 "National standard of the Russian Federation. Air transport. Unmanned aviation systems. General requirements". Moscow: Standartinform, 2020.

35 Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items (recast). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32009R0428

36 Aviation Code of the Russian Federation No. 60-FZ of March 19, 1997 (1997). Collection of legislation of the Russian Federation, 12, Article 1383.

37 Automated Vehicles for Safety. https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety

38 http://www.gesetze-im-internet.de

The presented conclusions testify to the absence of a unified approach to naming the new objects of the real world and determining their essential characteristics, as well as of a systemic approach to developing the legal regulation common for all modes of transport and taking into account the requirements of the contemporary transportation process.

Conclusion

The present work is the initial stage of developing legal research in the sphere of using intelligent transport systems. Stemming from the above said, the following conclusions can be made.

1. Formation of the legal regulation of the use of intelligent transport systems is of fragmentary character. This is due to the fact that normative regulation is created separately for different modes of transport both at the national and international levels. Besides, the development of normative regulation is largely of self-contained, national character.

2. There is currently no clear determination of the essential content of the notion "intelligent transport systems". Thus, it is necessary to improve the normative notion of "intelligent transport systems". This is due to the fact that any legal regulation is based on the conceptual apparatus consisting of coordinated, interrelated notions.

3. The structural elements forming the architecture of intelligent transport systems are important for building interconnections within the system. This said, the architecture of intelligent transport systems is not "rigid" but transforms with the changes in its individual elements under the influence of digital technologies.

References

Abduljabbar, R., Dia, H., Liyanage, S., & Bagloee, S. A. (2019). Applications of artificial intelligence in transport: An overview. *Sustainability*, *11* (1), 189. https://doi.org/10.3390/su11010189

Ananenko, A. O. (2020). Key directions of improving civil-legal legislation in the sphere of unmanned vehicles regulation. *Transportnoye pravo i bezopasnost*, *2*(34),76–83.

Ananyeva, A. A. (2015). *System of normative legal constructions of civil-legal contracts of operative management in transport activity*. Saratov: Izdatelskiy tsentr "Nauka".

Bagreeva, E. G., Zemlin, A. I., & Shamsunov, S. K. (2019). Does Environmental safety Depend Upon the Legal Culture of Transport Specialists? *Ekoloji*, *28*(107).

Bazhina, M. A. (2022). De lega ferende system of conceptual apparatus of transport law. *Transportnoye pravo*, *4*, 34–39. https://doi.org/10.18572/1812-3937-2022-4-34-39

Begishev, I. R. (2021). Legal regulation of unmanned vehicles. *Transportnoye pravo*, *3*, 7–10. https://doi.org/10.18572/1812-3937-2021-3-7-10

Begishev, I., Bersei, D., Amvrosova, O., Dolgopolov, K., & Zhirov, R. (2022). Regulation of highly automated vehicles in the Russian Federation: problems, state and development prospects. In *X International Scientific Siberian Transport Forum. TransSiberia* (pp. 648–655). https://doi.org/10.1016/j.trpro.2022.06.058

Begishev, I., Bersei, D., Sherbakova, L. et al. (2022). Problems of legal regulation of unmanned vehicles. In *X International Scientific Siberian Transport Forum. TransSiberia* (pp. 1321–1327). https://doi.org/10.1016/j.trpro.2022.06.142

Du, Y-L., Yi, T-H., Li, X-J., Rong, X-L, Dong, L-J., Wang, D-W., Gao, Y., & Leng, Z. (2023). *Advances in Intelligentization of Transportation Infrastructures. Engineering*. https://doi.org/10.1016/j.eng.2023.01.011

Evstigneev, I. A. (2019). Road infrastructure and highly automated vehicles. *SAPR i GIS avtomobilnykh dorog*, *2*(13), 44–50. https://doi.org/10.17273/CADGIS.2019.2.7

Fomenko, Yu. V. (1970). Is a word combination a language unit? *Filologicheskiye nauki*, *5*, 60–65.

Gromova, E., & Ivanc, T. (2020). Regulatory Sandboxes (Experimental Legal Regimes) for Digital Innovations in BRICS. *BRICS LAW Journal*, *7*(2), 10–36. https://doi.org/10.21684/2412-2343-2020-7-2-10-36

Hasegawa, Takaaki. (2013). A Design Theory for New Transportation System. *IATSS Review*, *37*(3), 224–232.

Kharitonova, Yu. S. (2011). *Management in civil law: problems of theory and practice*. Moscow: Norma.

Korobeev, A. I., & Chuchaev, A. I. (2019). Unmanned vehicles: new challenges to public safety. *LexRussica (Russkiy zakon)*, *2*(147), 9–28. https://doi.org/10.17803/1729-5920.2019.147.2.009-028

Kutyur, S., & Toupin, S. (2020). What does "sovereignty" mean in the digital world? *Vestnik mezhdunarodnykh organizatsiy: obrazovaniye, nauka, novaya ekonomika*, *15*(4), 7. https://doi.org/10.17323/1996-7845-2020-04-03

Lakshmi Shankar Iyer. (2021). AI enabled applications towards intelligent transportation. *Transportation Engineering*, *5*. https://doi.org/10.1016/j.treng.2021.100083

O'Hern, S., & St. Louis, R. (2023, February 8). Technology readiness and intentions to use conditionally automated vehicles. *Transportation Research Part F: Traffic Psychology and Behaviour*, 1–8. https://doi.org/10.1016/j.trf.2023.02.001

Schubert, M. (2015). *Autonomous Cars – Initial Thoughts about Reforming the Liability Regime*. Phi., 46–51.

Sipetas, Ch., Roncoli, C., & Mladenovich, M. (2023). Mixed fleets of automated and human-driven vehicles in public transport systems: An evaluation of feeder line services. *Transportation Research Interdisciplinary Tendency*, *18*, 100791. https://doi.org/10.1016/j.trip.2023.100791

Sladkowski, A., & Pamula, W. (2016). *Intelligent transport systems – problems and perspectives* (Vol. 32). Springer, Switzerland.

Stepanyan, A. Zh. (2019). Problems of regulation of unmanned vehicles. *Vestnik Universiteta imeni O. E. Kutafina*, *4*(56), 169–174. https://doi.org/10.17803/2311-5998.2019.56.4.169-174

Takeyoshi, Imai. (2019). Legal regulation of autonomous driving technology: Current conditions and issues in Japan. *IATSS Research*, *43*(4), 263–267. https://doi.org/10.1016/j.iatssr.2019.11.009

Yudkina, V. V. (2022). Highly automated vehicles as a subject of public safety. *Administrativnoye pravo i protsess*, *10*. https://doi.org/10.18572/2071-1166-2022-10-49-53

Zemlin, A. I. (2022). Problem issues of the legal regulation of relations associated with using highly automated vehicles. *Zhurnal rossiyskogo prava*, *12*. https://doi.org/10.12737/jrl.2022.128

Zhihan, Lv., & Wenlong, Shang. (2023). Impacts of intelligent transportation systems of energy conservation and emission reduction of transport systems: a comprehensive review. *Green Technologies and Sustainability*, *1*(1). https://doi.org/10.1016/j.grets.2022.100002

Author information

Maria A. Bazhina – Doctor of Juridical Sciences, Associate Professor, Department of Entrepreneurial Law, V. F. Yakovlev Ural State Law University
Address: 21 Komsomolskaya Str., 620137 Yekaterinburg, Russian Federation
E-mail: mashsol@mail.ru
ORCID ID: https://orcid.org/0000-0003-1237-0052
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57807831200
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/record/32495219
Google Scholar ID: https://scholar.google.ru/citations?user=m5W9vIYAAAAJ
RSCI Author ID: https://elibrary.ru/author_items.asp?authorid=974423

Conflict of interest

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
ASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – April 29, 2023
Date of approval – May 30, 2023
Date of acceptance – August 15, 2023
Date of online placement – August 20, 2023

Научная статья
УДК УДК 346.7:34.096
EDN: https://elibrary.ru/vbowtb
DOI: https://doi.org/10.21202/jdtl.2023.27

Интеллектуальные транспортные системы – основа de lega ferenda транспортной системы Российской Федерации

Мария Анатольевна Бажина

Уральский государственный юридический университет имени В. Ф. Яковлева
г. Екатеринбург, Российская Федерация

Ключевые слова

Безопасность,
беспилотное транспортное средство,
высокоавтоматизированное транспортное средство,
интеллектуальная транспортная система,
искусственный интеллект,
право,
правовое регулирование,
транспортная инфраструктура,
транспортное законодательство,
цифровые технологии

Аннотация

Цель: исследование тенденций правового регулирования применения интеллектуальных транспортных систем в условиях цифровой трансформации транспортного сектора экономики, а именно нарастающего значения интеллектуальных транспортных систем в будущей транспортной системе Российской Федерации.

Методы: системно-структурный метод является основой изучения интеллектуальных транспортных систем. С помощью него представляется возможным изучить архитектуру интеллектуальных транспортных систем как сложного структурного единства. Наряду с указанным методом используются также сравнительно-правовой метод, направленный на иллюстрацию различий и сходных черт в правовом регулировании применения интеллектуальных транспортных систем. Методы правового моделирования и прогнозирования, а также формально-логический метод выступают второстепенными методами для полноценного изучения правового регулирования интеллектуальных транспортных систем.

Результаты: в статье представлены концептуальные подходы по определению понятия «интеллектуальные транспортные системы», выделению иерархии интеллектуальных транспортных систем, которым отводится основополагающее место в построении транспортной отрасли. На основе проведенного анализа делаются выводы о векторах формирования транспортного законодательства, направленного на регулирование применения интеллектуальных транспортных систем.

Научная новизна: в статье представлен концептуальный подход по формированию правового регулирования интеллектуальных транспортных систем. С этой целью рассмотрен вопрос о сущностном содержании понятия «интеллектуальные транспортные системы» на легальном и научном уровнях, показаны существующие терминологические проблемы для выстраивания правового регулирования. Анализ архитектуры интеллектуальных транспортных систем позволил впервые сформулировать основные подходы к формированию правового регулирования отдельных ее элементов (в том числе высокоавтоматизированных и полностью автоматизированных транспортных средств, «умной» инфраструктуры и т. д.) не обособленно, а как составных частей целого.

Практическая значимость: представленный в исследовании материал и сделанные на его основе выводы способствуют развитию правового регулирования транспортной отрасли в условиях цифровой трансформации. В статье делается акцент именно на правовом регулировании интеллектуальных транспортных систем с учетом их технических и технологических особенностей. Именно интеллектуальные транспортные системы являются de lega ferenda транспортной системы, которая предопределяет вектор трансформации транспортного законодательства. В свою очередь разработка правовых основ позволяет расширять географию внедрения технических новелл и делать их применение более масштабным.

Для цитирования

Бажина, М. А. (2023). Интеллектуальные транспортные системы – основа de lega ferenda транспортной системы Российской Федерации. *Journal of Digital Technologies and Law*, *1*(3), 629–649. https://doi.org/10.21202/jdtl.2023.27

Список литературы

Ананенко, А. О. (2020). Основные направления совершенствования гражданско-правового законодательства в области регулирования беспилотных транспортных средств. *Транспортное право и безопасность*, *2*(34), 76–83. https://elibrary.ru/zxiivh

Ананьева, А. А. (2015). *Система нормативных юридических конструкций гражданско-правовых договоров оперативного управления транспортной деятельностью*. Саратов: Издательский центр «Наука». https://elibrary.ru/zxiivh/uruyjt

Бажина, М. А. (2022). De lega ferende система понятийного аппарата транспортного права. *Транспортное право*, *4*, 34–39. EDN: https://elibrary.ru/jxkuko. DOI: https://doi.org/10.18572/1812-3937-2022-4-34-39

Бегишев, И. Р. (2021). Правовое регулирование беспилотных транспортных средств. *Транспортное право*, *3*, 7–10. EDN: https://elibrary.ru/bffkkj. DOI: https://doi.org/10.18572/1812-3937-2021-3-7-10

Евстигнеев, И. А. (2019). Дорожная инфраструктура и высокоавтоматизированные транспортные средства. *САПР и ГИС автомобильных дорог*, *2*(13), 44–50. EDN: https://elibrary.ru/elxzrz. DOI: https://doi.org/10.17273/CADGIS.2019.2.7

Землин, А. И. (2022). Проблемные вопросы правового регулирования отношений, связанных с использованием высокоавтоматизированных транспортных средств. *Журнал российского права*, *12*. EDN: https://elibrary.ru/bsmkwa. DOI: https://doi.org/10.12737/jrl.2022.128

Коробеев, А. И., Чучаев, А. И. (2019). Беспилотные транспортные средства: новые вызовы общественной безопасности. *Lex Russica (Русский закон)*, *2*(147), 9–28. EDN: https://elibrary.ru/swhgup. DOI: https://doi.org/10.17803/1729-5920.2019.147.2.009-028

Кутюр, С., Тоупин, С. (2020). Что означает «суверенитет» в цифровом мире? *Вестник международных организаций: образование, наука, новая экономика*, *15*(4), 7. EDN: https://elibrary.ru/zcvyrh. DOI: https://doi.org/10.17323/1996-7845-2020-04-03

Степанян, А. Ж. (2019). Проблемы регулирования беспилотных транспортных средств. *Вестник Университета имени О. Е. Кутафина*, *4*(56), 169–174. EDN: https://elibrary.ru/qkxcsc. DOI: https://doi.org/10.17803/2311-5998.2019.56.4.169-174

Харитонова, Ю. С. (2011). *Управление в гражданском праве: проблемы теории и практики*. Москва: Норма.

Фоменко, Ю. В. (1970). Является ли словосочетание единицей языка. *Филологические науки*, *5*, 60–65. https://elibrary.ru/xnfdfb

Юдкина, В. В. (2022). Высокоавтоматизированные транспортные средства как субъект общественной безопасности. *Административное право и процесс*, *10*. EDN: https://elibrary.ru/xhbcrb. DOI: https://doi.org/10.18572/2071-1166-2022-10-49-53

Abduljabbar, R., Dia, H., Liyanage, S., & Bagloee, S. A. (2019). Applications of artificial intelligence in transport: An overview. *Sustainability*, *11* (1), 189. https://doi.org/10.3390/su11010189

Bagreeva, E. G., Zemlin, A. I., & Shamsunov, S. K. (2019). Does Environmental safety Depend Upon the Legal Culture of Transport Specialists? *Ekoloji*, *28*(107). https://elibrary.ru/isipid

Begishev, I., Bersei, D., Amvrosova, O. et al. (2022). Regulation of highly automated vehicles in the Russian Federation: problems, state and development prospects. *X International Scientific Siberian Transport Forum. TransSiberia* (pp. 648–655). https://doi.org/10.1016/j.trpro.2022.06.058

Begishev, I., Bersei, D., Sherbakova, L. et al. (2022). Problems of legal regulation of unmanned vehicles. *X International Scientific Siberian Transport Forum. TransSiberia* (pp. 1321–1327). https://doi.org/10.1016/j.trpro.2022.06.142

Du, Y-L., Yi, T-H., Li, X-J., Rong, X-L, Dong, L-J., Wang, D-W., Gao, Y. & Leng, Z. (2023). *Advances in Intellectualization of Transportation Infrastructures. Engineering*. https://doi.org/10.1016/j.eng.2023.01.011

Gromova, E., & Ivanc, T. (2020). Regulatory Sandboxes (Experimental Legal Regimes) for Digital Innovations in BRICS. *BRICS LAW Journal*, *7*(2), 10–36. https://doi.org/10.21684/2412-2343-2020-7-2-10-36

Hasegawa, Takaaki. (2013). A Design Theory for New Transportation System. *IATSS Review*, *37*(3), 224–232.

Lakshmi Shankar Iyer. (2021). AI enabled applications towards intelligent transportation. *Transportation Engineering*, *5*. https://doi.org/10.1016/j.treng.2021.100083

O'Hern, S., & St. Louis, R. (2023, February 8). Technology readiness and intentions to use conditionally automated vehicles. Transportation Research Part F: Traffic Psychology and Behaviour, 1–8. https://doi.org/10.1016/j.trf.2023.02.001

Schubert, M. (2015). *Autonomous Cars – Initial Thoughts About Reforming the Liability Regime*. Phi., 46–51.

Sipetas, Ch., Roncoli, C., & Mladenovich, M. (2023). Mixed fleets of automated and human-driven vehicles in public transport systems: An evaluation of feeder line services. *Transportation Research Interdisciplinary Tendency*, *18*, 100791. https://doi.org/10.1016/j.trip.2023.100791

Sladkowski, A., Pamula, W. (2016). *Intelligent transport systems – problems and perspectives* (Vol. 32). Springer, Switzerland.

Takeyoshi Imai. (2019). Legal regulation of autonomous driving technology: Current conditions and issues in Japan. *IATSS Research*, *43*(4), 263–267. https://doi.org/10.1016/j.iatssr.2019.11.009

Zhihan, Lv., Wenlong, Shang. (2023). Impacts of intelligent transportation systems of energy conservation and emission reduction of transport systems: a comprehensive review. *Green Technologies and Sustainability*, *1*(1). https://doi.org/10.1016/j.grets.2022.100002

Сведения об авторе

Бажина Мария Анатольевна – доктор юридических наук, доцент, доцент кафедры предпринимательского права, Уральский государственный юридический университет имени В. Ф. Яковлева
Адрес: 620137, Российская Федерация, г. Екатеринбург, ул. Комсомольская, д. 21
E-mail: mashsol@mail.ru
ORCID ID: https://orcid.org/0000-0003-1237-0052
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57807831200
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/record/32495219
Google Scholar ID: https://scholar.google.ru/citations?user=m5W9vIYAAAAJ
РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=974423

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: 10.23.51 / Правовое регулирование отдельных отраслей экономики
Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 29 апреля 2023 г.
Дата одобрения после рецензирования – 30 мая 2023 г.
Дата принятия к опубликованию – 15 августа 2023 г.
Дата онлайн-размещения – 20 августа 2023 г.

Research article
DOI: https://doi.org/10.21202/jdtl.2023.28

Violating the Rules of Centralized Management of Technical Means of Counteracting the Threats to Information Security

Evgeniy A. Russkevich

Kutafin Moscow State Law University
Moscow, Russian Federation

Keywords

Communication network,
communication operator,
criminal liability,
cyber resilience,
cybercrime,
digital technologies,
information security,
Internet,
law,
legislation

Abstract

Objective: to acquire new knowledge about the liability for violating the rules of managing technical means of counteracting the threats to information security; to elaborate theoretical recommendations and proposals for improving legislation and law enforcement.

Methods: the methodological basis of the research is a set of scientific cognition methods, including abstract-logic, dogmatic, comparison, etc.

Results: based on studying documents and publications, the following conclusions were made: 1) the measures taken at the national level for regulating the relations associated with introduction of technical means of counteracting the threats generally comply with the provisions of the Doctrine on information security of the Russian Federation; 2) one of the main directions of development of the foreign legislation on telecommunications is building a system of public-private interaction, in which communication operators would perceive the information security problem not as their internal task but as an element of the overall security of the state. In this regard, one may clearly trace the statement of the need to efficiently control the activities of communication operators, first of all, in the sphere of the newly introduced standards providing cyber resilience; 3) regulation of relations in the sphere of managing the technical means of counteracting threats in Russia is characterized by their multiplicity, multi-leveledness,

hence, rather predictable complexity; 4) the model of communication operators' liability for violations in the field of exploitation of technical means of counteracting threats, implemented in Article 274.2 Of the Russian Criminal Code, is not optimal. Rather disputable is the approach to describing the administratively prejudicial elements of crime. Despite the significance of the relations, the possibility of a criminal-legal reaction to a particular incident appears not in connection with the occurrence of certain publicly dangerous consequences and not even with the traditional recurrence, but only with the third documented violation. We consider more preferable the model of criminalization of violating the management of technical means of counteracting threats depending on infliction of substantial harm to the rights and legal interests of citizens or organizations, or the legally protected interests of the society or the state.

Scientific novelty: the novelty of the research is mainly due to the actual underdevelopment of the issues related to the legal definition and implementation of criminal liability for violating the rules of centralized management of technical means of counteracting the threats to sustainability, security and integrity of functioning of the telecommunication network Internet and the general purpose communication network in the territory of the Russian Federation.

Practical significance: the main provisions and conclusions of the research can be used for improving the mechanism of criminal-legal protection of information security, further development of the Russian doctrine of criminal law on liability for crimes in the sphere of computer information.

For citation

Russkevich, E. A. (2023). Violating the Rules of Centralized Management of Technical Means of Counteracting the Threats to Information Security. *Journal of Digital Technologies and Law, 1*(3), 650–672. https://doi.org/10.21202/jdtl.2023.28

Contents

Introduction

Digital world is both the present and future of the humanity. Our everyday activity inevitably implies interacting with devices and technologies which rapidly change the idea of the reality. Through accounts, the digital alter egos, a person communicates, performs labor activity, receives services, and purchases goods. As a result, a modern person finds themselves in a position of a parallel being – physical and virtual. One can distance oneself from it, slow down digitalization in a certain sense, but the inevitability and irreversibility of the process makes us put a question: why do it? Answering this question, some researchers point out the negative consequences of introducing telecommunication technologies from the viewpoint of the state and dynamics of crime and its changed characteristics. As a rule, they demonstrate virtualization of the mechanisms of criminal turnover of illegal items, which significantly complicates the activity of law enforcement bodies. Also, they rather thoroughly explain that the development of some research directions (for example, in the sphere of artificial intelligence and robotics) bears a definite threat to humanity as a whole.

The above said is rather true in a certain sense. However, it is also true that this discourse in general does not go beyond confusion, traditional for the humanity, in front of something new, unexplored, the nature and probable impact of which are not completely clear. Any technology can be used for criminal purposes. This, however, cannot cancel progress as such, i. e. the human striving to arrange life in the most reasonable way. For this reason, one should speak not of protection humans against technologies but of building a model of technologies protection or, to be more precise, the model of legal provision of information-telecommunication development, which would allow preventing and adequately reacting to particular criminal infringements. In this sense, it is rather logical to focus on the issues of qualitative provision of sustainability of digital networks in relation to negative impacts, or their cyber resilience.

By Federal Law of July 14, 2022, No. 260-FZ "On making amendments in the Criminal Code of the Russian Federation and Criminal-Procedural Code of the Russian Federation", Chapter 28 of the Criminal Code of the Russian Federation[1] (further – CC RF) was complemented with a new norm, stipulating liability for violation of special rules of managing technical means providing normal functioning of the Internet and communication networks of general use in the territory of the state (Article 274.2 CC RF). The draft law passport does not allow acquainting with the justification of the implemented legislative initiative, as in the original edition Article 274.2 CC RF was not included. The respective amendments

[1] Criminal Code of the Russian Federation of June 13, 1996, No. 63-FZ. (1996, June 17). *Collection of legislation of the Russian Federation*, *25*, Article 2954.

appeared only by the second reading of the draft law[2]. Meanwhile, it is very important not only to comprehend the reasons for criminalizing certain violations associated with managing technical means of counteracting threats (further – TMCT) but also to analyze the legal-technical features of Article 274.2 CC RF, identify its advantages and possible drawbacks.

1. Methods of researching violations of the rules of centralized management of technical means of counteracting the threats to information security

The methodological tools of the research represent a complex combination of philosophical, general scientific and specific scientific means of cognition. The general scientific methods of cognition used in the work include analysis, synthesis, deduction, induction, classification, structural-functional method, etc. Special attention was paid to systemic method, which served as a starting prerequisite for solving the set tasks.

Empirical methods (analysis of documents, printed and electronic publications) were used for accumulating and studying the research materials. In the process of the article preparation, a letter to the federal unitary enterprise "General radio frequency centre"[3] (further – GRFC) was sent in order to obtain clarification about TMCT (an official response was received on December 25, 2022).

As for the specific scientific methods of cognition, they included comparative-legal, formal-legal (dogmatic), etc. The formal-legal method was used when studying normative-legal acts of the Russian Federation in the sphere of regulation and protection of information relations, Russian and foreign criminal legislation. The dogmatic method allowed solving a number of research tasks, for example, revealing the legal-technical definition of the elements according to Article 274.2 CC RF.

2. Information security and technical means of counteracting the threats

To comprehend the processes resulting in the Russian criminal legislation receiving a special norm of liability for violation of the centralized management of TMCT (Article 274.2 CC RF), one should, first of all, turn to the category of information security and strategic planning documents in this sphere.

---

2 Draft law No. 130406-8 "On making amendments in the Criminal Code of the Russian Federation and Criminal-Procedural Code of the Russian Federation" (with a view of improving criminal-legal protection of the national interests of the Russian Federation, rights and freedoms of citizens against new forms of criminal activity and threats to public security). https://sozd.duma.gov.ru/bill/130406-8

3 GRFC is a departmental expert center providing execution of the tasks and functions imposed on the radio frequency service, as well as support of control-surveillance and regulatory functions of Roskomnadzor by the main directions of its activity in the sphere of communication, mass media and mass communications. https://grfc.ru

In the Russian scientific literature, the notion of information security is rather well elaborated[4]. M. A. Efremova justly emphasizes that information security is a dynamic system of public relations. The openness of this system is due to the fact that information security cannot be of a constant, unchangeable character (Efremova, 2018).

The category of information security (in a narrower sense – cyber resilience) is also well studied in foreign literature (Colding et al., 2020; Espinoza-Zelaya & Moon, 2022; Hausken, 2020; Li et al., 2020; Prasad & Moon, 2022; Tonhauser & Ristvej, 2019; Tsao et al., 2022).

As is known, information security is normatively defined in the Doctrine of information security of the Russian Federation[5]. In compliance with this document, "information security is a condition of protection of a personality, society, and the state against internal and external information threats, ensuring implementation of constitutional rights and freedoms of a person and citizen, decent quality and standard of living of citizens, sovereignty, territorial integrity and sustainable social-economic development of the Russian Federation, defense and safety of the state"[6].

The task of ensuring information security, including through effective control over the activity of communication operators, is rather comprehensible to the extent that implies the absence of the need to specially justify it. All communication operators in Russia constitute a single communication network in the state and ensure integrity, accessibility, and in certain cases confidentiality of data, sustainability and security of information-communication infrastructure as a whole. As was justly noted by A. K. Zharova, the Internet, the general purpose networks, and the local networks functioning on the territory of the Russian Federation, though not being state information systems, provide access to the information contained in state information systems. Accordingly, the security of functioning of such technologies and access channels must be ensured by legal tools (Zharova, 2022).

National security is no longer determined solely by a military component and the state borders. Cyber threats are of sporadic and multidimensional character, creating risks of colossal harm. At that, these threats cannot be prevented by solely traditional means, such as military force or law enforcement mechanism; they require effective bilateral cooperation between governments and the private sector (Li & Liu, 2021).

---

4 See, for example: Kalmykov, D. A. (2005). *Information security: notion, position in the criminal legislation of the Russian Federation, problems of legal protection*: thesis for a Candidate Degree in Jurisprudence. Yaroslavl. https://elibrary.ru/nnomvb; Kubyshkin, A. V. (2002). International-legal problems of ensuring the information security of a state: thesis for a Candidate Degree in Jurisprudence. Moscow; Lopatin, V. N. (2000). Information security of Russia: thesis for a Doctoral Degree in Jurisprudence. Saint Petersburg.

5 Order of the President of the Russian Federation No. 646 of 05.12.2016. (2016, December 12). *Collection of legislation of the Russian Federation*, *50*, Article 7074.

6 *Ibid*.

Nevertheless, Russia has for a long time not built the architecture of regulating the public-private interaction in this sphere. Accordingly, the question of liability of communication operators for inobservance of the necessary information security standards was not posed. One cannot say that such decisions were not maturing in the public conscience and were not being discussed as promising in the professional community. Discussion was held rather actively, but, as often happens, direct implementation required the changed social conditions and the formation of an actual demand in terms of providing state security.

It is easy to understand why the respective changes in the Russian criminal legislation regarding the liability for violations in using TMCT appeared at the present stage. Recently, cyber attacks on the information infrastructure have increased exponentially (Elchaninova, 2020; Truntsevsky, 2019; Krasinsky & Mashko, 2023; Bokshitskii & Meltseva, 2017), including during the COVID-19 pandemic (Lallie et al., 2021; Hoheisel et al., 2023; Khisamova & Begishev, 2022). Besides, they are of a complex character, testifying to the thorough preparation of such actions, presence of high competencies and costly equipment of the wrongdoers (Horsman, 2021; Kouloufakos, 2023; Boughton, 2019). Roskomnadzor refers to it in its comments about the legislative innovations under study. In particular, they specially marked that "under a hybrid war, including elements of information confrontation and regular cyber attacks, protection of the information space of Russia is critically important for the state and society. In this regard, communication operators must unconditionally comply with the requirements to installation, exploitation and modernization of TMCT and requirement to pass all traffic through them. All technical means for counteracting threats are under control of the Center for monitoring and management of the general purpose communication network (further – CMM GPCN), which ensures counteracting information attacks"[7].

Another relevant circumstance is that, under the growing international tension and information confrontation, of utmost significance is the observance of the introduced restrictions in access to certain network resources. In other words, it was necessary not only to bring the information flow under technological control (filtration) and build barriers preventing citizens' access to certain traffic and mobile applications, but also effectively ensure liability of communication operators for evading from following these standards. Roskomnadzor also explained as follows: "Operators often pass traffic beyond TMCT or for one reason or another allow switching off this equipment. This may threaten the stable functioning of the Internet in Russia and lead to a failure in the work of information resources of state bodies. If TMCT are switched off or traffic is passed beyond them, Russian users get access to dangerous information: children's pornography, pro-drug content, propaganda of suicide, fakes, extremist information"[8].

---

7 Roskomnadzor states that operators' refusing to use TMCT threatens citizens. (2022, July 15). https://tass.ru/obschestvo/15228891

8 *Ibid*.

Decision on building a monitoring system using TMCT generally complies with the provisions of the Doctrine of information security of the Russian Federation, which defines the following main directions of its implementation: counteraction against using information technologies for propaganda of extremist ideology, dissemination of xenophobia, ideas of national exclusiveness with a view of undermining sovereignty, political and social stability, violent alteration of constitutional order, violation of territorial integrity of the Russian Federation; disruption of the activity inflicting harm to the national security of the Russian Federation, performed using technical means and information technologies by special services and organizations of foreign states and individuals, etc.

It is important to note that the measures on regulating relations associated with TMCT introduction, taken at the national level, largely comply with the trends of foreign countries (Bitzer et al., 2023; Cascavilla et al., 2021; Mohamed, 2013; Nguyen & Golman, 2021; Broadhead, 2018; Qamar et al., 2023). In this article, we do not pursue the goal of giving a detailed estimation to the processes taking place globally. At the same time, it is necessary to form a general idea of them, in order to better understand the situation with TMCT functioning in Russia.

In a certain sense, the Russian model of regulating and protecting the relations associated with introduction and use of TMCT repeats the experience of the People's Republic of China (further – PRC). As is justly marked in literature, billions of Internet users in PRC gave the state great economic advantages, but it also creates real threats to its economic and political security (Dremliuga et al., 2017). China was one of the first to face the risks and estimate the "benefits" emerging in case of nonintervention into the activity of telecommunication operators at the national level (Ye & Zhao, 2023). Today, many popular foreign Internet resources are blocked in PRC because they disseminate information contradicting the ideology of China and moral attitudes of the society, have signs of terroristic or extremist propaganda. Moreover, a PRC Law of on security of the Internet of 2016[9] obliges providers demand from the users to register under their real names, filter the content and implement blocking the resources, use only certified equipment, follow the requirement to localize users data, provide technical support and assistance to the bodies of public and state safety, etc. Violating of the respective rules providing the safety of the PRC network space may lead to forcible termination of the activity of the communication operator, as well as bringing their employees to liability, including criminal one.

In the Russian literature it is justly stated that the repressive Chinese legislation in the Internet sphere, besides violation of the rights and freedoms apparent for the western

[9] *In China, a headline-making Law on cyber security is coming into force*. https://ria.ru/20170601/1495523455.html

community, also seriously contribute to the "filtration" of the illegal content occurring in the Chinese segment, thus protecting statehood and citizens against terrorism, extremism, cults, pornography, violence, attacks of foreign intelligence services, etc. (Luzyanin & Troshchinsky, 2018).

Within the Commonwealth of Independent States (further – CIS), the approach associated with determining liability for violating the rules of using TMCT is not widely spread. The Agreement on cooperation of the CIS member states in struggling against crimes in the sphere of information technologies[10] also lacks respective recommendations. Probably the closest in meaning are the provisions of Article 2781 "Violation of informatization rules" of the Criminal Code of the Republic of Uzbekistan[11].

On December 20, 2018, the EU Directive 2018/1972 of 11.12.2018 of the European Parliament and of the Council establishing the European Electronic Communications Code[12] came into force. According to it, the member states must provide that suppliers of public electronic communication networks or public electronic communication services take due and proportionate technical and organizational measures for proper management of risks associated with the safety of the networks and services. Given the level of technology, these measures must ensure the level of safety corresponding to the current risks. European Union Agency for Cybersecurity (ENISA) is intended to coordinate activities of member states to avoid discrepancies in national requirements, which might create the risks to security and barriers for the internal market. The member states also must ensure that the suppliers of public electronic communication networks or public electronic communication services notify, without unjustified delays, an authority body of a security incident which had significantly influenced the functioning of the networks and services.

Member states must ensure that authority bodies are entitled to issue mandatory guidelines, including referring to the measures necessary to eliminate a security incident or prevent its occurrence, to the suppliers of public electronic communication networks or public electronic communication services. Member states must ensure that competent bodies are entitled to demand from the suppliers of public electronic communication networks or public electronic communication services: to provide the information necessary to estimate the safety of their networks and services, including documented safety policies; to be subject to safety audit, carried out by a qualified independent body or a competent body, and submit its results to a competent body; the audit is paid for by the supplier[13].

---

10 Agreement on cooperation of member states of the Commonwealth of Independent States in struggling against crimes in the sphere of information technologies. (2022, August 15). *Collection of legislation of the Russian Federation*, *33*, Article 5883

11 https://lex.uz/docs/111457#111470

12 *Consolidated text: Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02018L1972-20181217

13 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L1972#d1e4938-36-1

The Directive determined the changes in legislation of EU states on telecommunication technologies and data protection. For example, on April 22, 2021, Germany adopted the Telecommunications Modernization Act (TKMG). Also, Telecommunications Telemedia Data Protection Act (TTDSG) was adopted – the law on data protection in telecommunications in Germany, accompanied by a new technical regulation on implementing the legal measures for monitoring of telecommunications. The new requirements to the security of telecommunications sector introduce a category of "critical components of telecommunications". These components may be used only if they are tested and certified by an officially recognized certification body and if the component producer submitted to the communication operator a "reliability declaration". In compliance with the new regulatory regime, operators with the increased potential risk must use relevant intrusion detection systems (IDS) and/or attack detection systems (ADS). Also, such operators must undergo external security audit every two years[14].

On November 17, 2021, Great Britain adopted the Telecommunications (Security) Act 2021[15]. This law introduced changes in the Communications Act of 2003.[16] Among the most significant provisions is the direct definition in Article 105A of obligation of communication operators to identify threats to cyber resilience and take steps to overcome and prevent them. Also, Article 105B stipulates the obligation of communication operators to execute the instructions of a state regulator. Article 105E stipulates that a state controlling body possesses authorities to prepare and adopt the rules of providing cyber resilience. The respective rules stipulating technical standards and specific practices of security are obligatory for providers. The functions of immediate control and supervision over executing the rules are imposed on the Office of Communications (OFCOM).

Violation of rules and standards of telecommunication security, evading the instructions of OFCOM entails significant fines, including turnover-based ones. Article 404 of the British Communications Act stipulates the issue of the probable brining to criminal liability of a company head, "if the deed is committed by a legal person and it is proved that it was committed with the consent or with the connivance of, or was associated with any negligence on the part of a director, a manager, a secretary or another person executing managerial functions".

On June 14, 2022, discussion of Bill C-26 was initiated in Canada, aimed at making amendments in the Communications Act[17]. Its aim is to promote the state security and to ensure cyber resilience of the telecommunication infrastructure by giving the respective state structures new authorities regarding control over the activities

14 https://www.gesetze-im-internet.de/ttdsg/

15 https://www.legislation.gov.uk/ukpga/2021/31/contents/enacted

16 https://www.legislation.gov.uk/ukpga/2003/21/contents

17 https://www.parl.ca/legisinfo/en/bill/44-1/C-26

of communication operators. Examining the draft law allows making a conclusion that the list of such authorities is very large and implies not only surveillance over the observance of the stipulated security standards, but also the possibility to impose prohibitions on using certain equipment, to provide communication services to certain users, etc. Notably, the draft law caused active discussions. For example, an open letter to the Minister of public safety was published, stating that "Bill C-26 empowers the government to secretly order telecom providers "to do anything or refrain from doing anything". This opens the door to imposing surveillance obligations on private companies, and to other risks such as weakened encryption standards – something the public has long rejected as inconsistent with our privacy rights"[18]. Professional community claimed a substantial and unjustified restriction of the freedom of economic activity, as well as the fact that the proposed standards would ruin small participants of the telecommunications services market. The bill was not adopted so far.

Thus, if we try to define the direction of development of the foreign legislation on telecommunications in the most general terms, one may make a conclusion that it consists of an attempt to build a system of public-private interaction, in which communication operators would perceive the problem of information security not as their internal task, but as an element of the overall state security. In this regard, it is easy to trace the statement of the need for effective control over the activity of communication operators, first of all in the sphere of the introduced technical standards of providing cyber resilience.

3. Regulation in the sphere of centralized management of technical means of counteracting the threats to information security

The obligation of a communication operator rendering services of access to information-telecommunication network Internet to ensure installation of TMCT in their network is stipulated by clause 5.1 of Article 46 of Federal Law of July 7, 2003, No. 126-FZ "On communication"[19]. The respective provision for the first time appeared in the Russian legislation with the adoption of Federal Law of May 1, 2019, No. 90-FZ "On making amendments in the Federal Law 'On communication' and Federal Law 'On information, information technologies and protection of information'"[20].

It is important to note that the legislative initiative appeared as a response to the USA National Cyber Strategy adopted in September 2018. As was stated in the explanatory memorandum to the law draft, "the document signed by the US President declares the principle of 'forcible peace maintenance'. At the same time, Russia is explicitly and groundlessly accused of committing hacker attacks; punishment is explicitly mentioned: "Russia, Iran,

18 https://ccla.org/privacy/joint-letter-of-concern-regarding-bill-c-26/

19 (2003, July 14). *Collection of legislation of the Russian Federation*, *28*, Article 2895.

20 http://publication.pravo.gov.ru/Document/View/0001201905010025

and North Korea conducted reckless cyber attacks that harmed American and international businesses and our allies and partners without paying costs likely to deter future cyber aggression". Under these conditions, protective measures are necessary to provide long-term and sustainable functioning of the Internet in Russia and to increase the reliability of the Russian Internet resources. The necessary rules of traffic routing are determined; control over their implementation is organized. Possibility is created to minimize data transfer abroad, exchanged by the Russian users. Trans-border communication lines and traffic exchange points are determined. Possibility is implied to install technical means on communication networks to identify the source of the traffic transferred. The technical means would be able to limit access to resources with prohibited information not only by network addresses but also by prohibiting the transfer of the traffic passed"[21].

The Law of May 1, 2019 No. 90-FZ, also known as the Law "On sovereign Runet", caused fundamental disputes and even protests among some representatives of the industry and civil society. It was noted that its implementation creates unjustified risks to constitutional rights and freedoms of citizens, will require billions of costs, threaten competition in the communication services market, and will facilitate corrupt behavior[22]. This situation is largely similar to the one around discussing Bill C-26 in Canada, which was mentioned before. Nowadays, one may definitely say that there was no other possible solution for Russia. Undoubtedly, creation of a single contour of information infrastructure protection in the state requires significant funding. One also has to agree with the thesis of a cardinal broadening of state control over citizens' activity in the virtual environment. At the same time, the balance is important, which determines the state of information security as a dynamic system changing under the influence of external conditions.

The main document currently determining the regulation in the sphere of managing the technical means of ensuring cyber resilience of digital networks is the Decree of the Government of the Russian Federation of February 12, 2020 No. 126 "On installation, exploitation, and modernization in the communication networks of a communication operator of the technical means of counteracting the threats to sustainability, safety and integrity of functioning on the territory of the Russian Federation of information-telecommunication network Internet and general purpose communication network"[23].

Analysis of this legal act allows concluding that the mechanism of interaction between radio frequency service and a communications operator is of multistage character. The rules stipulate that not later than 90 calendar days before the planned date TMCT

---

21 Explanatory memorandum "To the draft of Federal Law 'On making amendments to certain legislative acts of the Russian Federation'". *SPS KonsultantPlyus*.

22 See: Business critiqued the details of transiting to a 'sovereign Runet'". (2019, June 26). *Kommersant*. https://www.kommersant.ru/doc/4012730?ysclid=ldkccj43i272099969; Head of RSPP stated corruption risks of the Law on 'sovereign Runet'". (2019, July 30). RBK. https://www.rbc.ru/technology_and_media/30/07/2019/5d3f08389a7947ada3baf05b

23 (2020, February 24). *Collection of legislation of the Russian Federation*, *8*, Article 1001.

installation, a communications operator is sent an inquiry to submit information including: patterns of building the network of the communications operator; technical characteristics of the communication means of the communications operator; locations of the planned installation of TMCT; number of data transfer channels with indication of physical properties of such channels, their technology and carrying capacity; information on average and maximal load of channels; information on the node structure at the location of the planned installation of TMCT; information of the plans of modernization, reconstruction of the communication node, liquidation of a fragment of communication network; technical information and technological parameters of communication means of the communications operator, necessary for the development of project documentation on installation and connection of TMCT.

A communications operator is obliged to prepare an answer to the relevant inquiry within 15 working days after receiving it. The decree stipulates the possibility of sending a clarification inquiry during seven working days after receiving the answer. In that case, the communications operator must prepare an answer within three working days after receiving it.

In general, this procedure of information exchange is intended to ensure the necessary preparation for implementing the coordinated plan for installation and/or modernization of TMCT. From the criminal-legal viewpoint, of interest is the qualification of the actions of communications operator's officials who purposefully evade from submitting the relevant information or knowingly submit incorrect data. We assume that, in the presence of factual evidences, one should consider the possibility to apply Article 201 CC RF and 327 CC RF, respectively. While the situation is rather unambiguous in case of using a knowingly fake document, in case of authority abuse it is necessary to establish not only inaction of the person but also occurrence of negative consequences, for example, a large-scale failure in the functioning of information-communication facilities, etc. At that, it is important and, apparently, difficult for implementing the criminal liability mechanism to establish the cause-effect connection between the evasion of submitting data, absence of TMCT at specific communication channels, and the actual dangerous consequences.

Of great importance for applying the provisions of administrative and criminal legislation is clause 10 of the Rules, which stipulates the obligations of communications operator when exploiting technical means for counteracting threats: to supply electric energy to TMCT; to provide technical support of TMCT functioning in terms of switching them to their communications network, organizing a technological channel for controlling these means, including in compliance with the technical conditions of the TMCT installation; to provide, not later than 48 hours from the moment of occurrence of a requirement from the Radio Frequency Service, an access to TMCT by representatives of the Radio Frequency Service; not to bar the Radio Frequency Service to conduct remote control of TMCT using special software; to observe the requirement to providing the functioning of TMCT, stipulated by exploitation documentation; to provide execution of a complex of measures aimed at safe exploitation of TMCT, including those implying the exclusion of hardware, software and physical impact of unauthorized persons on the TMCT functioning, etc.

Analysis of the above provisions of the Rules allows concluding that, in some cases, bringing the representatives of communications operator to liability will imply the need to directly indicate the violation of specific provisions and requirements stipulated by other documents (for example, an instruction on interaction of the authorized persons of communications operator with the Radio Frequency Service, equipment, etc.).

The technical conditions of installation, as well as the requirements to networks when using TMCT, are stipulated by the Order of Roskomnadzor of July 31, 2019 No. 228 "On adopting the technical conditions of installation of technical means for counteracting threats, as well as requirements to communication networks when using the technical means for counteracting threats"[24].

In addition, one should mention that regulation in terms of TMCT management is not limited to the cited normative acts and is currently characterized as numerous, multilevel and, accordingly, predictably complex. Among such regulation one should specifically mention: Decree of the Government of the Russian Federation of November 3, 2022 No. 1978 "On adopting requirements to the system of ensuring observance by communications operators, rendering communication services and services of passing traffic in the general purpose communications network, of requirements and Rules of functioning and interaction of the system of ensuring observance by communications operators of requirements when rendering communication services and services of passing traffic in the general purpose communications network with information systems and other systems, including with the systems of communications operators"[25], Order of the Russian Ministry of Communications of October 7, 2019 No. 572 "On adopting requirements to ensuring the functioning of traffic exchange points, including the requirements to ensuring the stable functioning of technical and software means of communication, communication facilities, and the order of observing the requirements stipulated by clause 4 of Article 56.2 of the Federal Law of July 7, 2003 No. 126-FZ "On communication"[26], etc.

4. Criminal liability for violating the centralized management of technical means of counteracting the threats to information security

One has to assume that an object of crime stipulated by Article 274.2 CC RF is the public relations associated with exploitation of TMCT and provision of sustainability, security and integrity of functioning in the territory of the Russian Federation of information-telecommunication network Internet and general purpose communication network. Occurrence of these relations between the state and communications operators, as was shown above, has taken place rather recently and had relevant social-legal prerequisites.

24 http://publication.pravo.gov.ru/Document/View/0001201909120028

25 (2022, November 14). *Collection of legislation of the Russian Federation*, *46*, Article 7995.

26 https://minjust.consultant.ru/documents/45269

Of interest is the approach according to which, under the modern condition, an object of crime in the sphere of computer information is public relations in the sphere of digital economy and information society (Dremliuga, 2022). In a certain sense one may agree with this interpretation, based on strategic documents in the sphere of digital economy development. Assumingly, its only drawback is the obvious broadness of the terminology used, which under certain circumstances does not allow identifying the specificity of the given group of publicly dangerous infringements with the special part of CC RF.

The object is the technical means for counteracting threats (TMCT). It is worth noting that there is no list of the relevant equipment in open access. According to the clarifications of the Radio Frequency Service, information about this equipment is a commercial secret.

Part 1 of Article 274.2 CC RF stipulates liability for violating the order of installation, exploitation and modernization in the communication network of technical means for counteracting threats to the stable functioning of the Internet and general purpose communication network, or inobservance of technical conditions of their installation or requirements for their use. Disposition is a blanket one and refers to the Decree of the Government of the Russian Federation of February 12, 2020 No. 126[27].

The objective part of this crime implies both active and passive behavior of a subject and may consist in impeding the distant control of the Radio Frequency Service over the technical means for counteracting threats; violation of requirements contained in exploitation documentation; switching off the technical means for counteracting threats from energy supply; blocking access to the relevant equipment by representatives of the Radio Frequency Service, etc.

According to Part 2 of Article 274.2 CC RF, the objective part consists in passing the traffic via the technical means for counteracting threats. The respective requirements are stipulated by the Order of the Ministry of Digitalization of the Russian Federation of January 26, 2022 No. 44 "On adopting the Requirements to the order of passing the in data transfer networks"[28].

In compliance with the Decree of the Government of the Russian Federation of February 12, 2020 No. 127 "On adopting the Rules of centralized control over the general purpose network"[29], a communication operator is entitled not to route the traffic via the technical means for counteracting threats in the following cases: a) violation of the functioning of the technical means for counteracting threats, when the passage of traffic via the given technical means is terminated, provided the requirements to exploitation of technical means for counteracting threats are observed; b) violation of the functioning of a technical means for counteracting threats, when the parameters of the traffic passage do not correspond

---

27 Decree of the Government of the Russian Federation No. 126 of 12.02.2020. *Collection of legislation of the Russian Federation*, *8*, Article 1001.

28 http://publication.pravo.gov.ru/Document/View/0001202203010002

29 (2020, February 24). *Collection of legislation of the Russian Federation*, *8*, Article 1002.

to the parameters indicated in the project documentation for the installation and functioning of the technical means for counteracting threats, provided the requirements to exploitation of technical means for counteracting threats are observed; c) identification of information or information resources, access to which is not to be restricted in compliance with the legislation of the Russian Federation. Passage of traffic beyond the technical means for counteracting threats in other cases, not stipulated by the Decree No. 127, may be qualified as violation of requirements to the passage of traffic by implication of part 2 of Article 274.2 CC RF.

Both bodies of evidences are constructed using administrative preclusion and imply that the respective violation of rules must be committed during the period when a person is considered subject to administrative punishment for law breaches stipulated by qualification types of Article 13.42 of the Code on Administrative Breaches of the Russian Federation[30] (further – CAB RF) and 13.421 CAB RF. An aggravating element in both cases is the repeatability of the administrative breach of law. Thus, by implication of Article 274.2 CC RF, the signs of a criminally punishable act will only occur after the third violation of the rules of centralized TMCT control.

From the view point of a legislative description, the deed stipulated by Article 274.2 CC RF refers to a numerous group of crimes associated with the violation of special rules, the dual nature of which, in apt words by N. I. Pikurov, are characterized by a combination of an offense and a crime (a "juridical Russian doll" format) (Pikurov, 2009).

The proposed legislative model of liability of the representatives of communications operators for violations in the sphere of TMCT exploitation does not seem optimal. First, rather doubtful is the approach to description of the administratively preclusive signs of the body of evidence. Despite the significance of the relations provided by the system of TMCT centralized control, the possibility of criminal-legal reaction to a particular incident appears not in connection with the occurrence of specific publicly dangerous consequences and even not in case of a traditional repetition, but only after the third documented violation.

In continuation of this idea, one should assume that a legislator has wrongly rejected the model of criminalization of violating TMCT control as a function of inflicting substantial harm to the rights and legal interests of citizens or organizations, or to the legally protected interests of the society or state. In a certain sense, this even now poses the question of qualification of the actions of a representative of a communications operator, who, using their managerial authorities, interfered into the TMCT functioning, which resulted in publicly dangerous consequences (for example, a cyberattack led to the loss of personal data of several thousand users, an information infrastructure of large economic subjects was destroyed, large sums of money were stolen, etc.). We believe that in the presence of the signs of a special subject stipulated by Article 201 CC RF, application of this norm should

[30] (2002, January 7). *Collection of legislation of the Russian Federation*, *1* (part I), Article 1.

be prioritized. This, in particular, is indicated by the coordination of sanctions in the Article 274.2 CC RF and 201 CC RF.

The subject of both crimes is special – an official, as formulated in the note to Article 274.2 CC RF, that is, a person temporary, permanently or by a special authority executing managerial, organizational-administrational or administrative-economic functions in a commercial or other organization, or an individual entrepreneur, subjected to administrative punishment for the respective deeds stipulated by the Code on Administrative Breaches of the Russian Federation.

In the norm under study, a legislator commits a rather not appropriate terminology. They call "officials" the subjects possessing managerial functions in a commercial or another organization (see note to Article 201 CC RF). Thus, two types of officials are stipulated – in commercial or other organizations, as well as in state bodies, local self-government bodies, etc. (see note to Article 285 CC RF).

The subjective part is not directly disclosed in Article 274.2 CC RF. Taking into attention the formal construction of the bodies of evidences, one should conclude that the subjective part of the violation of special rules, by implication of part 1 of Article 274.2 CC RF, and violation of the requirements to traffic passage according to part 2 of Article 274.2 CC RF are expressed by guilt in the form of direct intention. At that, the content of motives and goals does not influence the qualification of crime.

If the respective violations were committed by negligence, due to recklessness in observing exploitation requirements and other rules, the deeds committed, depending upon the circumstances, can be qualified in accordance to Article 274 CC RF or part 3 of Article 2741 CC RF.

Conclusion

In conclusion, one should highlight once again that the decision on creating a closed contour of information protection in Russia by introducing TMCT and building a respective system of relations between the state and communications operators can only be welcomed. Essentially, it does not matter which external or internal causes facilitated the implementation of reforms in the sphere of telecommunications. It is rather wrong to imply that the "sovereign Runet" is a specifically Russian idea, the extraordinary reaction to extraordinary circumstances. It was promoted by much more complex and in-depth processes. This is confirmed by the experience of some foreign countries which either have implemented the respective reforms or are actively moving in that direction.

At the same time, the model of criminal-legal provision of relations in the sphere of TMCT centralized control, stipulated by Article 274.2 CC RF, can hardly be assumed free from drawbacks and contradictions. This is not only the continuation of a rather disputable direction of development of the Russian criminal legislation, associated with broadening the bodies with administrative preclusion in the Special part of CC RF, although this approach has largely excluded the very possibility to differentiate liability for this crime.

The problem is in the very condition of preliminary repeated bringing to administrative liability for the respective deed twice during a year. Rather disputable is also the decision to use the category of an official, to which a legislator has attributed its own "autonomous" meaning exclusively in Article 274.2 CC RF.

The relevance and quality of the norm will very soon be verified by practice. In this respect, one should only rely on time. As for the doctrine, it should traditionally hope for the best and be prepared for the worst, discussing and developing the possible prospective steps to change the law and overcome the problems of law enforcement.

References

Bitzer, M., Häckel, B., Leuthe, D., Ott, J., Stahl, B., & Strobel, J. (2023). Managing the Inevitable – A Maturity Model to Establish Incident Response Management Capabilities. *Computers & Security*, *125*, 103050. https://doi.org/10.1016/j.cose.2022.103050

Bokshitskii, V., & Meltseva, I. (2017). Improving the protection of socially significant information resources. *Voprosy Kiberbezopasnosti*, *S2*(20), 11–14. (In Russ.).

Boughton, N. (2019). Protecting infrastructure from cyber attack. *Network Security*, *2019*(4), 18–19. https://doi.org/10.1016/S1353-4858(19)30051-0

Broadhead, S. (2018). The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments. *Computer Law & Security Review*, *34*(6), 1180–1196. https://doi.org/10.1016/j.clsr.2018.08.005

Cascavilla, G., Tamburri, D. A., & Van Den Heuvel, W. (2021). Cybercrime threat intelligence: A systematic multi-vocal literature review. *Computers & Security*, *105*, 102258. https://doi.org/10.1016/j.cose.2021.102258

Colding, J., Colding, M., & Barthel, S. (2020). Applying seven resilience principles on the Vision of the Digital City. *Cities*, *103*, 102761. https://doi.org/10.1016/j.cities.2020.102761

Dremliuga, R. I. (2022). *Criminal-legal protection of digital economy and information society against cybercriminal infringements: doctrine, law, law enforcement*: monograph. Moscow: Yurlitinform. (In Russ.).

Dremliuga, R. I., Korobeev, A. I., & Fedorov, A. V. (2017). Cyberterrorism in China: Criminal Law and Criminological Aspects. *Russian Journal of Criminology*, *11*(3), 607–614. (In Russ.). https://doi.org/10.17150/2500-4255.2017.11(3).607-614

Efremova, M. A. (2018). *Criminal-legal protection of information security*: monograph. Moscow: Yurlitinform. (In Russ.).

Elchaninova, N. B. (2020). Protection of critical information infrastructure as a new institute of legally enforcing information security. *Information Society*, *2*, 58–65. (In Russ.).

Espinoza-Zelaya, C., & Moon, Y. B. (2022). Resilience Enhancing Mechanisms for Cyber-Manufacturing Systems against Cyber-Attacks. *IFAC-PapersOnLine*, *55*(10), 2252–2257. https://doi.org/10.1016/j.ifacol.2022.10.043

Hausken, K. (2020). Cyber resilience in firms, organizations and societies. *Internet of Things*, *11*, 100204. https://doi.org/10.1016/j.iot.2020.100204

Hoheisel, R., Van Capelleveen, G., Sarmah, D. K., & Hartel, P. H. (2023). The development of phishing during the COVID-19 pandemic: An analysis of over 1100 targeted domains. *Computers & Security*, *128*, 103158. https://doi.org/10.1016/j.cose.2023.103158

Horsman, G. (2021). Digital evidence and the crime scene. *Sci. Justice*, *61*(6), 761–770. https://doi.org/10.1016/j.scijus.2021.10.003

Khisamova, Z. I., & Begishev, I. R. (2022). Digital crime in the context of a pandemic: main trends. *Russian Journal of Criminology*, *16*(2), 185–198. (In Russ.). https://doi.org/10.17150/2500-4255.2022.16(2).185-198

Kouloufakos, T. (2023). Untangling the cyber norm to protect critical infrastructures. *Computer Law & Security Review*, *49*, 105809. https://doi.org/10.1016/j.clsr.2023.105809

Krasinsky, V. V., & Mashko, V. (2023). Cyberterrorism: criminological characteristics and qualification. *State and Law*, *1*, 79–91. (In Russ.). https://doi.org/10.31857/S102694520024122-5

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248. https://doi.org/10.1016/j.cose.2021.102248

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends

and recent developments. *Energy Reports*, *7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Li, Y., Tong, Y., & Giua, A. (2020). Detection and Prevention of Cyber-Attacks in Networked Control Systems. *IFAC-PapersOnLine*, *53*(4), 7–13. https://doi.org/10.1016/j.ifacol.2021.04.001

Luzyanin, S. G., & Troshchinsky, P. V. (2018). Ensuring China's national security at the present stage (normative and legal aspect). *Journal of Foreign Legislation and Comparative Law*, *1*, 60–69. (In Russ.). https://doi.org/10.12737/art.2018.1.8

Mohamed, D. (2013). Combating the threats of cybercrimes in Malaysia: The efforts, the cyberlaws and the traditional laws. *Computer Law & Security Review*, *29*(1), 66–76. https://doi.org/10.1016/j.clsr.2012.11.005

Nguyen, C. L., & Golman, W. (2021). Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: 'Law on the books' vs 'law in action'. *Computer Law & Security Review*, *40*, 105521. https://doi.org/10.1016/j.clsr.2020.105521

Pikurov, N. I. (2009). *Qualification of crimes with blanket characteristics of the components of crime*: monograph. Moscow: Russian State Academy of Justice. (In Russ.).

Prasad, R., & Moon, Y. (2022). Architecture for Preventing and Detecting Cyber Attacks in Cyber-Manufacturing System. *IFAC-PapersOnLine*, *55*(10), 2246–2251. https://doi.org/10.1016/j.ifacol.2022.10.042

Qamar, S., Anwar, Z., & Afzal, M. (2023). A systematic threat analysis and defense strategies for the metaverse and extended reality systems. *Computers & Security*, *128*, 103127. https://doi.org/10.1016/j.cose.2023.103127

Tonhauser, M., & Ristvej, J. (2019). Disruptive acts in cyberspace, steps to improve cyber resilience at National Level. *Transportation Research Procedia*, *40*, 1591–1596. https://doi.org/10.1016/j.trpro.2019.07.220

Truntsevsky, Yu. V. (2019). Unlawful impact on critical information infrastructure: the criminal liability of its owners and operators. *Journal of Russian Law*, *5*(269), 99–106. (In Russ.). https://doi.org/10.12737/art_2019_5_9

Tsao, K. Y., Girdler, T., & Vassilakis, V. G. (2022). A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks. *Ad Hoc Networks*, *133*, 102894. https://doi.org/10.1016/j.adhoc.2022.102894

Ye, W., & Zhao, L. (2023). "I know it's sensitive": Internet censorship, recoding, and the sensitive word culture in China. *Discourse, Context & Media*, *51*, 100666. https://doi.org/10.1016/j.dcm.2022.100666

Zharova, A. K. (2022).The legal regulation of relations in the sphere of prevention of possible information technology vulnerabilities. *Bezopasnost biznesa*, *1*, 19–26. (In Russ.). https://doi.org/10.18572/2072-3644-2022-1-19-26

Author information

Evgeniy A. Russkevich – Doctor of Juridical Sciences, Associate Professor, Professor of the Department of Criminal Law, Kutafin Moscow State Law University
Address: 9 Sadovaya-Kudrinskaya Str., 125993 Moscow, Russian Federation
E-mail: russkevich@mail.ru
ORCID ID: https://orcid.org/0000-0003-4587-8258
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57919310600
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/record/2510065
Google Scholar ID: https://scholar.google.ru/citations?user=rwKPImIAAAAJ
RSCI Author ID: https://elibrary.ru/author_items.asp?authorid=539093

Conflict of interest

The author is a member of the Editorial Board of the Journal; the article has been reviewed on general terms.

Financial disclosure

The research was performed as part of a state order «Russian legal system under the realities of digital transformation of the society and state: adaptation and prospects of reacting to the modern challenges and threats (FSMW-2023-0006)». Registration number: 1022040700002-6-5.5.1.

Thematic rubrics

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

Article history

Date of receipt – February 6, 2023
Date of approval – April 13, 2023
Date of acceptance – August 15, 2023
Date of online placement – August 20, 2023

Научная статья
УДК 34:343.3/.7:004:654.1
EDN: https://elibrary.ru/fiseet
DOI: https://doi.org/10.21202/jdtl.2023.28

Нарушение правил централизованного управления техническими средствами противодействия угрозам информационной безопасности

Евгений Александрович Русскевич

Московский государственный юридический университет имени О. Е. Кутафина (МГЮА)
г. Москва, Российская Федерация

Ключевые слова

Законодательство,
Интернет,
информационная безопасность,
киберпреступление,
киберустойчивость,
оператор связи,
право,
сеть связи,
уголовная ответственность,
цифровые технологии

Аннотация

Цель: получение нового знания об ответственности за нарушение правил управления техническими средствами противодействия угрозам информационной безопасности, разработка теоретических рекомендаций и предложений по совершенствованию законодательства и правоприменения.

Методы: методологическую основу исследования составляет совокупность методов научного познания, в том числе абстрактно-логический, догматический, сравнения и др.

Результаты: на основе изучения документов, изданий сделаны следующие выводы: 1) предпринятые на национальном уровне меры по регулированию отношений, связанных с внедрением технических средств противодействия угрозам, в целом соответствуют положениям Доктрины информационной безопасности Российской Федерации; 2) одним из основных направлений развития зарубежного законодательства о телекоммуникациях является построение системы государственно-частного взаимодействия, при котором операторы связи стали бы воспринимать проблему информационной безопасности не как их внутреннюю задачу, а как элемент общей безопасности государства. В этом отношении предельно четко прослеживается констатация необходимости эффективного контроля за деятельностью операторов связи, прежде всего в сфере вводимых технических стандартов обеспечения киберустойчивости; 3) регулирование отношений в сфере управления техническими средствами противодействия угрозам в России характеризуется многочисленностью, многоуровневостью и, соответственно, вполне

предсказуемой сложностью; 4) реализованная в ст. 274.2 Уголовного кодекса Российской Федерации модель ответственности представителей операторов связи за нарушения в области эксплуатации технических средств противодействия угрозам не представляется оптимальной. Довольно уязвимым является подход к описанию административно преюдициальных признаков состава. Несмотря на значимость отношений, возможность уголовно-правовой реакции на конкретный инцидент возникает не в связи с наступлением тех или иных общественно опасных последствий и даже не при традиционной повторности, а лишь при третьем задокументированном нарушении. Более предпочтительной представляется модель криминализации нарушения управления техническими средствами противодействия угрозам в зависимости от причинения существенного вреда правам и законным интересам граждан или организаций либо охраняемым законом интересам общества или государства.

Научная новизна: во многом определяется фактической неразработанностью вопросов, связанных с законодательным определением и реализацией уголовной ответственности за нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети Интернет и сети связи общего пользования.

Практическая значимость: основные положения и выводы исследования могут быть использованы для совершенствования механизма уголовно-правовой охраны информационной безопасности, дальнейшего развития отечественной доктрины уголовного права об ответственности за преступления в сфере компьютерной информации.

Для цитирования

Русскевич, Е. А. (2023). Нарушение правил централизованного управления техническими средствами противодействия угрозам информационной безопасности. *Journal of Digital Technologies and Law*, *1*(3), 650–672. https://doi.org/10.21202/jdtl.2023.28

Список литературы

Бокшицкий, В. И., Мельцева, И. С. (2017). Совершенствование защиты общественно значимых информационных ресурсов. *Вопросы кибербезопасности*, *S2*(20), 11–14. https://www.elibrary.ru/zvzggl

Дремлюга, Р. И. (2022). *Уголовно-правовая охрана цифровой экономики и информационного общества от киберпреступных посягательств: доктрина, закон, правоприменение*: монография. Москва: Юрлитинформ. https://www.elibrary.ru/hsbxrm

Дремлюга, Р. И., Коробеев, А. И., Федоров, А. В. (2017). Кибертерроризм в Китае: уголовно-правовые и криминологические аспекты. *Всероссийский криминологический журнал*, *11*(3), 607–614. EDN: https://www.elibrary.ru/zhnbdp. DOI: https://doi.org/10.17150/2500-4255.2017.11(3).607-614

Ельчанинова, Н. Б. (2020). Защита критической информационной инфраструктуры как новый институт правового обеспечения информационной безопасности. *Информационное общество*, *2*, 58–65.

Ефремова, М. А. (2018). *Уголовно-правовая охрана информационной безопасности*: монография. Москва: Юрлитинформ. https://www.elibrary.ru/zihcgl

Жарова, А. К. (2022). Правовое регулирование отношений в области предотвращения возможных уязвимостей в информационных технологиях. *Безопасность бизнеса*, *1*, 19–26. EDN: https://www.elibrary.ru/mnaski. DOI: https://doi.org/10.18572/2072-3644-2022-1-19-26

Красинский, В. В., Машко, В. В. (2023). Кибертерроризм: криминологическая характеристика и квалификация. *Государство и право*, *1*, 79–91. EDN: https://www.elibrary.ru/omupsq. DOI: https://doi.org/10.31857/S102694520024122-5

Лузянин, С. Г., Трощинский, П. В. (2018). Обеспечение национальной безопасности Китая на современном этапе (нормативно-правовой аспект). *Журнал зарубежного законодательства и сравнительного правоведения*, *1*, 60–69. EDN: https://www.elibrary.ru/yshope. DOI: https://doi.org/10.12737/art.2018.1.8

Пикуров, Н. И. (2009). *Квалификация преступлений с бланкетными признаками состава*: монография. Москва: Российская академия правосудия.

Трунцевский, Ю. В. (2019). Неправомерное воздействие на критическую информационную инфраструктуру: уголовная ответственность ее владельцев и эксплуатантов. *Журнал российского права*, *5*(269), 99–106. EDN: https://www.elibrary.ru/krnlwx. DOI: https://doi.org/10.12737/art_2019_5_9

Хисамова, З. И., Бегишев И. Р. (2022). Цифровая преступность в условиях пандемии: основные тренды. *Всероссийский криминологический журнал*, *16*(2), 185–198. https://doi.org/10.17150/2500-4255.2022.16(2).185-198

Bitzer, M., Häckel, B., Leuthe, D., Ott, J., Stahl, B., & Strobel, J. (2023). Managing the Inevitable – A Maturity Model to Establish Incident Response Management Capabilities. *Computers & Security*, *125*, 103050. https://doi.org/10.1016/j.cose.2022.103050

Boughton, N. (2019). Protecting infrastructure from cyber attack. *Network Security*, *4*, 18–19. https://doi.org/10.1016/S1353-4858(19)30051-0

Broadhead, S. (2018). The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments. *Computer Law & Security Review*, *34*(6), 1180–1196. https://doi.org/10.1016/j.clsr.2018.08.005

Cascavilla, G., Tamburri, D. A., & Van Den Heuvel, W. (2021). Cybercrime threat intelligence: A systematic multi-vocal literature review. *Computers & Security*, *105*, 102258. https://doi.org/10.1016/j.cose.2021.102258

Colding, J., Colding, M., & Barthel, S. (2020). Applying seven resilience principles on the Vision of the Digital City. *Cities*, *103*, 102761. https://doi.org/10.1016/j.cities.2020.102761

Espinoza-Zelaya, C., & Moon, Y. B. (2022). Resilience Enhancing Mechanisms for Cyber-Manufacturing Systems against Cyber-Attacks. *IFAC-PapersOnLine*, *55*(10), 2252–2257. https://doi.org/10.1016/j.ifacol.2022.10.043

Hausken, K. (2020). Cyber resilience in firms, organizations and societies. *Internet of Things*, *11*, 100204. https://doi.org/10.1016/j.iot.2020.100204

Hoheisel, R., Van Capelleveen, G., Sarmah, D. K., & Hartel, P. H. (2023). The development of phishing during the COVID-19 pandemic: An analysis of over 1100 targeted domains. *Computers & Security*, *128*, 103158. https://doi.org/10.1016/j.cose.2023.103158

Horsman, G. (2021). Digital evidence and the crime scene. *Sci. Justice*, *61* (6), 761–770. https://doi.org/10.1016/j.scijus.2021.10.003

Kouloufakos, T. (2023). Untangling the cyber norm to protect critical infrastructures. *Computer Law & Security Review*, *49*, 105809. https://doi.org/10.1016/j.clsr.2023.105809

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248. https://doi.org/10.1016/j.cose.2021.102248

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Li, Y., Tong, Y., & Giua, A. (2020). Detection and Prevention of Cyber-Attacks in Networked Control Systems. *IFAC-PapersOnLine*, *53*(4), 7–13. https://doi.org/10.1016/j.ifacol.2021.04.001

Mohamed, D. (2013). Combating the threats of cybercrimes in Malaysia: The efforts, the cyberlaws and the traditional laws. *Computer Law & Security Review*, *29*(1), 66–76. https://doi.org/10.1016/j.clsr.2012.11.005

Nguyen, C. L., & Golman, W. (2021). Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: 'Law on the books' vs 'law in action'. *Computer Law & Security Review*, *40*, 105521. https://doi.org/10.1016/j.clsr.2020.105521

Prasad, R., & Moon, Y. (2022). Architecture for Preventing and Detecting Cyber Attacks in Cyber-Manufacturing System. *IFAC-PapersOnLine*, *55*(10), 2246–2251. https://doi.org/10.1016/j.ifacol.2022.10.042

Qamar, S., Anwar, Z., & Afzal, M. (2023). A systematic threat analysis and defense strategies for the metaverse and extended reality systems. *Computers & Security*, *128*, 103127. https://doi.org/10.1016/j.cose.2023.103127

Tonhauser, M., & Ristvej, J. (2019). Disruptive acts in cyberspace, steps to improve cyber resilience at National Level. *Transportation Research Procedia*, *40*, 1591–1596. https://doi.org/10.1016/j.trpro.2019.07.220

Tsao, K. Y., Girdler, T., & Vassilakis, V. G. (2022). A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks. *Ad Hoc Networks*, *133*, 102894. https://doi.org/10.1016/j.adhoc.2022.102894

Ye, W., & Zhao, L. (2023). "I know it's sensitive": Internet censorship, recoding, and the sensitive word culture in China. D*iscourse, Context & Media*, *51*, 100666. https://doi.org/10.1016/j.dcm.2022.100666

Сведения об авторе

Русскевич Евгений Александрович – доктор юридических наук, доцент, профессор кафедры уголовного права, Московский государственный юридический университет имени О.Е. Кутафина (МГЮА)
Адрес: 125993, Российская Федерация, г. Москва, ул. Садовая-Кудринская, 9
E-mail: russkevich@mail.ru
ORCID ID: https://orcid.org/0000-0003-4587-8258
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57919310600
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/record/2510065
Google Scholar ID: https://scholar.google.ru/citations?user=rwKPImIAAAAJ
РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=539093

Конфликт интересов

Автор является членом редакционной коллегии журнала, статья прошла рецензирование на общих основаниях.

Финансирование

Исследование выполнено в рамках государственного задания «Российская правовая система в реалиях цифровой трансформации общества и государства: адаптация и перспективы реагирования на современные вызовы и угрозы (FSMW-2023-0006)». Регистрационный номер: 1022040700002-6-5.5.1.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.77.51 / Отдельные виды преступлений
Специальность ВАК: 5.1.4 / Уголовно-правовые науки

История статьи

Дата поступления – 6 февраля 2023 г.
Дата одобрения после рецензирования – 13 апреля 2023 г.
Дата принятия к опубликованию – 15 августа 2023 г.
Дата онлайн-размещения – 20 августа 2023 г.

Research article
DOI: https://doi.org/10.21202/jdtl.2023.29

Sovereignty vs. Digital Sovereignty

Margarita Robles-Carrillo

University of Granada
Granada, Spain

Keywords

Concept,
context,
digital sovereignty,
digital technologies,
digital transformation,
functions,
law,
safety,
security,
sovereignty,
state power

Abstract

Objective: the aim of this paper is to analyze the relationship between sovereignty and digital sovereignty in order to determine whether they are linked or autonomous concepts and in which cases and to what extent there is or is not a connection between the two categories.

Methods: the methodology is based on the analysis of international, European and national practice and scientific discourse, taking into account sovereignty and digital sovereignty from a threefold perspective: contextual, conceptual and functional.

Results: 1) analysis of the correlation between sovereignty and digital sovereignty showed that both are related concepts; 2) important consequences that digital sovereignty has in the case of States and the European Union are defined: a) there is a substantial difference between sovereignty and digital sovereignty because the former is only applied to States, while the latter is also used in reference to the EU; b) digital sovereignty is not necessarily a consequence or an extension of sovereignty; c) while in the case of States, digital sovereignty is justified as a safeguard of traditional sovereignty, in case of European Union its function must necessarily be different, since the European Union lacks sovereignty.

Scientific novelty: the analysis of this relationship provides an objective scientific premise for a comprehensive understanding of the idea of digital sovereignty. From the perspective of the context where they operate, as well as their concept and functions, sovereignty and digital sovereignty seem to be autonomous and, in some cases, complementary categories.

Practical significance: the dual functionality of digital sovereignty as a concept attached to national sovereignty and as an autonomous concept helps to explain the use of this category in the case of states and in the case of an organization such as the European Union, as well as the differences in its scope and meaning in each scenario.

For citation

Robles-Carrillo, M. (2023). Sovereignty vs. Digital Sovereignty. *Journal of Digital Technologies and Law, 1*(3), 673–690. https://doi.org/10.21202/jdtl.2023.29

Contents

Introduction

Sovereignty has traditionally been, for several reasons, a controversial legal and political category. For some time now, the processes of globalization and technification pose a particularly significant challenge to sovereignty. From the beginning, the digital realm appears to be an environment hardly appropriate for the exercise of sovereignty. It has no boundaries by itself and cuts across the rest of the physical spaces, blurring the effect of geographical borders. Despite time since its origins, the question of sovereignty in the digital world is still a matter of controversy. In 2020, Muller wrote the article "Against Sovereignty in Cyberspace" (Muller, 2020) while, in 2021, K. J. Heller published "In Defense of Pure Sovereignty in Cyberspace" (Heller, 2021). As these discussions continue, a new concept has emerged: digital sovereignty.

The idea of digital sovereignty has been introduced in the political, institutional and academic debate at international, national and European level. Despite the quantity and quality of scientific contributions on the subject, there is no consensus on this concept, its scope and meaning, its nature or even, particularly, its relationship with its physical counterpart. Actually, digital sovereignty is claimed both by States and by the European Union, which lacks the attribute of sovereignty.

Digital sovereignty does not seem to be just the online version of the principle of sovereignty (Chander & Sun, 2021; Franzese, 2009). The relationship between sovereignty and digital sovereignty is far from being settled. This is, nevertheless, a question that must be addressed in order to ascertain if they are equivalent, complementary, autonomous or different concepts as a necessary first step towards a better understanding of the idea of digital sovereignty.

The paper examines the relationship between sovereignty and digital sovereignty from a triple and complementary approach: the contextual, the conceptual and the functional. From the first perspective, the *contextual*, the aim is to analyze if sovereignty and digital sovereignty are equivalent, complementary, different or autonomous categories in the digital realm. The context is relevant because is where the principle of sovereignty is exercised and where the idea of digital sovereignty is born. From the second approach, the *conceptual*, the point is to determine if conceptually there are similarities or differences between the two categories. From the third perspective, the *functional*, the purpose is also to determine whether there are differences or similarities regarding their functions and, more precisely, why digital sovereignty is necessary when sovereignty exists or why digital sovereignty is used for where sovereignty is absent. So, the question is what function digital sovereignty performs when sovereignty exists and what function is attributed to it when there is no sovereignty.

Digital sovereignty is addressed by analyzing the political and institutional debate and the research carried out by the doctrine particularly in the European Union, where it has been frequently invoked in recent times.

1. Concepts of Sovereignty and Digital Sovereignty

Sovereignty is considered to be the most important principle of international law as the foundation of the architecture of this legal order. In addition to being the structural principle par excellence of international law, it is the maximum expression of the identity of the State. State and sovereignty are, moreover, two inseparable concepts that have been formalized in the Charter of the United Nations[1] and in several international norms.

Digital world is a major challenge to the principle of sovereignty from various perspectives. It is also a challenge for the States that appear to have been negatively affected by the processes of globalization and privatization. Furthermore, in an ecosystem in which non-State actors have gained increasing prominence, States maintain and reinforce their identity by asserting their sovereignty. Sovereignty is an exclusive attribute of the State defined as absolute, exclusive and exclusionary power. It is the symbol of the State.

In this context, the emergence of the concept of digital sovereignty raises new and different questions. It is a concept supported by different countries and with different

[1] United Nations Charter. https://www.un.org/en/about-us/un-charter/full-text

objectives and different motivations. It is a concept promoted by the European Union itself. It is a concept simultaneously claimed by this organization and its member States with no controversy or contest over its use in reference to the European Union, in contrast to what has always been the case with the principle of national sovereignty. There are similarities but also appreciable differences between these categories. The expression "digital sovereignty" seems to have a meaning that goes beyond what is normally conveyed by an adjective in relation to a noun. In order to understand this concept, it is necessary to analyze its relationship with the principle of sovereignty.

Sovereignty is not actually really questioned and, in addition, digital sovereignty is emerging as an original and powerful concept. Both the status and the relationship between the two categories are analyzed from a contextual, conceptual and functional perspective.

2. Contextual to Define the Correlations between Sovereignty and Digital Sovereignty

Nearly three decades ago, in 1996, John Perry Barlow launched the Declaration on the Independence of Cyberspace proclaiming the absence of sovereignty in this domain[2]. Since then, the debate on sovereignty in cyberspace has been ongoing in the political, institutional and academic world. However, in international practice, there is no evidence of a substantial change of the idea of sovereignty, except for the fact that certain countries and organizations are promoting multi-stakeholder governance approaches. As Mainwaring states, "sovereignty and state authority are changed, not erased" (Mainwaring, 2020).

Long after Barlow's proclamation, sovereignty has not disappeared but has been reaffirmed to a greater or lesser extent by the whole of States. In addition, the idea of digital sovereignty has become a main issue in political, institutional and academic discourse.

An analysis of that discourse provides some preliminary considerations. Firstly, digital sovereignty is not simply an online version of the traditional sovereignty. Secondly, digital sovereignty does not replace or displace this legal-political category. Thirdly, it is neither a consequence nor an extension of the sovereignty principle. Actually, digital sovereignty is the core of a specific legal, political and scientific discourse which is not always, nor necessarily, linked to its physical embryo. In fact, there are not always and generally connected or related arguments on both concepts.

Following a narrative different from the one of digital sovereignty, the principle of sovereignty has been expressed itself through its assertion in cyberspace in different ways.

Firstly, the principle of cyber sovereignty has been affirmed as the model of governance defended by some countries and international organizations, mainly China (Jiangyu & Huaer, 2022), Russia (Budnitsky & Jia, 2018) and the Shanghai Cooperation

[2] Barlow, J. P. (1996). *Declaration on the Independence of Cyberspace*. https://www.eff.org/cyberspace-independence

Organization, and as an alternative to the multi-stakeholder governance model promoted by the United States, the G7 or the European Union[3]. According to Flonk et al, it is a conflict between sovereigntists and liberals (Flonk et al., 2020).

Secondly, the principle of sovereignty over infrastructures, networks and systems located in the State territory has been endorsed by a large majority of countries as well as agreed upon in the framework of the work of the Groups of Governmental Experts and the Open-Ended Working Group set up by the United Nations General Assembly to debate the progress of ICTs and international security (Christakis, 2020).

Thirdly, some States have even implemented the principle of cyber sovereignty by creating their own digital space, aimed to be distinct and be separate from the general one. This is the case of China with the so-called Digital Wall (Zeng et al., 2017), as well as the Russian Federation with the launching of Yandex and Runet (Budnitsky & Jia, 2018).

As a matter of fact, there are several levels and motivations behind this process of progressive assertion of sovereignty in cyberspace (Kaloudis, 2021). Not all states claim it in the same way, to the same extent or with the same strength.

Something similar is happening with digital sovereignty insofar as not all States, not even the majority, have the same objective or try to achieve it in a similar way. There are specific grounds for defending digital sovereignty. Chander and Sun identify three main ones: "(f)irst, governments demand digital sovereignty to better protect their population – seeking, for example, to remove material deemed illegal under their laws or to protect the rights of citizens in the digital domain. <…> Second, governments seek digital sovereignty in an effort to grow their own digital economy, sometimes by displacing foreign corporations, from fintech to social media. Third, governments seek digital sovereignty to better control their populations – to limit what they can say, read, or do" (Chander & Sun, 2021). Not all of the countries pursue the same objectives and not all of them do it with the same scope and consistency.

Moreover, in this context, there is no exactly coincidence between those who defend the principle of sovereignty in cyberspace and those who advocate for digital sovereignty. Whereas the principle of cyber sovereignty is mainly supported by China, the Russian Federation and the Shanghai Cooperation Organization, the concept of digital sovereignty is primarily sponsored by the EU and among European countries. Nevertheless, in any case, when autocratic countries claim digital sovereignty, they do so with different motivations than those justifying its use in democratic countries. According to Pohle, there is a fundamental difference between them because "maintaining or strengthening digital sovereignty is shown

[3] Khawly, N., Arias-Oliva, M., & De Andrés, J. (2021). Technology and Geoeconomics: Emerging Conflicts in the Digital World. In Pelegrín Borondo, J. (coord.). *Moving technology ethics at the forefront of society, organisations and governments*. Universidad Complutense de Madrid and Universidad Rovira i Virgili. https://repository.ukim.mk/bitstream/20.500.12188/14702/1/Dialnet-MovingTechnologyEthicsAtTheForefrontOfSocietyOrgan-829454.pdf

in democratic countries to be an effective means of preserving liberal values and ideas of order in the course of the digital transformation. In contrast, the sovereignty concept in autocratic states serves to secure State power and make use of new ways for maintaining autocratic structures to suppress potentially democratizing effects of the digital sphere" [4]. As Kaloudis explains, the concept of sovereignty of autocratic states "is also underpinned with digital sovereignty in order to justify autocratically motivated sovereignty internally and strong economic and regulatory policies externally. Examples include Russia and China. Characteristics of these states are digital autarky, technological isolation and control of citizens" (Kaloudis, 2021). Ruohonen states that digital sovereignty has long been "a baton in geopolitics, with some countries using the concept in their political rhetoric seeking justify increasing state control over the Internet" (Ruohonen, 2021). Following Crespi et al, digital or technological sovereignty is "conceived as a nationalist concept" (Crespi et al., 2021). Pohle and Thiel consider that que the idea of strengthening digital sovereignty means "not only actively managing dependencies, but also creating infrastructures of control and (possible) manipulation" (Pohle & Thiel, 2020). As Fabiano argues, digital sovereignty "has multidisciplinary connotations, and it can assume different meaning or describe several aspects depending on the context in which we refer to it" (Fabiano, 2020).

From a contextual perspective, sovereignty and digital sovereignty have different uses and approaches. In addition, whereas sovereignty is a general principle with an equal scope and meaning for all States and everywhere, digital sovereignty has not the same understanding in all the cases. According to doctrine and in practice, in particular comparing democratic and autocratic countries, the different contexts in which digital sovereignty is invoked changes both its function and its concept.

3. Conceptual Approach to Define the Correlations between Sovereignty and Digital Sovereignty

Although the principle of sovereignty has been defined in different ways (Brack et al., 2019), the concept itself is generally agreed to be an absolute, exclusionary and exclusive power of the States. A different situation arises in the case of digital sovereignty. According to Prokscha, "(d)ue to its inflationary use, many conceptualisations of digital sovereignty take place outside the academic community, leading to confusion between the various terminologies. As a result of this, digital sovereignty is associated with different features ranging from regulatory authority over data, services, and algorithms, to control over hardware and infrastructure, and varies in context, meaning and purpose … Digital sovereignty is

[4] Pohle, J. (2020). *Digital sovereignty. A new key concept of digital policy in Germany and Europe.* Konrad-Adenauer-Stiftung. https://www.econstor.eu/bitstream/10419/228713/1/Full-text-report-Pohle-Digital-sovereignty.pdf

thus a fluid concept whose connotation and intended effect changes frequently" [5]. Elms states that digital sovereignty "is by nature a fuzzy concept" (Elms, 2021). In this sense, Allen is concerned about the fact that this concept "is being used as a cover for other policies: it has been described by some critics as a spectre haunting Europe and as a Trojan horse for protectionism"[6].

From a conceptual point of view, two different but related problems arise: the definition itself of digital sovereignty and whether or not to distinguish it from analogous concepts such as technological or strategic sovereignty.

As regards to the first question, digital sovereignty is defined as a power, as an ability, as just autonomy or from an axiological perspective. In a first line of thought, there are authors such as Chander and Sun for whom digital sovereignty "should be defined broadly to encompass the sovereign power of a state to regulate not only the cross-border flow of data through the use of Internet filtering technologies and data localization mandates, but also the activities of expression and access to technologies" (Chander & Sun, 2021). For these authors, it is practically an extension of traditional sovereignty. In the second meaning, Posch defines digital sovereignty as "the ability to have full knowledge and control by the individual or society over who can access one's data and where it is transferred" (Posch, 2015). In a third group, there are authors such as Crespi et al. who understand that the concept of sovereignty has been subject to various reformulations, but is "increasingly used to describe various forms of independence, control and autonomy over digital technologies and content" (Crespi et al., 2021). Finally, taking an axiological approach, the term digital sovereignty "is used to refer to an orderly, value-based, regulated and secure digital sphere that meets the demands of individual rights and freedoms, equality and fair economic competition"[7]. As can be appreciated, just one sector in the academic literature, the first mentioned, aligns the concept of digital sovereignty with the classical principle of sovereignty.

Moreover, according to a report published by the German Presidency of the European Union, digital sovereignty "is not a clearly defined concept, but rather a political vision of the respective social-economic order. It essentially addresses the reduction of existing and emerging dependencies in the digitalized world"[8].

---

5 Prokscha, A. (2021, June). *Digital Sovereignty for the European Union - Analysing Frames and Claims for Digital Sovereignty in the European Union's Digital Strategy*. https://www.researchgate.net/publication/354888060_Digital_Sovereignty_for_the_European_Union_-_Analysing_Frames_and_Claims_for_Digital_Sovereignty_in_the_European_Union%27s_Digital_Strategy

6 *European Sovereignty In the Digital Age*. (2021, July 19). https://www.iiea.com/images/uploads/resources/European_Sovereignty_in_the_Digital_Age.pdf

7 *Euro pean Digital Sovereignty. Institute of European Democrats*. https://www.iedonline.eu/download/2021/IED-Research-Paper-Innerarity.pdf

8 *Report of German Presidency on Digital Sovereignty*. https://erstelesung.de/wp-content/uploads/2020/10/20-10-14_Germany_EU_Digital-Sovereignty.pdf

As a matter of fact, there is no single or prevalent concept of digital sovereignty, nor is there consensus on the term itself. Alongside with digital sovereignty, there are expressions such as technological or strategic sovereignty often used alternatively, cumulatively or interchangeably.

It is said that these terms cannot be used synonymously because each of them represents "an aspect of the overarching, broader concept of digital sovereignty"[9]. According to Pohle and Thiel, digital sovereignty "has become a much more encompassing concept, addressing not only issues of internet communication and connection but also the much wider digital transformation of societies" (Pohle & Thiel, 2020). Burwell and Propp also recognize that digital sovereignty is a much broader concept "that includes a strong, innovative industrial base with sufficient cybersecurity protections" [10].. Supporting this idea, Edler et al define technological sovereignty as "the ability of a state or a federation of states to provide the technologies it deems critical for its welfare, competitiveness, and ability to act, and to be able to develop these or source them from other economic areas without one-sided structural dependency"[11]. Csernatoni, by contrast, argues that "by and large digital sovereignty is yet another iteration of technological sovereignty from external players in cyberspace" based on three inseparable pillars: computing power, control over our data and secure connectivity"[12].

A study of the practice reveals that the different denominations are generally used interchangeably, particularly in the case of the European Union. However, in logical terms and according to the opinion of the majority of the academic doctrine, digital sovereignty is to be a broader and more generic concept, while technological sovereignty would be a component focused on issues of this nature, just as strategic sovereignty would convey that specific political dimension of digital sovereignty as a whole.

At present, as has been seen, most doctrine defines digital sovereignty as a concept different from traditional sovereignty. However, neither the concept nor the term still enjoys consensus. Also, unlike the principle of sovereignty, there is neither consensus on the function or purpose of digital sovereignty.

---

9 *Europe's Quest for Digital Sovereignty: GAIA-X as a Case Study*. Istituto Affari Internazionali (IAI), Roma. https://www.iai.it/en/pubblicazioni/europes-quest-digital-sovereignty-gaia-x-case-study

10 Burwell, F. G., & Propp, K. (2020). *The European Union and the Search for Building "Fortress Europe" or Preparing for a New World?* https://www.atlanticcouncil.org/wp-content/uploads/2020/06/The-European-Union-and-the-Search-for-Digital-Sovereignty-Building-Fortress-Europe-or-Preparing-for-a-New-World.pdf

11 Edler, J., Blind, K., Frietsch, R., Kimpeler, S., Kroll, H., Lerch, Ch., Reiss, T., Roth, F., Schubert, T., Schuler, J., & Walz, R. (2020). *Technology sovereignty from demand to concept. Fraunhofer Institute for Systems and Innovation Research*. https://www.isi.fraunhofer.de/content/dam/isi/dokumente/publikationen/technology_sovereignty.pdf

12 Csernatoni, R. (2021). *The EU's Rise as a Defense Technological Power: From Strategic Autonomy to Technological Sovereignty*. Carnegie Europe Program. https://carnegieeurope.eu/2021/08/12/eu-s-rise-as-defense-technological-power-from-strategic-autonomy-to-technological-sovereignty-pub-85134

4. Functional Approach to Define the Correlations between Sovereignty and Digital Sovereignty

Sovereignty is an absolute, exclusive and exclusionary principle which translates the supreme power among powers. As such, it is still a power that can be exercised independently of the environment, physical or virtual, and with no need to be complemented by a digital version or dimension. The question therefore has to be asked: the why and the wherefore of digital sovereignty? Actually, why is digital sovereignty necessary if and when sovereignty already exists? What does digital sovereignty bring or what is digital sovereignty for when sovereignty lacks? There is no simple answer. France and the EU exemplify the two different cases of use of digital sovereignty when there is and there is not sovereignty.

France has promoted digital sovereignty as a basic principle of its political action at both the domestic and the European level. In the former, digital sovereignty is conceived as an essential prerequisite for guaranteeing national sovereignty[13]. In the European framework, the meaning is quite different because it is not associated with State sovereignty in the proper and traditional sense, thus evidencing the versatility or functionality of this category.

At the Joint Council of Ministers held on 7 April 2016, France and Germany justify the need to reinforce European digital sovereignty around three main pillars:

1. Strengthening the capacity of EU Member States to defend their networks and reinforce their digital resilience;

2. The development of an autonomous, innovative, efficient and diversified industry at European level, in particular in the fields of cybersecurity and trusted digital products;

3. The ability of Europeans to decide autonomously on the level of security of their data, in particular in the context of trade agreement negotiations[14].

In October 2020, the European Council states that "(t)o be digitally sovereign, the EU must build a true digital single market, strengthen its capacity to define its own rules, make autonomous technological choices and develop and deploy strategic digital capabilities and infrastructures. At the international level, the EU will activate its regulatory instruments and competences to help shape global rules and standards"[15]. On 21 March

---

13 Aktoudianakis, A. (2020, December). *Digital sovereignty for growth, rules and cooperation*. European Policy Centre. Konrad Adenauer Stiftung. https://www.epc.eu/content/PDF/2020/Digital_SA_paper_EPC_and_KAS.pdf

14 *The European digital sovereignty: a common objective for France and Germany*. https://www.ssi.gouv.fr/en/actualite/the-european-digital-sovereignty-a-common-objective-for-france-and-germany

15 *European Council Conclusions*. https://www.consilium.europa.eu/en/press/press-releases/2021/10/22/european-council-conclusions-21-22-october-2021

2021, a Statement of the Members of the European Council expressly recognizes "the need to enhance Europe's digital sovereignty in a self-determined and open manner by building on its strengths and reducing its weaknesses and through smart and selective action, preserving open markets and global cooperation" [16]. According to the Joint Communication on EU Policy on Cyber Defense, published in December 2022, the EU must ensure "its technological and digital sovereignty in the cyber field. The EU's capacity to act will depend on its ability to master and develop cutting edge technologies for cybersecurity and cyber defense in the EU" [17]. As Christakis argues, the simple fact that the Union talks about sovereignty "is rather puzzling <…>. Nowadays, the quantity of discourse by politicians in Europe and the EU in favor of digital or technological sovereignty is impressive" (Christakis, 2020).

These various references prove that the idea of digital sovereignty has become part of the European discourse despite the fact that, as is well known, the EU lacks the attribute of sovereignty retained by its member states. An evident conclusion is therefore that digital sovereignty does not depend on the possession of sovereignty, nor does it put national sovereignty in question.

It is justified that EU digital sovereignty is based of three needs: "1. The EU needs to invest in the creation of values by design technologies and critical infrastructure. 2. The EU needs to develop a concrete list of lasting guiding principles for digital policies based on democratic values and human rights that provide direction and purpose to the legal character of existing regulations and proposals. 3. The EU needs strategies that rely on global cooperation rather than attempting to shield Europe from the outside"[18]. Burwell and Propp considers that the current European focus on digital sovereignty "has its roots in a much broader discussion about Europe's ability to protect its citizens from an increasingly hostile and challenging world[19]. According to Siebert, "(t)he conversation about digital sovereignty also has a geopolitical dimension. The dependence on the U.S. and China for digital technologies has not been perceived as a problem for a long time in Europe. During the Trump administration, however, the relationship between the U.S. and China has become tenser and Europe risks being caught up in the middle"[20]. Digital sovereignty has emerged as "a means of promoting

---

16 *Statement of the members of the European Council*. https://www.consilium.europa.eu/en/press/press-releases/2021/03/25/statement-of-the-members-of-the-european-council-25-march-2021

17 *EU Policy on Cyber Defense*. https://www.eeas.europa.eu/sites/default/files/documents/Comm_cyber%20defence.pdf

18 Obendiek, A. (2021, May 11). *Take back control? Digital sovereignty and a vision for Europe*. Policy Paper. Hertie School. Jacques Delors Center. https://www.delorscentre.eu/fileadmin/2_Research/1_About_our_research/2_Research_centres/6_Jacques_Delors_Centre/Publications/20210511_Policy-Paper_Obendiek_Digital-Sovereignty__1_.pdf

19 Burwell, F. G., & Propp, K. (2020). *The European Union and the Search for Building "Fortress Europe" or Preparing for a New World?* https://www.atlanticcouncil.org/wp-content/uploads/2020/06/The-European-Union-and-the-Search-for-Digital-Sovereignty-Building-Fortress-Europe-or-Preparing-for-a-New-World.pdfvision-for-europe

20 *Digital Sovereignty – The EU in a Contest for Influence and Leadership*. The Green Political Foundation, https://www.boell.de/en/2021/02/10/digital-sovereignty-eu-contest-influence-and-leadership

the notion of European leadership and strategic autonomy in the digital field"[21]. For Irion et al, "with its quest for digital sovereignty the EU embraces a new assertive rhetoric, juxtaposing its value-based approach vis-a-vis a more market-based US and a top-down state-centric Chinese one" (Irion et al., 2021). Similarly, EU digital sovereignty is linked to a global battle over the model of digitalization. China, the United States, Russia and the European Union now find themselves in a competition of different digitalization models, a battle in which the shape of global markets and regulations is contested. At stake are conceptions of privacy, human rights, the platform economy and, ultimately, how markets, states and societies should relate to each other. In short, there are different explanations for European digital sovereignty, but none of them is linked to traditional sovereignty.

Moreover, the use of the expression digital sovereignty interchangeably in the national and European contexts reveals, firstly, that there is a substantial difference between the concepts of sovereignty and digital sovereignty. The former is only applied to States, while the latter is also used in reference to the EU, so it is not an exclusive or exclusionary category. Secondly, to the extent that it is applied to the States that are sovereign and to an international organization that is not, digital sovereignty is not necessarily a consequence or an extension of sovereignty in the traditional sense. Thirdly, while in the case of States, digital sovereignty is justified as a safeguard of traditional sovereignty, in the case of an international organization like the EU its function must necessarily be different, since the EU lacks sovereignty. In this regard, Floridi explains that the debate on digital sovereignty in the EU "is not about replacing national modern-analogue sovereignty, which is necessary but increasingly insufficient. It is about complementing it with a supranational, contemporary-digital one" (Floridi, 2020). Roberts et al consider that it is "a signal of intent and a reflection of a newfound policymaking agenda within the EU. Digital sovereignty is seen as a basis for strengthening the EU's role in an interconnected world, promoting its core interests, and protecting the fundamental values upon which the Union is based, namely, human dignity, freedom, democracy, equality, the rule of law and respect of human rights" (Roberts et al., 2021).

Conclusions

The relationship between sovereignty and digital sovereignty is far from simple. From as contextual perspective, they are autonomous categories. In the digital context, there is no coincidence between those States who defend the principle of sovereignty in cyberspace and those who advocate for digital sovereignty. Moreover, when the former also claim for digital sovereignty, both their motivations and the meaning of this idea are different. Whereas sovereignty is a general principle with an equal scope and meaning for all States

[21] Towards a more resilient EU. Digital sovereignty for Europe. *EPRS Ideas Paper*. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf

and everywhere, digital sovereignty has not the same understanding in all the cases and for all the States. The different contexts in which digital sovereignty is invoked alters both its concept and its function.

From a conceptual point of view, digital sovereignty is defined as a power, an ability, autonomy or from an axiological perspective. Although there is no consensus on this concept, in most cases, the definition of digital sovereignty is not linked to the principle of sovereignty.

From a functional perspective, unlike the principle of sovereignty, there is no consensus on the function or purpose of digital sovereignty. However, the call for digital sovereignty both in the case of States and the European Union has some important consequences.

Firstly, there is a substantial difference between sovereignty and digital sovereignty because the former is only applied to States, while the latter is also used in reference to the EU.

Secondly, to the extent that it is applied to the States that are sovereign and to an international organization that is not, digital sovereignty is not necessarily a consequence or an extension of sovereignty in the traditional sense.

Thirdly, while in the case of States, digital sovereignty is justified as a safeguard of traditional sovereignty, in the case of an international organization like the EU its function must necessarily be different, since the EU lacks sovereignty. There are different explanations for European digital sovereignty, but none of them is linked to traditional sovereignty. The functions assigned to sovereignty and digital sovereignty are therefore different, and the functions of digital sovereignty are also somewhat different in the case of States and in the case of the EU.

Digital sovereignty has emerged and developed as a complementary category to national sovereignty in the States and as an autonomous category in the EU. So, only for the States and not in general terms, it is a consequence or an extension of the sovereignty principle. In any case, digital sovereignty is not simply an online version of the traditional sovereignty and it does not replace or displace the sovereignty principle. Being something different from its physical counterpart from the contextual, conceptual and functional perspectives, it would be possible to consider its autonomy as a category of knowledge.

References

Brack, N., Coman, R., & Crespy, A. (2019). Unpacking old and new conflicts of sovereignty in the European polity. *Journal of European Integration*, *41*(7), 817–832. https://doi.org/10.1080/07036337.2019.1665657

Budnitsky, S., & Jia, L. (2018). Branding Internet sovereignty: Digital media and the Chinese–Russian cyberalliance. *European Journal of Cultural Studies*, *21*(5), 594–613. https://doi.org/10.1177/1367549417751151

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

Chander, A., & Sun, H. (2021). *Sovereignty 2.0*. Georgetown University Law Center. http://dx.doi.org/10.2139/ssrn.3904949

Christakis, T. (2020). *"European Digital Sovereignty": Successfully Navigating Between the Brussels Effect and Europe's Quest for Strategic Autonomy*. Studies of Digital Governance. Data institute. Université Grenoble Alpes. https://ai-regulation.com/european-digital-sovereignty-successfully-navigating-between-the-brussels-effect-and-europes-quest-for-strategic-autonomy/

Elms, D. (2021). *Digital Sovereignty: protectionism or autonomy*. Hinrich foundation, Asian Trade Centre.

Fabiano, N. (2020). Digital Sovereignty Between "Accountability" and the Value of Personal Data. *Advances in Science, Technology and Engineering Systems Journal*, *5*(3), 270–274. https://doi.org/10.25046/aj050335

Flonk, D., Jachtenfuchs, M., & Obendiek, A. (2020). Authority conflicts in internet governance: Liberals vs. sovereigntists? *Global Constitutionalism*, *9*(2), 364–386. https://doi.org/10.1017/S2045381720000167

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

Franzese, P. W. (2009). Sovereignty in Cyberspace: Can it exist? *The Air Force Law Review; Maxwell AFB*, *64*, 1–42. https://www.proquest.com/docview/195182873

Heller, K. J. (2021). In Defense of Pure Sovereignty in Cyberspace. *International Law Studies*, *97*, 1432–1499. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2987&context=ils

Irion, K., Burri, M., Kolk, A., & Milan, S. (2021). Governing "European values" inside data flows: interdisciplinary perspectives. *Internet Policy Review*, *10*(3). https://doi.org/10.14763/2021.3.1582

Jiangyu, W., & Huaer, Che. (2022). China's Approach to International Law: From Traditional Westphalianism to Aggressive Instrumentalism in the Xi Jinping Era. *The Chinese Journal of Comparative Law*, *10*(1), 140–153. https://doi.org/10.1093/cjcl/cxac020

Kaloudis, M. (2021). Digital sovereignty – European Union's action plan needs a common understanding to succeed. *History Compass*, *8*. https://doi.org/10.1111/hic3.12698

Mainwaring, S. (2020). Always in control? Sovereign states in cyberspace. *European Journal of International Security*, *5*(2), 215–232. https://doi.org/10.1017/eis.2020.4

Mueller, M. L. (2020). Against Sovereignty in Cyberspace. *International Studies Review*, *22*(4), 779–801. https://doi.org/10.1093/isr/viz044

Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, *9*(4). https://doi.org/10.14763/2020.4.1532

Posch, R. (2015). Digital Sovereignty and IT-Security for a Prosperous Society. En Werthner, H. y Van Harmelen, F. *Informatics in the Future. Proceedings of the 11th European Computer Science Summit* (ECSS 2015). Vienna. https://doi.org/10.1007/978-3-319-55735-9_7

Roberts, H., Cowls, J., Casolari, F., Morley, J., Taddeo, M., & Floridi, L. (2021). Safeguarding European values with digital sovereignty: an analysis of statements and policies. *Internet Policy Review*, *10*(3). https://doi.org/10.14763/2021.3.1575

Ruohonen, J. (2021). The Treachery of Images in the Digital Sovereignty Debate. *Minds and Machines*, *31*, 439–456. https://doi.org/10.48550/arXiv.2012.02724

Zeng, J., Stevens, T., & Chen, Y. (2017). China's solution to global cyber governance: Unpacking the domestic discourse of "Internet sovereignty". *Politics & Policy*, *45*(3), 432–464. https://doi.org/10.1111/polp.12202

Author information

Margarita Robles-Carrillo – PhD, Full Professor of International Law and European Law, Network Engineering & Security Group, University of Granada
Address: Plaza de la Universidad, 1, CP:18071, Granada, Spain
E-mail: mrobles@ugr.es
ORCID ID: https://orcid.org/0000-0002-6324-4665
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57203316304
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/record/ADD-1696-2022
Google Scholar ID: https://scholar.google.ru/citations?user=PSUjIYgAAAAJ

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

This work is supported by the Spanish Government-MINECO (Ministerio de Econom´ıa y Competitividad), using the Fondo Europeo de Desarrollo Regional (FEDER), under Project TIN2017-83494-R.

Thematic rubrics

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

Article history

Date of receipt – February 2, 2023
Date of approval – April 30, 2023
Date of acceptance – August 15, 2023
Date of online placement – August 20, 2023

Научная статья
УДК 34:342.3:004
EDN: https://elibrary.ru/nfwlyf
DOI: https://doi.org/10.21202/jdtl.2023.29

Суверенитет и цифровой суверенитет

Маргарита Роблес-Каррильо

Гранадский университет
г. Гранада, Королевство Испания

Ключевые слова

Безопасность,
государственная власть,
защищенность,
контекст,
концепция,
право,
суверенитет,
функции,
цифровая трансформация,
цифровой суверенитет,
цифровые технологии

Аннотация

Цель: анализ взаимоотношений между суверенитетом и цифровым суверенитетом и определение того, являются ли они взаимосвязанными или независимыми понятиями, а также в каких случаях и в какой степени прослеживается связь между данными категориями.

Методы: методология основана на анализе международной, европейской и государственной практики и научного дискурса, рассматривающего суверенитет и цифровой суверенитет с трех точек зрения: контекстуальной, концептуальной и функциональной.

Результаты: 1) анализ корреляции между суверенитетом и цифровым суверенитетом показал, что эти понятия взаимосвязаны; 2) определены важные следствия цифрового суверенитета для государств и Евросоюза в целом, а именно: а) между суверенитетом и цифровым суверенитетом существуют значительные отличия, поскольку первый относится только к государствам, тогда как второе понятие используется также по отношению к Евросоюзу; б) цифровой суверенитет не обязательно является следствием или продолжением обычного суверенитета; в) в случае отдельных государств цифровой суверенитет оправдан в качестве гарантии традиционного суверенитета, тогда как в случае Евросоюза его функция должна быть иной, поскольку Евросоюз не обладает суверенитетом.

Научная новизна: анализ данных взаимоотношений дает объективную научную базу для глубокого понимания концепции цифрового суверенитета. С точки зрения контекста, в котором действуют суверенитет и цифровой суверенитет, а также их концепций и функций эти категории представляются независимыми и в некоторых случаях взаимодополняющими.

Практическая значимость: дуальная функциональность цифрового суверенитета как понятия, тесно связанного с государственным суверенитетом, и как независимого понятия помогает объяснить использование этой категории по отношению к отдельным государствам и по отношению к такой организации, как Европейский союз, а также различия в масштабах и значении каждого из этих сценариев.

Для цитирования

Роблес-Каррильо, М. (2023). Суверенитет и цифровой суверенитет. *Journal of Digital Technologies and Law*, *1*(3), 673–690. https://doi.org/10.21202/jdtl.2023.29

Список литературы

Brack, N., Coman, R., & Crespy, A. (2019). Unpacking old and new conflicts of sovereignty in the European polity. *Journal of European Integration*, *41*(7), 817–832. https://doi.org/10.1080/07036337.2019.1665657

Budnitsky, S., & Jia, L. (2018). Branding Internet sovereignty: Digital media and the Chinese–Russian cyberalliance. *European Journal of Cultural Studies*, *21*(5), 594–613. https://doi.org/10.1177/1367549417751151

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

Chander, A., & Sun, H. (2021). *Sovereignty 2.0.* Georgetown University Law Center. http://dx.doi.org/10.2139/ssrn.3904949

Christakis, T. (2020). *"European Digital Sovereignty": Successfully Navigating Between the Brussels Effect and Europe's Quest for Strategic Autonomy.* Studies of Digital Governance. Data institute. Université Grenoble Alpes. https://ai-regulation.com/european-digital-sovereignty-successfully-navigating-between-the-brussels-effect-and-europes-quest-for-strategic-autonomy/

Elms, D. (2021). *Digital Sovereignty: protectionism or autonomy*. Hinrich foundation, Asian Trade Centre.

Fabiano, N. (2020). Digital Sovereignty Between "Accountability" and the Value of Personal Data. *Advances in Science, Technology and Engineering Systems Journal*, *5*(3), 270–274. https://doi.org/10.25046/aj050335

Flonk, D., Jachtenfuchs, M., & Obendiek, A. (2020). Authority conflicts in internet governance: Liberals vs. sovereigntists? *Global Constitutionalism*, *9*(2), 364–386. https://doi.org/10.1017/S2045381720000167

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

Franzese, P. W. (2009). Sovereignty in Cyberspace: Can it exist? *The Air Force Law Review*; Maxwell AFB, 64, 1–42. https://www.proquest.com/docview/195182873

Heller, K. J. (2021). In Defense of Pure Sovereignty in Cyberspace. *International Law Studies*, *97*, 1432–1499. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2987&context=ils

Irion, K., Burri, M., Kolk, A., & Milan, S. (2021). Governing "European values" inside data flows: interdisciplinary perspectives. *Internet Policy Review*, *10*(3). https://doi.org/10.14763/2021.3.1582

Jiangyu, W., & Huaer, Che. (2022). China's Approach to International Law: From Traditional Westphalianism to Aggressive Instrumentalism in the Xi Jinping Era. *The Chinese Journal of Comparative Law*, *10*(1), 140–153. https://doi.org/10.1093/cjcl/cxac020

Kaloudis, M. (2021). Digital sovereignty – European Union's action plan needs a common understanding to succeed. *History Compass*, *8*. https://doi.org/10.1111/hic3.12698

Mainwaring, S. (2020). Always in control? Sovereign states in cyberspace. *European Journal of International Security*, *5*(2), 215–232. https://doi.org/10.1017/eis.2020.4

Mueller, M. L. (2020). Against Sovereignty in Cyberspace. *International Studies Review*, *22*(4), 779–801. https://doi.org/10.1093/isr/viz044

Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, *9*(4). https://doi.org/10.14763/2020.4.1532

Posch, R. (2015). Digital Sovereignty and IT-Security for a Prosperous Society. En Werthner, H. y Van Harmelen, F. *Informatics in the Future. Proceedings of the 11th European Computer Science Summit* (ECSS 2015). Vienna. https://doi.org/10.1007/978-3-319-55735-9_7

Roberts, H., Cowls, J., Casolari, F., Morley, J., Taddeo, M., & Floridi, L. (2021). Safeguarding European values with digital sovereignty: an analysis of statements and policies. *Internet Policy Review*, *10*(3). https://doi.org/10.14763/2021.3.1575

Ruohonen, J. (2021). The Treachery of Images in the Digital Sovereignty Debate. *Minds and Machines*, *31*, 439–456. https://doi.org/10.48550/arXiv.2012.02724

Zeng, J., Stevens, T., & Chen, Y. (2017). China's solution to global cyber governance: Unpacking the domestic discourse of "Internet sovereignty". *Politics & Policy*, *45*(3), 432–464. https://doi.org/10.1111/polp.12202

Сведения об авторе

Маргарита Роблес-Каррильо – доктор наук, профессор международного и европейского права, Группа сетевых технологий и безопасности, Гранадский университет
Адрес: Королевство Испания, г. Гранада, Университетская площадь, 1, CP:18071
E-mail: mrobles@ugr.es
ORCID ID: https://orcid.org/0000-0002-6324-4665
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57203316304
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/record/ADD-1696-2022
Google Scholar ID: https://scholar.google.ru/citations?user=PSUjIYgAAAAJ

Конфликт интересов

Автор заявляет об отсутствии конфликта интересов.

Финансирование

Работа выполнена при поддержке Министерства экономики и конкурентоспособности Правительства Испании в рамках проекта TIN2017-83494-R Европейского фонда регионального развития.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.15.41 / Государственный суверенитет
Специальность ВАК: 5.1.2 / Публично-правовые (государственно-правовые) науки

История статьи

Дата поступления – 2 февраля 2023 г.
Дата одобрения после рецензирования – 30 апреля 2023 г.
Дата принятия к опубликованию – 15 августа 2023 г.
Дата онлайн-размещения – 20 августа 2023 г.

Research article
DOI: https://doi.org/10.21202/jdtl.2023.30

Features of Online Settlement of Consumer Disputes by e-commerce Platforms in the People's Republic of China

Elena P. Ermakova

Peoples' Friendship University of Russia named after Patrice Lumumba
Moscow, Russian Federation

Keywords

Buyer,
court,
digital technologies,
e-commerce,
Internet store,
law,
online dispute resolution,
online dispute settlement,
seller,
Taobao

Abstract

Objective: to research the features of online dispute settlement by e-commerce platforms in the People's Republic of China, to reveal positive features and drawbacks of ODS technologies applied by the platforms.

Methods: empirical methods of comparison, description, interpretation; theoretical methods of formal and dialectical logic. Specific scientific methods were used: legal-dogmatic and the method of legal norms interpretation.

Results: it was found that the internal ODS model on e-commerce Taobao ODS platforms is a direct, clear and effective means of online resolution of consumer disputes. However, being a non-independent "third party", the internal ODS mechanism of e-commerce platforms will never be able to substitute other external systems of dispute resolution. ODS relies on the data and Internet processes much stronger than traditional dispute resolution. Among the many safety factors emerging as a result of online processes, ODS creates the risk of data leakage, lack of confidentiality and unsafe consumer protection. ODS also causes concerns due to traditional principles of justice such as objectivity, confidentiality and safety of data in the process of dispute settlement. Not only the People's Republic of China but any country introducing the ODS technologies into the procedures of dispute resolution should take serious measures to ensure the ODS processes are just, unbiased and guarantee observance of procedural rights.

Scientific novelty: consists in a complex research of online dispute settlement by e-commerce platforms in the People's Republic of China, the practice of implementation thereof has its specific features stemming from the model of self-regulation of thee relations, further stipulated by normative legal acts of the People's Republic of China and reflected in the activity of private ODS platforms.

Practical significance: is due to the current absence of possibility to apply the legal norms and rules, taking into account the specific features of ODS technologies on private platforms, to the relations using such technologies. The main provisions and conclusions of the research can be used to improve the mechanisms of legal regulation of ODS technologies in the procedural legislation of the Russian Federation.

For citation

Ermakova, E. P. (2023). Features of Online Settlement of Consumer Disputes by e-commerce Platforms in the People's Republic of China. *Journal of Digital Technologies and Law, 1*(3), 691–711. https://doi.org/10.21202/jdtl.2023.30

Contents

Introduction

In 2021, the People's Republic of China (further – China, PRC) possessed over 37% of the global market of e-commerce from the viewpoint of volume of payments (over 50% by the number of transactions). Currently, the Chinese e-commerce market is the largest in the world and is expected to demonstrate a steady growth in 2022 to reach CNY 14.5 trillion ($23 trillion), as predicted by GlobalData agency. According to statistical reports, Chinese and foreign consumers on Chinese e-commerce platforms more and more often transfer from offline to online. The COVID-19 pandemic accelerated the e-commerce activity in China, as cautious consumers more and more often use online channel for purchases, in order to avoid contacting with transmitters of disease, and this trend persists after the pandemic, as was shown by the GlobalData leading analyst R. Sharma[1]. The average annual growth rate of the Chinese e-commerce market is expected to reach 11.3% from 2022 to 2027. The main factors stimulating the growth of e-commerce market in the region are: culture of mobile trade based on smartphones; innovative systems of digital payments and growing platforms for online trade.

The boom of e-commerce has brought dozens of millions disputes on e-commerce sites – Internet platforms. Beyond any doubt, no country of the world has a million of arbitrators or a million of mediators to settle these disputes. Thus, the online trading platforms first in the United States and Europe (eBay, Amazon), then in China (Alibaba) platforms for online dispute settlement started to appear spontaneously, without normative regulation on the part of the state. As was marked by E. Katsh and O. Rabinovich-Einy in 2018, eBay platform, for example, informed that it was considering over 60 million disputes a year via its ODR system; eth Chinese e-commerce giant Alibaba informed about hundreds of millions disputes a year. Some of these disputes emerge in relation to the platform, others in relation to other consumers. Most of these disputes will never reach courts or alternative means of dispute resolution: they are associated with small amounts of money and require rapid, accessible and effective settlement. Characteristics of online disputes often make them unsuitable for traditional mechanisms of offline dispute resolution, namely, courts and alternative dispute resolution (ADR). The need to find a relevant means to settle online disputes appeared in the mid-1990s, when the Internet opened for trading (Katsh & Rabinovich-Einy, 2018).

A well-known American expert C. Rule, Director of the ODR Modria Department, as well as eBay and PayPal from 2003 to 2011, wrote: "Technology is also changing people's expectations about how disputes should be resolved. People now believe that they should be able to report a problem at any time of day and get quick, round-the-clock support to resolve it transparently and effectively. Now that society has embraced technology so thoroughly, the key question for dispute resolution professionals is, how can we leverage technology to best assist parties in resolving their disputes?" (Rule, 2015).

---

[1] China continues to lead global e-commerce market with over $2 trillion sales in 2022. (2022, August 9). *GlobalData*. https://www.globaldata.com/media/banking/china-continues-to-lead-global-e-commerce-market-with-over-2-trillion-sales-in-2022-says-globaldata

Today, the Chinese legislation and state policy in regard to the Internet are among the most advanced in the world, comprising the detailed and specific provisions determining the relations between e-commerce platforms, business operators and consumers in online transactions. An example of the Chinese state policy in this sphere is establishing of Internet courts in Hangzhou, Beijing and Guangzhou, using the experience of Alibaba company (Taobao ODS platform).

The autonomous ODS platform in Taobao was developed according to the American eBayODR platform. But the developers of Taobao ODS platform went further – the company introduced a new system of making decisions by a quasi jury, namely, Alibaba public jury, which became the company's specific feature and advantage in confirming the characteristics of justice and transparency of the ODS procedure. The stunning success of the ODS system in Taobao facilitated its going beyond other Chinese platforms, such as WeChat and DiDi. It is this aspect that determined the choice of this research topic.

One should mark that the Chinese doctrine distinguishes between the terms "online dispute settlement (ODS) and "online dispute resolution (ODR). This was emphasized by the Chinese, American and German experts (Shang & Guo, 2020; Shi et al., 2021). In their opinion, ODS is performed by state Internet courts and internal e-commerce platforms, while ODR is performed, first of all, by arbitration institutions (arbitration tribunal) and various mediator institutions in China.

The Russian authors do not attach much significance to distinguishing between the notions of ODR and ODS. For example, A. N. Kutovaya and K. R. Khadzhi highlighted: "the term 'online dispute resolution', ODR, appeared in the 1990s. According to one of interpretations, this is one of the forms of alternative dispute settlement (ODS), performed (partially or fully) using the Internet. It may also include disputes started in the cyberspace, but with an external source. In literature, the terms 'electronic ODS', 'online ODS' and 'dispute settlement in the Internet' are considered to be synonyms. Modern researchers tend to feature ODS as an absolutely new and distinct method of dispute resolution" (Kutovaya & Khadzhi, 2020).

1. Features of dispute settlement on Taobao ODS platform

The Chinese government developed a structured system to resolve the disputes related to online commerce. In August 2017 in Hangzhou (where Alibaba company is registered), the first Internet court in China opened aimed at settling the disputes related to online commerce and violation of copyright, as well as disputes between users and Internet companies; the whole procedure took place online. In 2018, similar courts were established in Beijing (where Baidu company is registered) and Guangzhou (where Huawei company is registered) (Rusakova, 2021). These courts work autonomously from private platforms for online dispute settlement, but their services still may be used. Nevertheless, only three Internet court exist in China so far, and most of the disputes in the sphere of e-commerce are resolved via private e-commerce platforms, which also provide ODS services (Wei & Tian, 2021).

Notably, the Chinese government consulted with Alibaba about the design of the Internet court of Hangzhou. Besides, Alibaba company provides cloud services to the Internet court of Hangzhou. Alibaba company also created a means to transfer evidences to the Internet court from its e-commerce websites with a mouse click. In 2019, a new project was introduced in the Internet court of Hangzhou – a pilot AI judge assistant (试点AI助理法官), also developed by Alibaba.

In 2019, PRC adopted the E-Commerce Law[2], which allowed e-commerce operators to create their own online systems for dispute settlement. In June 2021, the Supreme Court of PRC published the "Regulation of online court procedures of people's court", and in December of the same year amendments to the Civil-Procedural Code of PRC were adopted regarding the development of online hearings. All normative acts were created based on the studies and summarization of the practice of dispute resolution on Chinese e-commerce platforms.

We agree with the American authors L. Liu (Georgetown University) and B. R. Weingast (Stanford University), who wrote in a 2020 work "Law, Chinese Style: Solving the Authoritarian's Legal Dilemma through the Private Provision of Law" that the Chinese government consented with the Taobao efforts; moreover, it started to actively cooperate with Taobao (Liu & Weingast, 2020). E-commerce platforms adopted from the state the authorities to ensure law observance within their competence; besides, they helped the state to create formal legislation, experimenting with the character and content of legal norms suitable for managing their platforms. In many respects, this development took place similarly to earlier Chinese reforms (1980s – beginning of 1990s), which created Chinese-style federalism.

The PRC government is not the only one striving for cooperation with private technological companies with a view of digital reforming of their legal system. Notably, the Thomson Reuters media corporation and the software developer McGirr are the largest suppliers of technologies of Internet courts in Australia, USA and Great Britain[3].

TaobaoMarketplace e-commerce platform was created by Alibaba company in 2003 and since then has turned into a giant of online purchases in China and became the eighth most visited website in the world (Liu & Weingast, 2018). Taobao platform is considered to be a Chinese analog of eth American eBay platform, founded eight years earlier – in 1995 (Ballesteros, 2021). As of March 2021, monthly active uses of Taobao reached 792 million, ranking the first among Chinese and global e-commerce platforms[4]. According to statistical data, Taobao platform was the most popular e-commerce platform as of August 2022

---

2 E-Commerce Law of the People's Republic of China (adopted at the Fifth Session of the Standing Committee of the 13th National People's Congress on August 31, 2018). *IPKey*. https://ipkey.eu/sites/default/files/documents/resources/PRC_E-Commerce_Law.pdf

3 Mingay, A. (2019, October 17). Size matters: Alibaba shapes China's first "Court of the Internet". *Merics*. https://merics.org/en/analysis/size-matters-alibaba-shapes-chinas-first-court-internet

4 You, X. (2018, September 3).Six key features of Taobao – Alibaba's online shopping platform. *Croud*. https://croud.com/blog/six-key-features-of-taobao-alibabas-online-shopping-platform

in China[5]. Like American commercial platforms eBay and Amazon, Taobao is a platform for retail trade from client to client (C2C), therefore, large brands, small enterprises and individuals may open their own Internet stores on Taobao platform.

The platform offers four ways to settle an online dispute in accordance with Taobao ODS regulations:

a) negotiations between the parties;

b) intervention of Taobao client service;

c) public control system;

d) online report.

An unbiased, rapid and accessible system of dispute settlement may reduce the uncertainty associated with e-commerce and increase trust to online markets. The PRC's experience showed that the construction of internal system of online dispute settlement (ODS) of Alibaba company is scientific, reasonable, cheap and highly effective, as was marked by a researcher from Macao University (PRC) (Juanjuan, 2018).

Taobao ODS model was also extended to solve the problems with ODS systems implementation onto some other Internet platforms in China, such as WeChat (a mobile communication system for sending text and voice messages) and Didi (a platform rendering the services of a taxi aggregator, car sharing and ridesharing). Notably, none of these systems became as popular or successful as Taobao ODS system, as was highlighted by researchers C. S. Shang (California Polytechnic State University, USA) and W. K. Guo (Beiming Software Co Ltd) (Shang & Guo, 2020).

2. Characteristics of Taobao ODS technology

In the opinion of Chinese researchers, the scientific approach to forming the internal Taobao ODS system showed itself in the following factors: a) modular construction of the platform; b) strict observance of the terms stipulated by internal regulations of dispute resolution; c) coinciding characteristics of e-commerce and Taobao ODS platform; d) social participation to create the "e-commerce ecosystem" (Juanjuan, 2018). Below we consider each aspect in detail.

2.1. Modular construction of Taobao ODS platform

Taobao ODS specialists found that in different categories of goods the causes of disputes and the settlement results always coincide. Having made a market research and a statistical analysis, Taobao ODS experts summarized the most popular causes of disputes, including:

a) the goods is damaged;

b) the goods is wrongly delivered or not delivered;

[5] E-commerce in China. (2022, August 3). *Moore MS Advisory*. URL: https://www.msadvisory.com/ecommerce-in-china

c) the goods needs repair;

d) the goods does not meet the description;

e) the goods is of poor quality;

f) the goods is not delivered on time, etc.

The methods of dispute settlement are summarized in the following groups:

a) change of the price of the goods;

b) return of the goods;

c) reimbursement of costs, etc.

When developing the dispute settlement procedure, Taobao specialists used a modular method to provide choice for applicants. For an applicant, on the one hand, this could save time for describing the problem they faced; on the other hand, the result could be predicted. Moreover, this could make consumer protection services be more professional when they intervene in disputes (Juanjuan, 2018).

2.2. Strict observance of the terms stipulated by internal regulations of dispute resolution

Each stage of the dispute settlement procedure at Taobao ODS platform is strictly limited in time. For example, three days after submitting an application on returning money a buyer may turn to the consumer support service which must make a decision on intervention into the dispute during two days, then a final decision during 15 days. The parties must submit evidences, including: photos of the goods, recordings of Aliwangwang chat, a recording on Taobao platform referring to the transaction, etc.[6] Dispute settlement must correlate with this tempo, which is an important content for provision of justice on Taobao ODS platform. If any party fails to provide evidences during the set period, it will lose.

2.3. Coinciding characteristics of e-commerce and Taobao ODS platform

Taobao ODS platform has characteristics comparable to the rules of e-commerce:

a) high speed;

b) simple procedure;

c) low costs of dispute settlement.

The platform popularity demonstrates that in B2C and C2C disputes, efficiency and cost-effectiveness are more important than justice, neutrality, professionalism and relevancy, which coincide with the characteristics of e-commerce.

[6] Taobao Rules of Dispute Settlement (2019, June 5). 淘宝平台争议处理规则. https://rulechannel.taobao.com/?type=detail&ruleId=99&cId=1154&spm=a2177.72311#/rule/detail?ruleId=99&cId=1154&spm=a2177.72311

2.4. Social participation to create an "e-commerce ecosystem"

Due to the procedures of dispute settlement on Taobao ODS platform –"Public control system" and "Online report" – introduced social powers, including a buyer and a seller, to mutually participate in creating and managing the Ali e-commerce ecosystem. To remove some pressure from its customer support service, the Chinese largest online-market uses a "people's court" with half a million amateur judges to help regulate common complaints of consumers[7].

From the viewpoint of justice, Taobao ODS system uses the method of delivering the task to the interviewer at random and the challenge system in order to effectively prevent a reviewer from choosing cases (disputes) in their own interests. Moreover, both the buyer and the seller may participate in the "Public control system" and "Online report" in person, which is a good chance to tell the participants about the cause of the dispute and then to take steps to its peaceful settlement. Foreign authors believe that the most important feature is that the Taobao ODS system is a means of implementing social corporate governance (Iqbal et al., 2022).

3. Comparing the practice of dispute resolution between various ODS platforms (state court, arbitration, private e-commerce platforms)

3.1. Advantages of ODR

An American author C. Rule outlined the following advantages of ODR[8]:

1) efficiency and convenience;

2) procedural cost-effectiveness;

3) satisfaction of dispute participants;

4) "cooling distance" (the asynchronous character of ODR creates a "cooling distance" to give time to the contestants to check their answers instead of reacting impulsively)[9];

5) asynchronous interactions;

6) preliminary communication reframing (in neurolinguistic programming, reframing is the means of change associated solely with combining the elements of experience, without adding anything from "outside" – reframing allows a different interpretation of the situation)[10];

---

7 Staff, A. (2014, July 17). How Taobao Is Crowdsourcing Justice in Online Shopping. *Alizila*. https://www.alizila.com/how-taobao-is-crowdsourcing-justice-in-online-shopping-disputes

8 Rule, C. (2010, November 1).*Using Technology to Manage High Volume Caseloads: The eBay/PayPal Experience*. https://www.archives.gov/files/ogis/events-presentations/acus-colin.pdf

9 Condlin, R. (2017). Online Dispute Resolution: Stinky, Repugnant, or Drab? *Faculty Scholarship*, 1576. https://digitalcommons.law.umaryland.edu/fac_pubs/1576

10 Lyubimov, A. (2022). *NLP model: reframing*. https://trenings.ru/entsiklopediya-nlp/modeli/959-model-nlp-refrejming.html

7) simultaneous conferencing;

8) archived messages;

9) automated procedures ("fourth party") (Wing et al., 2021).

As for the last point, it is worth citing the explanations of a Russian mediator M. A. Avdyev that "in online dispute resolution, the role of managing information flows is often played by not only arbitrators and mediators, but also computers and software. ICT participation of dispute settlement is called "the firth party", as ODR is viewed as an independent entry point into managing the conflict" (Avdyev, 2015). American authors Ethan Katsh and Janet Rifkin believe that the main advantage of ODR is introduction of technology into the process of dispute resolution as the "forth party" supporting "the third party" (arbitrator, mediator, expert, etc.) (Katsh & Rifkin, 2001).

It should be noted that the question of demarcating between the terms "online dispute settlement" (ODS) and "online dispute resolution" (ODR) was not posed in other countries (except PRC). As a rule, the term ODR is most often used for online dispute settlement systems on private e-commerce platforms (Wing et al., 2021). For example, C. Rule wrote that dispute resolution on e-commerce platforms Modria, eBay and PayPal takes place in the form of ODR[11]. One may also turn to a well-known 2018 work by the British lawyers J. Barnett and P. Treleaven "Algorithmic Dispute Resolution – the Automation of Professional Dispute Resolution Using AI and Blockchain Technologies", demarking online dispute resolution (ODR) into: a) consumer ODR; b) judicial ODR; and c) corporate ODR" (Barnett & Treleaven, 2017).

J. Tan from Montreal University highlighted that the "cooling distance" (the asynchronous character of ODR) reduces the efficiency of communication[12]. Thus, one may conclude that asynchronous written communication is considered to be an advantage of ODR technology by some experts (C. Rule, J. Barnett, P. Treleaven, etc.), while other authors (J. Tan) believe it to be a drawback (Iqbal et al., 2022).

A Chinese researcher Z. Juanjuan marked that the advantages of dispute resolution on private ODS platforms are: a) terms of dispute processing; and b) simple dispute resolution. One of the largest achievements of private ODS platforms is a channel of rapid dispute settlement (internal ODS mechanism of the e-commerce platform) (Juanjuan, 2018).

---

11 Rule, C. (2015). Modria – The Operating System for ODR. *MediatorAcademy*. https://www.judiciary.uk/wp-content/uploads/2015/02/colin_rule_modria_os_for_odr.pdf

12 Tan, J.(2022, July 19). The Future of ODR: Immersive technology enhancement and underlying technology evolution. *Laboratoire de cyberjustice*. https://www.cyberjustice.ca/2022/07/19/the-future-of-odr-immersive-technology-enhancement-and-underlying-technology-evolution

3.2. Terms of dispute processing and decision making on ODS platforms

The terms of dispute processing and decision making on various ODS platforms are:

1) with the intervention of the consumer support service or the public control system of Taobao ODS (Alibaba company) – seven days after making decision on intervening into the dispute;

2) in the China International Economic and Trade Arbitration Commission (CIETAC) under the accelerated procedure – 15 days after forming the Arbitration Court (Article 50 of the CIETAC Arbitration regulation)[13];

3) in the state court of the People's Republic of China under a summary procedure – three months (Article 161 of the Chinese Civil-procedural Code).

According to Chinese authors, the speed of dispute settlement is closely connected with the procedure complexity. Usually, the simpler the procedure, the less time it takes to solve the problem. If we compare three ODS mechanisms, the Taobao ODS procedure of Alibaba company is the simplest:

the first stage – consultations;

the second stage – intervention of the consumer support service or the public control system;

the third stage – submitting evidences;

the forth stage – making the final decision (Juanjuan, 2018).

ODR on the platform of any arbitration court in PRC is twice as complicated:

a) although the negotiation and mediation procedure is similar to that of Taobao ODS, it is more difficult for the parties to collect evidences because, as Alibaba is an e-commerce platform, all traces of transactions left can be taken directly as evidences in the ODS procedure. As the ODR platform of arbitration court is an independent third party, all evidences are not transferred automatically to the arbitration but must be collected by the parties and submitted to the platform;

b) the procedure of online arbitration is similar to that of offline arbitration, which is more complex than on the Taobao platform.

Arbitration procedure in China is as follows:

first, if there is an arbitration agreement, the claimant submits an application for online arbitration;

second, an online arbitration tribunal must be formed;

third, the defendant must submit an answer;

forth, the parties submit evidences;

fifth, the online arbitration tribunal makes a decision.

Finally, the online judicial procedure in a state court must comply with the civil-procedural legislation, which is generally more complex (Juanjuan, 2018).

---

[13] Online Arbitration Rules of CIETAC, art 50. Arbitration Law. https://arbitrationlaw.com/sites/default/files/free_pdfs/CIETAC Online Arbitration Rules.pdf

3.3. Possibility of introduction in the Russian Federation

Given the positive characteristics, the ODR system should be introduced in Russia, first of all, on private platforms of online commerce, such as Wildberries or Ozon. We share the opinion of C. Rule that the main reason of ODR popularity in many countries of the world is convenience (Rule, 2015). For the citizens living in remote regions, ODR may be a great advantage compared to physical attendance to court at a certain time. The second important advantage of ODR is low costs or free provision of such services. The third important factor is accessibility of ODR for all categories of citizens (those who cannot pay to a lawyer; those taking care of children or the elderly, etc.). The forth advantage is the speedy procedure of ODR.

4. Drawbacks in the functioning of Taobao ODS platform

Researchers like C. S. Shang, W. Guo, Z. Juanjuan, J. Tan, P. Fu, A. Nikitkov, D. Bay and others marked that the drawbacks of Taobao ODS mechanism are obvious (Shang & Guo, 2020; Juanjuan, 2018; Zheng, 2016; Fu et al., 2013). These are the same reasons why other means of dispute resolution are necessary, such as arbitration, mediation, etc. They are:

a) uncertainty of dispute settlement rules;

b) no legal force of Taobao ODS platform decisions[14];

c) limited methods of establishing facts on the platform;

d) the third party, which helps to settle the dispute, may be related to one or both parties and have its own interests in the case;

e) no mechanism of supervision and regulation of dispute resolution on the platform;

f) doubtful justness of dispute resolution on the Taobao ODS platform (Cheng, 2022);

g) finally, there is an ungrounded immunity of the platform itself from liability.

4.1. Non-independence of a third party in dispute resolution on a private ODR platform

Being a non-independent third party, the internal ODS mechanism of e-commerce platforms will never be able to substitute other external systems of dispute resolution. Considering the issue of independence and neutrality of the jury (arbitrators), Chinese authors state that the neutrality of arbitrators in ODR in arbitration and that of judges in ODS in a state court is much higher than that of a private ODS platform of Alibaba company. The internal ODS mechanism is provided by the e-commerce platform itself (Taobao Marketplace), the consumer support service consists of the platform employees,

[14] Tan, J. (2022, July 19). The Future of ODR: Immersive technology enhancement and underlying technology evolution. *Laboratoire de cyberjustice*. https://www.cyberjustice.ca/2022/07/19/the-future-of-odr-immersive-technology-enhancement-and-underlying-technology-evolution

and a reviewer of the public control service of the platform is also a buyer or seller of the platform. Inevitably, the said third party may have a more or less interest or relations with the platform, which may influence its neutrality.

On the contrary, in ODR in arbitration or ODS in a state court, a mediator, arbitrator, or judge are an independent and more neutral third party. Neutrality and independence influence the justness of the final decision of an arbitrator or a judge (Juanjuan, 2018).

In practice, in China (and other countries) there are many complaints about unjust servicing of the Taobao ODS platform clients. Even more serious is the problem of corruption in the sphere of customer services: from early disguised means, such as fake reputation of a company on the platform and removal of bad comments to direct violations, such as bribe-taking (Fu et al., 2013). Since 2012, Taobao Marketplace platform has closed many e-commerce stores and launched a judicial procedure in which the platform's consumer support service is suspected of bribery. In May 2012, after an internal anticorruption investigation, Alibaba company announced that it sued some of its employees working on the Taobao platform. As reported, the internal investigation showed that several Taobao platform employees helped some online sellers remove negative comments of the clients in order to increase the rankings of suppliers. For unlawful access to the website of comments, the employees obtained illegal payments from the sellers[15].

One of the reasons why the consumer support service could be easily involved into the bribery affair was the absence of any special qualification requirements to the employees of this service. On the contrary, Taobao platform created some requirements for the reviewers of the public control service: a buyer (or a seller) could apply for the position of a reviewer only if they are a Taobao platform participant and their term of registration is up to one year, and the Alipay system confirms the real identification (ID) of the reviewer. At the same time, the buyer (seller) was to comply with other preliminary requirements, such as no debts on the platform, a certain amount of deals on the platform, and observing the rules of the platform, etc., which, in the opinion of the platform employees, was to help the reviewer make more grounded decisions (Qin, 2017).

4.2. Bias of artificial intelligence technologies in ODR systems

Researchers C. S. Shang and W. Guo marked that another obstacle for a due legal procedure in using ODR technologies occurs because of the biases inherent in the algorithm-based solutions. Such biases undermine the use of algorithms by the Chinese judicial system and ODR system. These biases include result accuracy, "algorithm black

[15] Colwell, G. (2012, June 11). Monthly China Anticorruption Update Report– May 2012. *Squire Patton Boggs*. https://www.anticorruptionblog.com/china/monthly-china-anticorruption-update-report-may-2012/#:~:text=Monthly%20China%20Anticorruption,June%2011%2C%202012

boxes" of ODR codes and conflicts of interests in public-private partnerships when creating ODR systems (Shang & Guo, 2020). The general problem of ODR systems is that the results of algorithm-based decisions are not always accurate. Artificial intelligence and other types of well constructed algorithms may help people make decisions; however, the usefulness of these algorithms in more complex cases is not absolutely clear. Besides, the mechanisms of algorithm-based decision making have systemic errors, and coding mistakes and distortions may also lead to distorted results (Katsh & Rabinovich-Einy, 2018). The use of algorithms and data analysis may also make the ODR system less reliable, as the reasons for decisions made by these automated tools are subject to weak public control. The artificial intelligence systems which learn to recognize regularities in data to make decisions are often described as "black boxes", because even their developers may not know how they come to conclusions. As the algorithm running the ODR are secret and are only known to their owners and creators, the participants of such systems cannot know how the algorithms understand the correct result or whether the information used by the algorithms in decision making is accurate.

Other lawyers are of the same opinion. For example, an Australian researcher T. Ballesteros marked that the advantages of ODR must be weighed against the background of digital environment traps. Among the many safety factors, emerging as a result of online processes, ODR creates the risk of data leakage, lack of confidentiality and unsafe consumer protection. Due to these reasons, ODR can be successful in settling minor claims, but is not always suitable for more complex ones. Using technology-based ODR can be the most relevant means for settling disputes over minor claims, first of all, in B2C and C2C segments. However, more complex and individual cases, associated with B2B (business-to-business), and potentially collective suits, related to B2C disputes, the discretionary authorities of court will be still extremely relevant (Ballesteros, 2021).

4.3. Data safety

ODR relies on the data and online processes much stronger than traditional dispute resolution. This causes additional problems with data safety. The two issues of data safety and security, which are especially vivid in ODR, are:

1) information protection in private cases against the external parties striving to hack the system to get obtain this information ("external protection");

2) information protection in private cases against the undue disclosure or unlawful use by the persons managing the system ("internal protection").

External protection refers to the integrity of the platform or the system, when it is used to generate, send, receive, store, exchange or otherwise process information. In China, despite rapid pace of ODR development, actually not changes have occurred to provide safety of systemic data. Only limited scientific research focus on this sphere, as was marked by the Chinese authors (Shang & Guo, 2020).

The issue of data protection against internal unlawful use or undue disclosure of information was somewhat better studied. In the recent years, the Chinese government toughened regulation of cybersecurity, data safety and personal information protection. Since 2016, three important laws were adopted:

a) the PRC law on cybersacurity of 2016 (中华人民共和国网络安全法);

b) the PRC law on data safety of 2021 (中华人民共和国数据安全法;

c) the PRC law on personal information protection of 2021 (PIPL) (中华人民共和国个人信息保护法)[16].

It is worth highlighting that the Chinese system of regulating cybersecurity, data safety and personal information protection is still dynamically developing, and many issues of its implementation are to be clarified[17]. Today, many types of dispute prevention technologies developed by the Chinese ODR forums are based on broad collection, analysis and exchange of large amounts of consumer information and data, related to court proceedings; however, this generates hidden dangers associated with internal data safety (Simkova & Smutny, 2021).

Despite all the above mentioned drawbacks and taking into account the features of rapid, large scale and low cost transactions in B2C (business-to-consumer) and C2C (consumer-to-consumer) sectors, the internal ODS model on Taobao ODS e-commerce platforms is undoubtedly the most direct and effective means of online dispute resolution, as was stated by several researchers (Juanjuan, 2018; Simkova & Smutny, 2021; Liu, 2022).

4.4. Necessity of strict legislative regulation

Given the drawbacks of ODR procedures revealed during the functioning of the Taobao ODS platform, the ODR procedures must be strictly regulated. The Russian legislator should borrow the experience of the PRC, where such regulation is stipulated by the PRC Law on e-commerce of 2019. This law toughly stipulated that e-commerce platforms must disclose the channels of submitting claims, as well as other original information about transactions, to courts, arbitration and mediation bodies. The platforms also must timely accept and consider any claims. The platforms are subject to punishment for altering, destroying, falsifying or refusing to submit such information. These provisions were aimed at consumer rights protection.

[16] Sadovnikov, D. (2021, September 17). Review of the PRC law on personal information protection (Personal Information Protection Law of the People's Republic of China (PIPL)). *"Zakon" Publishing group*. https://zakon.ru/blog/2021/09/17/obzor_zakona_knr_o_zaschite_personalnoj_informaciipersonal_information_protection_law_of_the_peoples

[17] Si, J. et al. (2022, January 3). Overview of Chinese Cybersecurity, Data and Privacy Laws. *ZhongLun Law Firm*. https://www.zhonglun.com/Content/2022/03-01/1621106430.html

Conclusion

1. One may agree with the opinion of Chinese researchers that the internal ODS model on Taobao ODS e-commerce platforms is, undoubtedly, a direct, clear and effective means of online resolution of consumer disputes. However, being a non-independent third party, the internal ODS mechanism of e-commerce platforms will never be able to substitute other external systems of dispute resolution. ODS relies on the data and Internet processes much more than the traditional dispute resolution. Among the many safety factors emerging during online processes, ODS creates the risks of data leakage, lack of confidentiality and unsafe consumer protection.

2. Thus, the rapid growth of online dispute settlement on e-commerce platforms in Chine should be treated with caution. Online dispute settlement on the platforms has changed the traditional concepts of justice. The broad use of ODS technologies in creating Internet courts in China has changed the relations in courts between practicing lawyers and contestants, transformed judicial results, and ultimately changed the overall experience of justice. Chinese experts emphasized that the political incentives leading to the more rapid introduction of ODS technologies in courts will continue to stress the positive aspects of ODS, including accessibility, efficiency, predictability and prevention of disputes. However, ODS also causes serious concerns with regard to the traditional principles of justice, such as objectivity, confidentiality and data safety in dispute settlement.

3. Not only in China but in any country introducing ODS technologies into dispute resolution procedures should take important measures to ensure that the ODS processes are just, unbiased, and guarantee observance of procedural rights.

References

Avdyev, M. A. (2015). Dispute resolution services online: selected cases. *Modern Management Technology*, *8*(56), 2–8. https://www.elibrary.ru/ykrunf

Ballesteros, T. (2021). International Perspectives on Online Dispute Resolution in the E-Commerce Landscape. *International Journal of Online Dispute Resolution*, *8*(2), 85–101. https://doi.org/10.5553/ijodr/235250022021008002002

Barnett, J., & Treleaven, P. (2017). Algorithmic Dispute Resolution – The Automation of Professional Dispute Resolution Using AI and Blockchain Technologies. T*he Computer Journal*, *61*(3), 399–408. https://doi.org/10.1093/comjnl/bxx103

Cheng, Z. (2022). Antitrust Concerns Over Digital Self-regulation of Chinese E-Commerce Platform. *US-China L. Rev.*, *19*(3), 99–113. https://doi.org/10.17265/1548-6605/2022.03.001

Fu, P., Nikitkov, A., & Bay, D. (2013). Fraud on Taobao: an application of routine activity theory. *International Journal of Business Information Systems*, *14*(3), 305–321. https://doi.org/10.1504/ijbis.2013.056719

Iqbal, M. O., Obaid, A. J., Agarwal, P., Mufti, T., & Hassan, A. R. (2022). Blockchain Technology and Decentralized Applications Using Blockchain. In *ICT Infrastructure and Computing: Proceedings of ICT4SD 2022* (pp. 555–563). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-19-5331-6_57

Juanjuan, Z. (2018). On China Cross-Border Online Dispute Settlement Mechanism-Following UNCITRAL Tnodr and Alibaba Experience. *Victoria University of Wellington. Hors serie, 22*, 191–228. https://www.wgtn.ac.nz/__data/assets/pdf_file/0004/1642594/10-juanjuan.pdf

Katsh, E. E., & Rifkin, J. (2001). Online dispute resolution: *Resolving conflicts in cyberspace*. John Wiley & Sons, Inc.

Katsh, E., & Rabinovich-Einy, O. (2018, May 1). Facebook, Big Data, and the Privatization of Justice in the Digital Age. *Foundation for Law, Justice and Society*. https://www.fljs.org/facebook-big-data-and-privatization-justice-digital-age

Kutovaya, A. N., & Khadzhi, K. R. (2020). Online dispute resolution: international, domestic and private practices and further prospects for development. *International Trade and Trade Policy*, *4*(24), 95–112. https://doi.org/10.21686/2410-7395-2020-4-95-112

Liu, L., & Weingast, B. R. (2018). *Taobao, Federalism, and the Emergence of Law, Chinese Style*. Minnesota Law Review, 111. https://scholarship.law.umn.edu/mlr/111

Liu, L., & Weingast, B. R. (2020). *Law, Chinese Style: Solving the Authoritarian's Legal Dilemma through the Private Provision of Law*. Unpublished manuscript.

Liu, S. (2022). Book Review: Dispute Resolution in China: Litigation, Arbitration, Mediation, and their Interactions. *Social & Legal Studies*, *31*(5), 796–798. https://doi.org/10.1177/09646639221088529

Qin, P. (2017). Integration in Chinese e-commerce and public policy concerns: An analysis of Alibaba Group. *Thammasat Review of Economic And Social Policy*, *3*(1), 68–84. https://doi.org/10.13140/RG.2.2.16772.01921

Rule, C. (2015). Technology and the Future of Dispute Resolution. *Dispute Resolution Magazine*. https://law.scu.edu/wp-content/uploads/Rule-Technology-and-the-Future-of-Dispute-Resolution-copy.pdf

Rusakova, E. P. (2021). Integration of "smart" technologies in the civil proceedings of the People's Republic of China. *RUDN Journal of Law*, *25*(3), 622-633. https://doi.org/10.22363/2313-2337-2021-25-3-622-633

Shang, C. S., & Guo, W. (2020). The rise of online dispute resolution-led justice in China: An initial look. *ANU Journal of Law and Technology*, *1*(2), 25–42.

Shi, C., Sourdin, T., & Li, B. (2021). The Smart Court – A New Pathway to Justice in China? *International Journal for Court Administration*, *12*(1). https://doi.org/10.36745/ijca.367

Simkova, N., & Smutny, Z. (2021). Business E-NeGotiAtion: A Method Using a Genetic Algorithm for Online Dispute Resolution in B2B Relationships. *Journal of Theoretical and Applied Electronic Commerce Research*, *16*(5), 1186–1216. https://doi.org/10.3390/jtaer16050067

Wei, D., & Tian, Z. (2021). Comparison of Online Dispute Resolution Mechanisms in the European Union, the United States and China: Suggestions on Possible Future Work The United Nations Commission on International Trade Law (UNCITRAL). *Victoria University of Wellington. Hors serie, Dispute Resolution, Digital Economy and Contemporary Issues in Harmonisation of International Commercial Law*, XXVI, 78–110. https://www.wgtn.ac.nz/law/research/publications/about-nzacl/publications/special-issues/hors-serie-volume-xxvi-2021/04-dan-wei-and-zehua-tian-pdf

Wing, L., Martinez, J., Katsh, E., & Rule, C. (2021). Designing ethical online dispute resolution systems: The rise of the fourth party. *Negotiation Journal*, *37*(1), 49–64. https://doi.org/10.1111/nejo.12350

Zheng, J. (2016). The Role of ODR in Resolving Electronic Commerce Disputes in China. *International Journal of Online Dispute Resolution*, *3*(1), 41–48. https://doi.org/10.5553/ijodr/235250022016003001006

Author information

Elena P. Ermakova – Candidate of Sciences in Jurisprudence, Associate Professor, Department of Civil Law and Procedure and International Private Law, Peoples' Friendship University of Russia named after Patrice Lumumba
Address: 6 Mikluho-Maklaya Str., 117198 Moscow, Russian Federation
E-mail: ermakovaep@mail.ru
ORCID ID: https://orcid.org/0000-0001-5722-3641
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57194130098
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/record/S-4388-2017
Google Scholar ID: https://scholar.google.com/citations?user=1BUYJfUAAAAJ
RSCI Author ID: https://elibrary.ru/author_profile.asp?id=613926

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research was carried out with the financial support of the Russian President's grant No. NSh-3270.2022.2 "Evolution or evolution of the civil court procedure: digitalization through the prism of artificial intelligence".

Thematic rubrics

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

Article history

Date of receipt – January 23, 2023
Date of approval – April 23, 2023
Date of acceptance – August 15, 2023
Date of online placement – August 20, 2023

Научная статья
УДК 34:347.469:004
EDN: https://elibrary.ru/ozhvue
DOI: https://doi.org/10.21202/jdtl.2023.30

Особенности онлайн-урегулирования потребительских споров платформами электронной торговли в Китайской Народной Республике

Елена Петровна Ермакова

Российский университет дружбы народов имени Патриса Лумумбы
г. Москва, Российская Федерация

Ключевые слова

Taobao,
интернет-магазин,
онлайн-разрешение споров,
онлайн-урегулирование споров,
покупатель,
право,
продавец,
суд,
цифровые технологии,
электронная торговля

Аннотация

Цель: исследование особенностей онлайн-урегулирования споров платформами электронной торговли в Китайской Народной Республике, выявление положительных черт и недостатков технологий ODS, применяемых платформами.

Методы: эмпирические методы сравнения, описания, интерпретации; теоретические методы формальной и диалектической логики, а также частно-научные методы: юридико-догматический и метод толкования правовых норм.

Результаты: выявлено, что внутренняя модель ODS на платформах электронной торговли Taobao ODS является прямым, ясным и эффективным способом онлайн-разрешения потребительских споров. Однако, будучи не независимой «третьей стороной», внутренний механизм ODS платформ электронной торговли никогда не сможет заменить другие внешние системы разрешения споров. ODS полагается на данные и интернет-процессы гораздо больше, чем традиционное разрешение споров. Среди многих факторов безопасности, возникающих в результате онлайн-процессов, ODS создает риски утечки данных, отсутствия конфиденциальности и небезопасной защиты потребителей. ODS также вызывает серьезную озабоченность в связи с традиционными принципами правосудия, такими как принципы беспристрастности, конфиденциальности и безопасности данных в процессе урегулирования споров. Не только Китайской Народной Республике, но и любой стране мира, внедряющей технологии ODS в процедуры разрешения споров, необходимо предпринять важные шаги для обеспечения того, чтобы процессы ODS были справедливыми, непредвзятыми и гарантировали процессуальные права.

Научная новизна: состоит в комплексном исследовании онлайн-урегулирования споров платформами электронной торговли в Китайской Народной Республике, практика применения которых имеет свою специфику, вытекающую из модели саморегулирования указанных отношений, закрепленной впоследствии нормативными правовыми актами Китайской Народной Республики и отражающейся в деятельности частных платформ ODS.

Практическая значимость: обусловлена отсутствием в настоящее время возможности применения к отношениям, использующим технологии ODS на частных платформах правовых норм и правил, учитывающих их специфику. Основные положения и выводы исследования могут быть использованы для совершенствования механизмов правового регулирования технологий ODS в процессуальном законодательстве Российской Федерации.

Для цитирования

Ермакова, Е. П. (2023). Особенности онлайн-урегулирования потребительских споров платформами электронной торговли в Китайской Народной Республике. *Journal of Digital Technologies and Law*, *1*(3), 691–711. https://doi.org/10.21202/jdtl.2023.30

Список литературы

Авдыев, М. А. (2015). Сервисы разрешения споров онлайн: избранные кейсы. *Современные технологии управления*, *8*(56), 2–8. https://www.elibrary.ru/ykrunf

Кутовая, А. Н., Хаджи, К. Р. (2020). Онлайн-урегулирование споров: международные, страновые и частные практики и дальнейшие перспективы. *Международная торговля и торговая политика*, *4*(24), 95–112. EDN: https://www.elibrary.ru/zlwqtk. DOI: https://doi.org/10.21686/2410-7395-2020-4-95-112

Русакова, Е. П. (2021). Интегрирование «смарт» технологий в гражданское судопроизводство КНР. *Вестник Российского университета дружбы народов. Серия: Юридические науки*, *25*(3), 622–633. https://doi.org/10.22363/2313-2337-2021-25-3-622-633

Ballesteros, T. (2021). International Perspectives on Online Dispute Resolution in the E-Commerce Landscape. *International Journal of Online Dispute Resolution*, *8*(2), 85–101. https://doi.org/10.5553/ijodr/235200022021008002002

Barnett, J., & Treleaven, P. (2017). Algorithmic Dispute Resolution – The Automation of Professional Dispute Resolution Using AI and Blockchain Technologies. *The Computer Journal*, *61*(3), 399–408. https://doi.org/10.1093/comjnl/bxx103

Cheng, Z. (2022). Antitrust Concerns Over Digital Self-regulation of Chinese E-Commerce Platform. *US-China L. Rev.*, *19*(3), 99–113. https://doi.org/10.17265/1548-6605/2022.03.001

Fu, P., Nikitkov, A., & Bay, D. (2013). Fraud on Taobao: an application of routine activity theory. *International Journal of Business Information Systems*, *14*(3), 305–321. https://doi.org/10.1504/ijbis.2013.056719

Iqbal, M. O., Obaid, A. J., Agarwal, P., Mufti, T., & Hassan, A. R. (2022). Blockchain Technology and Decentralized Applications Using Blockchain. In *ICT Infrastructure and Computing: Proceedings of ICT4SD 2022* (pp. 555–563). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-19-5331-6_57

Juanjuan, Z. (2018). On China Cross-Border Online Dispute Settlement Mechanism-Following UNCITRAL Tnodr and Alibaba Experience. *Victoria University of Wellington. Hors serie*, *22*, 191–228. https://www.wgtn.ac.nz/__data/assets/pdf_file/0004/1642594/10-juanjuan.pdf

Katsh, E. E., & Rifkin, J. (2001). *Online dispute resolution: Resolving conflicts in cyberspace*. John Wiley & Sons, Inc.

Katsh, E., & Rabinovich-Einy, O. (2018, May 1). Facebook, Big Data, and the Privatization of Justice in the Digital Age. *Foundation for Law, Justice and Society*. https://www.fljs.org/facebook-big-data-and-privatization-justice-digital-age

Liu, L., & Weingast, B. R. (2018). *Taobao, Federalism, and the Emergence of Law, Chinese Style*. Minnesota Law Review, 111. https://scholarship.law.umn.edu/mlr/111

Liu, L., & Weingast, B. R. (2020). *Law, Chinese Style: Solving the Authoritarian's Legal Dilemma Through the Private Provision of Law*. Unpublished manuscript.

Liu, S. (2022). Book Review: Dispute Resolution in China: Litigation, Arbitration, Mediation, and their Interactions. *Social & Legal Studies*, *31*(5), 796–798. https://doi.org/10.1177/09646639221088529

Qin, P. (2017). Integration in Chinese e-commerce and public policy concerns: An analysis of Alibaba Group. *Thammasat Review Of Economic And Social Policy*, *3*(1), 68–84. https://doi.org/10.13140/RG.2.2.16772.01921

Rule, C. (2015). Technology and the Future of Dispute Resolution. *Dispute Resolution Magazine*. https://law.scu.edu/wp-content/uploads/Rule-Technology-and-the-Future-of-Dispute-Resolution-copy.pdf

Shang, C. S., & Guo, W. (2020). The rise of online dispute resolution-led justice in China: An initial look. *ANU Journal of Law and Technology*, *1*(2), 25–42.

Shi, C., Sourdin, T., & Li, B. (2021). The Smart Court – A New Pathway to Justice in China? *International Journal for Court Administration*, *12*(1). https://doi.org/10.36745/ijca.367

Simkova, N., & Smutny, Z. (2021). Business E-NeGotiAtion: A Method Using a Genetic Algorithm for Online Dispute Resolution in B2B Relationships. *Journal of Theoretical and Applied Electronic Commerce Research*, *16*(5), 1186–1216. https://doi.org/10.3390/jtaer16050067

Wei, D., & Tian, Z. (2021). Comparison of Online Dispute Resolution Mechanisms in the European Union, the United States and China: Suggestions on Possible Future Work The United Nations Commission on International Trade Law (UNCITRAL). *Victoria University of Wellington. Hors serie, Dispute Resolution, Digital Economy and Contemporary Issues in Harmonisation of International Commercial Law*, XXVI, 78–110. https://www.wgtn.ac.nz/law/research/publications/about-nzacl/publications/special-issues/hors-serie-volume-xxvi-2021/04-dan-wei-and-zehua-tian-pdf

Wing, L., Martinez, J., Katsh, E., & Rule, C. (2021). Designing ethical online dispute resolution systems: The rise of the fourth party. *Negotiation Journal*, *37*(1), 49–64. https://doi.org/10.1111/nejo.12350

Zheng, J. (2016). The Role of ODR in Resolving Electronic Commerce Disputes in China. *International Journal of Online Dispute Resolution*, *3*(1), 41–48. https://doi.org/10.5553/ijodr/235250022016003001006

Сведения об авторе

Ермакова Елена Петровна – кандидат юридических наук, доцент, доцент кафедры гражданского права и процесса и международного частного права, Российский университет дружбы народов имени Патриса Лумумбы
Адрес: 117198, Российская Федерация, г. Москва, ул. Миклухо-Маклая, 6
E-mail: ermakovaep@mail.ru
ORCID ID: https://orcid.org/0000-0001-5722-3641
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57194130098
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/record/S-4388-2017
Google Scholar ID: https://scholar.google.com/citations?user=1BUYJfUAAAAJ
РИНЦ Author ID: https://elibrary.ru/author_profile.asp?id=613926

Конфликт интересов

Автор заявляет об отсутствии конфликта интересов.

Финансирование

Исследование выполнено при финансовой поддержке Гранта Президента РФ № НШ-3270.2022.2 «Эволюция или революция гражданского судопроизводства: цифровизация через призму искусственного интеллекта».

Тематические рубрики:

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.23.65 / Ответственность в предпринимательском праве. Споры в предпринимательской деятельности и порядок их разрешения
Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 23 января 2023 г.
Дата одобрения после рецензирования – 23 апреля 2023 г.
Дата принятия к опубликованию – 15 августа 2023 г.
Дата онлайн-размещения – 20 августа 2023 г.

Research article
DOI: https://doi.org/10.21202/jdtl.2023.31

Human Interpreters in Virtual Courts: A Review of Technology-Enabled Remote Settings in Australia

Yi Ran

University of New South Wales
Sydney, Australia

Keywords

Court,
court interpreting,
digital technologies,
interpreter in court,
law,
linguistic equity,
procedural justice,
videoconferencing,
virtual courtroom,
virtual hearings

Abstract

Objective: This interdisciplinary review intends to inform legal scholars, practitioners, and users of language interpretation services in the judiciary of challenges encountered by professional interpreters in virtual hearings and remote settings.

Methods: Situated at the intersection of law, language, and communication, this review analyses the latest discourses about technology-enabled remote settings and synthesises insights into recommended practices in effective legal communication mediated by interpreters in virtual courts.

Results: With an overarching aim to improve effective collaboration between interpreting service providers and users in multilingual legal communication for procedural equity and access to justice, this review establishes three central claims: (1) the technology-enabled virtual hearings is accelerated by the covid-19 pandemic, (2) the need for effective legal communication mediated by the use of interpreters in remote settings is mounting, and (3) successful collaboration between the service user and provider can achieve a win-win outcome.

Scientific novelty: A review of existing studies in law and language reveals three main gaps: (1) procedural justice in videoconferencing hearings and remote technologies, (2) equity and access for people with limited

proficiency in the official language of the court system, and (3) effective legal communication mediated by human interpreters in virtual courts. This review bridges the existing gaps in knowledge.

Practical significance: it touches on three aspects of the law-language nexus: (1) Covid-19 accelerated adoption of the virtual courtroom technologies in Australia and its impact on court interpreting, (2) challenges for interpreters in remote settings, and (3) achieving linguistic accuracy and intercultural appropriateness when preserving the manner in which the content is expressed as intended or implied by the original speaker. Grounded in courtroom interpreting practices, it highlights the importance of effective collaboration in successful multilingual legal communication rooted in mutual purpose, shared expectations, and interprofessional understanding.

For citation

Ran, Yi. (2023). Human Interpreters in Virtual Courts: A Review of Technology-Enabled Remote Settings in Australia. *Journal of Digital Technologies and Law, 1*(3), 712–724. https://doi.org/10.21202/jdtl.2023.31

Contents

Introduction

Much has been written and researched about monolingual legal communication in face-to-face settings. Little has been explored about interlingual and intercultural legal communication in technology-enabled virtual hearings and remote settings. A review of existing studies in law and language reveals three main gaps: (1) procedural justice in videoconferencing hearings and remote technologies, (2) equity and access for people with limited proficiency in the official language of the court system, and (3) effective legal communication mediated by human interpreters in virtual courts. This review bridges the existing gaps in knowledge. Situated at the intersection of law, language, and communication, this review analyses the latest discourses about technology-enabled remote settings and synthesises insights into recommended practices in effective legal

communication mediated by interpreters in virtual courts. This interdisciplinary review intends to inform legal scholars, practitioners, and users of language interpretation services in the judiciary of challenges encountered by professional interpreters in virtual hearings and remote settings. With an overarching aim to improve effective collaboration between interpreting service providers and users in multilingual legal communication for procedural equity and access to justice, this review establishes three central claims: (1) the technology-enabled virtual hearings is accelerated by the covid-19 pandemic, (2) the need for effective legal communication mediated by the use of interpreters in remote settings is mounting, and (3) successful collaboration between the service user and provider can achieve a win-win outcome. This review adopts the following structure: (1) Covid-19 accelerated adoption of the virtual courtroom technologies in Australia and its impact on court interpreting, (2) challenges for interpreters in remote settings, and (3) achieving linguistic accuracy and intercultural appropriateness when preserving the manner in which the content is expressed as intended or implied by the original speaker. Grounded in courtroom interpreting practices, it highlights the importance of effective collaboration in successful multilingual legal communication rooted in mutual purpose, shared expectations, and interprofessional understanding.

1. An Overview of Interpreters in Court

Court interpreting is a language service provided by a certified interpreter who is trained to interpret between English and community languages other than English, both spoken and signed languages. The provision of adequate language interpretation services provided by competent court interpreters is important to ensure that justice is carried out fairly for litigants, defendants, and other parties in court. Court interpreters are obliged by the professional code of ethics and conduct to interpret accurately to the best of their ability. Professional court interpreters are trained specialists who possess a near-native mastery of English and other language(s), acquire broad general knowledge, and perform under different modes of interpreting: consecutive interpreting, simultaneous or whisper interpreting, and sight translation in court. Court interpreters serve as a critical link to ensure equitable access and accessibility to court proceedings, particularly for new arrival migrants, asylum-seeking minorities, Indigenous and tribal people(s), victim-survivors, minors, vulnerable and mobile populations with limited English proficiency or those who are deaf or hard-of-hearing.

2. The Importance of Interpreters: An Australian Case

In Australia's multilingual and multicultural society, with over half of its population born overseas and more than 300 languages spoken at home, there has been applaudable progress made in certification and professionalisation. These efforts are evident from four trends: (1) the growing membership of the professional association Australian Institute

of Interpreters and Translators (AUSIT), (2) the introduction of the specialised certification for court interpreters, (3) the advocacy of JCDI in fostering effective collaboration rooted in mutual purpose, shared expectations, and interprofessional understanding, and (4) the increased recognition from the judiciary on the importance of interpreters, as reflected by Justice Robert-Smiths (Robert-Smiths, 2009) and Hon. Justice Perry and Zornada[1].

3. The Development of Technology-Enabled Virtual Courtrooms

The collaboration has extended from face-to-face to virtual courtrooms, marked by the increasing adoption of audiovisual link and videoconferencing technologies in court. Endeavours have been made from both sides of the aisle, evidenced by three clear achievements: (1) the court's technical note on working with interpreters, (2) the professional association's guidelines for remote interpreting practice and recommended national standards for working with interpreters in court and tribunals, and (3) the provision of additional resources for court interpreters, including briefing materials, glossary templates, and FAQs available on government home affairs[2], community legal centres[3], Law Access[4], and other community legal service websites.

However, despite the progress made, three emerging issues require urgent attention: (1) the impact of the covid-19 accelerated adoption of the virtual courtroom and remote interpreting option on how court interpreters are used and expected, (2) ethical dilemmas encountered by interpreters in remote settings, and (3) linguistic accuracy and intercultural appropriateness in preserving the same force and effect of the language used by lawyers in court, so that the power dynamics can be faithfully reproduced in another language for a fair outcome.

To put these concerns into perspective, a review of investments made in financial resources, technical expertise, time and energy, supported by sources of legislation and practical considerations, is necessary. In financial terms, millions of dollars have been allocated to the implementation of litigation technologies, such as audiovisual technologies, videoconference technologies, and electric file lodgment, before

1 "The principles of fairness and equality before the law are fundamental to a democratic society, and their observance is essential to the maintenance of public confidence in the judiciary". See Perry, J. M., & Zornada, K (2015, March 13–14). *Working with Interpreters: Judicial Perspectives.* Federal Court of Australia. https://www.fedcourt.gov.au/digital-law-library/judges-speeches/justice-perry/perry-j-20150313

2 Australian Government Department of Home Affairs. Translation and Interpreting Service. https://www.tisnational.gov.au

3 https://www.clcnsw.org.au

4 https://www.legalaid.nsw.gov.au

the covid-19 pandemic[5]. The use of these litigation technologies is informed by the Evidence Acts[6] and announced by Australian states and territories[7]. For practical considerations, audiovisual technologies and videoconferencing hearings are mainly intended for interstate proceedings that involve affected children witnesses and other special interest groups in remote locations. The use of these remote technologies is further endorsed by the Federal Court of Australia, exhibited in the 2016 Technology and the Court Practice Note (GPN-TECH), which includes a guide to the preparation and conduct of digital or hybrid hearings across Australian court jurisdictions[8].

During the covid-19 lockdown, the adoption of technology-enabled hearings and remote interpreting options has been accelerated. However, the evaluations of virtual court experiences are rather mixed, with contested voices either appreciating or critiquing such experiences expressed by legal scholars, judicial officers, and professional societies. For example, members of the judicial sector perceived the transition to digital technology-enabled court proceedings as a 'forced innovation' during the early days of the covid-19 pandemic[9]. Such a view is further justified by legal scholars (Legg & Song, 2021) cautioning against the use of audio-visual links and its implications for vulnerable witnesses, witnesses based in foreign jurisdictions, prisoners in correctional facilities, and ancillary service providers, such as interpreters and experts. As a matter of fact, scholars who held cautionary views have highlighted the need to stay vigilant for the possibility of a loss of fairness and legitimacy due to the nature of court proceedings altered by the medium of the trial[10]. Similar concerns over the vulnerability of remote technologies also have been expressed by McIntyre, Olijnyk, and Pender (McIntyre et al., 2020), citing a number of challenges in decision-making, such as the issue of presence and zoom fatigue[11].

---

5 Smith, R., Savage, R., & Emami, C. (2021). Benchmarking the Use of Audiovisual Link Technologies. *Australian Government Institute of Criminology*. https://www.aic.gov.au/publications/rr/rr23

6 Evidence Act 1929 SA, Evidence Act 1939, Evidence Act QLD 1977, Evidence, Audio and Audio Visual Links Act NSW 1998, Evidence, Audio and Audio Visual Links Ac TAS 1999.

7 Parliament of Australia, Factsheet 20 – The Australian System of Government. https://www.aph.gov.au/About_Parliament/House_of_Representatives/Powers_practice_and_procedure/00_-_Infosheets/Infosheet_20_-_The_Australian_system_of_government

8 Allsop, J. L. B. (2016). Technology and the Court Practice Note (GPN-TECH). *Federal Court of Australia*. https://www.fedcourt.gov.au/law-and-practice/practice-documents/practice-notes/gpn-tech

9 Australia's courts keep the justice system going during coronavirus pandemic. (2020, 9 May). *SBS News*. https://www.sbs.com.au/news/article/australias-courts-keep-the-justice-system-going-during-coronavirus-pandemic/meo0niykf

10 Legg, M., & Song, A. (2021). The courts, the remote hearing and the pandemic: from action to reflection. *UNSW Law Journal*, *44*(1), 126–166. https://www.unswlawjournal.unsw.edu.au/wp-content/uploads/2021/04/04-Legg-Song.pdf

11 Courts and COVID-19: Challenges and Opportunities in Australia. (2020). *Australian Public Law*. https://www.auspublaw.org/blog/2020/05/courts-and-covid-19-challenges-and-opportunities-in-australia

However, in spite of these concerning voices, virtual access to NSW courts has been favoured as a more flexible option for people to access the justice system. To exemplify this favourable position, NSW Attorney General Mark Speakman has marked that more than $43 million had been invested in expanding audio-visual technologies and facilities for domestic and family violence victims in more than 17 courtrooms[12]. This positive view on virtual legal access substantiated by financial and logistic investments is further supported by the overall positive feedback on virtual access to the justice system. A notable survey study conducted by the Law Society conducted in 2021 has revealed that more than 90 per cent of respondents favoured the online proceedings when compared with the face-to-face mode because these virtual proceedings allowed greater flexibility for online direction hearings and other appearances, not to mention other conveniences brought by the remote option for justice, including the hours of commuting have been saved for both legal professionals and applicants.

4. Ensuring Rights in Virtual Courtrooms: Challenges and Collaboration

With several scholars supporting that the remote option for justice is here to stay, it seems reasonable to understand the impact of interpreter-mediated remote justice on the multilingual population with limited proficiency in the official language of the court system. This commentary highlights three key approaches to the issue of interpreter-mediated interactions in remote settings: (1) human rights, (2) procedural justice, and (3) linguistic equity. Three central questions are noted here: (1) the right to a fair representation, as reflected by normative documents at international (Article 14, UNICCPR 1966), supranational (EU Directive 2010/64), and local (Evidence Act 1995 NSW) levels, (2) the right to the free assistance of an interpreter, as reflected by the Section 32, Human Rights Act 2019 QLD, and (3) the right to use one's own language, particularly for Indigenous people, as reflected by the United Nations Declaration of the Rights of Indigenous Peoples (UNDRIP)[13] and the International Labour Organisation (ILO) Convention Concerning Indigenous and Tribal Peoples in Independent Countries[14].

However, regardless of the recognition of the importance of language right and the right to an interpreter in court, little has been known about the linguistic challenges encountered by interpreters in remote settings, while mostly about technical and administrative challenges of remote interpreting to immigration tribunals (Grieshofer, 2022), police,

12 Stonehouse, G. (2022, June 17). Survey finds virtual NSW courts favourable. *The West Australian*. https://thewest.com.au/news/crime/survey-finds-virtual-nsw-courts-favourable-c-7196555

13 *United Nations Declaration on the Rights of Indigenous Peoples*. https://www.un.org/development/desa/indigenouspeoples/wp-content/uploads/sites/19/2018/11/UNDRIP_E_web.pdf

14 International Labour Organization. Indigenous and Tribal Peoples Convention, 1989 (No. 169). https://www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:12100:0::NO::P12100_ILO_CODE:C169

and other legal scenarios (Braun, 2020). Anecdotal accounts from interpreters working in remote settings suggest that interpreters encounter ethical dilemmas when interpreting service users have little to no previous experience working with interpreters in remote settings. The lack of practical experience in collaboration with interpreters may lead to expectations that may go beyond the interpreters' professional duties and capabilities. For example, it would be technically challenging and ethically tricky for sworn interpreters to join the same videoconferencing hearing from different devices using multiple accounts in order to channel the off-record side conversations between a private client and their lawyer. It is ethically problematic because professional interpreters are bound by the professional code of ethics[15] to faithfully interpret everything that has been said in the exact same manner as the original speaker.

This accuracy principle mandates interpreters to render both the content and the linguistic manner in which the content is expressed. In reality, the attainment of linguistic equivalence in the manner is very complex. The complexity is resulted from three main reasons: (1) the use of manner by the original speaker is nuanced, as represented by what is intended and implied by the original speaker through linguistic devices (Gallai, 2022), such as questioning techniques, discourse markers, tone and intonation, and gaze, and gesture; (2) the manner-related features can be decoded differently by different people, due to subject knowledge, socio-economic and educational backgrounds, psychological traits, individual and group cultural identity, and institutional norms and expectations in country of origin (Yi, 2023a, 2023b); and (3) they are difficult to interpret into an equivalent form with a matching force and effect in another language, given the issue of translatability (Lee, 2011) and difficulties in achieving linguistic equivalence (Liu, 2020) and intercultural appropriateness (Yi, 2022).

To address these challenges mentioned above, two-way communication is key to successful collaboration in multilingual legal communication. The two-way approach is characterised by two responses from both the interpreting service provider and the service user. These responses are: (1) for interpreters, understanding the expectations from the judicial users and (2) for judicial users, getting to know what makes the manner difficult to translate in remote settings. For interpreters, a useful reference to understand the judicial perspective on expectations for interlingual accuracy and intercultural appropriateness is the General Practice Note, "Working with Interpreters (GPN-INTERP)", released by the Federal Court of Australia on 24 March 2023[16]. The Note highlights two specific considerations in achieving accuracy expected by the judicial sector: (1) the meaning of interpreting "accurately" and (2) the importance of transferring both the content and the intent of the communication without omission or distortion, as shown below. "resulting in the optimal and complete transfer of the meaning from the other language

[15] AUSIT Code of Ethics and Code of Conduct. (2012, November). https://ausit.org/wp-content/uploads/2020/02/Code_Of_Ethics_Full.pdf

[16] Allsop, J. L. B. (2023, 24 March). *Working with Interpreters (GPN-INTERP)*. https://www.fedcourt.gov.au/law-and-practice/practice-documents/practice-notes/gpn-interpret

into English and from English into the other language, preserving the content and intent of the communication made in the other language or in English (as the case may be) without omission or distortion and including matters which the interpreter may consider inappropriate or offensive".

The judicial expectations on accuracy can be dissected into three elements: (1) interpreting everything that has been said in court, including emotionally charged expressions and languages, including curses and hated speech, (2) reproducing what is said and how it is said in court, including the content, manner (through use of fillers, hedges, self-repairs, tone, and intonation), intent (in explicit and implicit form), and (3) applying professional discernment in retaining the optimal and complete transfer to the best of their knowledge and ability. However, in practice, translating the manner intended or implied by the original speaker into the equivalent form with matching force and effect in another language is challenging. There are three main reasons for such difficulties: (1) the specificities concerning the indexicalities of these manner-related features, or in other words, manner-related features mean different things to different people, socio-cultural groups, and language communities; (2) they seem less visible, compared with a whole chunk of content-intensive speech marked by legal arguments, facts, and sources of law in courtroom examinations; and (3) they seem to be less substantive to the case.

In order to establish counter-claims, it is important to provide a working definition of the manner-related features in accordance with their functions and significance in courtroom examinations. In court interpreting studies, the literature on the Manner of Speech is scarce. Instead of affording a rigid linguistic definition, the applicability of which is yet to be tested in actual courtroom practices, the preferred approach here is to propose a working definition that is consistent with the occurrences of such features in practice. The Manner of Speech refers to the way in which the speaker expresses the content in a certain context to a specific audience. It can include a person's linguistic choice and use of discursive devices, such as markers and style features indicating the degree of clarity through fillers and hedges, the distinctness of characteristic style (e.g. politeness, register, and vulgar languages), and the individual manner of expressing (e.g. repetitions and self-repairs). It can also encompass the use of paralinguistic communication, such as tone of voice and intonation.

The Manner of Speech carries important pragmatic functions in intercultural/interlingual communication in the courtroom. The way in which a person speaks can directly influence the meaning given to the message or perceived by the receiver. For example, existing studies (Kerr-Thompson, 2002; Hildebrand-Edgar & Ehrlich, 2017) have shed light on how speech style features can influence the perception of assertiveness and power dynamics in face-to-face courtroom examinations. In remote settings, the perception of speech style features is further complicated by the use of technology. For instance, studies have pointed out that a lack of non-verbal communication cues and simulated eye contact restricted by camera angle, screen size, audio/video definition, and the quality of network connection could make it easier to misinterpret the intention and implications of the speaker through the use of manner-related features in virtual hearings.

Conclusions

Considering the significance of reproducing the manner-related features in remote settings, future studies are needed to facilitate successful multilingual communication in virtual courtrooms. In summary, this short commentary intends to provide legal scholars, practitioners, and users of language interpretation services in the judiciary with an up-to-date review of challenges encountered by interpreters in technology-enabled virtual hearings and remote interpreting settings. The right to a fair representation through a competent and ethical professional interpreter for court participants with limited proficiency in the official language of the justice system is not only a basic human right but also an integral part of procedural justice and linguistic equity in court. The commentary intends to raise awareness of the meaning and importance of the Manner of Speech in technology-enabled courtroom interactions mediated by interpreters.

References

Braun, S. (2020). "You are just a disembodied voice really": Perceptions of video remote interpreting by legal interpreters and police officers. In H. Salaets, & G. Brone (Eds.), *Linking up with video: Perspectives on Interpreting Practice and Research*. Amsterdam: Benjamins. https://doi.org/10.1075/btl.149.03bra

Gallai, F. (2022). *Relevance Theory in Translation and Interpreting: A Cognitive-Pragmatic Approach* (1st ed.). Routledge. https://doi.org/10.4324/9781003183969

Grieshofer, T. (2022). Remote Interpreting in Immigration Tribunals. *International Journal for the Semiotics of Law-Revue internationale de Sémiotique juridique*, *36*, 767–788. https://doi.org/10.1007/s11196-022-09908-3

Hildebrand-Edgar, N., & Ehrlich, S. (2017). She was quite capable of asserting herself": Powerful Speech Styles and Assessments of Credibility in a Sexual Assault Trial. *Linguagem e Direito* [*Language and Law*], *4*(2), 89–107.

Kerr-Thompson, J. (2002). "Powerful/Powerless" language in court: A critical re-evaluation of the Duke Language and Law Programme. *International Journal of Speech, Language and the Law*, *9*(2), 153–167.

Lee, J. (2011). Translatability of Speech Style in Court Interpreting. International J*ournal of Speech Language and the Law*, *18*(1), 1–33. https://doi.org/10.1558/ijsll.v18i1.1

Legg, M., & Song, A. (2021). The courts, the remote hearing and the pandemic: From action to reflection. *UNSW Law Journal*, *44*(1), 126–166. https://doi.org/10.53637/ZATE4122

Liu, X. (2020). Pragmalinguistic challenges for trainee interpreters in achieving accuracy: An analysis of questions and their interpretation in five cross-examinations. *Interpreting*, *22*(1), 87–116. https://doi.org/10.1075/intp.00035.liu

McIntyre, J., Olijnyk, A., & Pender, K. (2020). Civil courts and COVID-19: Challenges and opportunities in Australia. *Alternative Law Journal*, *45*(3), 195–201. https://doi.org/10.1177/1037969X20956787

Roberts-Smith, L. (2009). Forensic Interpreting: Trial and Error. https://doi.org/10.1075/btl.87.03rob

Yi, R. (2022). Does Style Matter in Remote Interpreting: A Survey Study of Professional Court Interpreters in Australia. *International Journal of Translation and Interpretation Studies*, *2*(1), 48–59. https://doi.org/10.32996/ijtis.2022.2.1.7

Yi, R. (2023a). The promise of linguistic equity for migrants in Australian courtrooms: a cross-disciplinary perspective, Australian Journal of Human Rights, 29(1), 174-180. https://doi.org/10.1080/1323238X.2023.2232171

Yi, R. (2023b). The Routledge Handbook of Public Service Interpreting. By Gavioli, Laura and Wadensjö, Cecilia, London, UK: Routledge. *Public Integrity*. https://doi.org/10.1080/10999922.2023.2206236

Author information

Ran Yi – PhD, Researcher, School of Humanities and Languages, The University of New South Wales
Address: High Street, Kensington, NSW 2052, Sydney, Australia
E-mail: ran.yi@unsw.edu.au
ORCID ID: https://orcid.org/0000-0003-0630-8623
Google Scholar ID: https://scholar.google.com/citations?user=InIjgmwAAAAJ
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/record/HPH-4932-2023

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

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

Article history

Date of receipt – June 12, 2023
Date of approval – June 27, 2023
Date of acceptance – August 15, 2023
Date of online placement – August 20, 2023

Научная статья
УДК 34:347.973:004:81`2:81`25
EDN: https://elibrary.ru/pqiafk
DOI: https://doi.org/10.21202/jdtl.2023.31

Люди-переводчики в виртуальных судах: обзор дистанционных технологических решений в Австралии

Йи Рэн

Университет штата Новый Южный Уэльс
г. Сидней, Австралийский Союз

Ключевые слова

Видеоконференции,
виртуальные слушания,
виртуальный зал суда,
нормы процессуального права,
перевод в суде,
переводчик в суде,
право,
суд,
цифровые технологии,
языковое равенство

Аннотация

Цель: данный междисциплинарный обзор ставит своей целью информирование правоведов, практиков и пользователей услуг лингвистического перевода в судебной системе о проблемах профессионального перевода на виртуальных слушаниях и в дистанционных режимах.

Методы: исследование проведено на стыке права, лингвистики и теории коммуникации и анализирует новейшие подходы к использованию технологий в дистанционном формате. Результаты работы синтезируются в форме практических рекомендаций для эффективной коммуникации в юридической сфере, осуществляемой при посредстве переводчиков в виртуальных судах.

Результаты: преследуя глобальную цель – повышение эффективности сотрудничества между поставщиками и пользователями переводческих услуг в процессе многоязычного общения в юридической сфере для достижения процессуального равноправия и равного доступа к правосудию, данное исследование позволяет сделать следующие основные выводы: (1) переход к использованию виртуальных слушаний с применением технологий значительно ускорился благодаря пандемии COVID-19, (2) растет потребность в эффективной коммуникации в юридической сфере, осуществляемой при посредстве переводчиков в дистанционном формате, и (3) успешное сотрудничество между пользователями и поставщиками услуг может привести к обоюдной выгоде.

Научная новизна: обзор исследований в области права и лингвистики выявил три основные проблемы: (1) соблюдение норм процессуального права во время слушаний в формате видеоконференций и при использовании дистанционных технологий, (2) реализация принципов равноправия и доступности правосудия для лиц с ограниченным владением официальным языком судебной системы

и (3) осуществление эффективной коммуникации в юридической сфере при посредстве людей-переводчиков в виртуальных судах. Представленная работа восполняет пробелы в изучении данных вопросов.

Практическая значимость: статья затрагивает три аспекта системы взаимоотношений между правом и языком: (1) пандемия COVID-19 ускорила внедрение технологий виртуальных залов судов в Австралии и повлияла на переводческую деятельность в судах, (2) переводчики испытывают трудности при дистанционной работе, (3) необходимо добиваться лингвистической точности и межкультурной адекватности при сохранении стиля передачи содержания, заложенного автором оригинального сообщения. Исследование опирается на практику судебного перевода и подчеркивает важность эффективного сотрудничества в процессе успешной многоязычной коммуникации в юридической сфере на основе общих целей, ожиданий и понимания между профессионалами.

Для цитирования

Рэн, Йи. (2023). Люди-переводчики в виртуальных судах: обзор дистанционных технологических решений в Австралии. *Journal of Digital Technologies and Law*, *1*(3), 712–724. https://doi.org/10.21202/jdtl.2023.31

Список литературы

Braun, S. (2020). “You are just a disembodied voice really”: Perceptions of video remote interpreting by legal interpreters and police officers. In H. Salaets, & G. Brone (Eds.), *Linking up with video: Perspectives on Interpreting Practice and Research*. Amsterdam: Benjamins. https://doi.org/10.1075/btl.149.03bra

Gallai, F. (2022). *Relevance Theory in Translation and Interpreting: A Cognitive-Pragmatic Approach* (1st ed.). Routledge. https://doi.org/10.4324/9781003183969

Grieshofer, T. (2022). Remote Interpreting in Immigration Tribunals. *International Journal for the Semiotics of Law-Revue internationale de Sémiotique juridique*, *36*, 767–788. https://doi.org/10.1007/s11196-022-09908-3

Hildebrand-Edgar, N., & Ehrlich, S. (2017). She was quite capable of asserting herself”: Powerful Speech Styles and Assessments of Credibility in a Sexual Assault Trial. *Linguagem e Direito* [*Language and Law*], *4*(2), 89–107.

Kerr-Thompson, J. (2002). “Powerful/Powerless” language in court: A critical re-evaluation of the Duke Language and Law Programme. *International Journal of Speech, Language and the Law*, *9*(2), 153–167.

Lee, J. (2011). Translatability of Speech Style in Court Interpreting. International J*ournal of Speech Language and the Law*, *18*(1), 1–33. https://doi.org/10.1558/ijsll.v18i1.1

Legg, M., & Song, A. (2021). The courts, the remote hearing and the pandemic: From action to reflection. *UNSW Law Journal*, *44*(1), 126–166. https://doi.org/10.53637/ZATE4122

Liu, X. (2020). Pragmalinguistic challenges for trainee interpreters in achieving accuracy: An analysis of questions and their interpretation in five cross-examinations. *Interpreting*, *22*(1), 87–116. https://doi.org/10.1075/intp.00035.liu

McIntyre, J., Olijnyk, A., & Pender, K. (2020). Civil courts and COVID-19: Challenges and opportunities in Australia. *Alternative Law Journal*, *45*(3), 195–201. https://doi.org/10.1177/1037969X20956787

Roberts-Smith, L. (2009). Forensic Interpreting: Trial and Error. https://doi.org/10.1075/btl.87.03rob

Yi, R. (2022). Does Style Matter in Remote Interpreting: A Survey Study of Professional Court Interpreters in Australia. *International Journal of Translation and Interpretation Studies*, *2*(1), 48–59. https://doi.org/10.32996/ijtis.2022.2.1.7

Yi, R. (2023a). The promise of linguistic equity for migrants in Australian courtrooms: a cross-disciplinary perspective, Australian Journal of Human Rights, 29(1), 174-180. https://doi.org/10.1080/1323238X.2023.2232171

Yi, R. (2023b). The Routledge Handbook of Public Service Interpreting. By Gavioli, Laura and Wadensjö, Cecilia, London, UK: Routledge. *Public Integrity*. https://doi.org/10.1080/10999922.2023.2206236

Информация об авторе

Рэн Йи – доктор наук, научный сотрудник, Школа гуманитарных наук и языков, Университет штата Новый Южный Уэльс
Адрес: Австралийский Союз, г. Сидней, Хай Стрит, Кенсингтон, NSW 2052
E-mail: ran.yi@unsw.edu.au
ORCID ID: https://orcid.org/0000-0003-0630-8623
Google Scholar ID: https://scholar.google.com/citations?user=InIjgmwAAAAJ
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/record/HPH-4932-2023

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: 10.31.41 / Процессуальные акты и действия
Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 12 июня 2023 г.
Дата одобрения после рецензирования – 27 июня 2023 г.
Дата принятия к опубликованию – 15 августа 2023 г.
Дата онлайн-размещения – 20 августа 2023 г.

Research article
DOI: https://doi.org/10.21202/jdtl.2023.32

International and Russian Legal Regulation of the Turnover of Crypto-assets: Conceptual-Terminological Correlation

Iaroslav K. Iarutin ✉

Diplomatic Academy of the Ministry of Foreign Affairs of the Russian Federation
Moscow, Russian Federation

Elena E. Gulyaeva

Diplomatic Academy of the Ministry of Foreign Affairs of the Russian Federation
Moscow, Russian Federation

Keywords

Cryptoasset,
cryptocurrency,
digital currency,
digital technologies,
international law,
law,
legislation,
stablecoin,
token,
virtual asset

Abstract

Objective: to assess the Russian legislation for its compliance with the international-legal approaches to shaping symmetrical regulation of crypto-assets and possibility to complement it with new international-legal categories reflecting the in-depth changes in the global economy and structure of international finance, determined by the broad introduction of new financial technologies based on distributed ledger technologies.

Methods: the methodological basis of the research is a set of general scientific methods of scientific cognition, among which of utmost importance are special-legal (formal-legal and comparative-legal) methods, complemented with risk-oriented approach, legal modeling and juridical forecasting. Applied integrally, they allowed comprehending the architecture, "letter and "spirit" of the modern international financial law and national legislation in their conceptual-terminological correlation and to forecast further development and adjustment of the legal regulation of crypto-assets turnover.

✉ Corresponding author

Results: it was found that there appears a stable trend in the crypto-assets turnover regulation, according to which "soft" law dominates among the law sources (this is especially notable in the sphere of international financial law compared, for example, with conventions or international treaties); at the same time, there is a strengthening trend of "fragmentation" of international law with regard to crypto-assets turnover; the authors mark inconsistency of the conceptual framework contained in international acts and in the Russian legislation, as well as the gaps in the regime of crypto-assets turnover at the level of national law; the trends and forecasts are presented referring to the development of international-legal regulation of the sphere of crypto-assets.

Scientific novelty: consists, first of all, in a complex comparison, based on, among other aspects, the fundamentally new concepts of regulation of such progressive international-legal categories as cryptoasset, virtual asset, cryptocurrency, stablecoin, etc., some of them rarely used in the Russian legal discourse and actually never applied in legislation.

Practical significance: the scientifically grounded proposals are formulated, aimed at improving the conceptual-terminological framework of the Russian legislation in the sphere of crypto-assets turnover, implementation of which will allow constructing a common legal space with the technologically most advanced states, will help to improve investment climate and financial attraction of the state; will improve the national-legal regime of crypto-assets turnover from the viewpoint of not only actual market demands, but also state security interests and improving competitiveness of the Russian legislation.

For citation

Iarutin, Ia. K., Gulyaeva, E. E. (2023). International and Russian Legal Regulation of the Turnover of Crypto-assets: Conceptual-Terminological Correlation. *Journal of Digital Technologies and Law, 1*(3), 725–751. https://doi.org/10.21202/jdtl.2023.32

Contents

Introduction

According to the World Economic Forum, 10 per cent of the world's GDP will be saved through blockchain technology by 2025[1]. This said, according to the Financial Stability Board, in early 2022, the capitalization of the crypto-assets' market was $2.6 trillion[2]. In-depth changes in the structure of international finance, determined by the broad introduction of distributed ledger technologies, require that the global community build a symmetrical international-legal regulation, comprehensible for the market participants and national regulators. Besides, satisfying the interests of states, such regulation must not excessively hinder the development of financial technologies and new sectors of the global economy.

On the other hand, stemming solely from the current condition of the architecture of the norms of international financial law, one should ascertain the utmost importance of the national law. It is national law that stipulates the practical requirements having priority significance for the market participants.

At the same time, crypto-assets, apparently, are used beyond state boundaries. For this reason, despite the current international situation, the global community and developed countries are interested in cooperation (at least, in the sphere under study), aimed at regulating this environment. In this sense, the Russian Federation seems highly interested in an in-depth comprehension of not only "letter" bit also "spirit" of international-legal regulation. The above factors determine the need to conceptualize the Russian legislation and its evaluation for the compliance with the international-legal approaches. Given the "fragmentation of international law, it is especially important to synchronize financial regulation not only with the interests of state security but also with the imperatives of our time and actual needs of the market. We believe that building of legal regulation at the national level will require practice-oriented proposals in terms of complementing the Russian law with advanced international-legal categories (cryptoasset, virtual asset, cryptocurrency, stablecoin).

1. International-legal regulation of crypto-assets

1.1. Features of international financial law

Globalization of economy and formation of a common global economic system, assumingly, changes also the patterns in those fields of international law which are aimed at regulating economic relations. This enhances the trends of "fragmentation" and "denationalization" of the respective fields of international law (Mazhorina, 2018).

---

1 Schwab, Klaus. The Fourth Industrial Revolution. Moscow, Eksmo. 2016.

2 FSB (2022). *Assessment of Risks to Financial Stability from Crypto-assets*. FSB, Basel. https://www.fsb.org/wp-content/uploads/P160222.pdf

Besides, the currently dominating source in the international; financial law is the "soft" law acts (Kudryashov, 2013a, 2013b, 2013c, 2014; Ní Aoláin, 2021; Borlini, 2020; Brummer, 2010). This is probably due to the fact that the procedure of "soft" law acts adoption allows their coordination in short timeframes (compared, for example, with conventions or international treaties). In a certain sense, the rapid development of financial technologies did not leave any choice for the humanity: either regulation is adopted quickly (after a concern of an international community emerges), or new economic sectors function beyond an international-legal field, which may ultimately directly influence the efficiency of the whole international law architecture.

This approach has its disadvantages, however. As was mentioned above, the international-legal regulation formed by the "soft" law acts is, as a rule, of narrowly specialized character. Thus, the main problem is the fact that the legal regulation being formed is not comprehensive; it is limited to certain practical fields. Moreover, with the "soft" law acts the international community points out to the states to some general directions of law-making; these directions are of recommendation character. The actual content of these international-legal norms, which are supposed to provide guidelines for the market participants, is determined by the states.

Nevertheless, one should also account for the fact that the international-legal regulation may change radically, as authoritative researchers propose fundamentally new concepts of regulation, including the concept of "decentralized regulation" (Nabilou, 2019).

1.2. Notion of crypto-assets in the international law

Although the notion of "cryptoassets" is very rarely used in the Russian legal discourse, including academic one, and is actually absent in law, its use seems most correct from the viewpoint of international-legal research. This is due to the fact that this notion is used not only by international market participants, but also by the leaders of G20 states (for example, cryptography issues were reflected in a number of clauses of G20 Bali Leaders' Declaration as of November 16, 2022[3]).

According to a definition formulated by the Financial Stability Board, crypto-assets are a digital representation of value, based on cryptography and distributed ledger technology (DLT), similar technologies, and which can be in both payment and investment goals[4] (Droll & Minto, 2022). Financial Stability Board emphasized that this definition does not

[3] *G20 Bali Leaders' Declaration*. (2022, 16 November). G20, Bali. https://www.g20.org/content/dam/gtwenty/gtwenty_new/document/G20 Bali Leaders' Declaration.pdf

[4] FSB. (2020). Final Report and High-Level Recommendations on Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements. FSB, Basel. https://www.fsb.org/wp-content/uploads/P131020-3.pdf

comprise a digital representation of fiat currencies[5]. Apparently, this comment was made in order to demarcate crypto-assets and central bank digital currencies (CBDC), which are now actively developed by some states (Tsang & Chen, 2022; Keister & Sanches, 2023; Zellweger-Gutknecht et al., 2021). Also, Financial Stability Board implicitly indicated: although central bank digital currencies are not crypto-assets (Pomulev, 2021), the notion of crypto-assets includes cryptocurrencies, which are also digital currencies[6] (Geva, 2019).

Guided by prudential goals, the Bank for International Settlements (BIS) decided to devide between crypto-assets into groups with various risk levels, thus distinguishing tokenized traditional assets, crypto-assets with stabilization mechanism, i. e. stablecoins, and other crypto-assets, including, for example, the most well-known cryptocurrency Bitcoin[7]. Thus, an international-legal approach was elaborated, in compliance with which regulators and international financial institutions making transactions with crypto-assets are recommended to apply the following risk levels:

– for tokenized forms of traditional assets – at least, the risk level characteristic for the traditional (basic) asset;

– for stablecoins – the risk level based on the evaluation of the stabilization mechanism quality;

– for other crypto-assets without a stabilization mechanism – a fixed risk coefficient of 1250 %[8].

It is worth mentioning that international regulators pay special attention to stablecoins (Ferreira, 2021), as they carry a threat to the global financial system (Khisamova, 2020). First, criteria for evaluating the stabilization mechanism quality are actively elaborated today at international level[9]. Second, turning to the provision on the level of risks inherent to stablecoins, one may notice the following: it is recommended to consider the possibility of the risk level increasing beyond the risks associated with the stabilization mechanism (with further consideration for capital add-ons). Combined with the global nature of stablecoins, such concerns of the global community allows assuming that in the next few years it is the issues of stablecoins that will determine the need to form

5 *Ibid*.

6 Frankenfield, J. (2023, April 20). Digital Currency Types, Characteristics, Pros & Cons, Future Uses. *Investopedia*. https://www.investopedia.com/terms/d/digital-currency.asp

7 BCBS. (2021). *Consultative Document: Prudential treatment of cryptoasset exposures*. BCBS, Basel. https://www.bis.org/bcbs/publ/d519.pdf ; BCBS. (2022). *Consultative Document: Second consultation on the prudential treatment of cryptoasset exposures*. BCBS, Basel. https://www.bis.org/bcbs/publ/d533.pdf

8 BCBS. (2021). *Consultative Document: Prudential treatment of cryptoasset exposures*. BCBS, Basel. https://www.bis.org/bcbs/publ/d519.pdf

9 BCBS. (2022). *Consultative Document: Second consultation on the prudential treatment of cryptoasset exposures*. BCBS, Basel. https://www.bis.org/bcbs/publ/d533.pdf

a new – in a certain sense supranational – regulator, whose zone of responsibility will include the reduction of the global risks to financial stability (initially – solely in terms of stablecoins)[10].

On the other hand, as was stated in the G20 Finance Ministers and Central Bank Governors Meeting Communiqué as of June 9, 2019, the key concern of the global community lies not in the plane of ensuring financial stability, but in the issues of due combating money laundering[11].

It must be stated that the conceptual framework formed by the Financial Action Task Force (FATF) for these purposes is of cardinally different character.

FATF specifies the notion of a "virtual asset" (VA) and a derivate notion of a virtual asset service provider (VASP) (Schmidt, 2021). Thus, a virtual asset represents value in a digital form, which can be used both for payment and investment purposes. According to FATF legal position, virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations. FATF notices that all of the funds or value-based terms in the FATF Recommendations (e. g., "property," "proceeds," "funds," "funds or other assets," and other "corresponding value") include VAs[12].

Readers might be confused by a striking similarity of the notion "virtual asset", formulated by FATF, and the notion "digital asset", formulated by the Bank for International Settlements. The meaning and connotation of these notions, in the authors' opinion, differ: although cryptocurrencies (referring to digital currencies) are included into the "virtual asset" notion, FATF explicitly states that not all digital currencies – meaning central banks digital currencies – are subject to international standards in the sphere of virtual assets[13]. Thus, the word "digital", as estimated by the authors, in FATF interpretation has a connotation of "more reliable", "regulated", "controlled by the state", and in relation to assets proper (not "currencies") – "emitted by a large traditional business". Within a holistic consideration of the financial-technological landscape, this difference should be taken into account, we believe.

---

10 Iarutin, Ia. K. (2023, March 13). *The Impact of Crypto-Assets on Governments and the International Community: A Forecast for 2035*. https://russiancouncil.ru/en/blogs/iaroslav-iarutin/the-impact-of-cryptoassets-on-governments-and-the-international-commun/?ysclid=ll689ieit3661964369

11 *G20 Finance Ministers and Central Bank Governors Meeting Communiqué* (2019, June 9). G20, Fukuoka. https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/pdf/documents/en/communique.pdf

12 FATF. (2021). *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. FATF, Paris. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html

13 *Ibid.*

From the practical viewpoint, it is the virtual asset service provider (VASP) that carries practical requirements in terms of combating money laundering, funding terrorism, funding mass weapons proliferation (further – AML/CFT); persons registered as VASP or recognized as such rank on a par with other "obliged persons" (for example, banks, stock exchanges, funds). According to a FATF definition, VASP is a physical or legal person, executing entrepreneurial activity having signs of, at least, one of the following types of activity:

– participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

– safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and

– transfer of virtual assets;

– exchange between one or more forms of virtual assets;

– exchange between virtual assets and fiat currencies;

– virtual asset service provider means any natural or legal person who is not covered elsewhere under the FATF Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person.

As FATF emphasizes that the anchor notion of a "virtual asset", specific for the international-legal mechanism of AML/CFT, "does not include the digital representation of fiat currencies, securities and other financial assets, which had been regulated by FATF Recommendations before"[14], then for the purposes of AML/CFT the notion of "cryptoassets" appears fragmented: different rules are applied to virtual asset, i. e. cryptocurrencies, certain non-fungible tokens (NFT), tokens issued during initial coin offering (ICO), and other categories of crypto-assets, namely, tokenized forms of traditional assets and the most part of NFT[15]. This said, such division may be applied exclusively for legal norms in the sphere of AML/CFT; the so called virtual assets have no conceptual unity, as their purposes of use, frequency of transactions and market structure are fundamentally different. From the users' viewpoint, as a rule, cryptocurrencies are used for payment purposes, while tokens issues during ICO – for investment purposes (Blemus & Guégan, 2020), and NFT, which may be recognized as a virtual asset only in some cases, – for hedonistic and, probably, investment purposes.

Nevertheless, isolation of the "virtual asset" notion from the general landscape of crypto-assets has a broad practical significance. Specifically, in compliance with international-legal

[14] FATF. (2021). *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. FATF, Paris. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html

[15] However, it is important to note that such division is only relevant for the international-legal AML/CFT mechanism. In practice, including in the context of financial markets regulation, the "utility token" category is isolated more often. Besides, according to a number of researchers, at the level of EU law (in particular, MiCa provisions) there is a trend towards an extensive interpretation of this category; this, probably, presages elaboration of a more detailed demarcation and classification of NFT (Tomczak, 2022).

recommendations, it is necessary to implement preventive measures with regard to operations associated with virtual assets, at the minimal threshold level of US$ 1,000 (Salami & Iwa, 2021; Kinsburskaya, 2020) (given the "soft law" nature, it is acceptable to set a lower threshold at the national level)[16]. At the same time, FATF emphasizes that in relation to the types of property previously regulated by Recommendations (tokenized forms of traditional assets) the legal regime in the aspect of AML/CFT may remain unchanged, that is, the minimal threshold level is US$ 15,000[17]. In other words, the regulator estimates the risk of money laundering, inherent in tokenized forms of traditional assets, at the same level as the traditional (basic) asset – unlike the Bank for International Settlements, which adopted a different approach.

Thus, one should state that "fragmentation" of international law exists. We believe this to be inacceptable: a consequence of such "fragmentation" is misunderstanding experienced by national regulators, market participants and legislators.

2. Reflection of the international legal norms in the legal system of the Russian Federation

2.1. Issues of conceptual-terminological correlation in international acts and legislation of the Russian Federation

As is known, the current version of the Russian legislation regulates the turnover of "digital financial assets" and "digital currencies". Assumingly, the "digital financial asset" notion, defines as "digital rights, including monetary claims, the possibility to implement rights on emission securities, the rights to participate in the capital of a nonpublic joint stock company, the right to claim transition of emission securities, which are stipulated by a decision on emitting the digital financial assets in the order established by this Federal Law "On digital financial assets, digital currency and making changes in certain legislative acts of the Russian Federation" No. 259-FZ of July 31, 2020, while their issuance, accounting and circulation are only possible by making (changing) records in an information system based on distributed ledger, as well as in other information systems"[18].

The legislators and the financial regulator must have planned that this notion would correlate with the "digital asset" notion, formulated by the Financial Stability Board. At the international-legal level, digital assets are a digital representation of value, which can

16 *Ibid*.

17 FATF. (2012–2022). *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*. https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf

18 On digital financial assets, digital currency and making changes in certain legislative acts of the Russian Federation. Federal Law of July 31, 2020 No. 259-FZ: (ed. as of January 11, 2023). *Collection of legislation of the Russian Federation*. 2020. No. 31. Article 5018.

be used both for payment and investment goals[19]; according to the Financial Stability Board, digital assets include crypto-assets. Probably, it was planned that the Russian digital financial assets would be crypto-assets? By the idea of a Russian legislator, digital financial assets would be issued by large Russian and international companies, and the process of issuance and expanse of such assets would entirely comply with the high requirements of the Bank of Russia. Apparently, mentioning of the "distributed ledger" in the Russian definition refers us to the international-legal notion of "cryptoassets". However, it is worth noting that, in the absence of a widely spread practice of digital financial assets issuance, the Russian law may be interpreted ambivalently. On the one hand, one may assume that the reference to "other information systems" may indicate the possibility to issue "centralized" digital financial assets, which would definitely not be crypto-assets. On the other hand, an analogous structure of a norm, i. e. reference not only to DLT but other technologies as well, is present in the international-legal definition of "cryptoassets".

If we assume that the Russian legislator was guided by the approaches stated by the Financial Stability Board, then all digital financial assets are crypto-assets. However, in any case the notion of "digital financial assets" does not comprise cryptocurrencies, stablecoins, NFT, tokens issued at ICO. Thus, the Russian definition of "digital financial assets" does not fully coincide with the notion of "cryptoassets", but includes only the regulated part of such assets, controlled by the state and large business.

Such inconsistency is logically complemented by the fact that, according to some researchers, the Russian interpretation of "distributed ledger" is somewhat different from the one accepted within international standards, namely, ISO 22739:2020[20] (Vergeles, 2022).

Returning to definitions, even more questions arise about using the adjective "digital" for the notion of "digital currency" in the same law. According to the Russian definition, digital currency is a "set of electronic data (digital code or representation), contained in the information system, which are offered and/or can be accepted as a means of payment, being not a unit of currency of the Russian Federation, a unit of currency of a foreign state and/or an international unit of currency or unit of accounting, and/or as a means of investment and in relation to which there is no person obliged to each owner of such electronic data, except for an operator and/or nodes of the information system, obliged only to provide that the order of issuance of these electronic data and making (changing) records about them into the said information system complies with its rules"[21]. In other words, in Russia digital currency is interpreted as solely non-state "currency" – moreover,

---

19 FSB. (2020). *Final Report and High-Level Recommendations on Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements*. FSB, Basel. https://www.fsb.org/wp-content/uploads/P131020-3.pdf

20 *Blockchain and distributed ledger technologies – Vocabulary*. https://www.iso.org/standard/73771.html

21 *Ibid*.

such "currency" is also not developed by large business (the requirements of the Central Bank of the Russian Federation for its development are not observed).

In this case, the adjective "digital" is used incorrectly for two reasons. First, it does not take into account the international-legal category of "central bank digital currency", which, being a digital one, is a legal means of payment (for example, a digital ruble currently designed). At the same time, according to the Basel Committee on Banking Supervision[22], central bank digital currency – unlike digital currencies in the interpretation of a Russian legislation – are a direct obligation of a central bank; the latter is the due "obliged person". Second, in the international business community the notion of digital currency is used as an umbrella term for virtual currencies, cryptocurrencies, and CBDC[23].

Actually, as was mentioned above, at the international level there exists the notion of virtual currency (Brown-Hruska & Wagener, 2018), which entirely complies with the meaning implied by a Russian legislation in the notion of digital currency. Specifically, by the FATF typology, virtual currency is a digital representation of value; it can be digitally traded. According to FATF, virtual currency has the functions of money (as a means of exchange, storage, and payment), but is not a legal means of payment in any jurisdiction[24].

Although today FATF uses an umbrella term "virtual asset" (the international regulator has currently withdrawn from using the "virtual currency" notion) (Kinsburskaya, 2019; Rozhdestvenskaya, 2022; Rozhdestvenskaya & Guznov, 2020), we believe that the connotation of the word "digital", with which this term is used in the Russian law, does not fully comply with the norms of international law, as, actually, the law refers only to crypto-assets and virtual currencies, not digital currencies in general. We believe this discrepancy confuses the international community interested in the Russian market and diminishes the informal prestige of our state.

It is worth noting that the notion of "stablecoin", to which international regulators pay special attention, as was mentioned above, is currently factually not represented in the Russian law. Although there is an opinion in the practical sphere, that stablecoin lacks an "obliged person", providing the functioning of stabilization mechanism, we believe this position to be inconsistent. According to the Basel Committee on Banking Supervision, central bank digital currencies were called a direct obligation of a central bank. In the absence of such explanations about other types of digital currencies, one may conclude that only a state (territory) may emit digital money with legal guarantees, that is, be a duly obliged

22 BIS. (2020). *Central bank digital currencies: foundational principles and core features*. BIS, Basel. https://www.bis.org/publ/othp33.pdf

23 Frankenfield, J. (2023, April 20). *Digital Currency Types, Characteristics, Pros & Cons, Future Uses*. https://www.investopedia.com/terms/d/digital-currency.asp

24 FATF. (2014). *FATF Report on Virtual Currencies Key Definitions and Potential AML/CFT Risks*. FATF, Paris. https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

person. Thus, stablecoins are included into the notion of "digital currency", developed by the Russian law. At the same time, one has to state that – given the special attention paid by international regulators to the problem of stablecoins – this notion must be represented at the level of national law, including with the prospective development of macroprudential policies as the international legal norms in this sphere are inevitably developing.

Thus, the conceptual framework formulated in the current version of the Russian legislation does not fully comply with the international-legal recommendations; assumingly, the insufficient attention of legislators to the international-legal issues significantly complicates the legal regime of crypto-assets, making the Russian regulation murky for international business community. All this diminishes the competitive advantages of the Russian jurisdiction for the crypto business and interested financial structures.

2.2. Legal regulation of the crypto-assets turnover in the Russian Federation

If one turns to the essence of the international-legal position of the Russian Federation, it is essential to point out the lawful character of operations with crypto-assets, but with certain restrictions – both directly stipulated in law and existing exclusively at the practical level.

As for the prudential component, the Central Bank of the Russian Federation has not yet formulated the position regarding the level of risks inherent in digital financial assets[25]. It is obvious, however, that the turnover of digital financial assets will entirely remain within the Russian legal field, although with certain restrictions. For example, transactions with some digital financial assets are currently available exclusively for qualified investors[26]. At the same time, in regard to digital currencies (as interpreted by a Russian legislator), the position of a financial regulator is cardinally different. For example, according to Information Letter by the Central Bank of the Russian Federation "On certain types of financial instruments" of July 19, 2021 No. IN-06-59/52, trade organizers were recommended to refuse Russian and foreign emitters access to organized securities trading, if the rights of their owner to receive payments and/or the size of payments for them (size of income) or profitability of them depend on the rates of digital currencies[27].

---

25 Central Bank urged to regulate the assessment of risks of banks investing into digital financial assets. *Interfax*. https://www.interfax.ru/business/878897

26 On the signs of digital financial assets, which may only be purchased by a qualified investor, on the signs of digital financial assets, the purchase of which by a person not being a qualified investor can be performed only within the limits, stipulated by the Bank of Russia, of the monetary funds transferred for their payment, and the total value of other digital financial assets transferred in consideration, on the said amount of monetary funds and the total value of digital financial assets: Instruction of the Bank of Russia of November 25, 2020 No. 5635-U (registered in the Russian Ministry of Justice on 21.12.2020 N 61622).

27 Information Letter by the Central Bank of the Russian Federation "On certain types of financial instruments" of July 19, 2021 No. IN-06-59/52. https://cbr.ru/StaticHtml/File/117596/20210719_in_06_59-52.pdf

From the viewpoint of combating money laundering, one should also mark the differences in legal regulation of digital financial assets and digital currencies. According to Article 6 of the Federal Law of August 7, 2001 No. 115-FZ "On combating legalization (laundering) of illegal incomes and terrorism funding", operations with digital financial assets are subject to obligatory control if their size exceeds 1 million rubles[28]. In our opinion, this measure complies with the international-legal recommendations, stating that the legal regime regarding traditional assets in tokenized form (for example, securities) does not carry any special character[29]. On the other hand, all operations with digital currency (as interpreted by a Russian legislator) are, in the opinion of the Bank of Russia, a priori suspicious, which is directly stated in the Classifier of features indicating an unusual character of an operation or transaction, appended to the Policy Directive of the Bank of Russia of March 2, 2012 No. 375-P "On requirements to the rules of internal control of a credit organization with a view of combating legalization (laundering) of illegal incomes and terrorism funding"[30]. Moreover, it should be noted that at the level of a lawyer's practice it is perceived that the frequency of "freezing" and blocking of bank accounts when executing transactions with digital currencies (and broader – with all virtual assets) based on the Federal Law of August 7, 2001 No. 115-FZ "On combating legalization (laundering) of illegal incomes and terrorism funding"[31] has increased sharply since the end of spring 2022[32]. In other words, the state is trying hard to restrict the turnover of digital currencies, but is doing it without introducing the relevant changes in law[33].

It should be highlighted also, that there are currently a number of restrictions regarding to the turnover of digital currency (in the Russian interpretation of the term). Specifically, according to Article 14 of the Federal Law of July 31, 2020 No. 259-FZ "On digital financial assets, digital currency and making changes in certain legislative acts of the Russian

---

28 On combating legalization (laundering) of illegal incomes and terrorism funding: Federal Law of August 7, 2001 No. 115-FZ: (ed. as of January 9, 2023). (2001). *Collection of legislation of the Russian Federation*. *33*, part 1. Article 3418.

29 FATF. (2012–2022). *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*. FATF. https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf

30 On requirements to the rules of internal control of a credit organization with a view of combating legalization (laundering) of illegal incomes and terrorism funding: Policy Directive of the Bank of Russia of March 2, 2012 No. 375-P. (2012, April 18). *Vestnik Banka Rossii*, *20*.

31 On combating legalization (laundering) of illegal incomes and terrorism funding: Federal Law of August 7, 2001 No. 115-FZ: (ed. as of January 9, 2023). (2001, August 13). *Collection of legislation of the Russian Federation*, *33* (part I), Article 3418.

32 Iarutin, Ia. K. *Digital currency and the future of global policy*. https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/tsifrovaya-valyuta-i-budushchee-mirovoy-politiki/

33 *Ibid*.

Federation"[34], Russian organizations and physical persons – Russian residents – are prohibited to accept digital currency as a consideration for the goods and services transferred by them or to them. Although this thesis regarding digital currency was formulated for the first time at the law level, analysis of judicial practice shows that previously courts also negatively treated the use of digital currencies in contract obligations (Sereda, 2017). Besides, in compliance with the same Article, judicial protection for the above subjects is stipulated only in case of informing the Federal Taxation Service (further – FTS RF) about the existence of digital currency and execution of transactions with it. At the same time, it should be stated that in practice this issue turns on the absence of explanations of FTS RF, including the absence of a form for such reports. In this regard, it is apparent that only general obligations on informing a taxation body are currently detailed (for example, within the 3-NDFL form).

Besides, it is important to note a certain distinction, related to combating the illegal use of insider information and market manipulation – Countering Insider Dealing. By implication of Federal Law of July 27, 2010 No. 224-FZ "On combating the illegal use of insider information and market manipulation…"[35], it seems highly improbable to apply the Russian law on Countering Insider Dealing to organizations involved into circulation of digital currencies (as interpreted by the Russian law); assumingly, similar provisions will be applied in relation to the turnover of digital financial assets, although it is not explicitly stipulated by law (as follows from the regulated character of the organizations involved). We believe that the need to regulate the cardinally new types of property in this aspect will aggravate the numerous problems characteristic for the current mechanism of Countering Insider Dealing, including in its criminal-legal component (Lifshits & Yani, 2020; Arestova & Borbat, 2022; Ruchkina, 2019, 2022). On the other hand, applicability of the respective norms to the legal relations under study causes no doubts from the viewpoint of foreign (American) law as well (Verstein, 2019), which, assumingly, serves as an additional argument for inadmissibility of the above said distinction, made at the level of the Russian legislation and with the logic inherent in it.

Thus, the Russian legislation – in terms of conceptual framework, first of all – does not fully comply with the norms of international law. The built system of legal regulation has a number of drawbacks and inaccuracies. It appears that this situation – given the architecture of the international-legal norms under study – diminishes the authority of our country and its informal prestige; the unique interpretation of the norms

[34] Federal Law of July 31, 2020 No. 259-FZ "On digital financial assets, digital currency and making changes in certain legislative acts of the Russian Federation". (2020, August 3). *Collection of legislation of the Russian Federation*, *31* (part I), Article 501.

[35] On combating the illegal use of insider information and market manipulation and on making changes in certain legislative acts of the Russian Federation: Federal Law of July 27, 2010 No. 224-FZ: (ed. as of October 7, 2022). (2010). *Collection of legislation of the Russian Federation*, *31*. Article 4193.

of international financial law, stipulated in the Russian law, is unclear to the international business community. Despite the nature of the above norms of international law (mainly contained in the acts of "soft law"), that is, despite their recommendation character, the Russian Federation is extremely interested in their introduction. First, the international community offers certain common standards, introduction of which allows the state to exist in a common legal environment with the most technologically advanced states (speaking of a rather narrow sphere of crypto-assets); beyond any doubt, this promotes the investment attraction of the state, raises eh informal prestige of its leaders. At the same time – in the absence of introducing the legal approaches formulate in the "soft law" provisions – it is probable that the state ignoring them will face the methods known as "naming and shaming" (Fogelson, 2013a, 2013b). Second, given the high level of expertise of international regulators, one has to admit the usefulness of the formed international-legal approaches from the viewpoint of smoothing the structural problems of the global character, at the level of the Russian law.

3. Proposals on improving the Russian legislation

First of all, it seems important to bring the conceptual framework, formed at the level of the Russian law, in compliance with international standards. The notion of the "digital financial asset" should be substituted with the international-legal notion of "cryptoasset". We propose dividing crypto-assets into the "traditional asset in a tokenized form" (on the one hand, this notion is used at the level of the Bank for International Settlements; on the other hand, it is analogous to the currently used "digital financial assets") and the "unsecured (virtual) cryptoasset" (on the one hand, it is analogous to the term "unbacked cryptoasset" as an antonym for "asset-backed cryptoasset"; on the other hand, the presence of the adjective "virtual" refers us to the notion of "virtual asset" formulated by FATF).

We consider it important to additionally – probably in a separate law – specify the notion of a "digital currency", which, as was stated above, is broadly used by the market participants and international regulators, but with a different meaning. The meaning of the "digital currency" notion should be cardinally changed. There are two options in stating such novelties.

The first option: in a separate law, digital currency may be divided into the "secured digital currency", i. e. such digital currency for which there exists a person obliged for each owner of such electronic data, that is, a central bank, and "unsecured digital currency" ("digital currency" in the present edition of law). This variant seems logical , but somewhat utopian from the viewpoint of the state, as it devaluates the connotation of the word "currency" as a substance associated with the state (it turns out that cryptocurrency is also a currency, although of a different kind).

The second option: the "digital currency" notion would be abrogated and substituted for a "digital currency of a central bank", which would be divided by its functional purpose

(retail digital currency of a central bank, digital currency of a central bank for interbank settlements, etc.) and by a state (territorial) affiliation of the "obliged person" (national digital currency of a central bank, i. e. a digital ruble, and a foreign digital currency of a central bank, for example, a digital Yuan, a digital euro). This approach seems the most logical.

In that case, which category would "virtual currencies", including cryptocurrencies, belong to? As it appears, here one has to turn to the international-legal approach formulated by FATF. If one considers the situation on the long-term basis, then, guided by the goals of effective legal regulation, the state cannot isolate itself from the unpleasant theme, namely, introduction of the "virtual asset" notion, used by FATF, at the level of law. Then, virtual assets will comprise the above-mentioned virtual crypto-assets, non-state "currencies", including cryptocurrencies, stablecoins and certain non-fungible tokens recognized as virtual assets by the FATF logic. Given the current concern of the international community about these problems, is appears inevitable to distinguish the notion of "stablecoin" in law. According to the proposed logic, this will be an "unsecured (virtual) cryptoasset with a stabilization mechanism".

We believe it to be especially important to demarcate between the said types of property from the viewpoint that constructing of an efficient regulation cannot be performed in isolation from the practice of their implementation (Sereda, 2019); this said, attention to practical issues seems no less important than following international-legal recommendations.

Second, it is necessary to elaborate new approaches to macroprudential regulation. Assumingly, given the regulated and absolutely transparent architecture of digital financial assets (according to the proposed changes – traditional assets in tokenized form), it is admissible to set the level of risk characteristic for the traditional (basic) asset (with the regulator's right to increase the risk level). It also seems inevitable that the current prohibitory rhetoric regarding "virtual assets" will change. In the authors' opinion, given the public-legal nature of the issues of financial stability, such development is only possible after the respective approaches emerge at the level of international regulators and provided the Russian party is unconditionally consent with them.

At the same time, when constructing national regulation, it is essential to realize that, at the international law level, a scenario seems highly probable, according to which the attitude to stablecoins will change in the nearest years. Given the global nature of stablecoins, it would be logical to provide a common – supranational – supervision over their functioning, including, probably, in the form of setting common criteria for supervision at the national level. In the future, a new international body for prudential supervision might be formed[36]. Researchers believe that stablecoin may be identified in the future as

[36] Iarutin, Ia. K. (2023, March 13). *The Impact of Crypto-Assets on Governments and the International Community: A Forecast for 2035*. https://russiancouncil.ru/en/blogs/iaroslav-iarutin/the-impact-of-cryptoassets-on-governments-and-the-international-commun/?ysclid=ll689ieit3661964369

monetary funds (for the goals of accounting and reporting) (Tetyushin, 2022), but, as follows from the above-described positions of international regulators, the level of risk of such cryptoasset even now (theoretically) depends on the quality of the stabilization mechanism. The international-legal recommendations regarding the assessment of the stabilization mechanism will, undoubtedly, keep being specified.

From the viewpoint of our country, the lack of the "stablecoin" notion at the level of law may deprive the financial system of the Russian Federation, lready weakened by international sanctions, of a competitive advantage consisting in a hypothetic opportunity to use reliable (supervised) stablecoins, which face a lower level of sanction load.

Third, the lack of the "virtual asset" notion in the Russian legal framework logically leads to the lack of notion "a virtual asset service provider (VASP)". From the viewpoint of the whole international AML/CFT architecture, this notion is the axial one, as the international community imposes the main part of obligations in this sphere on the "obliged persons" (for example, banks, insurance companies); for the virtual assets, i. e. partially for crypto-assets as well, such person is VASP. Thus, such circumstance negatively influences the efficiency of the national AML/CFT system.

Fourth, despite numerous problems related to the Russian practice of applying the Law on combating the illegal use of insider information and market manipulation, it seems important to include into the list of insiders also "virtual asset service providers (VASPs)". Probably, insiders should include not all VASP, but only those complying with certain criteria, for example, those with an annual turnover exceeding an amount stipulated by the regulator. This change seems important, as from the financial-economic viewpoint the crypto-assets market does not differ from traditional financial markets; it also may face misuse and unfair practices, with significant economic damage.

Fifth, given the above proposals, it appears especially important that the state pays attention to the changes at the level of international law and positions of international regulators, including to expert analytics of these issues. The sphere of crypto-assets is too large-scale, and ignoring it by the state may lead to numerous consequences, including in such sensitive fields as combating money laundering, funding terrorism, and providing financial stability.

Conclusion

Thus, one may conclude that the international-legal position of the Russian Federation in regard to crypto-assets is of moderate liberal character. At the level of federal legislation, the notions of "digital financial asset" and "digital currency" were introduced; the turnover of these categories is legal, although some restrictions exist. We believe that the conceptual framework, formulated by the Russian legislation, does not fully comply with the international

standards, which is a substantial drawback of the national legal system (and, probably, financial system), diminishing the business attraction of our country. Assumingly, the unique Russian approach is simply incomprehensible for the international business community. Apart from that, i. e. in the issues of prudential regulation, combating money laundering, and civil-legal features, the Russian legislation entirely complies with the letter and spirit of international-legal recommendations.

Based on the above, one may assume that the further development of the Russian law will be consecutive. Undoubtedly, the conceptual framework will sooner or later be changed in compliance with the international-legal recommendations. Speaking of the logical vector of the Russian regulation, the state rightly places increased stake on digital financial assets, which will be issued by large business observing the high standards imposed by a financial regulator. The turnover of digital currencies (in the Russian interpretation) will continue to be restricted in practice, but in the absence of an explicitly prohibitory rhetoric at the level of law[37]. The market of the so called "digital currencies" will be substituted by a central bank digital currency, i. e. the digital ruble currently being designed.

It is highly likely that the more technologically advanced countries will opt for a deeper integration of crypto-assets into the legal reality, bringing new financial markets in compliance with international standards. Accordingly, from a conceptual point of view, when forming a legal regime at the level of national law, it is essential to stem from exactly this estimation.

At the same time, given the practical need for actualization of the national law, it seems necessary not only to comprehend the international-legal reality, but also to pay attention to futurology, that is, the trends and forecasts related to the development of international law. It is the requirements of the future that the national legal system should be maximally adapted to, if we really wish to be in the vanguard of the global development.

References

Arestova, E. N., & Borbat, A. V. (2022). Problems of initiating criminal cases on market manipulation and illegal use of insider information. *Russian Journal of Criminology*, *16*(3), 384–391. (In Russ.).

Blemus, S., & Guégan, D. (2020). Initial crypto-asset offerings (ICOs), tokenization and corporate governance. *Capital Markets Law Journal*, *15*(2),191–223. https://doi.org/10.1093/cmlj/kmaa005

Borlini, L. (2020). On Financial Nationalism and International Law: Sovereignty, Cooperation and Hard/Soft Governance in International Finance. *European Journal of International Law*, *31*(3), 1133–1155. https://doi.org/10.1093/ejil/chaa065

Brown-Hruska, S., & Wagener, T. (2018). The virtual currency regulatory framework in global context. *Capital Markets Law Journal*, *13*(4), 487–517. https://doi.org/10.1093/cmlj/kmy028

Brummer, C. (2010). Why Soft Law Dominates International Finance — and not Trade. *Journal of International Economic Law*, *13*(3), 623–643. https://doi.org/10.1093/jiel/jgq026

[37] Iarutin, Ia. K. *Digital currency and the future of global policy*. https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/tsifrovaya-valyuta-i-budushchee-mirovoy-politiki/

Droll, T., & Minto, A. (2022). "Hare or Hedgehog? The Role of Law in Shaping Current Technological Trends in the Securities Post-trading System". *Accounting, Economics, and Law: A Convivium*, 1–46. https://doi.org/10.1515/ael-2022-0029

Ferreira, A. (2021). The Curious Case of Stablecoins – Balancing Risks and Rewards? *Journal of International Economic Law*, *24*(4), 755–778. https://doi.org/10.1093/jiel/jgab036

Fogelson, Yu. B. (2013a). Soft law in the modern legal discourse (final part). *Journal of Russian Law*, *9*, 43–50. (In Russ.).

Fogelson, Yu. B. (2013b). Soft law in the modern legal discourse. *Journal of Russian Law*, *5*, 37–48. (In Russ.).

Geva, B. (2019). *Cryptocurrencies and the Evolution of Banking, Money and Payments*. In: Chris Brummer (Ed.). Crypto-assets Legal, Regulatory and Monetary Perspectives. pp. 11–38. Oxford University Press. https://doi.org/10.1093/oso/9780190077310.003.0002

Keister, T., & Sanches, D. (2023). Should Central Banks Issue Digital Currency? *The Review of Economic Studies*, *90*(1), 404–431. https://doi.org/10.1093/restud/rdac017

Khisamova, Z. I. (2020). Concept of central banks digital currencies: main risks in terms of observing the AML ("anti-money laundering") and KYC ("know your client") requirements. *Actual Problems of Economics and Law, 14*(3), 508–515. (In Russ.). http://dx.doi.org/10.21202/1993-047X.14.2020.3.508-515

Kinsburskaya, V. A. (2019). Identifying cryptocurrency holders for the purposes of counteracting laundering of illegally obtained moneys and financing of terrorism. *Nota Bene*, *3*, 1–13. (In Russ.). https://doi.org/10.7256/2454-0668.2019.3.29720

Kinsburskaya, V. A. (2020). Requirements of FATF for regulating cryptocurrencies: problems of implementation in the national legislation. *Nota Bene*, *4*, 1–18. (In Russ.). https://doi.org/10.7256/2454-0668.2020.4.33856

Kudryashov, V. V. (2013a). Soft law as a method of regulating international financial relations in the foreign doctrine of international financial law. *Finansovoye pravo*, *4*, 8–12. (In Russ.).

Kudryashov, V. V. (2013b). Soft law as a method of regulating international financial relations in the foreign doctrine of international financial law (continuation). *Finansovoye pravo*, *5*, 17–21. (In Russ.).

Kudryashov, V. V. (2013c). Soft law as a method of regulating international financial relations in the foreign doctrine of international financial law. *Moscow Journal of International Law*, *2*(90), 70–89. (In Russ.). https://doi.org/10.24833/0869-0049-2013-2-70-89

Kudryashov, V. V. (2014). International financial standarts as a contcept of regulating international financial relations. *Pravo i ekonomika*, *1*(311), 64–71. (In Russ.).

Lifshits, I. M., & Yani, P. S. (2020). Criminal liability for market manipulation according to the law of Russia and European Union. *Russian Journal of Criminology*, *14*(5), 764–776. (In Russ.). https://doi.org/10.17150/2500-4255.2020.14(5).764–776

Mazhorina, M. V. (2018). International private law under globalization: from de-stating to fragmentation. *Pravo. Zhurnal Vysshey shkoly ekonomiki*, *1*, 193–217. (In Russ.). https://doi.org/10.17323/2072-8166.2018.1.193.217

Nabilou, H. (2019). How to regulate bitcoin? Decentralized regulation for a decentralized cryptocurrency. *International Journal of Law and Information Technology*, *27*(3), 266–291. https://doi.org/10.1093/ijlit/eaz008

Ní Aoláin, F. (2021). 'Soft Law', Informal Lawmaking and 'New Institutions' in the Global Counter-Terrorism *Architecture. European Journal of International Law*, *32*, 919–942. https://doi.org/10.1093/ejil/chab071

Pomulev, A. A. (2021). Digital currency – an instrument for combating shadow economic activity? *Tenevaya ekonomika*, *5*(4), 267–274. (In Russ.). https://doi.org/10.18334/tek.5.4.113746

Rozhdestvenskaya, T. E. (2022). Risks of cryptocurrencies legalization for public law and order. In *Russia: trends and prospects of development*, *17-2*, 150–155. (In Russ.).

Rozhdestvenskaya, T. E., & Guznov, A. G. (2020). Using FATF approaches to regulating virtual assets in the legislation of the Russian Federation: prospects of development. *Courier of Kutafin Moscow State Law University (MSAL)*, *9*, 138–146. (In Russ.). https://doi.org/10.17803/2311-5998.2020.73.9.138-147

Ruchkina, G. F. (2019). Combating the illegal use of insider information and market manipulation: experience of the Bank of Russia. *Banking Law*, *1*, 9–22. (In Russ.).

Ruchkina, G. F. (2022). Illegal practices in the securities market: on the issue of improving legal regulation. *Banking Law*, *1*, 22–29. (In Russ.).

Salami, Iwa. (2021). Challenges and Approaches to Regulating Decentralized Finance. *AJIL Unbound*, *115*, 425–429. https://doi.org/10.1017/aju.2021.66

Schmidt, A. (2021). Virtual assets: compelling a new anti-money laundering and counter-terrorism financing regulatory model. *International Journal of Law and Information Technology*, *29*(4), 332–363. https://doi.org/10.1093/ijlit/eaac001

Sereda, A. V. (2017). Settlements with virtual currencies in the Russian Federation: analysis of the first law enforcement experience. *Sovremennyy yurist*, *2*, 57–64. (In Russ.).

Sereda, A. V. (2019). On the issue of legal regulation of blockchain technologies: analysis of foreign experience. *Economic Problems and Legal Practice*, *15*(5), 140–143. (In Russ.).

Tetyushin, A. V. (2022). Classification of digital financial assets and their identification in financial reporting. *Auditorskiye vedomosti*, *1*, 24–29. (In Russ.).

Tomczak, T. (2022). Crypto-assets and crypto-assets' subcategories under MiCA Regulation. *Capital Markets Law Journal*, *17*(3), 365–382. https://doi.org/10.1093/cmlj/kmac008

Tsang, C., & Chen, P. (2022). Policy responses to cross-border central bank digital currencies – assessing the transborder effects of digital yuan. *Capital Markets Law Journal*, *17*(2), 237–261. https://doi.org/10.1093/cmlj/kmac004

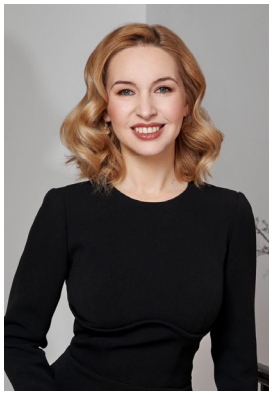
Vergeles, E. R. (2022). Crypto-assets: position in modern legislation. *Academic Thought*, *1*(18), 35–37. (In Russ.).

Verstein, A. (2019). Crypto Assets and Insider Trading Law's Domain. *Iowa Law Review*, *105*(1), 1–59.

Zellweger-Gutknecht, C., Geva, B., & Grünewald, S. N. (2021). Digital Euro, Monetary Objects, and Price Stability: A Legal Analysis. *Journal of Financial Regulation*, *7*(2), 284–318. https://doi.org/10.1093/jfr/fjab009

Authors information

Iaroslav K. Iarutin – post-graduate student, Department of International Law, Diplomatic Academy of the Ministry of Foreign Affairs of the Russian Federation
Address: 53/2 Ostozhenka Str., building 1, 119021 Moscow, Russian Federation
E-mail: iaroslaviarutin@icloud.com
ORCID ID: https://orcid.org/0000-0003-0036-6494
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/record/HJI-6696-2023
Google Scholar ID: https://scholar.google.com/citations?user=w-imCpMAAAAJ
RSCI Author ID: https://elibrary.ru/author_items.asp?authorid=1175345



Elena E. Gulyaeva – Candidate of Sciences in Jurisprudence, Associate Professor, Department of International Law, Diplomatic Academy of the Ministry of Foreign Affairs of the Russian Federation
Address: 53/2 Ostozhenka Str., building 1, 119021 Moscow, Russian Federation
E-mail: gulya-eva@yandex.ru
ORCID ID: https://orcid.org/0009-0002-2708-8332
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=56906889200
Web of Science ResearcherID:
https://www.webofscience.com/wos/author/record/ISB-2036-2023
Google Scholar ID: https://scholar.google.com/citations?user=KQqjjYAAAAAJ
RSCI Author ID: https://elibrary.ru/author_items.asp?authorid=756727

Authors' contributions

Iaroslav K. Iarutin compiled the manuscript draft; performed comparative analysis; collected, analyzed and summarized literature; prepared and edited the manuscript; interpreted the overall research results; formulated the key conclusions, proposals and recommendations; formatted the manuscript.
Elena E. Gulyaeva formulated the research idea, goals and tasks; elaborated the methodology; critically reviewed and edited the manuscript; interpreted the specific research results; approved the final version of the article.

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Acknowledgement

The authors are grateful to the administrators of the International Law Club of Diplomatic Academy of the Ministry of Foreign Affairs of the Russian Federation for organizing the International inter-university roundtable, commemorating the 220th anniversary of the Ministry of Justice of the Russian Federation, themed: “Topical issues of the international law”, within which the authors expressed and discussed some of the ideas further developed in this article.

Thematic rubrics

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

Article history

Date of receipt – January 20, 2022
Date of approval – May 6, 2022
Date of acceptance – March 6, 2023
Date of online placement – March 10, 2023

Научная статья
УДК 34:341.9:004:130.1
EDN: https://elibrary.ru/hgbqgl
DOI: https://doi.org/10.21202/jdtl.2023.32

Международное и российское правовое регулирование оборота криптоактивов: понятийно-терминологическая корреляция

Ярослав Кириллович Ярутин ✉

Дипломатическая академия Министерства иностранных дел Российской Федерации
г. Москва, Российская Федерация

Елена Евгеньевна Гуляева

Дипломатическая академия Министерства иностранных дел Российской Федерации
г. Москва, Российская Федерация

Ключевые слова

Виртуальный актив,
законодательство,
криптоактив,
криптовалюта,
международное право,
право,
стейблкоин,
токен,
цифровая валюта,
цифровые технологии

Аннотация

Цель: оценка российского законодательства на предмет его соответствия международно-правовым подходам к формированию симметричного регулирования оборота криптоактивов и возможности дополнения новыми международно-правовыми категориями, отражающими глубинные изменения в мировой экономике и структуре международных финансов, обусловленные широким внедрением новых финансовых технологий, в основе которых находятся технологии распределенного реестра.

Методы: методологическую основу исследования составляет совокупность методов научного познания, среди которых важное значение имеют специально-юридические (формально-юридический и сравнительно-правовой) методы, дополненные риск-ориентированным подходом, правовым моделированием и юридическим прогнозированием, в совокупности позволившие осмыслить архитектуру, «букву» и «дух» современного международного финансового права и национального законодательства в их понятийно-терминологической корреляции, спрогнозировать дальнейшее развитие и корректировку правового регулирования оборота криптоактивов.

✉ Контактное лицо

Результаты: выявлено, что в регулировании оборота криптоактивов устойчивой становится тенденция доминирования среди источников актов «мягкого» права (особенно это заметно в сфере международного финансового права в сравнении, например, с конвенциями или международными договорами); наряду с этим усиливается тенденция «фрагментации» международного права в части оборота криптоактивов; отмечено несоответствие понятийного аппарата, содержащегося в международных актах и российском законодательстве, и пробелы в режиме оборота криптоактивов на уровне национального права; обозначены тенденции и прогнозы развития международно-правового регулирования сферы криптоактивов.

Научная новизна: состоит прежде всего в комплексном сопоставлении на основе в том числе принципиально новых концепций регулирования таких прогрессивных международно-правовых категорий, как криптоактив, виртуальный актив, криптовалюта, стейблкоин и другие, отдельные из которых редко используются в российском правовом дискурсе и практически не употребляются в законодательстве.

Практическая значимость: сформулированы научно обоснованные предложения, направленные на совершенствование понятийно-терминологического аппарата российского законодательства в сфере оборота криптоактивов, реализация которых позволит в перспективе выстроить единое правовое пространство с наиболее технологически развитыми государствами, будет содействовать улучшению инвестиционного климата и финансовой привлекательности государства; усовершенствует национально-правовой режим оборота криптоактивов не только с точки зрения реальных потребностей рынка, но и интересов государственной безопасности и повышения конкурентоспособности Российской Федерации.

Для цитирования

Ярутин, Я. К., Гуляева, Е. Е. (2023). Международное и российское правовое регулирование оборота криптоактивов: понятийно-терминологическая корреляция. *Journal of Digital Technologies and Law*, *1*(3), 725–751. https://doi.org/10.21202/jdtl.2023.32

Список литературы

Арестова, Е. Н., Борбат, А. В. (2022). Проблемы возбуждения уголовных дел о манипуляции рынком и неправомерном использовании инсайдерской информации. *Всероссийский криминологический журнал*, *16*(3), 384–391. https://elibrary.ru/moixbc

Вергелес, Э. Р. (2022). Криптоактивы: место в современном законодательстве. *Академическая мысль*, *1*(18), 35–37. https://elibrary.ru/ldxclf

Кинсбурская, В. А. (2019). Идентификация держателей криптовалюты в целях противодействия отмыванию доходов, полученных преступным путем, и финансированию терроризма. *Национальная безопасность / Nota Bene*, *3*, 1–13. EDN: https://elibrary.ru/byjwhb. DOI: https://doi.org/10.7256/2454-0668.2019.3.29720

Кинсбурская, В. А. (2020). Требования ФАТФ по регулированию криптовалют: проблемы имплементации в национальное законодательство. *Национальная безопасность / Nota Bene*, *4*, 1–18. EDN: https://elibrary.ru/crgkhs. DOI: https://doi.org/10.7256/2454-0668.2020.4.33856

Кудряшов, В. В. (2013а). Мягкое право как метод регулирования международных финансовых отношений в зарубежной доктрине международного финансового права. *Финансовое право*, *4*, 8–12. https://elibrary.ru/qafzdz

Кудряшов, В. В. (2013b). Мягкое право как метод регулирования международных финансовых отношений в зарубежной доктрине международного финансового права (продолжение). *Финансовое право*, *5*, 17–21. https://elibrary.ru/qavehl

Кудряшов, В. В. (2013c). «Мягкое право» как метод регулирования международных финансовых отношений в зарубежной доктрине международного финансового права. *Московский журнал международного права*, *2*(90), 70–89. EDN: https://elibrary.ru/qzhcsb. DOI: https://doi.org/10.24833/0869-0049-2013-2-70-89

Кудряшов, В. В. (2014). Международные финансовые стандарты как концепция регулирования международных финансовых отношений. *Право и экономика*, *1*(311), 64–71. https://elibrary.ru/rvezrf

Лифшиц, И. М., Яни, П. С. (2020). Уголовная ответственность за манипулирование рынком по праву России и Европейского союза. *Всероссийский криминологический журнал*, *14*(5), 764–776. EDN: https://elibrary.ru/jdgqlc. DOI: https://doi.org/10.17150/2500-4255.2020.14(5).764-776

Мажорина, М. В. (2018). Международное частное право в условиях глобализации: от разгосударствления к фрагментации. *Право. Журнал Высшей школы экономики*, *1*, 193–217. EDN: https://elibrary.ru/yvvqnc. DOI: https://doi.org/10.17323/2072-8166.2018.1.193.217

Помулев, А. А. (2021). Цифровая валюта – инструмент противодействия теневой экономической деятельности? *Теневая экономика*, *5*(4), 267–274. EDN: https://elibrary.ru/yhdxrr. DOI: https://doi.org/10.18334/tek.5.4.113746

Рождественская, Т. Э. (2022). Риски легализации криптовалют для публичного правопорядка. В сб. *Россия: тенденции и перспективы развития* (т. 17–2, с. 150–155). https://elibrary.ru/qaqxtx

Рождественская, Т. Э., Гузнов, А. Г. (2020). Реализация подходов ФАТФ к регулированию виртуальных активов в законодательстве российской федерации: перспективы развития. *Вестник Университета им. О. Е. Кутафина*, *9*, 138–146. EDN: https://elibrary.ru/kjrwef. DOI: https://doi.org/10.17803/2311-5998.2020.73.9.138-147

Ручкина, Г. Ф. (2019). Противодействие неправомерному использованию инсайдерской информации и манипулированию рынком: опыт Банка России. *Банковское право*, *1*, 9–22. https://elibrary.ru/yvaxln

Ручкина, Г. Ф. (2022). Противоправные практики на рынке ценных бумаг: к вопросу совершенствования правового регулирования. *Банковское право*, *1*, С. 22–29. https://elibrary.ru/lgeios

Середа, А. В. (2017). Осуществление расчетов при помощи виртуальных валют в РФ: анализ первого правоприменительного опыта. *Современный юрист*, *2*, 57–64. https://elibrary.ru/yurqrp

Середа, А. В. (2019). К вопросу о правовом регулировании блокчейн-технологий: анализ зарубежного опыта. *Проблемы экономики и юридической практики*, *15*(5), 140–143. https://elibrary.ru/jycpbg

Тетюшин, А. В. (2022). Классификация цифровых финансовых активов и их идентификация в финансовой отчетности. *Аудиторские ведомости*, *1*, 24–29. https://elibrary.ru/wpzlco

Фогельсон, Ю. Б. (2013a). Мягкое право в современном правовом дискурсе. *Журнал российского права*, *5*, 37–48. https://elibrary.ru/pysarz

Фогельсон, Ю. Б. (2013b). Мягкое право в современном правовом дискурсе (окончание). *Журнал российского права*, *9*, 43–50. https://elibrary.ru/qztjov

Хисамова, З. И. (2020). Концепция цифровых валют центральных банков: основные риски в части соблюдения требований AML («противодействия отмыванию денег») и KYC («знай своего клиента»). *Актуальные проблемы экономики и права*, *14*(3), 508–515. EDN: https://elibrary.ru/eilmjw. DOI: http://dx.doi.org/10.21202/1993-047X.14.2020.3.508-515

Blemus, S., & Guégan, D. (2020). Initial crypto-asset offerings (ICOs), tokenization and corporate governance. *Capital Markets Law Journal*, *15*(2), 191–223. https://doi.org/10.1093/cmlj/kmaa005

Borlini, L. (2020). On Financial Nationalism and International Law: Sovereignty, Cooperation and Hard/Soft Governance in International Finance. *European Journal of International Law*, *31*(3), 1133–1155. https://doi.org/10.1093/ejil/chaa065

Brown-Hruska, S., & Wagener, T. (2018). The virtual currency regulatory framework in global context. *Capital Markets Law Journal*, *13*(4), 487–517. https://doi.org/10.1093/cmlj/kmy028

Brummer, C. (2010). Why Soft Law Dominates International Finance – and not Trade. *Journal of International Economic Law*, *13*(3), 623–643. https://doi.org/10.1093/jiel/jgq026

Droll, T., & Minto, A. (2022). Hare or Hedgehog? The Role of Law in Shaping Current Technological Trends in the Securities Post-trading System. *Accounting, Economics, and Law: A Convivium*, 1–46. https://doi.org/10.1515/ael-2022-0029

Ferreira, A. (2021). The Curious Case of Stablecoins – Balancing Risks and Rewards? *Journal of International Economic Law*, *24*(4), 755–778. https://doi.org/10.1093/jiel/jgab036

Geva, B. (2019). *Cryptocurrencies and the Evolution of Banking, Money and Payments*. In Ch. Brummer (Ed.). *crypto-assets Legal, Regulatory and Monetary Perspectives (pp. 11–38)*. Oxford University Press. https://doi.org/10.1093/oso/9780190077310.003.0002

Keister, T., & Sanches, D. (2023). Should Central Banks Issue Digital Currency? *The Review of Economic Studies*, *90*(1), 404–431. https://doi.org/10.1093/restud/rdac017

Nabilou, H. (2019). How to regulate bitcoin? Decentralized regulation for a decentralized cryptocurrency. *International Journal of Law and Information Technology*, *27*(3), 266–291. https://doi.org/10.1093/ijlit/eaz008

Ní Aoláin, F. (2021). 'Soft Law', Informal Lawmaking and 'New Institutions' in the Global Counter-Terrorism Architecture. *European Journal of International Law*, *32*, 919–942. https://doi.org/10.1093/ejil/chab071

Salami, I. (2021). Challenges and Approaches to Regulating Decentralized Finance. *AJIL Unbound*, *115*, 425–429. https://doi.org/10.1017/aju.2021.66

Schmidt, A. (2021). Virtual assets: compelling a new anti-money laundering and counter-terrorism financing regulatory model. *International Journal of Law and Information Technology*, *29*(4), 332–363. https://doi.org/10.1093/ijlit/eaac001

Tomczak, T. (2022). Crypto-assets and crypto-assets' subcategories under MiCA Regulation. *Capital Markets Law Journal*, *17*(3), 365–382. https://doi.org/10.1093/cmlj/kmac008

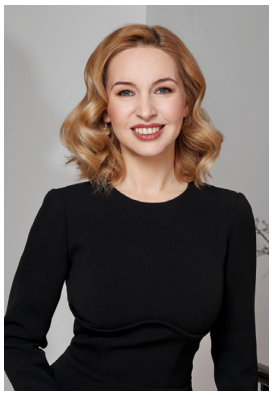
Tsang, C., & Chen, P. (2022). Policy responses to cross-border central bank digital currencies – assessing the transborder effects of digital yuan. *Capital Markets Law Journal*, *17*(2), 237–261. https://doi.org/10.1093/cmlj/kmac004

Verstein, A. (2019). Crypto Assets and Insider Trading Law's Domain. *Iowa Law Review*, *105*(1), 1–59.

Zellweger-Gutknecht, C., Geva, B., & Grünewald, S. N. (2021). Digital Euro, Monetary Objects, and Price Stability: A Legal Analysis. *Journal of Financial Regulation*, *7*(2), 284–318. https://doi.org/10.1093/jfr/fjab009

Сведения об авторах

Ярутин Ярослав Кириллович – аспирант кафедры международного права, Дипломатическая академия Министерства иностранных дел Российской Федерации, г. Москва
Адрес: 119021, Российская Федерация, г. Москва, ул. Остоженка, 53/2, стр. 1
E-mail: iaroslaviarutin@icloud.com
ORCID ID: https://orcid.org/0000-0003-0036-6494
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/record/HJI-6696-2023
Google Scholar ID: https://scholar.google.com/citations?user=w-imCpMAAAAJ
РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=1175345



Гуляева Елена Евгеньевна – кандидат юридических наук, доцент кафедры международного права, Дипломатическая академия Министерства иностранных дел Российской Федерации
Адрес: 119021, Российская Федерация, г. Москва, ул. Остоженка, 53/2, стр. 1
E-mail: gulya-eva@yandex.ru
ORCID ID: https://orcid.org/0009-0002-2708-8332
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=56906889200
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/record/ISB-2036-2023
Google Scholar ID: https://scholar.google.com/citations?user=KQqjjYAAAAAJ
РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=756727

Вклад авторов

Я. К. Ярутин осуществлял составление черновика рукописи; проведение сравнительного анализа; сбор, анализ и обобщение литературы; подготовку и редактирование текста статьи; интерпретацию общих результатов исследования; формулировку ключевых выводов, предложений и рекомендаций; оформление рукописи.
Е. Е. Гуляева осуществляла формулирование идеи, исследовательских целей и задач; разработку методологии; критический пересмотр и редактирование текста рукописи; интерпретацию частных результатов исследования; утверждение окончательного варианта статьи.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Благодарность

Авторы выражают благодарность руководству Клуба международного права Дипломатической академии Министерства иностранных дел Российской Федерации за организацию Международного межвузовского круглого стола, приуроченного к 220-летию Министерства юстиции Российской Федерации на тему «Актуальные проблемы международного права», на котором в рамках дискуссии авторами были высказаны отдельные идеи, получившие свое развитие в настоящей статье.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.89.25 / Право собственности
Специальность ВАК: 5.1.5 / Международно-правовые науки

История статьи

Дата поступления – 20 января 2023 г.
Дата одобрения после рецензирования – 6 мая 2023 г.
Дата принятия к опубликованию – 15 августа 2023 г.
Дата онлайн-размещения – 20 августа 2023 г.

Research article
DOI: https://doi.org/10.21202/jdtl.2023.33

Genesis and Prospects of Development of Legal Regulation of Digital Financial Assets in the Russian Federation

Artem P. Peretolchin

East Siberia Institute of the Ministry of Internal Affairs of the Russian Federation
Irkutsk, Russian Federation

Keywords

Blockchain,
cryptocurrency,
digital financial assets,
digital rights,
digital technologies,
distributed ledger,
law,
legal regulation,
legislation,
token

Abstract

Objective: to research the existing problems and promising directions of the legal regulation of digital financial assets as a relatively new tool of the modern digital economy.

Methods: the methodological basis of the work is the set of scientific cognition methods such as theoretical analysis, research, comparison, synthesis, and summarization of scientific literature.

Results: the work analyzes the existing approaches to legal regulation of digital financial assets in the Russian Federation and some foreign countries, reveals the existing gaps in the Russian legislation in the field of circulation of digital financial assets, gives estimation to the prospects of development of the legal regulation of these tools and forms proposals for its improving. Also, during the research, the approaches to legal regulation of digital currencies and digital financial assets, adopted in certain foreign countries, were analyzed, the trends were considered, and the positive and negative aspects of using cryptographic algorithms for the goals in economic and juridical spheres of the global economy were reflected.

Scientific novelty: within the work, the topical issues of legislative regulation of such a relatively new notion as digital financial assets are considered. The positions of Russian and foreign jurist are considered concerning

the existing problems and risks associated with "tokenization" and "blockachainization" of private law. Besides, the author comes to a conclusion about the existence of significant gaps in the current approach to legal regulation of digital financial assets, indicates them and proposes certain mechanisms to solve these problems.

Practical significance: is due to the imperfect current legislation in the sphere of relations occurring when using the technologies based of distributed ledger, including digital financial assets. Research of these problems allows evaluating the risks, considering the existing ways of overcoming and solving the emerging disputable questions. Also, the conclusions obtained can be used to improve the Russian legislation, as well as in the academic literature devoted to the topical issues of developing the digital legislation.

For citation

Peretolchin, A. P. (2023). Genesis and Prospects of Development of Legal Regulation of Digital Financial Assets in the Russian Federation. *Journal of Digital Technologies and Law, 1*(3), 752–774. https://doi.org/10.21202/jdtl.2023.33

Contents

Introduction

The global economic crises of the recent years cause a significant growth of mistrust of the population towards traditional financial tools, such as banking technologies, state or municipal securities, investment insurance. Another consequence of the catastrophically reducing periods between global shocks, resulting from political and regulatory mistakes, is the striving of the society to get rid of extra middlemen in the financial sector. The reasons for that are both the growing doubts of citizens in the reliability of political systems, and the significantly growing, despite a widespread digitalization of financial processes, fees for the basic services in the financial sector. This trend is reflected in the development of the contemporary, system-based areas of economics which allow establishing peer-to peer (P2P) contacts between the parties. This, in turn, creates significant prerequisites

for rapid development of various systems, based on distributed ledger technologies, such as blockchain (Garcia-Teruel, 2019).

The most popular of such systems is the blockchain of the first digital currency – bitcoin, which was developed as a digital, unmodifiable, jointly used and synchronized database. The cryptographic mechanisms built-in by its creator (or creators – it is still not known for certain, who launched a bitcoin), as well as the basic functional principles allow speaking of high reliability of the tool and of the absent necessity in the mediation institution when implementing the system functionality.

Blockchain is based on technology of the so-called smart contracts, i.e. sequences of computer codes automatically executing preset instructions determined by the internal executable code. Today, smart contracts allow almost instantly transferring any cryptocurrency or digital asset between two virtual wallets. This to become possible, the technology was developed and introduced of creating a digital asset intended for certifying a user right. In the modern world, this digital asset is called "token", and the phenomenon – "digital tokenization".

Later, technological development allowed creating virtual tokens of various types. For example, using ERC-20 protocol, the parties may create fungible tokens which may be exchanged for a respective digital equivalent or converted. With ERC-721 protocol, it became possible to create non-fungible tokens, which comprise in their metadata some specific properties and characteristics differentiating them from other tokens and making them unique. This opened wide prospects of using digital assets not only in the financial sector but also in other sectors such as medicine, notary, state registration, tourism, education, etc.

As a result, in the recent years, digital financial assets (further – DFA) become a more and more popular tool in the system of commercial and other interrelations in cyberspace and even beyond it. A high interest to DFA, as well as to the related processes, is due to the global digitalization. The current transformations in the sphere of economy and information technologies allow simplifying various types of human activity, including in the sphere of financial relations. Besides, one of the key factors stimulating the process of virtualization of certain economic processes is the pandemic. The growing popularity of digital money, in particular cryptocurrencies, caused the need in their legal regulation.

Digital tokenization in various spheres of human activity and in cyberspace may give a number of advantages in the future, such as potentially cheaper and safer transactions, increased transparency of transaction data and emitter information, providing investors with direct access to primary and secondary markets, increased level of assets liquidity, including digital assets, from the viewpoint of selling them to a much broader circle

of participant. In the sphere of real estate, this technology can be used to develop platforms facilitating transborder transactions with real estate assets in Russia and abroad, and, at the same time, due to the cryptographic safety algorithms built in the technology, to resist the challenges associated with digitalization of the global economy under the changing global balance of forces and the new economic reality, which emerges after the COVID-19 crisis (Garcia-Teruel, 2020).

It should be noted that the development of such Internet initiatives is also beneficial for the economic processes taking place within individual states, as they increase their investment attraction, reveals economic and intellectual potential. However, the documented cases of violation of the rights and interests of the participants of economic relations in the sphere of DFA circulation, as well as infringement of the interests of state and society, allow concluding that it is necessary to create a balanced and relevant normative base, regulating the order of functioning and ensuring the work of the said systems in a definite territory.

Attempts to act in this direction have been made in many countries, for example, in Germany, France, Italy, USA, Monaco, Luxemburg, and Malta. Some Asian countries, like China and Vietnam, have totally prohibited using cryptocurrency as a means of payment, while in some others it is not recognized as such (for example, in Philippines and Malaysia) (Garcia-Teruel & Simón-Moreno, 2021). Other countries, like Portugal, have not taken any steps in this sphere, content with preventing and prophylactic work among investors, aimed at informing them about the risks and difficulties associated with the turnover of cryptocurrency and other DFA (Basilio, 2019). A number of advanced countries attempted to integrate the distributed ledger technology into the existing state processes; for example, Sweden and Georgia experiment with using a special blockchain functional for registering transactions with land plots and executing their cadastre accounting.

Russian Federation is not standing back, searching for relevant and promising approaches to the legal regulation of cryptocurrencies and DFA. In this respect, one should accentuate a novel in the legal regulation of modern cryptographic instruments, namely, Federal Law of July 31, 2020 No. 259-FZ "On digital financial assets, digital currency and making changes in certain legislative acts of the Russian Federation"[1] (further – Law on digital financial assets), which came into force on January 1, 2021.

At the same time, the very structure and content of the said law imply building a whole system of legislative and sub-legislative acts, aimed at regulating modern blockchain technologies, as well as instruments created on their basis, including cryptocurrencies and digital financial assets. However, this structure has not been built so far, which ultimately

[1] On digital financial assets, digital currency and making changes in certain legislative acts of the Russian Federation. No. 259-FZ of 31.07.2020. (2020). *Collection of legislation of the Russian Federation*, *31* (part I), Article 5018.

creates substantial difficulties in the legal regulation of the said technologies, leading to a restricted and narrow profile character of the law adopted, and in some cases – to zero efficiency and impossibility to apply some of its norms. In this regard, it seems expedient to perform analysis and formulate proposals to overcome the problems and gaps in legal regulation of the public relations associated with digital currencies and DFA. In this article, we will focus on the issues of legal regulation of digital financial assets.

Assumingly, the problems associated with systemic analysis of the development and legal regulation of digital financial assets are not sufficiently elaborated today.

To achieve the set research goals, one should consider feasible to solve the following tasks:

to study the existing approaches to legal regulation of digital financial assets in the Russian Federation and certain foreign countries;

to reveal the current gaps in the Russian legislation in the sphere of DFA circulation;

to estimate the prospects of legal regulation of digital financial assets in the Russian Federation.

The object of study is administrative and civil-legal norms regulating the DFA circulation, as well as the practice of applying the respective legal norms and the opinions of scholars regarding the efficiency of the current Russian system of DFA legal regulation.

Assumingly, the theoretical and practical value of this research consists in the conclusions, which may be used both in scientific-research activity in this sphere and in law-making when elaborating and improving the administrative, criminal and civil legislation.

1. Genesis of legal regulation of digital financial assets in the Russian Federation

Since the moment of appearance and development of blockchain, digital currencies and related cryptographic financial tools, the Russian legal doctrine manifested various opinions and approaches regarding the need to legislatively regulate cryptocurrencies and tokens. Some scholars spoke for the need to discretely regulate the digital assets circulation, only when such need was due, as establishing rigid regulations in the sphere of digital assets circulation, in their opinion, contradicts the very essence of this phenomenon and its origins (Kudryashova, 2018). Other representatives of academic community insisted on elaborating a comprehensive regulatory legislation for the processes of digitalization and tokenization (Ryzhov, 2018).

At the official level, the need of cryptocurrencies legal regulation in Russia was first declared about nine years ago. In January 2014, recommendations of the Bank of Russia “On using ‘virtual currencies’, in particular, a ‘bitcoin’, in transactions” were published, according to which, it was proposed to consider cryptocurrency to be a monetary surrogate,

and its use in transactions – a basis for referring such transactions (operations) to those aimed at funding terrorism[2]. At that moment, the position of the Bank of Russia referring cryptocurrencies to a monetary surrogate was supported by the Russian Finance Monitoring Service[3] and the Prosecutor General's Office of the Russian Federation[4].

For a long time, the role of digital financial assets and digital currency in the Russian system of civil rights' objects was not defined, as they were not isolated as a separate object of civil law and their legal nature did not allow referring them to any objects of legal relations stipulated by Article 128 of the Civil Code of the Russian Federation[5] (further – CC RF). This resulted in forming and adopting opposite approaches in the law-enforcement practice of courts and state authorities in the issues of whether digital financial assets and digital currency are civil rights' objects and whether their circulation is restricted.

In October 2017, as part of the program "Digital economy of the Russian Federation", the Russian President charged the Russian Government and the Bank of Russia with introducing changes in the Russian legislation to determine the status of modern digital and cryptographic technologies used in the financial sector and to determine the conditions of their legal regulation, based on the approach, according to which a ruble is the only legal means of payment on the territory of the Russian Federation.

The result was Federal Law of July 31, 2020 No. 259-FZ, in accordance to which, digital financial assets[6] were recognized as digital rights. In turn, digital rights, in compliance with Article 128 CC RF, act as property rights. Relevance of this conclusion is further confirmed in the commentaries of the Committee of the Federation Council on budget and financial markets[7].

---

2 Bank of Russia. (2014, January 27). *On using 'virtual currencies', in particular, a 'bitcoin', in transactions*. https://www.cbr.ru/press/pr/?file=27012014_1825052.htm

3 Federal Finance Monitoring Service. (2014, February 6). *On using cryptocurrencies*. https://www.fedsfm.ru/news/957

4 *In the Russian Prosecutor General's Office, a meeting was held on the legality of using anonymous payment systems and cryptocurrencies*. Official website of the Prosecutor General's Office of the Russian Federation. https://epp.genproc.gov.ru/web/gprf/search?article=83101813

5 Civil Code of the Russian Federation. (1994, December 5). (1994). *Collection of legislation of the Russian Federation*, *32*, Article 3301.

6 "Digital financial assets are the digital rights, including monetary claims, the possibility to implement rights on emission securities, the rights to participate in the capital of a nonpublic joint stock company, the right to claim transition of emission securities, which are stipulated by a decision on emitting the digital financial assets in the order established by this Federal Law, while their issuance, accounting and circulation are only possible by making (changing) records in an information system based on distributed ledger, as well as in other information systems". (On digital financial assets, digital currency and making changes in certain legislative acts of the Russian Federation. No. 259-FZ of 31.07.2020. (2020). *Collection of legislation of the Russian Federation*, 31 (part I), Article 5018).

7 *Conclusion on the Federal Law "On digital financial assets, digital currency and making changes in certain legislative acts of the Russian Federation" (draft No. 419059-7).* Official website of the Federation Council of the Federal Assembly of the Russian Federation. http://budget.council.gov.ru/activity/legislation/resolutions_law/118341

In cryptographic world, DFA most often acts as so called tokens and are, actually, digital accounting units, issued by particular persons, the value of which comprises various goods, services, shares, rights, etc. In compliance with the Russian legislation, digital financial assets may include:

1) DFA as the right of claim;

2) DFA for the right to participate in nonpublic joint stock company;

3) DFA for the rights on emission securities;

4) hybrid DFA, complemented with the signs of utilitarian digital right.

It should be noted also that the issuance of digital financial assets requires just one document – decision on the issuance of DFA, which contains all the key details of the asset and all its main parameters (value, amount, information on the emitter, etc.). This document is the key for launching a digital asset into circulation.

The Russian legislation implies using a distributed ledger system, a so called blockchain, for DFA circulation. This technology simplifies the circulation of financial assets by possessing the following important properties: unmodifiable information within the system, operational sustainability, mutual dependence of blocks within the system, resistance to hacking, and efficiency, as distributed systems are much cheaper than centralized ones.

To better understand the tool of digital financial assets, it is expedient to compare them with the current tools already existing in the market.

1. The most popular tool is DFA as a monetary claim.

A monetary claim is a claim to transfer rubles or other currency. Due to the specificity of DFA, they may act as a right of claim when transferring digital currency. However, it should be emphasized that cryptocurrencies, in particular, bitcoin or ether, do not refer to money, although are considered as a possible means of payment according to the federal legislation.

This type of DFA is most close to a bond or credit, depending on what the DFA is based on. For example, if it implies systematic fixed payments to the investor, then it is similar to bonds with coupon income.

A distinctive feature of DFA compared to a classic bond is that this tool is much more accessible in the market both for investors and emitters. An emitter of any size may issue DFA, and its attraction for investors will depend only on the reliability of the emitter and degree of trust in them, which, in turn, makes emitters do their business in a more open and reliable manner.

It should be noted that this kind of DFA is per se a monetary claim of an investor to an emitter. Thus, the emitter cannot transfer their obligations of payment to a third party, for example, their debtor. This is very important, as the main factor in investors making a decision on investing into a particular type of DFA is, first of all, reliability of the emitter, not their debtors.

2. Another type is DFA for the right to participate in nonpublic joint stock company. This type of digital financial assets suits for creating a new nonpublic joint stock company. Although one may not tokenize an old nonpublic joint stock company with this tool,

in the sphere of large business this tool can be applying to quickly create joint companies. Accordingly, this functional of DFA serves to attract share funding (the so called equity financing), if one of the participants of a joint stock company is a bank, for example. For small businesses and promising startups, DFA for the right to participate in nonpublic joint stock company is suitable to perform an ICO (Initial Coin Offering), i. e. primary placement of digital shares in compliance with the Russian legislation.

3. Another tool is DFA for the rights on emission securities. Definition of emission securities is found in Article 2 of the Federal Law of April 22, 1996 No. 39-FZ "On securities market": various securities characterized simultaneously with such properties as equal volume and terms of the right implementation within one issue; observance of the stipulated form and order of consolidation of a set of property and non-property rights; placement by issues or additional issues[8].

According to the Russian legislation, emission securities include shares, bonds, emitter's options, and Russian depositary receipts.

4. Hybrid digital financial assets are digital rights including simultaneously DFA and other digital rights. Other digital rights, in particular, include the right to use a service, goods, or a discount. In other words, hybrid DFA have signs of both digital financial assets and utilitarian digital right.

An example of a hybrid digital financial asset is a stablecoin. Stablecoins are not homogeneous and may have varied economic-legal signs. Most of stablecoins are issued by clearly identified emitters based on blockchain both in the form of circulating digital obligations and depositary receipts, used as a means of exchange, storage and payment. The most popular stablecoins are centralized ones, secured by fiat currencies and gold. Such stablecoins are used to execute stock exchange operations or retail payments. Local stablecoins are used as a means of storage and exchange. Global stablecoins can accelerate transborder payments and reduce their cost, as well as increase financial accessibility of cryptoassets for users without the need to open accounts.

The described legislative approach is an important step towards legalizing DFA and creates a good platform for further development of the legal regulation system currently created. Nevertheless, to implement the potential advantages of using various DFA tools, it is necessary to solve legal, normative and supervisory tasks associated with the national and transborder circulation.

8 "On securities market" No. 39-FZ of 22.04.1996. *Collection of legislation of the Russian Federation*, *17*, Article 1918.

2. Gaps in the Russian legislation on digital financial assets

In the recent years, the market of cryptocurrencies is growing. Despite a significant fall by 65% in 2022, it should be noted that the overall capitalization of cryptocurrencies reached over $2.4 trillion at some moment. Today, there are grounds to assume that the actual global crises and challenges, as well as the advantages and prospects of blockchain technology will facilitate the market returning to the previous positions and, most likely, significantly growing in the future. In this regard, the issues of legalizing the income obtained and implementing their activities within the legal framework are still topical for all companies and physical persons actively working with modern cryptographic financial tools[9].

Besides, the academic community actively discusses, alongside with technological aspects of the system, the possibility and prospects of using blockchain for the market and society needs (Raskin, 2017), possibility of tokenization of property rights (Yapicioglu & Leshinsky, 2020), including in the context of changes in the current processes of registration and keeping of land and cadastre registers, real estate registers, and other accounting bases (Verheye, 2017). Assumingly, the opportunities provided by the distributed ledger and nonfungible tokens (further – NFT) technologies should be introduced into these processes even today, as this opens broad opportunities for optimizing the activity of state authorities, improving the quality of state services and optimizing budget expenses.

A number of scholars point out certain problems associated with the risks of "tokenization" and "blockchainization" of private law (Savelyev, 2018). One of the actual and prospective issues is the potential opportunity to substitute the existing mechanism of transferring the property rights with new coded rules, used within the distributed ledger and digital tokens technologies. However, in this regard, there is a grave need for qualitative definition of the legal nature of such tokens and elaboration of regulatory legislation in the sphere of property digitalization (Ishmaev, 2017; Vasilevskaya, 2019). We believe NFT technologies can be rather successfully applied here.

Another interesting and disputable question is extrapolation of contract and property relations to smart contracts, which may lead, according to some authors, to the beginning of the end of the "classical" contract law (Savelyev, 2017). At the same time, some researchers believe that the choice of which technology to use for implementation of one's rights and obligations should be left to citizens and they should have an opportunity to use both classical concepts of contract law and modern ones, implemented through cryptographic algorithms (Konashevych, 2020). We completely agree with that, at least, under the conditions of the current transitional period.

The above and many other questions constitute a serious challenge for contemporary and future legislators and academic community, which consists in the need for profound

[9] "Law on DFA caused disappointment". Jurists on the problems of cryptocurrencies regulation. (2021, January 25). *rbc.ru*. https://www.rbc.ru/crypto/news/600eba6f9a79470a85424efa

analytic conceptualization of the technologies, their legal nature, risks and prospects, as well as in creating, based on this analysis, a relevant, modern and effective legislation, able not only to ease the life of citizens but also to successfully protect their interests.

We believe that this process should unfold stage by stage, in close cooperation between practitioners and theoreticians of law, as well as specialists in the field of information technologies. Although a Federal Law regulating DFA came into force in Russia on January 1, 2021, some questions remained uncovered.

The said legal act regulates the relations associated with using new digital instruments which may significantly influence the Russian financial market. A Russian legislator abstained from complete prohibition of cryptocurrency and digital tokens, as such taboo could have resulted in a substantial development of certain segments of shadow economy. However, within the frameworks of this law, a number of restrictions were stipulated regarding the process of circulation of digital financial assets.

As was mentioned above, to the category of digital financial assets the Russian legislator referred certain rights to possession and operation execution, implemented within an information system complying with the requirements stipulated in legislation. This caused a lot of questions, as it largely contradicts the forming global practice and factual circumstances.

Besides, the expectations were not met that the Law on digital financial assets would regulate the both the process of initial placement of digital financial assets (ICO), and the procedure of issuance and circulation of virtual currency and mining. As for the features of investing using blockchain-based digital instruments, they continue causing disputes in the Russian juridical community (Sarnakov, 2019).

When considering and adopting the Law on digital financial assets, the Central Bank of the Russian Federation, Ministry of Economic Development of the Russian Federation, Federal Agency for Financial Monitoring and Prosecutor General's Office of the Russian Federation, acting, as was mentioned above, initially concordantly, expressed opposing positions in regard to how DFA should be regulated; this gravely hindered the law adoption and resulted in three serious changes in the law draft wording (Emtseva & Morozov, 2018).

Difficulties with adopting the Law on digital financial assets showed that a Russian legislator failed to quickly define was cryptocurrency and DFA are and how to regulate them. At the same time, in the final version of the draft law the legislator marked that the said cryptographic tools exist, but failed to comprehensively explain how they are regulated. Hence, the order of their circulation was largely left without legal regulation.

Meanwhile the fact that cryptocurrency is considered as a potential object of civil rights shows that in the nearest future one should expect the adoption of a normative legal act regulating the order of its using.

As for the digital financial assets called tokens in the cryptographic community, most of the provisions of the said Law are devoted to them and the procedure of their issuance. In this regard, it seems an urgent necessity to study what risks and advantages they have

for the Russian investors and other financial market participants, and whether they correspond to the trends of digital economy development.

Prior the adoption of the said Law, Russian scholars expressed various concerns related to tokens. In particular, they marked that the existing legal regimes of the civil rights' objects might be substituted for the token legal regime (Savelyev, 2018) and emphasized that a problem arises how to define the character of rights to tokens and means of legal protection for their owners (Belykh & Bolobonova, 2019). Besides, certain concerns were expressed regarding difficulties with taxation (Troyanskaya et al., 2020; Grigoriev, 2020).

Thus, adoption of the on digital financial assets determines the need to consider the main provisions of the legislation referring to digital financial assets, its influence on the financial market and investors, and the sphere of financial technologies.

The finally adopted version of the draft law is largely similar to its second version, but contains fewer prohibitions and restrictions applied to the digital tokens circulation. The Russian researchers call this variant a compromise, unlike the previous two (Rozhdestvenskaya & Guznov, 2020). Indeed, many provisions barring DFA legalization were excluded from its text.

Although the adopted approach to regulating DFA and their issuance was generally rather fully reflected in the said normative act, it still has significant drawbacks, in particular, due to the issues of determining the legal status of the instruments under consideration.

According to Article 1 of the said Law, digital financial assets are essentially a certain object existing in the digital form and certifying corporate rights of their owner. This thesis directly follows from part 4 of Article 1 of the Law, according to which the issues of digital tokens issuance, if they certify the rights to securities, are subsidiarily regulated by Federal Law of April 22, 1996 No. 39-FZ "On securities market"[10] taking into account the features stipulated by the Law on digital financial assets.

From the above it is obvious that in the Law on digital financial assets the definition of digital financial assets stems from the notion of token inferred in the cryptographic community, but significantly narrows it. Besides, the law does not stipulate dividing digital financial assets into various types depending on their purpose. This does not account for the actual situation, within which investment, raw materials, utility, hybrid and other types of tokens exist. While investment tokens confirm the right to participate in a company management, utility tokens do not possess this quality and only confirm the right to a certain item (service) or a discount. Both types of tokens cardinally differ from each other; hence, they require different approaches to regulating their issuance and circulation.

[10] "On securities market" No. 39-FZ of 22.04.1996. (1996). *Collection of legislation of the Russian Federation*, 17, Article 1918.

At the same time, hybrid digital financial assets (the Law on digital financial assets does not directly stipulate but implies the possibility of their issuance) are digital rights comprising DFA and other digital rights. In other words, hybrid DFA have signs of both digital financial assets and utilitarian digital right.

In connection with this, adoption of a single procedure of issuance and accounting of all digital assets in a single mechanism makes doubtful the possibility of legal circulation of certain types of tokens in Russia. This step of a Russian legislator cannot be estimated as positive. We assume it is appropriate to demarcate between types of tokens, as differences in their purposes determine the different order of their circulation and use, which also needs legal regulation in order to eliminate the probable controversies and to form clear mechanisms of issuance and circulation of the respective assets.

Thus, the Law on digital financial assets does not contain a clear, complying with the modern realities, definition of tokens, does not reveal their actual properties. It just lists the rights which the tokens may conform. We believe this situation is a serious gap in legislation and will not promote clearance in the sphere of legal regulation of digital technologies. In this connection, a Russian legislator should make amendments in the law or issue a special clarification, which would allow distinguishing between various types of digital financial rights.

Stemming from clause 5 of Article 1 of the Law on digital financial assets, Russian legislation is applied to initial token placement (ICO). This rule is applied even when digital tokens are issued with participation of foreign legal persons. Such legal stipulation confirms the dominion of the Russian legislation, which cannot be called an excessive restriction. It corresponds to the international trends referring to ICO.

For example, in Singapore, which is justly recognized as one of the leaders in digitalization, clause 339 of the Law on securities and futures stipulates that, in case a Singapore citizen purchases digital tokens, Singapore legislation is applied exterritorialy to a foreign operator of the platform where such digital tokens are placed (Gorian, 2020). Hence, the persons executing ICO and located outside Singapore must have a respective license, issued by a competent body of that state. Such approach ensures a legal basis for legal prosecution of platform operators regardless of their location and the place of crime. Thus, exterritorial application of the Russian legislation to the persons executing ICO in Russia can be estimated as positive, but the competent bodies should provide official clarifications for the foreign organizations attracting the funds of Russian investors to understand the consequences of activity in Russia.

Also, it is necessary to decide how ICO will be regulated if the Russian legislation contradicts to the foreign one. These issues are extremely important and must be solved when elaborating the regulatory legislation in pursuance of Federal Law of July 31, 2020 No. 259-FZ “On digital financial assets, digital currency and making changes in certain legislative acts of the Russian Federation”. We believe, if a token is initially issued

in the Russian segment by a person located within the Russian jurisdiction, the Russian legal regulation must be prioritized.

Articles 2, 3, and 15 of the Law on digital financial assets stipulate the ICO rules. Thus, ICO can be performed solely by a nonpublic joint stock company. At the same time, only a licensed organization may register the issuance of tokens and keep records of operations performed with them. This requirement is aimed at protecting the rights of investors and maintaining the stability of the stock market.

ICO can be carried out only based on the decision complying with the requirements of Article 3 of the Law on digital financial assets. In particular, a decision on issuance of digital financial assets must contain information on the emitter of digital tokens; information on the type of rights certified by tokens, number and price of tokens, and the means of their payment; information on the operator of the information system in which digital financial assets are issued, etc.

Although the list of information which must be reflected in the decision on this issue is rather broad, the Central Bank of Russia is entitled to set additional requirements to the decision on issuance of digital financial assets. This demonstrates its key role in issuing by-laws in the sphere of digital financial assets.

Given that the placement of tokens takes occurs in a digital environment, a legislator stipulated the requirement that the decision on DFA issuance must be signed with an enhanced qualified electronic signature and placed on the website of emitter and operator of the information system. This provision of law allows guaranteeing that the decision on tokens issuance actually comes from a person entitled to do it.

Analyzing of the provisions of the Law on digital financial assets and comparing them with the rules of shares issuance allows concluding that the Russian legislation has maximally approximated the ICO rules to the way shares are issued. As it clearly stems from the Law, the Russian approach to DFA is analogous to the approach to securities regulation (Alekseenko, 2020). It is not a russian invention. For example, in Singapore, according to the Law on securities and futures, a token is viewed as a digital expression of a security. Other countries also have an experience of applying the legislation on securities to tokens.

Adoption of the Law on digital financial assets in Russia is one of the most important events in the country. It will help to draw a significant segment of digital economy out of the shadow. Despite the striving, manifested in 2018, to maintain balance between the total control and “anarchy” in legal relations associated with digital assets, a legislator still opted for stricter control. This was done to protect the rights of investors, but at the same time to protect the state interests in the financial sector. The state, by strictly establishing control over the circulation of digital financial assets, will, on the one hand, reduce its risks, and on the other hand, will manage to provide judicial protection to the deceived investors. Meanwhile, the feasibility of the methods chosen in Russia to regulate the activity of ICO operators still causes doubts. The adopted rules provide more advantages to large investment banks and IT companies. This may negatively influence the development of start-ups.

3. Prospects of development of legal regulation of digital financial assets in the Russian Federation

After the adoption of the Federal Law of July 31, 2020 No. 259-FZ, the Federal Taxation Service (further – FTS of Russia) proposed to make respective amendments into the Taxation Code of the Russian Federation. Upon the anvil, the draft law was repeatedly criticizes by experts in the field of finance, but ultimately the amendments to the respective legislation were approved in the first reading by the State Duma of the Russian Federation in February 2021.

One of the proposals by FTS of Russia was introduction of a tax on cryptocurrency, as it was officially equaled to property assets. Also, FTS of Russia considers it necessary to oblige all citizens possessing DFA and other cryptoassets to notify about the execution of transactions exceeding 600 thousand rubles. It is proposed to fine for delay in submitting this information – 10 % of the sum of transactions executed, and 40 % for evading taxes on cryptocurrencies. FTS of Russia proposed that these notifications are made prior to April 30 of the respective year.

In turn, Ministry of Finance of the Russian Federation started elaborating amendments to the Russian Criminal Code: repeated evasion of taxes by the results of the said activity was proposed to be fined, punished with compulsory labor, and in some cases with incarceration, if the sum of operation executed during three years is large or especially large. However, many of the issues and questions considered were not fully implemented so far.

Notably, although the Federal Law of July 31, 2020 No. 259-FZ laid the bases of regulating the digital financial sector, it is far from perfect. This is due to the fact that today there is no answer to the question, what physical and legal persons should do for the investments into cryptocurrencies and DFA or operations with cryptocurrencies and DFA not to bear substantial risks related to violation of legislation.

On the positive side, one should mention that the said law demarcates such notions as digital currencies and digital financial assets. The notion of digital currencies, stipulated by the law, largely corresponds to the classical approach to the definition of cryptocurrencies, that is, coins emitted an independent blockchain. At that, a legislator marks that with regard to the digital currencies, representing a set of electronic data contained in the information system, there is no person obliged to any owner of such electronic data. At the same time, digital financial assets, as was mentioned above, are by definition closer to cryptographic tokens (just partially, though), which, in turn, function on the basis of the existing blockchains of individual cryptocurrencies. This allows making a conclusion that the said Law distinguishes between cryptocurrencies, like Bitcoin or Ethereum, and digital financial assets, like DAI token, functioning within the Ethereum blockchain ecosystem, or TRC-20, using the blockchain of a Tron digital currency. This approach largely corresponds to the modern cryptographic realities, and

we consider it expedient to continue developing the Russian legislation through the prism of this position.

At the same time, the Law contains blanket norms, according to which the legal regulation of digital currencies' circulation is carried out in compliance with federal legislation. However, such federal legislation has not been so far adopted in the established order. This is explained both by the existing difficulties in determining the effective approaches to legislative regulation of cryptocurrencies, and by the need to maintain the balance between the interests of the state controlling the financial flows taking place in its territory and the users, who are attracted to cryptocurrencies by the absence of an external authoritative regulator. As a result, in the territory of the Russian Federation no restrictions or special conditions are stipulated for acquisition and selling of cryptocurrency, except specific cases listed in special legislation or internal departmental instructions. For example, according to Information Letter by the Russian Ministry of Labor of December 16, 2020 No. 18-2/10/B-12085[11], officials and the staff of security agencies are not allowed to buy and sell cryptocurrency.

Another problem is certain aspects related to regulating the activity of exchange systems and digital stock exchanges. Assumingly, the law defines them as "operators of exchange of digital financial assets", and this definition generally correlates with the existing approach to defining crypto stock exchanges and crypto exchange offices. At the same time, there are still unanswered questions, whether foreign exchange platforms and system are recognized in the territory of the Russian Federation, what the order of operators' licensing is, as well as jurisdictional interaction and regulation of liability for the violation of users' right.

Similar questions arise regarding the order of emitting digital currencies and digital financial assets. Certain aspects associated with counteraction to money laundering, distribution of drugs, corruption crimes are stipulated in special legislation. However, the general order of licensing the emitters of cryptocurrencies and tokens in the territory of the Russian Federation is not established, which creates difficulties in providing the due level of protection of the rights of citizens and participants of the digital assets' circulation.

The described problems open up a wide range of promising directions of development both for the Russian legislation and for digitalization of various aspects of social life, as well as increasing the efficiency of interaction between the citizens and the state.

Besides the above-mentioned, such directions include improving interaction and reaching the balance between large banking institutions and small and middle-sized finance-credit organizations. The specificity of digital transactions today is that small companies and physical persons can take an active part in them. However, large finance-credit organizations

[11] Letter by the Russian Ministry of Labor No. 18-2/10/B-12085 of December 16, 2020. https://mintrud.gov.ru/docs/mintrud/employment/62

are most often well-equipped with qualified staff and technical devices, enabling them to pursue a more aggressive market policy, establish exorbitant prices to their services, oust other participants of the financial services sector. However, as the practice of emergence and development of cryptocurrencies shows, there is currently an urgent need in the society to reduce dependence on external regulators, including by distributing liability among a large number of market participants in order to decrease the level of influence of large actors on economy both in the private segment and at the global level.

At that, it is important to maintain the balance which would allows the state, in the person of authorized executive bodies, including the Central Bank of the Russian Federation, to provide sustainability of a large amount of relatively disjoint digital financial ecosystems and to control their activity without restricting their development. Solution of these tasks is considered to be an extremely complicated but important prospective direction of the development of the digital financial assets market in Russia. The efficient implementation of this task largely determines the future of the country, and given the current political realities, also the possibility of survival of certain sectors of economy.

Based on the above, we may conclude that the further effective functioning and development of the state requires both specifying certain legislative acts and elaborating, actually from inception, a broad range of normative regulation of the new spheres of digital transformation of the society. The key in this process will be not only a balance of the system constructed but also efficiency of reducing the risks of data leakage and unauthorized access to the broadening private digital world.

Conclusion

Thus, the legislation novel in the sphere of DFA introduces substantial restriction, but at the same time opens certain opportunities for developing business in operations with digital financial assets. Analysis has shown that the terminology used in the Law on digital financial assets does not always correspond to the concepts and standards established in the international legal and business practice, as well as to modern realities.

The transition from the traditional system of financial services rendering to the digital one offers a lot of opportunities for both large actors and promising startups to work with financial organizations and assets. However, the reverse side is that the global financial market is entered by large technological companies, which receive more and more instruments to broaden their influence in the global market. This generates a number of risks and barriers, among which of primary importance are the risks of economic sectors monopolization. At the same time, the digital transformation becomes a part of objective reality and its pace is not likely to slow down in the nearest future, including in the territory of the Russian Federation.

Moreover, the current geopolitical realities create serious grounds for a Russian legislator paying more attention to the said technologies, allow considering them to be a means of strategic maneuvering, lifting the sanction pressure on the economy and unblocking

certain financial processes, implementing seamless payments for goods and services supplied by foreign partners, and fulfilling the contracted debts.

This is reflected in the decisions made recently. For example, on September 13, 2022, Chairman of the Government M. V. Mishustin tasked the Ministry of Finance of the Russian Federation, the Central Bank of the Russian Federation and other departments in follow-up of the strategic session of August 30, devoted to the country's financial development. The tasks include a large block of instructions regarding the development of digital currencies and digital financial assets. Up to December 1, 2022, the Ministry of Finance in cooperation with the Central Bank must submit coordinated proposals on developing the digital financial assets market in the country, including the use of decentralized technologies, and taking these proposals into account, implement a complex of measures to improve the Russian legislation in 2023.

Based on the above, allows concluding that the issues of legal regulation of digital financial assets will be substantially reviewed and broadened in the nearest future. However, we believe that for these changes to be really effective and reflect the modern trends, they must be implemented in cooperation with respective specialists and representatives of the academic community, engaged in the analysis of the issues of a legal status of blockchain technology and digital tools created on its basis.

References

Alekseenko, A. P. (2020). Russian approach to ICO regulation. *RevistaGênero e Direito*, *9*(4), 874–881.

Basilio, T. A. (2019). Investment (security) tokens: a captação de fundosatravés de initial coin offerings e-token sales. *Revista de direitofinanceiro e dos mercados de capitais*, *1*(2), 127–168.

Belykh, V. S., & Bolobonova, M. O. (2019). Legal regulation of digital financial assets in Russia: controversial issues of theory and practice. *Russian Law: Theory and Practice*, *2*, 38–47.

Emtseva, S. S., & Morozov, N. V. (2018). Comparative analysis of legal regulation of ICO in selected countries. *KnE Social Sciences*, *3*(2), 77–84. https://doi.org/10.18502/kss.v3i2.1527

Garcia-Teruel, R. M. (2019). A legal approach to real estate crowdfunding platforms. *Computer Law & Security Review*, *35*(3), 281–294. https://doi.org/10.1016/j.clsr.2019.02.003

Garcia-Teruel, R. M. (2020). Legal challenges and opportunities of blockchain technology in the real estate sector. *Journal of Property, Planning and Environmental Law*, *12*(2), 129–145. https://doi.org/10.1108/jppel-07-2019-0039

Garcia-Teruel, R. M., & Simón-Moreno, H. (2021). The digital tokenization of property rights. A comparative perspective. *Computer Law & Security Review*, *41*. https://doi.org/10.1016/j.clsr.2021.105543

Gorian, E. (2020). Singapore's cybersecurity act 2018: A new generation standard for critical information infrastructure protection. *Smart Innovation, Systems and Technologies*, *138*, 1–9. https://doi.org/10.1007/978-3-030-15577-3_1

Grigoriev, V. V. (2020). Regulation of token taxation based on the Australian experience. *Economics, Taxes & Law*, *2*, 146–154. (In Russ.). https://doi.org/10.26794/1999-849X2020-13-2-146-154

Ishmaev, G. (2017). Blockchain Technology as an Institution of Property. *Metaphilosophy*, *48*(5), 666–686. https://doi.org/10.1111/meta.12277

Konashevych, O. (2020). General concept of real estate tokenization on blockchain the right to choose. *European Property Law Journal*, *9*(1), 1–45. https://doi.org/10.1515/eplj-2020-0003

Kudryashova, E. V. (2018). Legal regulation of cryptocurrencies: choosing the vector of development. *Finansovoye pravo*, *6*, 7–11. (In Russ.).

Raskin, J. (2017). The law and legality of smart contracts. *Georget Law Technol. Rev.*, *305*, 1–37.

Rozhdestvenskaya, T. E., & Guznov, A. G. (2020). Digital financial assets: problems and prospects of legal regulation. *Aktualniye problemy rossiyskogo prava*, *15*(6), 43–54. (In Russ.). https://doi.org/10.17803/1994-1471.2020.115.6.043-054

Ryzhov, N. A. (2018). Analysis of the Prospects of Legal Regulation of Cryptocurrencies within the Framework of Ensuring National and International Security. *Juris*, *5*, 63–67. (In Russ.). https://doi.org/10.18572/1812-3929-2018-5-63-67

Sarnakov, I. (2019). Digital financial assets: segments and prospects of legal regulation in the BRICs countries. *BRICS Law Journal*, *4*, 95–113. https://doi.org/10.21684/2412-2343-2019-6-4-95-113

Savelyev, A. (2017). Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law. *Information & Communications Technology Law*, *26*(2), 116–134. https://doi.org/10.1080/13600834.2017.1301036

Savelyev, A. (2018). Some risks of tokenization and blockchainizaition of private law. *Computer Law and Security Review*, *34*(4), 863–869. https://doi.org/10.1016/j.clsr.2018.05.010

Troyanskaya, M., Tyurina, Y., & Ermakova, E. (2020). Taxation of digital financial assets: international practices and comparative legal analysis. *Talent Development & Excellence*, *12*(2), 1413–1421. https://doi.org/10.1007/978-3-030-15160-7_125

Vasilevskaya, L. Yu. (2019). Token as a new civil rights object: issues of legal classification of digital law. *Actual Problems of Russian Law*, *5*(102), 111–119. (In Russ.). https://doi.org/10.17803/1994-1471.2019.102.5.111-119

Verheye, B. (2017). Real estate publicity in a blockchain world: a critical assessment. *European Property Law Journal*, *6*(3), 441–477. https://doi.org/10.1515/eplj-2017-0020

Yapicioglu, B., & Leshinsky, R. (2020). Blockchain as a tool for land rights: ownership of land in Cyprus. *Journal of Property, Planning and Environmental Law*, *12*(2), 171–182. https://doi.org/10.1108/JPPEL-02-2020-0010

Author information

Artem P. Peretolchin – Candidate of Juridical Sciences, Senior Lecturer, Department of Civil-legal Disciplines, East Siberia Institute of the Ministry of Internal Affairs of the Russian Federation
Address: 110 Lermontov Str., 664074 Irkutsk, Russian Federation
E-mail: peretat@gmail.com
ORCID ID: https://orcid.org/0000-0003-1319-8119
RSCI Author ID: https://elibrary.ru/author_items.asp?authorid=735650

Conflict of interest

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 – February 1, 2022
Date of approval – April 23, 2023
Date of acceptance – August 15, 2023
Date of online placement – August 20, 2023

Научная статья
УДК 34:342.739:004
EDN: https://elibrary.ru/hlhzbu
DOI: https://doi.org/10.21202/jdtl.2023.33

Генезис и перспективы развития правового регулирования цифровых финансовых активов в Российской Федерации

Артем Павлович Перетолчин

Восточно-Сибирский институт Министерства внутренних дел Российской Федерации
г. Иркутск, Российская Федерация

Ключевые слова

Блокчейн,
законодательство,
криптовалюта,
право,
правовое регулирование,
распределенный реестр,
токен,
цифровые права,
цифровые технологии,
цифровые финансовые активы

Аннотация

Цель: исследование существующих проблем и перспективных направлений правового регулирования цифровых финансовых активов как относительно нового инструмента современной цифровой экономики.

Методы: методологической основой работы выступает совокупность методов научного познания, таких как теоретический анализ, исследование, сопоставление, синтез, а также обобщения научной литературы.

Результаты: в работе рассмотрены существующие подходы к правовому регулированию цифровых финансовых активов в Российской Федерации и отдельных зарубежных странах, выявлены существующие пробелы отечественного законодательства в области обращения цифровых финансовых активов, дана оценка перспективам развития правового регулирования указанных инструментов и сформированы предложения по его совершенствованию. Кроме того, в процессе исследования проанализированы подходы к правовому регулированию цифровых валют и цифровых финансовых активов, принятые в ряде иностранных государств, рассмотрены тенденции и отражены положительные и отрицательные моменты использования криптографических алгоритмов для целей экономической и юридической сфер глобальной экономики.

Научная новизна: в рамках работы рассмотрены актуальные вопросы законодательного регулирования такого относительно нового явления, как цифровые финансовые активы. Проанализированы позиции отечественных и иностранных ученых-правоведов относительно существующих проблем и рисков, связанных с «токенизацией»

и «блокчейнизацией» частного права. Помимо этого, в процессе исследования автор статьи приходит к выводу о существовании значительных пробелов в существующем подходе правового регулирования цифровых финансовых активов, указывает на них и предлагает отдельные механизмы решения данных проблем.

Практическая значимость: обусловлена несовершенством существующего законодательства в сфере регулирования отношений, возникающих в процессе использования технологий, базирующихся на базе распределенного реестра, в том числе цифровых финансовых активов. Исследование данных проблем позволяет оценить риски, рассмотреть существующие пути преодоления и разрешения возникающих дискуссионных вопросов. Кроме того, полученные в результате исследования выводы можно использовать для совершенствования отечественного законодательства, а также в учебной литературе, посвященной актуальным вопросам развития цифрового законодательства.

Для цитирования

Перетолчин, А. П. (2023). Генезис и перспективы развития правового регулирования цифровых финансовых активов в Российской Федерации. *Journal of Digital Technologies and Law*, *1*(3), 752–774. https://doi.org/10.21202/jdtl.2023.33

Список литературы

Василевская, Л. Ю. (2019). Токен как новый объект гражданских прав: проблемы юридической квалификации цифрового права. *Актуальные проблемы российского права*, *5*(102), 111–119. https://doi.org/10.17803/1994-1471.2019.102.5.111-119

Григорьев, В. В. (2020). Регулирование налогообложения токенов на основе австралийского опыта. *Экономика. Налоги. Право*, *2*, 146–154. https://doi.org/10.26794/1999-849X2020-13-2-146-154

Кудряшова, Е. В. (2018). Правовое регулирование криптовалют: выбор вектора развития. *Финансовое право*, 6, 7–11.

Рождественская, Т. Э., Гузнов, А. Г. (2020). Цифровые финансовые активы: проблемы и перспективы правового регулирования. *Актуальные проблемы российского права*, *15*(6), 43–54. https://doi.org/10.17803/1994-1471.2020.115.6.043-054

Рыжов, Н. А. (2018). Анализ перспектив правового регулирования криптовалют в рамках обеспечения национальной и международной безопасности. *Юрист*, *5*, 63–67. https://doi.org/10.18572/1812-3929-2018-5-63-67

Alekseenko, A. P. (2020). Russian approach to ICO regulation. *Revista Gênero e Direito*, *9*(4), 874–881.

Basilio, T. A. (2019). Investment (security) tokens: a captação de fundos através de initial coin offerings e-token sales. *Revista de direito financeiro e dos mercados de capitais*, *1*(2), 127–168.

Belykh, V. S., & Bolobonova, M. O. (2019). Legal regulation of digital financial assets in Russia: controversial issues of theory and practice. *Russian Law: Theory and Practice*, *2*, 38–47.

Emtseva, S. S., & Morozov, N. V. (2018). Comparative analysis of legal regulation of ICO in selected countries. *KnE Social Sciences*, *3*(2), 77–84. https://doi.org/10.18502/kss.v3i2.1527

Garcia-Teruel, R. M. (2019). A legal approach to real estate crowdfunding platforms. *Computer Law & Security Review*, *35*(3), 281–294. https://doi.org/10.1016/j.clsr.2019.02.003

Garcia-Teruel, R. M. (2020). Legal challenges and opportunities of blockchain technology in the real estate sector. *Journal of Property, Planning and Environmental Law*, *12*(2), 129–145. https://doi.org/10.1108/jppel-07-2019-0039

Garcia-Teruel, R. M., & Simón-Moreno, H. (2021). The digital tokenization of property rights. A comparative perspective. *Computer Law & Security Review*, *41*. https://doi.org/10.1016/j.clsr.2021.105543

Gorian, E. (2020). Singapore's cybersecurity act 2018: A new generation standard for critical information infrastructure protection. *Smart Innovation, Systems and Technologies*, *138*, 1–9. https://doi.org/10.1007/978-3-030-15577-3_1

Ishmaev, G. (2017). Blockchain Technology as an Institution of Property. *Metaphilosophy*, *48*(5), 666–686. https://doi.org/10.1111/meta.12277

Konashevych, O. (2020). General concept of real estate tokenization on blockchain the right to choose. *European Property Law Journal*, *9*(1), 1–45. https://doi.org/10.1515/eplj-2020-0003

Raskin, J. (2017). The law and legality of smart contracts. *Georget Law Technol. Rev.*, *305*, 1–37.

Sarnakov, I. (2019). Digital financial assets: segments and prospects of legal regulation in the BRICs countries. *BRICS Law Journal*, *4*, 95–113. https://doi.org/10.21684/2412-2343-2019-6-4-95-113

Savelyev, A. (2017). Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law. *Information & Communications Technology Law*, *26*(2), 116–134. https://doi.org/10.1080/13600834.2017.1301036

Savelyev, A. (2018). Some risks of tokenization and blockchainizaition of private law. *Computer Law and Security Review*, *34*(4), 863–869. https://doi.org/10.1016/j.clsr.2018.05.010

Troyanskaya, M., Tyurina, Y., & Ermakova, E. (2020). Taxation of digital financial assets: international practices and comparative legal analysis. *Talent Development & Excellence*, *12*(2), 1413–1421. https://doi.org/10.1007/978-3-030-15160-7_125

Verheye, B. (2017). Real estate publicity in a blockchain world: a critical assessment. *European Property Law Journal*, *6*(3), 441–477. https://doi.org/10.1515/eplj-2017-0020

Yapicioglu, B., & Leshinsky, R. (2020). Blockchain as a tool for land rights: ownership of land in Cyprus. *Journal of Property, Planning and Environmental Law*, *12*(2), 171–182. https://doi.org/10.1108/JPPEL-02-2020-0010

Сведения об авторе

Перетолчин Артем Павлович – кандидат юридических наук, старший преподаватель кафедры гражданско-правовых дисциплин, Восточно-Сибирский институт Министерства внутренних дел Российской Федерации
Адрес: 664074, Российская Федерация, г. Иркутск, ул. Лермонтова, 110
E-mail: peretat@gmail.com
ORCID ID: https://orcid.org/0000-0003-1319-8119
РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=735650

Конфликт интересов

Автор заявляет 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: 10.19.43 / Правовой режим информационных ресурсов
Специальность ВАК: 5.1.2 / Публично-правовые (государственно-правовые) науки

История статьи

Дата поступления – 1 февраля 2023 г.
Дата одобрения после рецензирования – 23 апреля 2023 г.
Дата принятия к опубликованию – 15 августа 2023 г.
Дата онлайн-размещения – 20 августа 2023 г.

Research article
DOI: https://doi.org/10.21202/jdtl.2023.34

Improving the System of Mandatory Requirements to Business under the Digital Transformation of Economy

Svetlana A. Minich

National Centre for Legislation and Legal Research of the Republic of Belarus
Minsk, Republic of Belarus

Keywords

Business activity,
business,
deregulation,
digital technologies,
economy,
law,
legal regulation,
legislation,
mandatory requirements,
regulatory guillotine

Abstract

Objective: to elaborate scientifically substantiated proposals for improving the system of mandatory requirements in the sphere of business and other economic activity under formation of digital economy, taking into account the foreign experience of eliminating barriers for business and the available practice of legislation optimization in this sphere.

Methods: the research methodological basis consists of traditional general and specific methods of scientific cognition: dialectical, formal-logical, historical-comparative, systematic, terminological, general logic methods (analysis, synthesis, generalization, induction, deduction, etc.), as well as special methods: historical-legal, formal-legal, and method of comparative jurisprudence.

Results: the author investigated and systematized theoretical approaches and experience of improving the system of mandatory requirements in foreign countries and the Russian Federation; the possibilities of introducing the most successful innovative legal instruments and practices to improve the regulation of economic relations were considered. The role of a retrospective assessment of the regulatory impact of existing regulatory legal acts containing mandatory requirements in addressing issues of reducing burdensome rules and ensuring legal stability in the context of digital transformation of the economy was determined. The international experience of implementing the regulatory guillotine

mechanism was considered; its essence, purpose, tasks, basic principles, and algorithm of operation were revealed. The issues of establishing and evaluating the application of the requirements for business contained in regulatory legal acts were analyzed.

Scientific novelty: the author's comprehensive analysis of existing scientific developments on improving the system of mandatory requirements for business; systematization of scientific and theoretical approaches to the selection of innovative legal instruments to eliminate excessive legal regulation of economic relations; generalization of successful foreign practices in the implementation of "regulatory guillotine" measures.

Practical significance: recommendations were developed for effective reduction of burdensome requirements that negatively affect the development of business in the context of digital transformation of the economy. Conditions were determined for the implementation of a full-fledged regulatory impact assessment procedure and the successful implementation of regulatory reforms. The results of the study can be used in standard-setting activities and in the educational process when elaborating educational programs in Economics and Law.

For citation

Minich, S. A. (2023). Improving the System of Mandatory Requirements to Business under the Digital Transformation of Economy. *Journal of Digital Technologies and Law, 1*(3), 775–802. https://doi.org/10.21202/jdtl.2023.34

Contents

Introduction

Under transition to a new technological and innovative reality, global digital transformations, the process of maintaining the current regulatory framework in an up-to-date state is a rather difficult task. Many norms and rules are becoming outdated, formal and redundant. The habitual legislative mechanisms cannot always quickly cope with the increasing volume of burdensome requirements for business in a certain area, which blocks the entrepreneurial activity development and facilitating the search for effective deregulation tools in order to streamline and optimize legislation.

Today, creating an effective system of mandatory requirements is a serious problem in many countries, the solutions to which often lead to the introduction of a full-fledged assessment of the regulatory impact of legislative acts containing mandatory requirements (including retrospective assessment), and to the use of some of the latest regulatory technologies, among which the regulatory guillotine is gaining the utmost popularity.

The advanced experience of some countries in improving the mandatory requirements system makes it possible to consider the introduction of the most successful innovative legal instruments and practices to improve the legislation regulation system in the economic sphere. The analysis of the implemented reforms also demonstrated that the "regulatory guillotine" is not used everywhere in the world in its pure form; some countries are developing their own mechanisms of deregulation (legislation with a self-expiring regulatory period, the principle of regularity of legislative revision, etc.). But their essence is the same – reducing excessive regulation when doing business in order to ensure sustainable economic growth and social well-being in the country by artificially restraining or terminating legal regulations as opposed to their arbitrary exclusion (Rowthorn et al., 2017). In addition, it should be borne in mind that any reform program is a multifaceted strategy that must be adapted to the priorities, institutions and public expectations of a particular country.

1. Directions for improving the system of mandatory requirements under the digital transformation of economy

1.1. Problems of legal regulation of economic relations caused by digitalization processes

The economic sphere has always been one of the most important in the life of society. The introduction of advanced digital technologies is transforming the traditional economy, opening up new market niches, improving the quality, availability and speed of services, changing market conditions, ways of doing business and making a profit, adjusting production to the individual tastes of consumers. The formation of a digital economy that meets the requirements of modern reality is achieved through an active dialogue between the law, business, society and government, through concentrating the state efforts on the effective regulation development using the latest regulatory technologies (RegTech), aimed,

among other things, at eliminating the bureaucratic burden, maximizing the reduction of unnecessary, burdensome rules and procedures that create certain obstacles to business development (Chao et al., 2022).

Under the changing regulatory paradigm, many countries are searching for and implementing the most successful innovative legal instruments and practices to improve the national regulatory system, striving to make it more flexible, consistent, responsive to market and technological changes and enjoying great confidence from the part of business. Despite the steps already taken by a number of states in the direction of updating, streamlining the legislative array and harmonious development of public relations in the economic sphere, the issues of creating a favorable regulatory environment are still on the agenda today.

Speaking about the improvement of legal regulation in the field under study, it is necessary to disclose the content of this concept in order to clearly identify its problem field and, through the adoption of innovative regulatory solutions, to seamlessly adapt it to the new technological reality. The analysis of the definitions established in legal science and available in legislation has shown that within the framework of the general theory of law, legal regulation is the impact of law on various groups of public relations[1]. S. S. Alekseev interpreted legal regulation as effective regulatory-organizational impact on public relations carried out with the help of a system of legal means (Alekseev, 1966).

The object of legal regulation per se may also be some of the most significant public relations. In particular, the legal regulation of economic relations associated with entrepreneurial activity is understood as a set of measures taken and applied by the state in relation to the recipients of regulation, including, first of all, the establishment of mandatory requirements for business entities, as well as permissive, notification and controlling (supervisory) procedures and measures of influence on persons who have violated mandatory requirements[2]. Based on the content of the concept of legal regulation in the field under study, it is possible to determine the sequence of its elements: the establishment of mandatory requirements (rules, standards); monitoring their compliance; the application of liability measures in case of their violation. The set of mandatory requirements acts as the foundation for regulating economic relations, the violation of which can lead to liability of a controlled entity or to other adverse consequences for business, as well as affect security in the regulated sphere of public relations.

---

1 Kudryavtsev, Yu. A. (2020). Legal deregulation of business activity (assessment and risks of the use of the "regulatory guillotine" in modern Russia). In: *Novellas of Law, Economics and Management 2019: collection of scientific works based on the materials of the 5th International scientific and practical conference, Gatchina, November 22, 2020* (pp. 97–102). Gatchina: State Institute of Economics, Finance, Law and Technologies.

2 On adopting the Rules for regulating services trade, institutions and activities: Decision of the Supreme Eurasian Economic Council No. 24 [adopted in St. Petersburg on December 26, 2016]. (2022). *ETALON*. Legislation of the Republic of Belarus. Minsk.

The above allows concluding that the qualitative and rational construction of a system of mandatory requirements, understandable both for business and for regulatory and supervisory authorities, is the foundation for effective legal regulation of economic activity in the digital reality. The effective, without incurring disproportionate costs, fulfillment of the established mandatory requirements by their addressees contributes to the formation of favorable and stimulating conditions for the development of all economic sectors and positively affects the overall business climate. Therefore, these requirements must be relevant, feasible, clear, and reasonable; they must correspond to the level of development of digital technologies, meet the needs and principles of a market economy (Polemis & Stengos, 2020).

However, despite all efforts on the part of the majority of states to ensure legal stability in the regulatory space, the transition to digital economy, the active introduction of innovative technologies has been a serious factor in the emergence of certain difficulties in business regulation (Purnomo et al., 2022). According to Yu . I . Gribanov, in the course of the digital transformation of the economy, it is business activity that was affected by the instability of legal regulation to a greater extent, since the fullest disclosure of the digital technologies potential is provided primarily through their active use in all aspects of business: processes, products and services, and approaches to decision-making[3].

In particular, the responsiveness of the legislator to changes has decreased, a significant number of legal norms have appeared, which are largely formal, redundant and not meeting the requirements of the existing digital reality; this, undoubtedly, leads to excessive regulation of economic behavior and bureaucratic red tape, slows down economic growth, negatively affects the overall business climate, rights and interests of economic entities (Youssef et al., 2021). In addition, the presence of a sufficiently large number of spheres of public relations, within which mandatory requirements and their corresponding types of control (supervision) are grouped, is the reason that many requirements, due to the contiguity of their spheres, are redundant, contradict or completely duplicate each other and are often “scattered” along various regulatory legal acts. This does not allow creating an exhaustive list of them, as a result of which the controlled persons do not have a clear understanding of what exactly can be checked. The situation is further complicated by the fact that traditional approaches to regulation, for objective reasons, have already significantly exhausted their reserve, and the latest regulatory technologies have insufficient description, methodological basis and are poorly adapted to existing institutions and real legal relations. The situation is further complicated by the fact that traditional approaches to regulation, for objective reasons, have already significantly exhausted their reserve, and the latest regulatory technologies have insufficient description, methodological basis and are poorly adapted to existing institutions and real legal relations (Grassi & Lanfranchi, 2022).

[3] Gribanov, Yu. I. (2019). *Digital transformation of socio-economic systems based on the development of the institute of service integration*: abstract of doctoral (Economic Sciences) thesis: 08.00.05. Saint Petersburg.

Thus, in the sphere of control and supervisory activities, a situation has been formed that is disadvantageous for all the interested parties (controlled persons, regulatory authorities, society). This required, besides optimizing the types of state control and unifying implementation of all forms of control, also improving the system of mandatory requirements as part of the introduction of new approaches to regulating economic relations, including the use of the latest regulatory technologies, in order to effectively update regulatory requirements, to analyze the regulatory content of regulatory legal acts establishing mandatory requirements, to comprehensively review and systematize all requirements, and maximally reduce inefficient requirements imposed on business and adjust the existing ones, etc.

1.2. Introduction of the latest regulatory technologies to improve legislation and eliminate barriers for business

A steady attempt to change the nature of regulation of economic relations was the adoption of verified and consistent approaches to the process of norm-making through the use of such economic policy instruments as consulting mechanisms, measurement and reduction of the administrative burden, open access to the legislative framework, etc. In addition, in the formation of clear guidelines, rules and techniques for establishing mandatory requirements aimed at improving the quality of regulatory decisions, alongside with the legal technologies and analytical tools already used, a special role was played by the introduction and development of such legal institutions as the assessment of regulating (regulatory) impact (hereinafter – ARI), regulatory impact analysis (hereinafter – RIA) and assessment of the actual impact (hereinafter – AAI). The use of these legal instruments allowed bringing to a new level the processes of designing normative legal acts and forecasting the legal consequences of their adoption (Shaulova, 2017). The experience of using, for example, ARI (RIA) to improve state regulation of the economy is typical for most countries of the Commonwealth of Independent States, due to the high degree of their economic integration (a number of countries are members of the Eurasian Economic Union). However, the traditional regulatory technologies and analytical tools used to optimize and inventory the current legislation are often slow, expensive and time-consuming. This hinders keeping up with acceleration and timely solving the emerging problems in the economic sphere, controlling the risks associated with them and protecting the opportunities offered by technological development. Besides, a comparative analysis of the practices of the said innovative verification institutions in the areas of law-making and law enforcement showed the following.

A preliminary (forecast, ex-ante) assessment of regulatory impact is carried out in absolutely all countries of the Commonwealth of Independent States.

An ex post assessment, which determines the regulatory potential of the existing regulatory legal acts, is carried out only in the Russian Federation, the Republic of Kyrgyzstan and the Republic of Uzbekistan. In the Republic of Kazakhstan, the RIA is implemented only

with respect to those existing regulatory instruments and/or requirements that previously had not been subject to the RIA. However, the assessment of the actual impact of legislative acts, which replaced the expertise, is carried out only in the Russian Federation, in compliance with the rules of its implementation approved by the Government of the Russian Federation (see Table 1).

Table 1. Assessment of existing regulatory legal acts in the Commonwealth of Independent States

Country	Type of assessment	Legislation
Russian Federation	Assessment of the actual impact of regulatory legal acts regulating legal relations in the field of business and other economic activities	Decree of the Government of the Russian Federation No. 83 of January 30, 2015 "On the assessment of the actual impact of regulatory legal acts and on amendments to certain acts of the Government of the Russian Federation"
Republic of Kyrgyzstan	Assessment of the current regulatory legal acts regulating business activity	Law of the Republic of Kyrgyzstan No. 55 of April 5, 2008 "On optimization of the regulatory legal framework for regulating business activity"
Republic of Uzbekistan	Assessment of regulatory legal acts affecting business activity, rights, freedoms and legitimate interests of citizens, as well as the environment	Law of the Republic of Uzbekistan of April 20, 2021 No. ZRU-682 "On regulatory legal acts"
Republic of Kazakhstan	Assessment of compliance of existing regulatory instruments and/or requirements with the established conditions for their formation (Article 81-1 of the Business Code of the Republic of Kazakhstan)	Code of the Republic of Kazakhstan of October 29, 2015 No. 375-V "Business Code of the Republic of Kazakhstan"; Order of the Minister of National Economy of the Republic of Kazakhstan of November 30, 2015 No. 748 "On approval of the rules for conducting and using regulatory impact analysis of regulatory instruments and/or requirements"

In addition, most countries of the Commonwealth of Independent States stipulate an accompanying (monitoring, on-going) assessment of the regulatory impact of regulatory legal acts, which rapidly provides information on whether regulation really reaches the target groups to which it was directed, whether there are side effects, how fair and effective this regulation is from the viewpoint of such groups; this allows making the necessary adjustments in the act implementation process. The Institute of Legal Monitoring (monitoring of law enforcement) is actively developed in the Russian Federation, the Republic of Kazakhstan, the Republic of Armenia, the Republic of Uzbekistan, etc. The legal bases of this type of monitoring are also being formed in the Republic of Belarus.

As the analysis of the use of the said legal technologies shows, in most of the countries of the Commonwealth of Independent States there is no comprehensive assessment of regulatory impact formed as a single procedure; first of all, insufficient attention is paid to the retrospective assessment of already adopted regulatory legal acts. This is not fully justified, since at the stage of evaluation of draft legislative acts it is impossible

to comprehensively take into account changes in the internal and external environment, as well as to predict all the consequences of regulation in the process of implementing legal norms. Besides, under the rapid development of digital technologies and the legislator's desire to respond as quickly as possible to the emergence of new public relations in the economic sphere, mistakes often arise as early as at the stage of project development due to their poor and hasty preparation; undoubtedly, this negatively affects the quality of law enforcement, reducing the effectiveness of legislation implementation, and creates serious obstacles to doing business (Jakupec & Kelly, 2016). For example, Scott Jacobs, speaking about the problems associated with the poor quality of the laws adopted, noted that the laws adopted in a hurry are one of the main causes of the global financial crisis. According to the expert, such ill-conceived laws are a direct source of corruption and losses of the largest economies. If it is impossible to predict what the laws will be, then it is impossible to build a high-quality business plan[4].

In order to avoid all possible risks caused, among other things, by the poor quality of the laws adoption process, it is necessary to carry out a comprehensive and transparent review of all existing regulations on a cyclical, permanent basis. This is due to the fact that this process is a closed continuous regulatory cycle (development of mandatory requirements – evaluation of their action – correction based on the evaluation results). Thus, it is the transition to the full ARI cycle, providing for the consistent passage of all stages of assessment and revision of the established rules, including a qualitative retrospective assessment, that can become the key to high-quality legal regulation, without which it is impossible to avoid certain difficulties in solving issues related to business activity. Unfortunately, against the background of accelerating digitalization processes and technological progress in general, the machinery of government is intensively developing more and more new requirements for business. Over time, some of these requirements lose their relevance, which leads to certain conflicts in law, creates legislative blockages, prerequisites for unjustified expenses on the part of business, leads to serious overregulation of certain sectors of the economy (Haidar, 2012). Despite the huge potential of the already tested legal technologies (ARI, AAI and legal monitoring), these tools, even in their entirety, taking into account digital transformations, cannot provide an effective revision of all mandatory requirements, especially in terms of analyzing all outdated regulations. Such difficulties in regulation create prerequisites for the introduction of new innovative legal mechanisms for evaluating and optimizing the current legislation while maintaining and improving the work of existing ones. The approach providing for the implementation of a single comprehensive ARI procedure makes it possible to effectively prevent the unjustified expansion of the regulatory field. In addition, the widespread use of a whole range of analytical tools to optimize legislation in the context of the constant expansion of digital

[4] *Regulatory Impact Analysis: Best Practices in OECD Countries*. OECD PUBLICATIONS, 2, rue Andre-Pascal, 75775 PARIS.

opportunities in the economic sphere has become a trend, an actual practice of reforming legislation in many countries (Degtyarev, 2022a). This vector in improving the system of mandatory requirements and achieving stability in the regulation of economic relations is chosen because many countries wish to form an integrated regulatory policy combining various regulatory mechanisms and technologies into a single whole.

Under the digital development and globalization, the introduction of effective deregulation mechanisms contributed to the rapid reduction of burdensome regulations and ensured legal stability; one of such deregulation mechanisms is the regulatory guillotine, which is a flexible and simple legal tool for undifferentiated reduction of the regulatory array. The regulatory guillotine can be used to carry out narrow and large-scale reforms of a one-time or systemic nature (Nosova & Norkina, 2021).

The regulatory guillotine allows quickly revising a large number of rules governing economic relations in a short time. The key idea of the regulatory guillotine is to point out the systemic nature of the problem of business activity overregulation, as well as to demonstrate the possibility of eliminating excessive requirements in the shortest possible time, to correct the current situation in an easy, reasonable and gentle way, to prevent another crisis in the economic sphere, to open wider opportunities for the introduction and development of new digital technologies and the implementation of innovative projects.

There are quite a lot of definitions of the "regulatory guillotine" concept in the legal literature. In a broad sense, this is a transparent and accessible means for calculating and quickly revising a large number of rules through the prism of developed scientific criteria for proper regulation, according to which those regulations that are no longer needed are evaluated and eliminated.

D. B. Tsygankov interprets the regulatory guillotine as a legal means for quickly revising a large number of regulations (Lyubimov et al., 2019).

I. V. Sekhin characterizes the regulatory guillotine as a tool for regulating public relations, based on a criteria-based assessment of the array of legal norms and the subsequent termination of excessive mandatory requirements (Didikin, 2021).

D. V. Novak considers that a key principle of the regulatory guillotine is the possibility of reviewing all mandatory requirements for their effectiveness in the system of current legal regulation (Lyubimov et al., 2019).

If one adheres to the position of M. V. Degtyarev, the regulatory guillotine is a scalable and operational integral tool for simplifying and/or transforming packaged "thinning" of arrays of regulatory legal acts, the continuation of regulatory existence and action of which no longer has (or did not initially have) good reasons and justifications from the point of view of legality, reasonable rationality, economic strategy development, or socio-economic necessity" (Degtyarev, 2022a).

Based on the above definitions, one can conclude that the essence of the regulatory guillotine is quite clear and simple. The regulatory technology under consideration consists in a large-scale revision of the current requirements contained in regulatory legal acts, as a result of which one of three decisions is made: remaining in force, making changes or liquidation.

At the same time, speaking in support of the tools for improving regulation that have already been verified and implemented in many countries, D. B. Tsygankov rightly notes that where ARI works normally and fully, the guillotine is not particularly needed, since excessive acts are canceled in a timely manner, which does not allow them to grow uncontrollably[5]. However, in the presence of clutter of the regulatory-legal array, a comprehensive and large-scale reform of legislation is needed. This problem becomes particularly acute in the most regulated economic sectors. Accordingly, such an instrument of rapid reforms as the regulatory guillotine is a definite step towards ensuring the regulation stability and legal security of business (Degtyarev, 2022b).

Thus, when solving the issues of reducing burdensome rules and ensuring legal stability, it is important to use an integrated approach, including the introduction of a comprehensive full-fledged ARI along with the use of the latest regulatory technologies, among which legal deregulation mechanisms are gaining the most popularity.

2. International experience of implementing the regulatory guillotine mechanism

2.1. Practice of using legal regulation instruments and their elements in foreign countries

For the first time, the mechanism of the regulatory guillotine was used in Europe. Its first manifestations were reflected in early attempts at deregulation in the 1980s, during which a central microeconomic strategy was developed for countries facing an economic crisis and seeking rapid reforms.

In 1984, the Regulatory Guillotine program was initiated in the Kingdom of Sweden. The Government of this country found that it was unable to compile a list of existing regulatory legal acts, and therefore decided to create a clear comprehensive unified legislative database and instructed all subordinate bodies to compile registers of their acts within a year. When preparing the lists, unnecessary and outdated regulations were selected and then automatically canceled, and all new rules and changes to existing regulatory legal acts began to be entered into the unified register within a day from the moment of adoption. This approach was considered a great success. Its use enabled to quickly comprehensively revise the regulatory framework and cancel everything that did not pass filtering, i.e. was recognized as outdated, retarding, inappropriate, excessive, entailing unreasonable costs associated with significant risks. For example, in the field of education, 90% of all rules were abolished.

[5] Golodnikova, A. E., Efremov, A. A., Sobol D. V., et al.; Tsygankov, D. B. (head of the team) (2018). *Regulatory policy in Russia: the main trends and architecture of the future*. Moscow: National Research University "Higher School of Economics".

As a result of a successful reform in the Kingdom of Sweden, the principle of the regulatory guillotine was borrowed by Hungary, and in the early 1990s this country got rid of all norms that did not meet the requirements of a market economy. The first stage involved working with the regulatory framework adopted before June 30, 1990, and the second – with the one adopted after that date.

Then the successful experience of optimizing legislation caused interest in the Republic of Korea, which faced the Asian financial crisis in 1997. Taking into account previous unsuccessful approaches to regulatory reform based on the "bottom-up" principle, this time the "top-down" approach was chosen. The reform program included two key initiatives: the first – deregulation, the second – a sustainable institutional reform. Thus, the Korean guillotine was introduced into a broader reform strategy. As a result, in 11 months of 1998 the pre-established Regulatory Reform Committee (RRC) abolished 5,430 (48.8%) and simplified 2,411 (21.7%) of the 11,125 regulations it revised, which contributed to an increase in the inflow of foreign direct investment (FDI), reducing administrative costs, almost halving the regulatory burden on business, creating new jobs, expanding access to foreign exchange markets and ensuring the country's long-term economic growth (Artemenko, 2020).

During the implementation of regulatory reform in the Republic of Korea, it was particularly important that, at the initial stage of the regulatory guillotine, the historical Basic Act on Administrative Regulations (BAAR) was adopted, which included the procedure for the RRC creation and operation (Articles 23-33 of BAAR), norms for the development of a Comprehensive Plan to improve regulation (Article 20 of BAAR), and for the first time stipulated the concept of regulations impact analysis (RIA) and its criteria (Articles 2, 7 of BAAR)[6].

However, it should be noted that the elements of deregulation, which contributed to the formation of the modern mechanism of the regulatory guillotine, were used in some countries even before 1980. This was due to the transition to the welfare state concept, implemented in most economically developed countries of the world since 1970. For example, during this period, the economy of the United States of America faced excessive regulation in the social sphere. The overregulation of economic relations burdened business and demonstrated the inefficiency of business regulation. In order to effectively solve the problem of removing barriers to doing business and reduce social costs, the United States of America, among other measures, introduced additional labor protection requirements for enterprises with hazardous production (Yuzhakov et al., 2021). The need to introduce new standards was due to the dismissal of occupational safety specialists. However, the rules tightening had a negative effect and became one of the reasons for mass layoffs of employees from such enterprises.

[6] Basic Act on Administrative Regulations (Act No. 5368, Aug. 22, 1997).

There are quite a lot of similar examples of excessive regulation in one area or another. The actual situation required a rapid revision and elimination of excessive, destructive regulations. As a result, in the late 1970s and early 1980s, elements of deregulation (less regulation) began to be introduced in the United States of America, the United Kingdom of Great Britain and Northern Ireland and a number of other countries (Contractor et al., 2020).

It should also be noted that the introduction of the regulatory guillotine and its elements was preceded by programs: 1) reduction of administrative barriers (red tape cutting, simplification); 2) temporary regulation (legislation with a self-expiring regulatory period), called "self-completing" norms, "sunset legislation", or "sunsetting", applied in Australia, for example ("Gesetzgebung auf Zeit" – in the Federal Republic of Germany, "tijdelijke wetgeving" – in the Kingdom of the Netherlands) (Degtyarev, 2021).

For example, in Australia, according to the Legislative Instruments Act 2003 (LIA), any regulations regarding businesses or non-profit organizations were automatically canceled after 10 years if measures were not taken to preserve them. To extend the validity of certain norms, a special procedure was stipulated related to the assessment of their regulatory impact. The said law ensured the updating of the regulatory array and keeping it up to date.

An example of a country where "sunset legislation" is used quite often is also Israel. For example, from 2000 to 2015 the country's legislative body Knesset adopted 281 temporary laws. In the United States of America, the use of the sunset legislation procedure was associated with the state congresses' activities. According to M. V. Degtyarev, the system of such acts can be qualified as temporary legislation (Degtyarev, 2022a).

The practice of applying certain elements of deregulation in Australia, the United Kingdom of Great Britain and Northern Ireland, the Netherlands, the United States of America and other countries, as well as the high results obtained during the use of the regulatory guillotine principle in Sweden and Korea, formed the basis of the modern regulatory guillotine. Being an innovator in issues related to the assessment of sources of regulatory problems since 2004, the company Jacobs, Cordova & Associates (JC&A) has been actively involved in the development and implementation of regulatory reform programs in the Republic of Croatia, the Socialist Republic of Vietnam, the Republic of Kenya, the Arab Republic of Egypt, the Republic of Moldova, Bosnia and Herzegovina, the Republic of Serbia and other countries, which demonstrated the effectiveness of the regulatory guillotine mechanism, including in developing countries.

The conducted research also allows identifying one of the reasons for such a quick decision by a number of countries to introduce a regulatory guillotine mechanism and to conduct an inventory of legislation in the shortest possible time. In most cases, this was due to their desire to join the European Union, which, in turn, required harmonization and coordination of the national regulatory framework with the European legislation. The process of optimizing legislation using the mechanism of the regulatory guillotine, according to D. B. Tsygankov, served as a kind of "window of opportunity" to combat excessive norms (Lyubimov et al., 2019).

2.2. Examples of effective large-scale regulatory reforms using the modern "regulatory guillotine" mechanism

The most classic example of the use of the regulatory guillotine is the experience of the Republic of Croatia (which applied for EU membership in 2003). The regulatory guillotine project was launched by the country's authorities in January 2006. The entire process of the reform implementation took nine months. The project is known as HITROREZ ("Rapid reduction").

The procedure for optimizing Croatian legislation included collection, analysis and streamlining of business rules. The developed project provided for a triple revision of all requirements: by the public administration bodies that issued them; by a special division of HITROREZ; and by companies and businesspersons[7].

The reform involved two stages.

The first stage implied the executive authorities' preparing a complete list of requirements related to business and submitting it to a special division of HITROREZ.

At the second stage, the requirements were subject to review by the departments in interaction with business stakeholders and in compliance with the established criteria. In the course of the analysis of the regulations contained in legislative acts, one of the following conclusions was adopted: cancel, change, or leave as it is.

The action plan for the implementation of the guillotine strategy in the Republic of Croatia consisted of 17 mandatory sequential steps and a clear schedule, where the first step was a decision by the authorities to launch the guillotine.

As a result of the HITROREZ project implementation, specific recommendations were developed for each regulatory act containing business requirements and submitted to the Government of the Republic of Croatia. This allowed canceling about 27% and simplifying more than 30% of all rules concerning business. According to the World Bank data, during the reform carried out on the basis of the regulatory guillotine, the country's economy managed to save $65.6 million annually (0.13% of GDP).

The HITROREZ project also served as the first step to start implementing further system-wide reforms in the country. For example, from 2006 to 2020, Croatia significantly improved its performance in the Doing Business global ranking of countries, rising from the 118th to the 51st position.

The success of the guillotine in the Republic of Croatia was ensured by the following factors:

– the systematic approach to the legislative framework revision and the allocation of funding for regulatory expenditures;

– the establishment of clear project standards, active participation of the business community in the project implementation;

– the desire to join the European Union;

---

7 Jacobs, S., & Astrakhan, I. (2005). Effective and Sustainable Regulatory Reform: The Regulatory Guillotine in Three Transition and Developing Countries. *World Bank Conference Reforming the Business Environment: From Assessing Problems to Measuring Results. 29 Nov. – 1 Dec. 2005, Cairo*.

– the introduction of new software to improve the efficiency and transparency of regulation (Aleksandrov, 2019).

Besides, an important element of the effective application of the regulatory guillotine in Croatia was the official establishment of the relevant structures and institutions. In particular, the Decree of the Government of the Republic of Croatia of June 28, 2007 "On the establishment of the Office for the coordination of the regulatory impact assessment system" stipulated the establishment of the Office for the Coordination of the Regulatory Impact Assessment System. It includes the Department of Analysis and Control over the implementation of the HITROREZ project.

Following the Republic of Croatia, the regulatory framework for entrepreneurs in the Republic of Moldova was optimized according to the same principle of regulation simplification in 2005-2007. It is noteworthy that the launch of a radical reform in Moldova was preceded by the adoption in 2004 of the Law on optimization of the regulatory framework for business regulation (the Guillotine Law), which implied a transition to bolder and more systematic reforms (Moldova had already had experience in implementing nationwide regulatory reforms before 2005). The said law established new standards for the quality of regulation and contained a list of principles for creating relevant, feasible, clear, reasonable rules corresponding to the level of digital technologies development:

– transparency and stability in business regulation;

– zero interference with business activity and/or suspension of business activity, except in cases expressly stipulated in the law;

– differentiation of controlling-supervisory and regulatory functions of executive authorities;

– administrative authorities may not demand and charge any additional fees for the issuance of licenses, permits and other certificates for doing business, except those that are explicitly stipulated in laws and regulations of the Government or Parliament, which determine the type of services and the fee charged for such services;

– it is prohibited to demand and request any documents for the issuance of licenses, permits and other certificates for doing business that are not expressly stipulated in the laws and regulations of the Government or Parliament.

The drawback of the above principles was their focus mainly on improving the legal regulation of business activity (legal security of business) without paying due attention to the economic side of the issue. Nevertheless, the reform in the Republic of Moldova was successful, allowing for the first time in many years to compile a comprehensive transparent list of legal acts regulating business issues. Created in order to implement the "regulatory guillotine", the National Working Group revised 1,130 regulatory legal acts regulating business activity in six months. During the reform, it was revealed that only 426 acts meet all the established criteria (they were included in the electronic register); 285 acts (35%) required amendments and additions; 99 regulatory legal acts (12%) were canceled (most of them were declared illegal). The use of the regulatory guillotine mechanism

in the country also significantly strengthened the central institutions responsible for carrying out reforms, increased confidence in the reform and increased the potential for more ambitious reforms in the future.

In general, the supporting structure of the regulatory guillotine had a universal character, which allowed it to be used in carrying out both large-scale reforms (for example, the Republic of Croatia, the Republic of Moldova), and sectoral ones, aimed at simplifying regulation in certain sectors of the economy or spheres, for example, improving investment processes, licensing systems, etc. Among the countries that successfully implemented the sector reform are the Republic of Kenya, the Arab Republic of Egypt, and others.

For example, in 2005, the Kenyan Government initiated a reform aimed at reducing the growing number of business licenses and fees and reducing the level of corruption, which had acquired serious proportions due to the redundancy of such licenses. The reform took 18 months. Under the leadership of the Ministry of Finance, the central committee for regulatory reform was established and the implementation of the nationwide deregulation program "Regulatory Behavior and Capacity Building of the Republic of Kenya" began[8].

A comprehensive inventory conducted as part of this reform showed that the private sector was faced with more than 1,300 business licenses and related fees charged by more than 60 government agencies and 175 local authorities, and regulators were constantly introducing more and more new licenses. The result was that the private sector was overwhelmed with licenses, fees and expenses. During the reform, many licenses were found unnecessary, illegal or unreasonably expensive. As of October 2007, 315 licenses were cancelled and 379 simplified. A total of 294 licenses were retained. Of the remaining licenses, approximately 300 were postponed due to new draft laws being developed or already adopted legislative acts, and 25 were reclassified and not counted as licenses[9].

Notably, the Kenyan Government, in the course of the reform, went beyond the previous projects based on the "one at a time" (one in – one out) licensing reform, and adopted a broader "guillotine approach", which provides for the rapid identification, revision and streamlining of all business licenses and related fees. The results of the licensing reform significantly contributed to improving the status of Kenya as a leading reformer in the World Bank's Doing Business ranking for 2008. According to the results of the "Monitoring and evaluation of the business licensing reform of the Government of the Republic of Kenya" within the program "Regulatory behavior and capacity building of the Republic of Kenya", certain types of licensing were canceled and simplified, which significantly reduced the costs of control and supervisory activities, reduced risks for entrepreneurs and investors. Experts estimated the reduction of business expenses at $146 million per year.

---

8 Jacobs, S., Ladegaard, P., & Musau, B. (2007, October). *Kenya's Radical Licensing Reform*.

9 Jacobs, S. (2005, December). *The Regulatory Guillotine Strategy. Preparing the Business Environment in Croatia for Competitiveness in Europe*.

An important and fundamentally new result of the licensing reform carried out in the Republic of Kenya was the decision to create an appropriate institutional framework to support the sustainability of reforms. In particular, the country's Government approved institutional initiatives: the formation of a permanent regulatory body under the Ministry of Finance, whose tasks included checking new business rules, as well as the development and implementation of larger regulatory reform programs in the future; creation of an electronic register of regulatory legal acts and a register of regulatory bodies.

A review of the implementation of the licensing reform in Kenya allows highlighting its main principles:

– introduction of an orderly and transparent process for calculating licenses in all state bodies with the authority to issue licenses;

– quick review and verification of licenses for compliance with the established criteria: legality, validity, necessity, convenience for business;

– the burden of proof for the preservation of certain licenses does not lie with the reformers;

– full transparency and broad participation of stakeholders in the reform process;

– creation of an institutional framework for carrying out regulatory reforms on a systematic basis.

Regulatory reform in the Arab Republic of Egypt also had a sectoral nature and was aimed at simplifying investment processes (2014). The result of the reform was the creation of a special structure "Egyptian Regulatory Reform and Development Activities" (ERRADA). Within its competence, the audit and improvement of legislation in the field of investments were carried out, burdensome administrative procedures were minimized. In 2015, in order to strengthen investor confidence, weaken bureaucracy and attract foreign investment, the Law of the Arab Republic of Egypt No. 17/2015 was adopted, which amended the Law of the Arab Republic of Egypt No. 8/1997 "On investments". This law provided for the standardization of investment initiatives, simplification of various bureaucratic procedures for investors and other measures, which enabled to reduce a large number of inefficient and inappropriate rules in this area.

The project using the regulatory guillotine was also implemented in the Socialist Republic of Vietnam. In 2007, this country adopted the "Plan to simplify administrative procedures in the field of public governance for the period of 2007–2010" (further – the Plan), which consisted of four main stages:

– inventory, including the preparation by state executive authorities of lists of administrative procedures and information about them, based on standardized forms, followed by the creation of registers;

– self-check, in which the executive authorities analyzed and evaluated procedures based on the criteria of legality, necessity, acceptability and reasonableness;

– collection of the specified information by a special working group and discussion with representatives of public authorities with the subsequent development of the administrative reforms concept;

– development of recommendations for each verified administrative procedure (Degtyarev, 2022a).

The economic benefits of the regulatory reform carried out in the Socialist Republic of Vietnam were substantial. The reduction of business costs related to regulation was estimated at $1.4 billion per year. 5,421 procedures at all levels were subject to revision, of which 8.8% were canceled, 77% were simplified.

The modern regulatory guillotine, in turn, has covered a large number of developed countries of the world. The introduction of "regulatory guillotines" in these countries was due not only to the processes of digitalization and the expansion of the legislative array, but also to a number of other reasons:

1. Exit from international agreements and unions (for example, the United Kingdom of Great Britain and Northern Ireland – cancellation of regulations due to the adoption of the Law on the country's exit from the European Union, 2018).

2. Simplification of labor relations regulation in order to increase labor productivity (France, 2017).

3. Introduction of effective legal regulatory institutions and practices (Australia, New Zealand, 2017).

4. Creation of simplified conditions for doing certain businesses where it was previously impossible to do, with a view of the economic development of regions and attracting direct investment in them (Japan, 2003).

5. Participation in the work of international organizations (for example, the Organization for Economic Cooperation and Development – OECD, which includes 38 states and plays a leading role in the international community in promoting regulatory reform and introducing sound regulatory practices based on a nationwide approach).

Japan's experience deserves special attention in carrying out regulatory reform among developed countries, as it is a unique example of a territorial approach to regulatory reform. Due to the program of special zones, based on legislation approved in 2002 (the Law "On special zones related to structural reforms"), some rules could be relaxed or abolished in geographically limited areas acting as the testing ground and the first step for reforms at the national level. In Japan, a territorial approach combining regulatory reform with elements of decentralization led to initiatives that could have take much longer otherwise[10].

The multifaceted international experience has shown that most of the implemented regulatory reforms are of a large-scale nature and are not limited to the use of the regulatory guillotine mechanism; this is absolutely justified. Digitalization processes create the basis for the latest regulatory technologies development, making them more flexible, highly efficient and low-cost (Beach et al., 2020). While initially the goal of the regulatory policy of many countries was to reduce the number of regulatory legal acts (deregulation) that hinder business development (the policy of "reducing regulation" – less regulation),

[10] *OECD Reviews of regulatory reform: Japan*. (1999).

regulatory reforms have acquired a comprehensive, balanced and systematic character over time. Their main goal was not to reduce the number of regulations, but to improve their quality and effectiveness (the concept of "quality regulation" – better regulation). Later, with the advent of new regulatory instruments (regulatory impact assessment; measuring and reducing the administrative burden; simplification of the existing legislation, including consolidation and codification; consultations with stakeholders; assessment of the actual impact; open access to the legislative framework, etc.), a certain modernization of regulation took place, which led to the change of the "quality regulation" concept to a more modern "smart regulation" concept. However, despite the evolution of regulatory concepts, the mechanism of the regulatory guillotine, even taking into account the digital transformations of the economy, remains relevant and acts as one of the key elements in implementing both sectoral and larger-scale reforms (Davydova, 2020).

The regulatory guillotine is just one example of reforms that can simultaneously produce short-term results and lay the foundation for sustainable changes in the field of business regulation. The regulatory guillotine implies a sort of cyclical inventory of legislation and almost never serves as a completion of reforms. Foreign experience has shown that regulatory reforms carried out from the bottom up, as well as haphazard, one-time reforms, do not lead to the expected success, since the achievements of improved regulation may again decline as a result of the adoption of a large number of new ones and loss of relevance of the existing requirements. Such cases occur especially when rather strong traditions of legal regulation are formed and rooted in the country for many years, which encourages the repetition of the same mistakes. A number of conditions are necessary for the successful implementation of the guillotine strategy; political, administrative and legal support for the reform is of primary importance. Also, any reform is based on guidelines containing the necessary characteristics of proper regulation. The "regulatory guillotine" principles are: the universality of the legislative framework revision; the speed and finality of making a decision on the preservation, simplification or abolition of legal norms; abolition in favor of reforming the burden of proving regarding the need to preserve legal norms (presumption of overregulation of public relations in business sphere); universality of criteria for evaluating legal acts.

The analysis of the reforms also showed that not everywhere in the world the "regulatory guillotine" is used in its pure form; a number of countries are developing their own mechanisms of deregulation. But their essence is the same – reducing excessive regulation when doing business in order to ensure sustainable economic growth and social well-being of the country.

2.3. Formation of a new legal institution of mandatory requirement in the Russian Federation

The economic policy of most countries, including the Russian Federation, is aimed at ensuring that legislation and regulation are friends, not foes of technological progress. However, regulation sometimes becomes excessive, imposing too many regulatory requirements that their addressees must comply with.

The analysis of the existing problems in the regulation of economic relations allowed identifying significant guidelines and priority areas for improving the legal regulation of business in Russia. Serious attention was paid to the issues of creating clear guidelines, general rules and techniques for establishing mandatory requirements, building an effective system of requirements for business using promising regulatory technologies, including a tool of legal deregulation – the regulatory guillotine.

The Government of the Russian Federation has repeatedly marked that consistency in legislation is becoming problematic. The redundancy of the requirements imposed on business prevents the adoption of more effective decisions, leads to the need to revise the regulatory array. In addition, legislation that becomes obsolete over time puts at stake the trust of citizens and society in the ability of the established rules to solve the issues for which they were adopted. This problem has become most obvious in the course of high achievements of technological progress, including the economic sphere. A huge number of mandatory requirements no longer corresponded to the modern needs of economic entities, the level of technological progress, and the changes caused by digitalization.

The concept of effective regulation consists in the continuous and systematic improvement of its quality. The need to restructure the regulatory framework for the purposes of successful business was marked as early as in 2014 in a number of policy and strategic documents of the Russian Federation. Prerequisites for making cardinal decisions to eliminate excessive regulation were the following:

– the adoption of a large number of legislative acts that are not provided for by a previously formed plan, but are related to the reaction of the state to various events;

– the autonomy of the existing procedures for assessing legislation, the weak interrelationship of the legal diagnostic tools used;

– the overregulation of many sectors of the economy;

– the mechanical cancellation of mandatory requirements without conducting a proper comprehensive analysis based on clear criteria;

– the lack of an accessible, comprehensive database (register) of mandatory requirements for all areas of regulation of business and other economic activities;

– the lack of planning and cyclicity in revaluation and revision of mandatory requirements for business, etc.

The launch of the regulatory guillotine was facilitated by the adoption of the Federal Law "On mandatory requirements in the Russian Federation" (further – Law No. 247-FZ)[11]. This law laid the foundation for the formation of a new legal institution of mandatory requirement.

[11] On mandatory requirements in the Russian Federation. Federal Law No. 247-FZ of 31.07.2020. (2020). *KonsultantPlyus*.

Law No. 247-FZ enabled to define uniform conditions for establishing all rules imposed on business, namely: it outlined the scope of application of its norms, defined the object, subjects and area of regulation; the sources in which these norms should be contained and their validity period; and forms of assessment of the mandatory requirements application. It was stated that the necessary conditions for establishing mandatory requirements are: analysis of socially significant risks in the relevant sphere of public relations; consideration of compliance with mandatory requirements of modern digital reality.

In addition, Law No. 247-FZ fixed the fundamental principles – general criteria, a kind of restrictions (requirements to requirements), on which the entire system of mandatory requirements should be based and strictly comply with them. In total, five principles were identified: legality, legal certainty and consistency, validity, openness and predictability, enforceability of mandatory requirements.

The activation of the regulatory guillotine mechanism made it possible to quickly and effectively revise a significant amount of existing regulatory legal acts containing mandatory requirements, in order to update them and cancel all outdated and redundant rules. This contributed to a significant reduction in financial costs for business both in all areas of business activity and at the level of individual sectors of the economy. The regulatory guillotine became a valuable tool for eliminating uncertainty and risks; rationalizing the law-making process; improving the legislation quality and the regulation effectiveness in the context of the development of innovations and new digital opportunities.

However, attention should be paid to a number of problematic aspects found during the implementation of the new legal regulator.

First, the regulatory guillotine is not a panacea that can eliminate numerous regulatory difficulties associated with the expansion of the regulatory field and the widening gap between law and reality.

Second, excessive use of the regulatory guillotine mechanism often does not allow for a qualitative and meaningful assessment of regulatory requirements and may lead to a thoughtless mass reduction of mandatory requirements, creating a situation of legal vacuum. In this connection, it should be assumed that the regulatory guillotine is just one of the effective mechanisms of legal deregulation, the wide potential of which must be used in conjunction with other regulatory technologies.

Despite the identified risks, Law No. 247-FZ acted as a structure-forming factor in the construction of a new legal institution of mandatory requirement for the Russian Federation, demonstrating the unity and complexity of the norms governing economic relations, allowed to form an integral system of legal regulation based on a risk-oriented approach, which is a standard matrix for each sphere of business activity. The introduction of the regulatory guillotine significantly reduced the regulatory burden on business and the number of control functions of government agencies.

Summing up the above, it should be noted that in the era of digital transformations of the economy and other spheres of life, the desire to combat overregulation caused by outdated and excessive legislation, which no longer corresponds to the pace of development

of modern society, by undifferentiated reduction of the regulatory array is increasing. The regulation of any social and technological phenomenon implies an understanding of its characteristics and a quick response to emerging difficulties. The law must keep pace with the "acceleration" and protect the opportunities offered by technological development. The expediency of using the mechanism of legal deregulation, based on the simultaneous revision and cutting off of a large number of outdated and inefficient regulations, in the context of global digital transformations and turbulence, is obvious and serves as a vivid example when regulatory measures become not only easy, but also reasonable, serve the interests of society and contribute to the timely introduction of innovations, opening up new digital opportunities. This regulatory technology makes it possible to adapt regulation to the changing digital reality and transformational processes in the economy, to revise the entire "life cycle" of the requirements for doing business, thus avoiding excessive regulation in a certain area of economic relations.

Conclusion

1. The processes of digitalization in the economic sphere have led, along with the opening of new business opportunities, to the problem associated with the emergence of a significant number of irrelevant, outdated, formal regulatory rules that do not meet the requirements and principles of a market economy. This state of affairs caused insurmountable barriers to doing business and increased the administrative burden on business entities, serving as the basis for the search for new effective legislative mechanisms to eliminate excessive legal regulation.

2. An essential role in solving the issues of reducing ineffective rules and ensuring legal stability is played by the active implementation of a comprehensive full-fledged ARI of legislative acts containing mandatory requirements (including retrospective assessment), along with the use of the latest regulatory technologies, among which the most popular are the mechanisms of legal deregulation, such as the regulatory guillotine; it can be used not only for one-time and sectoral adjustment of legislation (by individual sectors (sub-sectors) of the economy), but also for carrying out large-scale reforms that imply a systemic nature.

3. The legal science interprets the modern regulatory guillotine as a mechanism for a comprehensive analysis and revision of the current regulatory array and a necessary element for improving the system of mandatory requirements. This regulatory technology successfully performs the function of a filter, eliminating precisely those rules which become burdensome for business entities from the viewpoint of economic necessity, rationality and legality.

4. The principles of the "regulatory guillotine" are: the universal revision of the legislative framework; the speed and finality of making a decision on the preservation, simplification or abolition of legal norms; the abolition, in favor of reform, of the burden to prove the need to preserve legal norms (presumption of overregulation of economic relations); the universality of criteria for evaluating legal acts.

5. Successful implementation of a single full-fledged procedure for assessing the regulating (regulatory) impact together with other regulatory technologies, including the guillotine, requires a number of conditions:

– state and legal support for a full-scale review of all mandatory requirements for business;

– formation of special structures and institutions responsible for carrying out regulatory reforms;

– a top-down approach to reform, when decisions are made at the highest level;

– measuring the existing regulatory problem, determining its scope and the reform goal;

– transition to a full ARI cycle, which provides for strengthening the current ARI mechanism, combining all existing analytical regulatory tools into a single procedure;

– precise definition of the area (areas) of regulation for the legislation inventory;

– development of unified general scientific criteria for effective regulation and elimination of those norms that have lost their usefulness;

– transparency and broad participation of stakeholders in the process of reviewing the current legislative framework;

– availability of technical capabilities to support and implement reforms;

– creation of a universal unified register of requirements in order to systematize them and inform interested persons, etc.

6. Foreign experience has shown that the problem of overregulation of economic behavior is systemic, requiring repeated regulatory reforms. This is due to the fact that at the stage of intensive digital transformations of the economy, the state is constantly introducing new rules for doing business, which over time may lose their relevance, contradict each other, creating legislative blockages, leading to excessive regulation and unjustified costs for business entities.

7. The legal experience of the Russian Federation in improving the efficiency of regulation in the economic sphere has demonstrated a comprehensive approach to improving the system of mandatory requirements imposed on business. The introduction of a new independent legal institution of mandatory requirements, which included the regulatory guillotine – a promising tool for undifferentiated reduction of excessive requirements, enabled to form a clear unified procedure for developing and evaluating compliance with mandatory requirements, to carry out a cardinal regulatory reform of legislation, which allowed to untangle the complex regulatory knots and to revise the existing rules in all spheres of economic activity on a large scale basis.

References

Aleksandrov, O. V. (2019). Regulatory guillotines: international experience in removing barriers to business and investment. *Trade policy, 1*(17), 107–119. (In Russ.). https://doi.org/10.17323/2499-9415-2019-1-17-107-119

Alekseev, S. S. (1966). *Mechanism of legal regulation in a Socialist state.* Moscow: Yuridicheskaya literatura. (In Russ.).

Artemenko, E. A. (2020). The regulatory guillotine as a mechanism for deregulation and anti-corruption. *Tomsk State University Journal of Economics*, *52*, 7–31. (In Russ.). https://doi.org/10.17223/19988648/52/1

Beach, T. H., Hippolyte, J.-Laurent, & Rezgui, Y. (2020). Towards the adoption of automated regulatory compliance checking in the built environment. *Automation in Construction*, *118*(12). https://doi.org/10.1016/j.autcon.2020.103285

Chao, X., Ran, Q., Chen, J., Li, T., Qian, Q., & Ergu, D. (2022). Regulatory technology (Reg-Tech) in financial stability supervision: Taxonomy, key methods, applications and future directions. *International Review of Financial Analysis*, *80*(2), 1–14, 102023. https://doi.org/10.1016/j.irfa.2022.102023

Contractor, F. J., Dangol, R., Nuruzzaman, N., & Raghunath, S. (2020). How do country regulations and business environment impact foreign direct investment (FDI) inflows? *International Business Review*, *29*(2). https://doi.org/10.1016/j.ibusrev.2019.101640

Davydova, M. L. (2020). Smart Regulation as the Basis for Improving Modern Law-Making. *Journal of Russian Law*, *11*, 14–29. (In Russ.). https://doi.org/10.12737/jrl.2020.130

Degtyarev, M. V. (2021). The latest regulatory technologies and tools: definition and classification. *Law and State: The Theory and Practice*, *12*(204), 180–183. (In Russ.). https://doi.org/10.47643/1815-1337_2021_12_180

Degtyarev, M. V. (2022a). The latest regulatory technologies and tools: reasons and preferences, risks and problems. *Law and State: The Theory and Practice*, *1*(205), 179–183. (In Russ.). https://doi.org/10.47643/1815-1337_2022_1_179

Degtyarev, M. V. (2022b). *The latest regulatory technologies and tools: regulatory experiments, sandboxes, guillotines, ecosystems, platforms*. Moscow: Buki-Vedi. (In Russ.).

Didikin, A. B. (2021). Mandatory requirements and legal means for their assessment in the regulatory policy mechanism. *Monitoring of law enforcement*, *1*(38), 4–9. (In Russ.). https://doi.org/10.21681/2226-0692-2021-1-4-9

Grassi, L., & Lanfranchi, D. (2022). RegTech in public and private sectors: the nexus between data, technology and regulation. *Journal of Industrial and Business Economics*, *49*(3), 441–479. https://doi.org/10.1007/s40812-022-00226-0

Haidar, J. I. (2012). The impact of business regulatory reforms on economic growth. *Journal of the Japanese and International Economies*, *26*(3), 285–307. https://doi.org/10.1016/j.jjie.2012.05.004

Jakupec, V., & Kelly, M. (2016). Regulatory impact assessment: the forgotten agenda in ODA. *Assessing the Impact of Foreign Aid*, 95–106. https://doi.org/10.1016/b978-0-12-803660-0.00007-6

Lyubimov, Yu. S., Novak, D. V., & Tsygankov, D. B. (2019). Regulatory guillotine. *Statute*, *2*, 20–36. (In Russ.).

Nosova, S., & Norkina, A. (2021). Digital technologies as a new component of the business process. *Procedia Computer Science*, *190*, 651–656. https://doi.org/10.1016/j.procs.2021.06.076

Polemis, M. L., & Stengos, T. (2020). The impact of regulatory quality on business venturing: A semi-parametric approach. *Economic Analysis and Policy*, *67*, 29–36. https://doi.org/10.1016/j.eap.2020.05.005

Purnomo, A., Susanti, T., Rosyidah, E., Firdausi, N., & Idhom, M. (2022). Digital economy research: Thirty-five years insights of retrospective review. *Procedia Computer Science*, *197*(13), 68–75. https://doi.org/10.1016/j.procs.2021.12.119

Rowthorn, V., Plum, A., & Zervos, J. (2017). Legal and Regulatory Barriers to Reverse Innovation. *Annals of Global Health*, *82*(6), 991–1000. https://doi.org/10.1016/j.aogh.2016.10.013

Shaulova, T. (2017). Regulatory Impact Assessment: Another Hobby or Development Tool? *Nauchnye trudy Severo-Zapadnogo instituta upravleniya RANKhIGS*, *8*(1), 139–143. (In Russ.). https://doi.org/10.2139/ssrn.3826436

Youssef, A. B., Boubaker, S., Dedaj, B., & Carabregu-Vokshi, M. (2021). Digitalization of the economy and entrepreneurship intention. *Technological Forecasting and Social Change*, *164*(5), 120043. https://doi.org/10.1016/j.techfore.2020.120043

Yughakov, B., Dobrolyubova, E., Pokida, A., & Zybunovskaya, H. (2021). The Law Enforcement Reform and Regulatory Guillotine: What's the Outcome from the Business Perspective. *ECO*, *7*(565), 151–170. (In Russ.). https://doi.org/10.30680/ECO0131-7652-2021-7-151-170

Author information

Svetlana A. Minich – Junior Researcher of the Department of Research in the sphere of Civil, Environmental and Social Law, National Centre for Legislation and Legal Research of the Republic of Belarus
Address: 1a Berson Str., 220030 Minsk, Republic of Belarus
E-mail: ekabpils75@mail.ru
ORCID ID: https://orcid.org/0000-0003-0713-3378
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/record/GWC-0287-2022
Google Scholar ID: https://scholar.google.ru/citations?user=iYsfRdIAAAAJ
RSCI Author ID: https://www.elibrary.ru/author_items.asp?authorid=1022812

Conflict of interests

The authors declare no conflict of interests.

Funding

The research was not sponsored.

Thematic rubrics

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

Article history

Date of receipt – October 15, 2023
Date of approval – February 5, 2023
Date of acceptance – August 15, 2023
Date of online placement – August 20, 2023

Научная статья
УДК 34:346.5:004:33:006
EDN: https://elibrary.ru/ibfbaq
DOI: https://doi.org/10.21202/jdtl.2023.34

Совершенствование системы обязательных требований, предъявляемых к бизнесу в условиях цифрового преобразования экономики

Светлана Александровна Минич

Национальный центр законодательства и правовых исследований Республики Беларусь
г. Минск, Республика Беларусь

Ключевые слова

Бизнес,
дерегулирование,
законодательство,
обязательные требования,
право,
правовое регулирование,
предпринимательская деятельность,
регуляторная гильотина,
цифровые технологии,
экономика

Аннотация

Цель: подготовка научно обоснованных предложений по совершенствованию системы обязательных требований в сфере предпринимательской и иной экономической деятельности в условиях формирования цифровой экономики, с учетом зарубежного опыта по устранению препятствий для ведения бизнеса и имеющейся практики оптимизации законодательства в данной сфере.

Методы: методологическую основу исследования составляют традиционные общенаучные и частнонаучные методы научного познания: диалектический, формально-логический, историко-сравнительный, системный, терминологический, общелогические методы (анализ, синтез, обобщение, индукция, дедукция и др.), а также специальные методы: историко-правовой, формально-юридический, метод сравнительного правоведения.

Результаты: исследованы и систематизированы теоретические подходы и опыт совершенствования системы обязательных требований в зарубежных странах и Российской Федерации, рассмотрены возможности внедрения наиболее успешных инновационных правовых инструментов и практик для улучшения регулирования экономических отношений. Определена роль ретроспективной оценки регулирующего воздействия действующих нормативных правовых актов, содержащих обязательные требования, в решении вопросов по сокращению

обременительных правил и обеспечению правовой устойчивости в условиях цифровой трансформации экономики. Рассмотрен международный опыт реализации механизма регуляторной гильотины; раскрыты его суть, цель, задачи, основные принципы, алгоритм работы. Проанализированы вопросы установления и оценки применения содержащихся в нормативных правовых актах требований, предъявляемых к бизнесу.

Научная новизна: авторский всесторонний анализ имеющихся научных разработок по вопросам совершенствования системы обязательных требований, предъявляемых к бизнесу; систематизация научно-теоретических подходов к выбору инновационных правовых инструментов для устранения избыточного правового регулирования экономических отношений; обобщение успешных зарубежных практик реализации мероприятий «регуляторной гильотины».

Практическая значимость: выработка рекомендаций по эффективному сокращению обременительных требований, негативно влияющих на развитие предпринимательской деятельности в условиях цифровой трансформации экономики. Определение условий, необходимых для осуществления полноценной процедуры оценки регулирующего воздействия и успешной реализации регуляторных реформ. Результаты исследования могут быть использованы в нормотворческой деятельности, в образовательном процессе при освоении образовательных программ по экономическим и юридическим специальностям.

Для цитирования

Минич, С. А. (2023). Совершенствование системы обязательных требований, предъявляемых к бизнесу в условиях цифрового преобразования экономики. *Journal of Digital Technologies and Law*, *1*(3), 775–802. https://doi.org/10.21202/jdtl.2023.34

Список литературы

Александров, О. В. (2019). «Регуляторные гильотины»: международный опыт устранения препятствий для бизнеса и инвестирования. *Торговая политика*, *1*(17), 107–119. EDN: https://www.elibrary.ru/zauags. DOI: https://doi.org/10.17323/2499-9415-2019-1-17-107-119

Алексеев, С. С. (1966). *Механизм правового регулирования в социалистическом государстве*. Москва: Юридическая литература. https://www.elibrary.ru/sifyfj

Артеменко, Е. А. (2020). Регуляторная гильотина как механизм дерегулирования и борьбы с коррупцией. *Вестник Томского государственного университета. Экономика*, *52*, 7–31. EDN: https://www.elibrary.ru/hixdez. DOI: https://doi.org/10.17223/19988648/52/1

Давыдова, М. Л. (2020). «Умное регулирование» как основа совершенствования современного правотворчества. *Журнал российского права*, *11*, 14–29. EDN: https://www.elibrary.ru/ynerpx. DOI: https://doi.org/10.12737/jrl.2020.130

Дегтярев, М. В. (2021). Новейшие регуляторные технологии и инструменты: дефиниция и классификация. *Право и государство: теория и практика*, *12*(204), 180–183. EDN: https://www.elibrary.ru/zcmmne. DOI: https://doi.org/10.47643/1815-1337_2021_12_180

Дегтярев, М. В. (2022a). *Новейшие регуляторные технологии и инструменты: Регуляторные эксперименты, песочницы, гильотины, экосистемы, платформы*. Москва: Буки-Веди.

Дегтярев, М. В. (2022b). Новейшие регуляторные технологии и инструменты: резоны и преференции, риски и проблемы. *Право и государство: теория и практика*, *1*(205), 179–183. EDN: https://www.elibrary.ru/mpyvro. DOI: https://doi.org/10.47643/1815-1337_2022_1_179

Дидикин, А. Б. (2021). Обязательные требования и правовые средства их оценки в механизме регуляторной политики. *Мониторинг правоприменения*, *1*(38), 4–9. EDN: https://elibrary.ru/jxccxf. DOI: https://doi.org/10.21681/2226-0692-2021-1-4-9

Любимов, Ю. С., Новак, Д. В., Цыганков, Д. Б. (2019). Регуляторная гильотина. *Закон*, *2*, 20–36. https://www.elibrary.ru/yxaokl

Шаулова, Т. В. (2017). Оценка регулирующего воздействия: очередное увлечение или инструмент развития? *Научные труды Северо-Западного института управления РАНХиГС*, *8*(1), 139–143. EDN: https://www.elibrary.ru/ziwhxj. DOI: https://doi.org/10.2139/ssrn.3826436

Южаков, В. Н., Добролюбова, Е. И., Покида, А. Н., Зыбуновская, Н. В. (2021). Реформа госконтроля и «регуляторная гильотина»: что получилось с позиции бизнеса? *ЭКО*, *7*(565), 151–170. EDN: https://www.elibrary.ru/uskrrh. DOI: https://doi.org/10.30680/ECO0131-7652-2021-7-151-170

Beach, T. H., Hippolyte, J.-Laurent, & Rezgui, Y. (2020). Towards the adoption of automated regulatory compliance checking in the built environment. *Automation in Construction*, *118*(12). https://doi.org/10.1016/j.autcon.2020.103285

Chao, X., Ran, Q., Chen, J., Li, T., Qian, Q., & Ergu, D. (2022). Regulatory technology (Reg-Tech) in financial stability supervision: Taxonomy, key methods, applications and future directions. *International Review of Financial Analysis*, *80*(2), 1–14, 102023. https://doi.org/10.1016/j.irfa.2022.102023

Contractor, F. J., Dangol, R., Nuruzzaman, N., & Raghunath, S. (2020). How do country regulations and business environment impact foreign direct investment (FDI) inflows? *International Business Review*, *29*(2). https://doi.org/10.1016/j.ibusrev.2019.101640

Grassi, L., & Lanfranchi, D. (2022). RegTech in public and private sectors: the nexus between data, technology and regulation. *Journal of Industrial and Business Economics*, *49*(3), 441–479. https://doi.org/10.1007/s40812-022-00226-0

Haidar, J. I. (2012). The impact of business regulatory reforms on economic growth. *Journal of the Japanese and International Economies*, *26*(3), 285–307. https://doi.org/10.1016/j.jjie.2012.05.004

Jakupec, V., & Kelly, M. (2016). Regulatory impact assessment: the forgotten agenda in ODA. *Assessing the Impact of Foreign Aid*, 95–106. https://doi.org/10.1016/b978-0-12-803660-0.00007-6

Nosova, S., & Norkina, A. (2021). Digital technologies as a new component of the business process. *Procedia Computer Science*, *190*, 651–656. EDN: https://www.elibrary.ru/zryypb. DOI: https://doi.org/10.1016/j.procs.2021.06.076

Polemis, M. L., & Stengos, T. (2020). The impact of regulatory quality on business venturing: A semi-parametric approach. *Economic Analysis and Policy*, *67*, 29-36. https://doi.org/10.1016/j.eap.2020.05.005

Purnomo, A., Susanti, T., Rosyidah, E., Firdausi, N., & Idhom, M. (2022). Digital economy research: Thirty-five years insights of retrospective review. *Procedia Computer Science*, *197*(13), 68–75. EDN: https://www.elibrary.ru/zgdxjk. DOI: https://doi.org/10.1016/j.procs.2021.12.119

Rowthorn, V., Plum, A., & Zervos, J. (2017). Legal and Regulatory Barriers to Reverse Innovation. *Annals of Global Health*, *82*(6), 991–1000. https://doi.org/10.1016/j.aogh.2016.10.013

Youssef, A. B., Boubaker, S., Dedaj, B., & Carabregu-Vokshi, M. (2021). Digitalization of the economy and entrepreneurship intention. *Technological Forecasting and Social Change*, *164*(5), 120043. https://doi.org/10.1016/j.techfore.2020.120043

Сведения об авторе

Минич Светлана Александровна – младший научный сотрудник отдела исследований в области гражданского, экологического и социального права Института правовых исследований, Национальный центр законодательства и правовых исследований Республики Беларусь
Адрес: 220030, Республика Беларусь, г. Минск, ул. Берсона, 1а
E-mail: ekabpils75@mail.ru
ORCID ID: https://orcid.org/0000-0003-0713-3378
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/record/GWC-0287-2022
Google Scholar ID: https://scholar.google.ru/citations?user=iYsfRdIAAAAJ
РИНЦ Author ID: https://www.elibrary.ru/author_items.asp?authorid=1022812

Конфликт интересов

Автор заявляет 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: 10.23.31 / Государственное регулирование предпринимательской деятельности
Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 15 октября 2022 г.
Дата одобрения после рецензирования – 5 февраля 2023 г.
Дата принятия к опубликованию – 15 августа 2023 г.
Дата онлайн-размещения – 20 августа 2023 г.

Research article
DOI: https://doi.org/10.21202/jdtl.2023.35

"Smart Cities": Legal Regulation and Potential of Development

Elena Yu. Tikhaleva

Middle Russia Institute of Management – branch of the Russian Presidential Academy of National Economy and Public Administration
Orel, Russian Federation

Keywords

Digital platform,
digital technologies,
digitalization,
law,
legal regulation,
legislation,
local self-government,
municipal entity,
municipal law,
smart city

Abstract

Objective: to research the trends of development of the "smart cities" concept and their legal regulation.

Methods: general scientific (induction, deduction) and special (systemic-structural, comparative-legal analysis) methods were used. Also, review analysis was applied to analyze the status quo of "smart cities". Innovative research approaches are still rare in considering the "smart cities" concept, as well as the prospects referring to targeted knowledge management and cooperation between the respective stakeholders. As for the special research methods for studying digital relations, we used content analysis (the method of creating reproducible and substantiated conclusions from texts (or other meaningful materials) in the context of their use). As the results of previous research and concepts referring to "smart cities" are available, we also used deductive content analysis.

Results: a characteristic is given to public relations formed within the process of development of "smart cities" concept. The key legal acts, principles of formation and functioning of "smart cities" are identified, taking into account the Russian and foreign experience. In this connection, the examples of successful practices are given, of the activities of both Russian and foreign municipal entities, taking into account the competitions held and rankings determined by the central structures. The popular directions are summarized, which are broadly introduced at the local level, and the probable problems are identified in the sphere of implementation of this project in our state.

Scientific novelty: the article carries out an analysis of the current legal regulation and the results of introducing the "smart cities" concept. The promising technologies and methods are identified, which are necessary to achieve the tasks of the concept implementation. The elements are specified, which ensure sustainability of "smart cities" complying with the future demands. An author's position is expressed regarding a close interrelation of this phenomenon with the institute of local self-government in the context of possible development of the latter into the process of making managerial decisions involving artificial intelligence. This concerns, first of all, using the potential of the Internet of Things. In practice, a lot of problems occur, associated with the implementation of normatively stipulated provisions, which implies the need to perform further research in the sphere under study.

Practical significance: is due to the insufficient development of data about the features and prospects of introducing the idea of "smart cities". The provisions of the research performed will allow effectively improving the mechanisms of legal regulation and broad implementation of the concept under study.

For citation

Tikhaleva, E. Yu. (2023). "Smart Cities": Legal Regulation and Potential of Development. *Journal of Digital Technologies and Law, 1*(3), 803–824. https://doi.org/10.21202/jdtl.2023.35

Contents

Introduction

Nowadays, the significance of cities as the main centers of social-economic life is growing. On the one hand, they become the main places for the people to settle. Indeed, 55 % of the population worldwide now live in cities, and by 2050 this share will reach 70 %. In particular, in the European Union these figures are even higher – 70 and 80 %, respectively.

Modern digital technologies have led to significant changes in the life of various states and societies, and transformed the principles and methods of management arrangements. These processes also touched upon the local, not only state-wide, level.

While in the 1990s we spoke of the so-called eco-cities and low-carbon cities, nowadays more and more promising becomes the idea of the so-called smart cities broadly using

information and digital technologies, including the Internet of Things. This idea captures the minds of politicians all over the global community, including Russia, as it allows a city functioning as a single organism.

A smart city is a city using a set of the most advanced technologies, first of all, information and communication ones, in order to render higher quality services to its citizens and users. This general definition opens doors for participation of many stakeholders in drafting smart cities, including computer scientists, engineer programmers, business managers, city developers, city builders and officials. Indeed, creating a common structure for "smart cities" is difficult, and it is even more difficult to measure its success in implementing its vision.

The modern concept of smart cities appeared from the very first initiatives for creating digital cities in the 1990-s. Besides, over the years it has turned into an idea using new technologies of the Internet of Things to achieve the strategic goals of a "smart city".

"Smart cities" may become a factor of overcoming many of the current socio-economic problems and facilitate economic growth. The idea is based on the concept of possibilities for each person's self-implementation. This is an intersection of digital technologies and intellectual potentials of management systems. The concept became an effect of the urbanization phenomenon, the growth of the economic significance of cities, and the growing demand for a more stable life (Attaran et al., 2022).

A bright example is the experience of India. New cities emerge between urban centers in order to avoid overpopulation in large cities attracting upcountry people by their prospects. An incentive is the attractive prospects of the new "smart cities" with an advanced infrastructure, simple and accessible in use (Strelnikova & Tsutsiev, 2017). One hundred "smart cities" are currently launched in India, and the authorities hope he citizen will use innovations to solve demographic and economic problems (Jothimani et al., 2022). Similar trends gain momentum in China, from where digital platforms are starting to develop worldwide (for example, Alibaba's City Brain) (Caprotti & Liu, 2020).

1. Legal regulation of "smart cities"

As early as in 2015, the European Economic and Social Committee in its decision pointed out the possibility of using the "smart cities" concept for operative development of the European industrial economy (European Economic and Social Committee, 2015).

In 2016, the UNO Conference on Housing and sustainable Urban Development paid close attention to using the idea of a "smart city".

In Russia, a "smart city" appeared due to a departmental project of municipal facilities digitalization (uniting the Passports of national projects "Digital economy" and "Housing and urban environment") since 2018.[1] This expenditure line is included

[1] Decree of the President of the Russian Federation No. 204 of 07.05.2018. (2018). *Collection of legislation of the Russian Federation*, *20*, Article 2817.

into the federal budget. The list of the project pilot cities includes 79 cities (initially – 33 cities) (Ganin & Ganin, 2014).

The "Digital economy" project comprises the following federal projects: "Normative regulation of the digital environment", "Personnel for the digital economy", "Information infrastructure", Digital technologies", "Digital public governance", and "Artificial intelligence"[2]. As a whole, these projects imply development of an automated system of control and management of "smart cities".

Besides, the "National strategy for development of artificial intelligence up to 2030"[3] and the "Strategic guidelines in the sphere of digital transformation of construction sector, municipal and communal facilities of the Russian Federation up to 2030"[4] in order to ensure acceleration of the development of artificial intelligence, robotics services, and increasing the accessibility of the information provided. Undoubtedly, introduction of these documents into the life practice of the population influences the "smart city" concept, facilitating the efficiency of planning, forecasting and making managerial decisions, as well as the quality of services rendered, first of all, in the policy and social spheres.

In 2019, the methodology of IQ cities evaluation[5] was developed, which identifies important criteria for evaluating digitalization of municipal entities, for example, the presence of intelligent system of social services and the investment climate. In 2022, at the departmental level, the indices of city economy digitalization were stipulated, which determine the possibilities to consider a city to be "smart" (feedback from the citizens, energy sector, safety, etc. – 18 basic and additional indices)[6].

Detailed legal regulation at federal level accompanied the respective project of developing the city of Moscow[7].

At the international level, as early as in 2000, the Okinawa Charter "Global information society" was adopted, which laid the bases for further development

---

2 *Passports of the national project "Digital economy of the Russian Federation"* (adopted by the Presidium of the Council under the Russian President on strategic development and national projects, protocol of 04.06.2019 No. 7).

3 Decree of the President of the Russian Federation No. 490 of 10.10.2019. (2019). *Collection of legislation of the Russian Federation*, *41*, 5700.

4 Collection of legislation of the Russian Federation 3883-r of 27.12.2021. (2021). *Official Internet portal of legal information*. http://www.pravo.gov.ru

5 Order of the Ministry of Construction of the Russian Federation No. 924/pr of 31.12.2019. (2019). *SPS KonsultantPlyus*. https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=379313#q40fMiTCYjxSO6p22

6 Order of the Ministry of Construction of the Russian Federation No. 357/pr of 11.05.2022. (2022). https://docs.cntd.ru/document/350551073

7 On making experiment of establishing a special regulation with a view of creating the necessary conditions for elaborating and introducing artificial intelligence technologies in a Russian Federation subject – city of federal significance Moscow and making amendments in Articles 6 and 19 of Federal Law "On personal data" No. 123-FZ of 24.04.2020. *Collection of legislation of the Russian Federation*, *17*, Article 2701.

of "smart cities"[8]. In 2017, the Asilomar AI Principles were elaborated at a conference in US. In 2019, the UNESCO General Conference developed a resolution on elaborating ethical norms in the sphere of artificial intelligence.

The "smart city" model introduced in Europe since the end of the 2000s was implemented, first of all, on the basis of the work by European Innovative Partnership on Smart Cities and Communities (EIP-SCC).

In 2020, the OECD program on smart cities and inclusive growth was adopted, which comprises a great variety of models based on local peculiarities[9]. The program identifies six key parameters to measure the "smart city" efficiency. Emphasis is made on profitability of investment into the "smart city", as well as bringing the investments into compliance with the city's strategic priorities and citizens' needs.

Since 2021, the Global partnership program of the World Bank "Smart city" is functioning, which is aimed at determining the priority measures to eliminate inequality and digital gap in cities[10].

Speaking of individual countries, France has adopted the Law No. 2016-1321 of October 7, 2016, "On the digital republic", which implies access to public data accumulated by state structures[11].

Another example is the Strategy of smart cities' development elaborated in Budapest, which demonstrates a mixed pattern of "up-down" and "down-up" approaches, mainly due to a special view at strategic frameworks. The local self-government of Budapest is the key factor and participant of the activity developing "smart cities". The Hungarian government implements several projects within its jurisdiction, while the key state services are centralized at the national level, which leaves little space for the city to plan and implement its actions. The Budapest Strategy of smart cities' development is focused on technological approaches. In addition, the activity of developing "smart cities" involves most of the urban areas in an integrated manner; the city is well suited to the European interpretation of "smart cities", paying special attention to environmentally friendly solutions (Csukás & Szabó, 2022).

Similar work is carried out at the level of intergovernmental cooperation. For example, in 2018, the Ministry of Construction and Communal Facilities of the Russian Federation signed a Memorandum with the Ministry of Lands, Infrastructure, Transport and Tourism

8 Okinawa Charter "Global information society" of 22.07.2000. (2000, August). *Diplomaticheskiy vestnik*, *8*.

9 *The OECD Programme on Smart Cities and Inclusive Growth*. https://www.oecd.org/cfe/cities/smart-cities.htm/

10 Gunes Basat, Narae Choi. (July 09, 2021). *5 views: What makes a city 'smart'?* https://blogs.worldbank.org/sustainablecities/5-views-what-makes-city-smart/

11 LOI № 2016-1321 du 7 octobre 2016 pour une République numérique. (2016, 8 octobre). *Journal Officiel de la RÉPUBLIQUE FRANÇAISE*.

of Japan[12]. Japan actively creates and develops "smart cities", for example, the cities Tsunashima and Aizuwakamatsu imply a broad introduction of innovative technologies; Fujisawa and Suita emphasize the ecological component (Langendahl, 2021).

At sublegislative level, the definition of "smart city" is stipulated in our country, which implies an established paradigm of a city development, actively introducing advanced digital technologies in order to improve the quality of life of the citizens, the quality of the services rendered and the efficiency of the managerial processes coupled with the necessary provision of the citizen's needs[13]. Also, the basic directions of implementing this approach in specific municipal entities are identified:

– city environment;
– safe city;
– digital city management;
– investment climate;
– well-being of people.

Abroad, the following directions of smart city are specified[14]:

– smart care;
– smart energy;
– smart society;
– smart office;
– smart mobility;
– smart space;
– smart infrastructure;
– smart transportation;
– smart data.

Integration of various components, like the above listed, may increase the success of such a project. In our opinion, the point of contact here is the life quality of the citizens as one of the main values guaranteed in such a city.

---

12 Memorandum on the development of cooperation in the spheres of construction, communal facilities and urban environment with a view of creating "smart cities" between the Ministry of Construction and Communal Facilities of the Russian Federation and the Ministry of Lands, Infrastructure, Transport and Tourism of Japan (signed in Moscow on 26.05.2018). https://minstroyrf.gov.ru/docs/16971/

13 Order of the Ministry of Construction of the Russian Federation No. 866/pr of 25.12.2020. https://minstroyrf.gov.ru/docs/81884/; Passport of the federal project "Forming a comfortable urban environment" (adopted by the protocol of a meeting of the Project Committee on the national project "Housing and urban environment" of 21.12.2018 No. 3). https://www.consultant.ru/document/cons_doc_LAW_319514/

14 Maddox, T. (2016, August 1). Smart cities: six essential technologies. https://www.techrepublic.com/article/smart-cities-6-essential-technologies/; Marr, B. (2020, July 2). The smart cities of the future: five ways technology is transforming our cities. https://www.forbes.com/sites/bernardmarr/2020/07/02/the-smart-cities-of-the-future-5-ways-technology-is-transforming-our-cities/?sh=781277c673f8

2. Content of the "smart cities" concept

"Smart cities" are territories where local innovative systems function, which receive advanced opportunities; this is expressed in increased competitiveness, improved environment, increased numbers of jobs and citizens' well-being (Vukovic et al., 2021; Shkvarya & Semenov, 2020).

The city population, qualified employees and innovative enterprises are the fundamental elements on which this concept is built (Fedorchenko & Karlyavina, 2021). In this regard, it is important to promote the growth of education, incite initiatives and creative activities of the residents, and establish partnership relations. In an environment where smart people work, the emphasis is made on human resources, management of the potential, processing and analyzing data by the people in order to make managerial decisions and implement production processes.

The key directions in developing the "smart city" concept are:

1) comparing the municipalities and electing the best practices;

2) understanding the trends of a "smart city" development, their dynamics, identifying drawbacks and resources for their overcoming;

3) accounting for the local factors influencing the development of a specific municipality;

4) preparing a development plan including the main components;

5) creating a working group of representatives of authorities and the community to control over the project implementation.

The technologies applied may save lives, prevent crimes, reduce waste, save time, and elaborate solutions productive for the city. Another objective is to more effectively and dynamically respond to the challenges, needs and desires of the residents of the territory.

The main principles of the "smart city" concept are:

1) orientation towards a human (this principle is determined by the priority of the rights and freedoms of a human and citizen, the need to provide possibilities for self-implementation of every individual, and to solve their problems at the place of residence through organizing feedback, i. e. the main goal is improving the life quality of citizens);

2) forming a sustainable and safe environment (to the forefront come the safety of residents, ensuring the functioning of the established information networks, comfort of the urban environment, accessibility of social infrastructure; this principle implies active development of public surveillance systems, public and ecological safety, intelligent city illumination; widespread means of photo- and video-registering on roads, developing intelligent transport systems, stimulating development of energy saving systems) (Nizamieva, 2021; Kuranov, 2020);

3) observing the balance of interests, principles of development and possibilities (this principle implies accounting for the public opinion when making significant decisions influencing the urban environment (voting, polling); involving the population into self-organization at the local level, joint implementation of public projects; reaching consensus between the interests of the municipality, business structures, and local residents) (Yakushina, 2021);

4) accessibility and convenience of services (one of the advantages of living in a "smart city"; introduction of this principle is provided by internetization of the city, providing many services via electronic resources (for example, state services portal, electronic offices); it takes into account the needs of various groups of population depending on the age, gender, education, occupation, etc.) (Bekbolat et al., 2021);

5) integration, interaction and openness (this principle refers to the mechanism of functioning of city services, implying collection and analysis of all necessary data, exclusion of their dubbing, their transfer to stakeholders) (Belov & Smirnov, 2018);

6) constant improvement of the quality of management (the principle is implemented through the functioning of highly professional officials, first of all, managers; analyzing problematic aspects; creating data bases and registers complying to the global standards; using various subsystems in forming rational management) (Sharova, 2019);

7) emphasis on economic efficiency (this principle allows evaluating the investment attraction of the city, its investment climate (presence of business incubators, technoparks, etc.), facilitating creation of new jobs and increasing labor productivity; it implies the need to ensure financial independence of the city through active development of the key directions of investment activity) (Golikova, 2020);

8) predominance of long-term solutions over short-term benefits (this direction ensures economic growth for the future; allows avoiding negative consequences of instantaneous subjective decisions, as it is quality long-term decisions that directly influence short-term steps) (Kostko et al., 2022);

9) using the best available technologies (the principle implies evaluating technology from the viewpoint of cost, difficulty of introduction and feasibility in particular conditions, and the need to minimize negative consequences; it is possible to implement experimental legal regimes).

Depending on the order and objectives of their creation, "smart cities" may, in our opinion, be classified as follows:

– the new cities created artificially, initially built to use new information technologies and attract business structures (Fujisawa in Japan, Neom in Saudi Arabia, Rublevo-Arkhangelskoye in Moscow region);

– the existing cities with a rich history of development, currently undergoing the process of technological modernization as a necessary condition for their further development and adaptation for the forming conditions (London, Moscow, etc.);

– the specialized cities created with a particular goal and in this connection using the process of digitalization in relation to the chosen development direction (business incubator (Silicon Valley in the USA), eco-city (Masdar in UAE, Neapolis in Cyprus, etc.).

Speaking of the foreign experience of introducing the "smart cities" concept, one may highlight the following significant aspects.

Since 2019, the Federal Ministry of Transport, Construction and City development of Germany (BMWSB) promotes German cities and municipalities in terms of their planning and implementation of "digital strategies for liveable cities", with financing called "Smart cities made in Germany". In 2019, 13 cities and municipal projects were financed, in 2020 – another 32, and in 2021 – another 28 projects. In addition to elaborating and testing the integrated approaches to a "smart city", the objectives of this program are a combination of sustainability with digitalization, development of cloud infrastructures and services of the new generation (Treude et al., 2022).

Italy focuses on introducing applications and intellectual systems. Development of applications includes construction platforms, open source technologies and city data platforms. When designing the systems, special attention is paid to developing auxiliary systems, efficiency of transport systems, facilitating the transformation of vulnerable territories into "smart" and sustainable areas.

Great Britain makes an emphasis on applications and management, including development of joint innovative platforms, data safety and projects of transport infrastructure. The main activity is aimed at city administrators and development of services using mobile data. In particular, London plans to become a global city – a testing ground for innovations, where the best ideas, for example, from the sphere of artificial intelligence, are elaborated in compliance with the highest standards of confidentiality and security, and are disseminated all over the world.

Thus, green spaces, possibility of quick employment, availability of schools and safety of citizens are the key factors determining the European smart cities. The policy for the coming years in the sphere of "smart cities" takes into account the main components of their development and is an end-to-end task in the field of digitalization of state and municipal services and an in-depth reform of promoting business models and product marketing. Connectivity and safety of digitalized system will also form the behavior of the population through their inclination towards digital components and intelligence, which ensures sustainability, adaptive and future-oriented evaluation of risks (Apostu et al., 2022).

3. Practice of introduction of the "smart cities" concept

In order to activate the use of modern digital technologies, the states arrange various contests with prize funds.

In Russia, there is an annual contest "The best municipal practice", including a nomination related to integration of digital technologies or platform solutions for improving municipal facilities, i. e. what makes the basis of a "smart city" functioning[15]. This contributes to the accumulation of the best practices. The contest offers a prize fund of 200 million rubles in this nomination.

[15] Order of the Ministry of Construction of the Russian Federation No. 368/pr of 09.07.2020. (2020). *Official Internet portal of legal information*. http://www.pravo.gov.ru

The number of applications grows every year, which ensures involvement of various types of municipal entities (in 2020, 59 applications from 28 Russian subjects were submitted, in 2021 – 95 applications from 39 regions, and in 2022 – 101 applications from 41 regions).

To select among the applications, 58 criteria are used, including:

– the prospects for reproducing in other municipal entities;

– the possibilities for the local population participation;

– the degree of advanced technologies introduction;

– the interrelation between the practice implementation and the IQ index growth;

– the compliance with the current normative legal acts in the sphere under study;

– the possibility to resolve the problems existing in the municipal entity, etc. (Antonova, 2020).

For example, in 2021, the contest winners were Kaluga (organization of automated dispatcher service of "Kalugaoblvodokanal" state enterprise) and Strigunovskoye rural settlement of Borisovskiy region of Belgorod oblast (introduction of "Memorial" – an interactive database of the existing cemeteries)[16].

The most popular trends among the contest participants are:

– forming digital platforms or creating services of feedback with the local residents in the sectors most demanding them;

– modernizing the functioning of energy, heat and water supply networks, associated with the local issues under the authority of local self-government bodies.

Speaking of the global contests, one should mention Intelligent Community Awards[17] and AI City Challenge[18].

Intelligent Community Awards annually marks the contributions of territorial entities, intellectual communities and partners from public and private sectors. The program pursues two goals: to mark the achievements of communities in developing the inclusive flourishing based on information and communication technologies and to collect data for ICF research programs.

AI City Challenge was founded to stimulate development and use of artificial intelligence in urban environments. This is manifested, for example, in improving transportation by increasing the efficiency of road traffic and safety, improving the processes of exploiting buildings by increasing their energy efficiency, reducing collapses in retail by speeding up servicing at the cash register, etc. The common point for all those various solutions

16 Tikhaleva, E. Yu. (2022). Using digital technologies at the modern stage of reforming local self-government. In: *State and municipal governance in Russia: status, problems and prospects*. Works of the All-Russia scientific-practical conference (p. 150). Perm: Perm branch of RANEPA.

17 *Intelligent Community Forum*. https://www.intelligentcommunity.org/awards

18 *AI City Challenge*. https://www.aicitychallenge.org

is extracting useful information from multiple sensors by online streaming and package analysis of bog data (surveillance data).

Besides contests, governments may create websites demonstrating promising solutions in the sphere of introducing digital technologies, which particular cities use in any convenient form.

In the Russian Federation, one example is the Internet resource "Bank of solutions for a smart city"[19], comprising projects in the main directions of social life development (residential-communal, transport sphere, etc.). This refers to simplifying the processes of infrastructure management (development of automated software), reducing costs for city facilities servicing (control automation), or simplifying citizens' life (smart road crossing). The website contains passports of projects, which show the project content (its plan, including areas of implementation, the possible result of implementation (estimated and actual), the required functional properties, the developer), the period required for implementation, the financial costs, and the project integration in particular structures.

The leader in implementing these technologies in the Russian Federation is Moscow (in 2020 – 56th position in the global ranking of "smart cities"; 44th position in the ranking of smart cities by Z/Yen Group Limited (ranking of business activity of municipal entities)) (Esayan & Truntsevskiy, 2020). This is logical and reflects the trends forming in the global community. Apparently, the most advanced technologies are concentrated in capital cities (the examples are London and Seoul (Lee & Nam, 2021)).

For example, in London, within the "smart city" concept, such projects are supported as Barclays Cycle Hire (an application with which citizens may receive information about the availability and use of hired bicycles), Listen London Platform (a social networks application for listening to the cities topical problems), Love Clean London (a service in which citizens may inform the authorities about the drawbacks related to the cleanliness of the London streets and parks), etc.

Also, the Russian Ministry of Construction annually forms the IQ ranking of cities, which implies identifying the cities achieving the greatest success in digitalization. It uses 47 indices divided into 10 groups. Special attention is paid to balancing the indices, as high values in a separate group do not always testify to the efficiency of using digital technologies in general. As a result of 2021, Moscow receives the highest IQ index among the large cities (over one million people), and the city of Sarov in Nizhegorodskaya oblast – among municipal entities with less than one hundred thousand people[20].

---

[19] Smart city: departmental project of the Ministry of Construction of the Russian Federation. https://russiasmartcity.ru

[20] Tikhaleva, E. Yu. (2022). Using digital technologies at the modern stage of reforming local self-government. In: *State and municipal governance in Russia: status, problems and prospects*: works of the All-Russia scientific-practical conference (p. 151). Perm: Perm branch of RANEPA.

However, one should note that, in compliance with the federative structure of the country, Moscow has the status of a city of federal significance; hence, stemming from the Russian Constitution, it is a subject of the Russian Federation. In this research, we accentuate the analysis of development of municipal entities, first of all, urban districts.

Speaking of international rankings, one should pay attention to Smart City Index (developed by IMD's World Competitiveness Center (WCC) join forces with the Singapore University of Technology and Design (SUTD)), taking into account both economic and technological indicators: mobility, safety, prospects of development, etc. (the total of five groups of indicators divided by the respective criteria). As a result of 2021, Moscow ranked 54th and Saint Petersburg 79th[21].

The ranking of technological cities of the future is developed by an analytical agency fDi Intelligence, taking into account the infrastructure development and the ability to attract investments[22].

The strategic and consulting bureau Eden Strategy Institute annually publishes the ranking of Top 50 Smart City Government with three groups of indicators: sphere, scale and integration[23].

When implementing a "smart city" concept, it is expedient to the benchmarking (etalon estimation) technologies, modeling and ranking methods (Kamolov et al., 2022).

Benchmarking has been rather broadly used recently. This technology is based on comparing the significant aspects of a specific type of activity with the competitors' results, which is very promising in relation to implementing innovations in municipal entities. It implies constantly searching for new ideas, their actual adaptation and further using in practice with a view of improving own performance. Benchmarking can be also viewed as a tool of control (the main methods are evaluation and comparison, i. e. statistical methods) (Xu et al., 2022). At that, it is important to precisely define the parameters used for comparison, the objects suitable for analysis, the practical opportunities for adaptation, and the desired results. In this regard, there is comparative benchmarking (orients toward the planned changes judging by the level of municipal entity development compared to the leaders in the respective sphere) and procedural benchmarking (implies improving the activity in practical terms, through selecting the necessary set of tools to achieve the goal) (Moustaka et al., 2021).

Benchmarking is a consecutive implementation of a number of procedures; it must be systematic, thus, it cannot be used in a single situation. Most often, this technology includes such stages as:

---

21 Data shows effects of COVID-19 and climate change on citizens' perceptions of how 'smart' their cities are. (2021, October). IMD. https://www.imd.org/news/updates/data-shows-effects-of-covid-and-climate-change-on-citizens-perceptions-of-how-smart-their-cities-are

22 *FDI Intelligence*. https://www.fdiintelligence.com

23 *Eden Strategy Institute*. https://www.edenstrategyinstitute.com

– reengineering (implies a complex approach to solving the existing problems through monitoring, understanding the need to reconsider the current managerial processes and their quality reorientation towards a particular result) (Saragih et al., 2021);

– reaching a certain level of characteristics of competitiveness of a municipal entity;

– analysis and evaluation of various options in the municipal entity development based on the available positive experience of competitors;

– selecting a specific way of improving the municipal entity with a view of raising particular indicators.

Modeling allows objectively evaluating the current condition of the municipal entity with a view of satisfying the needs of its residents, and to forecast the use of the available potential to reach the goals. It allows using innovations combined with digital technologies on the condition that the information received is implemented in a complex and systematized manner and the technologies are introduced based on the specificity of activity of the particular city.

The method of ranking in relation to the "smart city" development implies the possibility to objectively estimate the activities of all elements of the "smart city", reveal the existing drawbacks and find ways to eliminate them. This method is aimed at increasing the ranking of a particular municipal entity among "smart cities". In this regard, it is possible to involve experts and analysts to perform respective works, which may be difficult to implement at the local level due to limited resources. That is why, such specialist may work as a public service.

Another important indicator of effective introduction of the "smart cities" concept, complying with the future requirements, is, in our opinion, their sustainability, including the following:

1. The current social-economic development determined by a road map of the community with a view of local sustainable development and reasonable policy, facilitating investment initiatives and integrated centers for the local growth from strategic viewpoint.

2. Supporting the development institutions which use the specificity, authenticity and potential of development. For example, not all industries sufficiently use the natural and anthropogenic potential and increase the value of the existing human capital and demographic support both by increasing the local population and mobility (internal mobility or immigrants).

3. Encouraging foreign investments to accomplish/diversify economic and social activity, as well as to preserve and develop the local qualified workforce.

4. Proper management at the local level should include, at least, three components: digitalization; reasonable development of public services, transport and communication, and quality of life.

5. The healthcare network supervised by the local community must be focused on the services improving quality of life in a megalopolis and the districts of regional impact,

specializing in the risks of zonal medical diseases, in order to assist public-private and municipal partnership in the sphere of preventive, therapeutic and rehabilitation medical services, to complement the network of healthcare services of national or international significance.

6. The educational network must maintain high quality of education in the spheres of specialization demanded by the local and regional labor markets, in order to retain the younger generation with attractive jobs, temporary or constant, as an alternative to external migration. University education and continuous education services must ensure integration into the national educational network as a center for advanced experience in the sphere of professional training or specialization. The educational sector must facilitate links between educational establishments and business by means of scholarships, probation periods and preliminary training before employment, as well as due management of structural demand in the labor market.

Apparently, in parallel with municipal programs on forming "smart cities", it is necessary to implement programs on energy saving and increasing energy efficiency, and forming the modern city environment[24].

Unfortunately, ideal solutions are usually hard to implement. Accordingly, introduction of the "smart cities" concept is accompanied with problems emerging when certain results are obtained.

Speaking about the obstacles faced by the development of "smart cities" in Russia, these include (Abramov & Andreev, 2022):

– governmental grants in most municipal entities (Snyrenkov, 2019);

– deficit of local qualified personnel;

– passivity of the local population and authorities, reluctance to introduce innovations;

– the existing gap (inequality) between large cities and small municipal entities, which does not allow the latter to fully use the scientific-technical achievements due to the lacking access to digital technologies (Molchanova, 2019);

– underestimated complex approach to implementing the goals of "smart cities" formation, the lack of the necessary coordination of activities, isolation of the intellectual systems used (Malchenko, 2020);

– long-term projects implemented.

Conclusion

"Smart cities" imply creating a certain industry in the sphere of information and communication technologies, a mechanism of interrelations between authorities and the population, and the use of modern digital technologies in everyday urban life.

[24] Khudzhatov, M. B. (2022). Municipal programs. *SPS KonsultantPlyus*.

"Smart city" may generate various private initiatives and partnerships, but usually it functions under the aegis of a municipality. City authorities are the main driving force of the "smart city" activity; this said, usually the authorities and private technological corporations have close relationships. "Smart city" innovations ultimately serve as a superstructure of the local self-government: they ease the work of a municipal administration, rendering public and municipal services and relations between officials and citizens. That is why the advanced forms of immediate implementation of local self-government (initiatives, crowdfunding) may become a support in the development of the phenomenon under study.

Therefore, a "smart city" plays the role of an ecosystem determining convenient and safe living conditions for the people. A "smart city" may be viewed as a city, effectively working in the promising directions of economy, management, transport mobility, ecology, built on a reasonable combination of the authorities' regulations and the activity of eager residents aware of the problems of their city.

Thus, the main goal of implementation of the ideas under study is improving the life quality of the population (achieved by providing a constant interaction between the local authorities and the population, involving the latter into solving the topical problems at the local level in real time mode and rendering maximal services to the population) and the quality of city management (achieved by introducing advanced digital and engineering solutions and optimizing the use of the existing resources).

Today, "smart cities" offer attractive prospects, strategy and relevant view into the future, operatively trace and integrate the status of the crucial systems of their infrastructure.

Having analyzed the basic legal acts determining the essence of the "smart cities" concept, we may conclude that most of them are of sublegislative and scattered character and include the main criteria of referring certain territorial entities to "smart cities". In this regard, we consider it necessary to adopt a common federal law in the Russian Federation, which would stipulate a complex approach and standards of "smart cities" regulation (stipulate the key notions, goals and spheres of development, competencies of authorities at all levels).

The "smart city" concept, in our opinion, is a promising direction of improving the institute of local self-government, facilitating the implementation of such basic principles as people's rule and independence from other authorities. This may also raise the credibility of the authorities through openness of their functioning for the residents, which is considered necessary nowadays to carry out research in the sphere of both constitutional and municipal law.

The imperative of well-being and improved life quality in the context of "smart cities" may be reached only if the intelligent services, playing such an important role in the "smart cities" concept, correlate to the needs, expectations and skills of the city residents. Given

that the Internet of Things generates and opens access points to huge amounts of data in real time mode, referring to well-being and life quality, such as citizens' opinions, as well as to the latest events related to normative-legal basis, debates, political decisions and elaboration of not only federal but also municipal policy, the promising directions are: transformation of the immediate forms of local self-government into electronic format; using the potential inherent in this system to improve efficiency of management, implemented in "smart cities", all over the state.

References

Abramov, V., & Andreev, V. (2022). Problems and prospects of digital transformation of state and municipal governance in a region (the case of the Kemerovo region). *Ars Administrandi*, *14*(4), 667–700. (In Russ.). https://doi.org/10.17072/2218-9173-2022-4-667-700

Antonova, A. V. (2020). Development of the city assessment technique by the criteria of a "smart" city. *Management Issues*, *6*(67), 122–141. (In Russ.). https://doi.org/10.22394/2304-3369-2020-6-122-141

Apostu, S., Vasile, V., Vasile, R., & Rosak-Szyrocka, J. (2022). Do Smart Cities Represent the Key to Urban Resilience? Rethinking Urban Resilience. *International Journal of Environmental Research and Public Health*, *19*(22), 15410. https://doi.org/10.3390/ijerph192215410

Attaran, H., Kheibari, N. A., & Bahrepour, D. (2022). Toward Integrated Smart City: a New Model for Implementation and Design Challenges. *GeoJournal*, *87*(S4), 511–526. https://doi.org/10.1007/s10708-021-10560-w

Bekbolat B. M., Mahatov N. B., & Damysbek B. D. (2021). The Convenience of Smart Technologies for Cities. *Molodoy ucheniy*, *9*(351), 36–38.

Belov, V. I., & Smirnov, I. I. (2018). Managing cities' life activity through implementation of the "Smart city" concept. *Sinergiya Nauk*, *24*, 439–445. (In Russ.).

Caprotti, F., & Liu, D. (2020). Platform Urbanism and the Chinese Smart City: the Coproduction and Territorialisation of Hangzhou City Brain. *GeoJournal*, *87*(3), 1559–1573. https://doi.org/10.1007/s10708-020-10320-2

Csukás, M., & Szabó, R. Z. (2022). What are the conditions to become smart? *Informacios Tarsadalom*, *22*(2), 9–26. https://doi.org/10.22503/inftars.xxii.2022.2.1

Esayan, A. K., & Truntsevskiy, Yu. V. (2020). Common approaches to the legal regulation of technologies in the smart city area. *Public International and Private International Law*, *1*, 36–41. (In Russ.).

European Economic and Social Committee. (2015). Opinion of the European Economic and Social Committee on "Smart cities as drivers for development of a new European industrial policy" (own-initiative opinion). *Official Journal of the European Union*, *58*, 24–33.

Fedorchenko, S. N., & Karlyavina, E. (2021). Smart City: the arrival of a New Democracy or Digital Totalitarianism? *Journal of Political Research*, *5*(1), 3–22. https://doi.org/10.12737/2587-6295-2021-5-1-3-22

Ganin, O., & Ganin, I. (2014). "Smart City": Development Prospects and Trends. *Ars Administrandi*, *1*, 124–135. (In Russ.).

Golikova, Yu. B. (2020). Economics and innovation management in cities and regions as a basis for forming the concept of the future "Smart city". *Sovremennye aspekty ekonomiki*, *3*–2(271), 18–27. (In Russ.).

Jothimani, P., Chenniappan, P., & Chidambaranathan, V. (2022). Factors Impinge on the Development of a Smart City: a Field Study. *Environmental Science and Pollution Research*, *29*(57), 86298–86307. https://doi.org/10.1007/s11356-021-17930-4

Kamolov, S., Glazyeva, S. S., & Tazhiyeva, S. K. (2020). Smart cities in Eurasian economic union: outlook for Russian regional technological leadership. *Russian Economic Journal*, *5*, 64–82. (In Russ.). https://doi.org/10.33983/0130-9757-2022-5-64-82

Kostko, N., Pecherkina, I., & Popkova, A. (2022). Implementation models for the "smart city" concept in the strategies for socio-economic development of large cities in the Russian Federation. *Public Administration Issues*, *4*, 197–223. (In Russ.). https://doi.org/10.17323/1999-5431-2022-0-4-197-223

Kuranov, A. S. (2020). "Smart city" as "safe city". *Obrazovaniye i nauka v Rossii i za rubezhom*, *4*(68), 191–194. (In Russ.).

Langendahl, P. (2021). The Politics of Smart Farming Expectations in Urban Environments. *Frontiers in Sustainable Cities*, *3*, 1–8. https://doi.org/10.3389/frsc.2021.691951

Lee, J. P., & Nam, J. H. (2021). Analysis of Regional Characteristics and Deficiency Areas of Smart City Living Service : Focused on the Seoul. *Journal of Korea Planning Association*, *56*(5), 30–43. https://doi.org/10.17208/jkpa.2021.10.56.5.30

Malchenko, Yu. A. (2020). From Digital Divide to Consumer Adoption of Smart City Solutions: a Systematic Literature Review and Bibliometric Analysis. *Vestnik of Saint Petersburg University. Mathematics*, *3*, 316–335.

Molchanova, V. A. (2019). From a smart city to a just city: problems of sustainable development under digital economy. *Kreativnaya ekonomika*, *13*(12), 2371–2386. (In Russ.). https://doi.org/10.18334/ce.13.12.41379

Moustaka, V., Maitis, A., Vakali, A., & Anthopoulos, L. (2021). Urban Data Dynamics: A Systematic Benchmarking Framework to Integrate Crowdsourcing and Smart Cities' Standardization. *Sustainability*, *13*(15), 8553. https://doi.org/10.3390/su13158553

Nizamieva, E. B. (2021). Smart city development as a driver of efficiency reorganization and improvement of cities. *Vestnik Tomskogo gosudarstvennogo arkhitekturno-stroitelnogo universiteta. Journal of Construction and Architecture*, *23*(6), 19–27. (In Russ.). https://doi.org/10.31675/1607-1859-2021-23-6-19-27

Saragih, L. R., Dachyar, M., & Zagloel, T. Y. M. (2021). Business Process Reengineering at ICT Operations, In Managing Smart Cities as New Customers (Non-Human). *International Journal of Technology*, *12*(2), 378–389. https://doi.org/10.14716/ijtech.v12i2.4418

Sharova, A. A. (2019). "Smart city" project as a complex solution to improve the quality of managing cities and standard of living in them. *Meridian-journal*, *14*(32), 3–5. (In Russ.).

Shkvarya, L. V., & Semenov, A. S. (2020). Smart cities: necessity and development strategies. *Informatsiya i Innovatsii*, *15*(2), 52–58. (In Russ.). https://doi.org/10.31432/1994-2443-2020-15-2-52-58

Shnyrenkov, E. A. (2019). Economic problems of "Smart city" project development in Russian cities. *Ekonomika i predprinimatelstvo*, *4*(105), 304–307. (In Russ.).

Strelnikova, S. A., & Tsutsiev, M. A. (2017). Spatial development of Russia: issues of strategy (interview with P. A. Chistyakov, Vice President of the Center for infrastructure economics). *Byudzhet*, *2*, 76–79. (In Russ.).

Treude, M., Schüle, R., & Haake, H. (2022). Smart Sustainable Cities – Case Study Südwestfalen Germany. *Sustainability*, *14*(10), 5957. https://doi.org/10.3390/su14105957

Vukovic N. A., Larionova V. A., & Morganti P. (2021). Smart Sustainable Cities: Smart Approaches and Analysis. *Ekonomika regiona*, *17*(3), 1004–1013. https://doi.org/10.17059/ekon.reg.2021-3-20

Xu, J., Song, R., & Zhu, H. (2022). Evaluation of Smart City Sustainable Development Prospects Based on Fuzzy Comprehensive Evaluation Method. *Computational Intelligence and Neuroscience*, *2022*, 1–11. https://doi.org/10.1155/2022/5744415

Yakushina, O. I. (2021). Organizing public space in the contemporary city within "open" and "smart" city framework. *Theory and Practice of Social Development*, *4* (158), 33–42. (In Russ.). https://doi.org/10.24158/tipor.2021.4.5

Author information

Elena Yu. Tikhaleva – Candidate of Juridical Sciences, Associate Professor, Department of Constitutional, Administrative and Criminal Law, Middle Russia Institute of Management – branch of the Russian Presidential Academy of National Economy and Public Administration
Address: 12 Oktyabrskaya Str., 302028 Orel, Russian Federation
E-mail: columbijka@mail.ru
ORCID ID: https://orcid.org/0000-0003-4612-4722
Google Scholar ID: https://scholar.google.com/citations?user=Rt1gtkoAAAAJ
RSCI Author ID: https://elibrary.ru/author_items.asp?authorid=852559

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 – September 9, 2023
Date of approval – February 15, 2023
Date of acceptance – August 15, 2023
Date of online placement – August 20, 2023

Научная статья
УДК 34:349.44:004:352
EDN: https://elibrary.ru/djkvsd
DOI: https://doi.org/10.21202/jdtl.2023.35

«Умные города»: правовое регулирование и потенциал развития

Елена Юрьевна Тихалева

Среднерусский институт управления – филиал Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации
г. Орел, Российская Федерация

Ключевые слова

Законодательство,
местное самоуправление,
муниципальное образование,
муниципальное право,
право,
правовое регулирование,
умный город,
цифровая платформа,
цифровизация,
цифровые технологии

Аннотация

Цель: исследование тенденций развития концепции «умных городов» и их правового регулирования.

Методы: в работе использовались общенаучные (индукция, дедукция) и специальные (системно-структурный, сравнительно-правовой анализ) методы. Кроме того, в исследовании применялись методы обзорного анализа, чтобы изучить статус-кво для «умных городов». До сих пор инновационные исследовательские подходы в рамках рассмотрения концепций «умного города» встречаются редко, как и перспективы, касающиеся целевого управления знаниями и сотрудничества соответствующих заинтересованных сторон. Если говорить о специальных методах исследования цифровых отношений, был использован контент-анализ (метод создания воспроизводимых и обоснованных выводов из текстов (или другого значимого материала) в контексте их использования). Поскольку результаты предыдущих исследований и концепций, касающиеся «умных городов», доступны, также применялся дедуктивный контент-анализ.

Результаты: дана характеристика общественных отношений, складывающихся в процессе развития концепции «умных городов». Обозначены ключевые правовые акты, принципы формирования и функционирования «умных городов» с учетом российского и зарубежного опыта. В связи с этим приведены примеры успешных практик из деятельности как российских, так и зарубежных муниципальных образований с учетом проводимых конкурсов, и рейтингов, определяемых центральными структурами. Обобщены популярные направления, широко внедряемые на местном уровне, и выделены возможные проблемы реализации данного проекта в нашем государстве.

Научная новизна: в статье осуществлен анализ имеющегося правового регулирования, а также результатов внедрения концепции «умных городов». Определены перспективные технологии и методы, необходимые для достижения целей реализации концепции. Выделены элементы, обеспечивающие устойчивость «умных городов», отвечающих требованиям будущего. Высказана авторская позиция о тесной взаимосвязи данного явления с институтом местного самоуправления в контексте возможного развития последнего с подключением искусственного интеллекта в процесс по принятию управленческих решений. Прежде всего речь идет об использовании потенциала интернета вещей. На практике возникает немалое количество проблем, связанных с реализацией нормативно закрепленных положений, что подразумевает необходимость проведения дальнейших научных исследований в анализируемой сфере.

Практическая значимость: обусловлена недостаточной разработанностью данных об особенностях и перспективах внедрения идеи «умных городов». Положения проведенного исследования позволят осуществлять эффективную работу по совершенствованию механизмов правового регулирования рассматриваемой концепции и ее повсеместному распространению.

Для цитирования

Тихалева, Е. Ю. (2023). Умные города: правовое регулирование и потенциал развития. *Journal of Digital Technologies and Law*, *1*(3), 803–824. https://doi.org/10.21202/jdtl.2023.35

Список литературы

Абрамов, В., Андреев, В. (2022). Проблемы и перспективы цифровой трансформации государственного и муниципального управления в регионе (на примере Кемеровской области). *Ars Administrandi (Искусство управления)*, *14*(4), 667–700. EDN: https://elibrary.ru/ctwmyg. DOI: https://doi.org/10.17072/2218-9173-2022-4-667-700

Антонова, А. В. (2020). Развитие методики оценки города по критериям «умного» города. *Вопросы управления*, *6*(67), 122–141. EDN: https://elibrary.ru/ugsecz. DOI: https://doi.org/10.22394/2304-3369-2020-6-122-141

Белов, В. И., Смирнов, И. И. (2018). Управление жизнедеятельностью городов посредством реализации концепции «Умный город». *Синергия Наук*, *24*, 439–445. https://elibrary.ru/usruiy

Ганин, О. Б., Ганин, И. О. (2014). «Умный город»: перспективы и тенденции развития. *Ars administrandi (Искусство управления)*, *1*, 124–135.

Голикова, Ю. Б. (2020). Экономика и управление инновациями в городах и регионах как основа формирования концепции будущего «Умный город». *Современные аспекты экономики*, *3-2*(271), 18–27. https://elibrary.ru/vovkmj

Есаян, А. К., Трунцевский, Ю. В. (2020). Общие подходы к нормативному правовому регулированию технологий в сфере «Умный город». *Международное публичное и частное право*, *1*, 36–41. https://doi.org/10.18572/1812-3910-2020-1-36-41

Камолов, С. Г., Глазьева, С. С., Тажиева, С. К. (2022). Умные города ЕАЭС как перспектива российского регионального технологического лидерства. *Российский экономический журнал*, *5*, 64–82. EDN: https://elibrary.ru/bdbkgd. DOI: https://doi.org/10.33983/0130-9757-2022-5-64-82

Костко, Н. А., Печеркина, И. Ф., Попкова, А. А. (2022). Модели реализации концепции «Умный город» в стратегиях социально-экономического развития крупных городов Российской Федерации. *Вопросы государственного и муниципального управления*, *4*, 197–223. EDN: https://elibrary.ru/uolfky. DOI: https://doi.org/10.17323/1999-5431-2022-0-4-197-223

Куранов, А. С. (2020). «Умный город» как «благополучный город». *Образование и наука в России и за рубежом*, *4*(68), 191–194. https://elibrary.ru/nzrlcj

Молчанова, В. И. (2019). От умного города к городу справедливому: проблемы устойчивого развития в условиях цифровой экономики. *Journal of Creative Economy*, *13*(12), 2371–2386. EDN: https://elibrary.ru/yeytsk. DOI: https://doi.org/10.18334/ce.13.12.41379

Низамиева, Э. Р. (2021). Внедрение принципов умного города как драйвер к реорганизации и повышению эффективности существующих городов. *Вестник Томского государственного архитектурно-строительного университета*, *23*(6), 19–27. EDN: https://elibrary.ru/xcwmwn. DOI: https://doi.org/10.31675/1607-1859-2021-23-6-19-27

Стрельникова, С. А., Цуциев, М. А. (2017). Пространственное развитие России: вопросы стратегии (интервью с П. А. Чистяковым, вице-президентом Центра экономики инфраструктуры). *Бюджет*, *2*, 76–79.

Шарова, А. А. (2019). Проект «Умный город» как комплексное решение повышения качества управления городами и уровня жизни в них. *Научный электронный журнал Меридиан*, *14*(32), 3–5. https://elibrary.ru/urppbj

Шкваря, Л. В., Семенов, А. (2020). Smart Cities: Necessity and Development Strategies. *Информация и Инновации*, *15*(2), 52–58. EDN: https://elibrary.ru/uzffyx. DOI: https://doi.org/10.31432/1994-2443-2020-15-2-52-58

Шныренков, Е. А. (2019). Экономические проблемы развития проекта «Умный город» в российских городах. *Экономика и предпринимательство*, *4*(105), 304–307. https://elibrary.ru/jwaqgd

Якушина, О. И. (2021). Организация социального пространства современных городов в свете концепций «открытого» и «умного» города. *Теория и практика общественного развития*, *4*(158), 33–42. EDN: https://elibrary.ru/kkughg. DOI: https://doi.org/10.24158/tipor.2021.4.5

Apostu, S., Vasile, V., Vasile, R., & Rosak-Szyrocka, J. (2022). Do Smart Cities Represent the Key to Urban Resilience? Rethinking Urban Resilience. *International Journal of Environmental Research and Public Health*, *19*(22), 15410. https://doi.org/10.3390/ijerph192215410

Attaran, H., Kheibari, N. A., & Bahrepour, D. (2022). Toward Integrated Smart City: a New Model for Implementation and Design Challenges. *GeoJournal*, *87*(S4), 511–526. https://doi.org/10.1007/s10708-021-10560-w

Bekbolat B. M., Mahatov N. B., & Damysbek B. D. (2021). The Convenience of Smart Technologies for Cities. *Молодой ученый*, *9*(351), 36–38. https://elibrary.ru/izvhbr

Caprotti, F., & Liu, D. (2020). Platform Urbanism and the Chinese Smart City: the Coproduction and Territorialisation of Hangzhou City Brain. *GeoJournal*, *87*(3), 1559–1573. https://doi.org/10.1007/s10708-020-10320-2

Csukás, M., & Szabó, R. Z. (2022). What are the conditions to become smart? *Informacios Tarsadalom*, *22*(2), 9–26. https://doi.org/10.22503/inftars.xxii.2022.2.1

European Economic and Social Committee. (2015). Opinion of the European Economic and Social Committee on «Smart cities as drivers for development of a new European industrial policy» (own-initiative opinion). *Official Journal of the European Union*, *58*, 24–33.

Fedorchenko, S. N., & Karlyavina, E. (2021). Smart City: the arrival of a New Democracy or Digital Totalitarianism? *Journal of Political Research*, *5*(1), 3–22. EDN: https://elibrary.ru/cpmywd. DOI: https://doi.org/10.12737/2587-6295-2021-5-1-3-22

Jothimani, P., Chenniappan, P., & Chidambaranathan, V. (2022). Factors Impinge on the Development of a Smart City: a Field Study. *Environmental Science and Pollution Research*, *29*(57), 86298–86307. https://doi.org/10.1007/s11356-021-17930-4

Langendahl, P. (2021). The Politics of Smart Farming Expectations in Urban Environments. Frontiers in Sustainable *Cities*, *3*, 1–8. https://doi.org/10.3389/frsc.2021.691951

Lee, J. P., & Nam, J. H. (2021). Analysis of Regional Characteristics and Deficiency Areas of Smart City Living Service : Focused on the Seoul. *Journal of Korea Planning Association*, *56*(5), 30–43. https://doi.org/10.17208/jkpa.2021.10.56.5.30

Malchenko, Yu. A. (2020). From Digital Divide to Consumer Adoption of Smart City Solutions: a Systematic Literature Review and Bibliometric Analysis. *Vestnik of Saint Petersburg University. Mathematics*, *3*, 316–335. https://elibrary.ru/txeveg

Moustaka, V., Maitis, A., Vakali, A., & Anthopoulos, L. (2021). Urban Data Dynamics: A Systematic Benchmarking Framework to Integrate Crowdsourcing and Smart Cities' Standardization. *Sustainability*, *13*(15), 8553. https://doi.org/10.3390/su13158553

Saragih, L. R., Dachyar, M., & Zagloel, T. Y. M. (2021). Business Process Reengineering at ICT Operations, In Managing Smart Cities as New Customers (Non-Human). *International Journal of Technology*, *12*(2), 378-389. https://doi.org/10.14716/ijtech.v12i2.4418

Treude, M., Schüle, R., & Haake, H. (2022). Smart Sustainable Cities—Case Study Südwestfalen Germany. *Sustainability*, *14*(10), 5957. https://doi.org/10.3390/su14105957

Vukovic N. A., Larionova V. A., & Morganti P. (2021). Smart Sustainable Cities: Smart Approaches and Analysis. *Экономика региона*, *17*(3), 1004–1013. EDN: https://elibrary.ru/yqyxyu. DOI: https://doi.org/10.17059/ekon.reg.2021-3-20

Xu, J., Song, R., & Zhu, H. (2022). Evaluation of Smart City Sustainable Development Prospects Based on Fuzzy Comprehensive Evaluation Method. *Computational Intelligence and Neuroscience*, 1–11. https://doi.org/10.1155/2022/5744415

Сведения об авторе

Тихалева Елена Юрьевна – кандидат юридических наук, доцент, доцент кафедры конституционного, административного и уголовного права, Среднерусский институт управления – филиал Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации
Адрес: 302028, Российская Федерация, г. Орел, ул. Октябрьская, 12
E-mail: columbijka@mail.ru
ORCID ID: https://orcid.org/0000-0003-4612-4722
Google Scholar ID: https://scholar.google.com/citations?user=Rt1gtkoAAAAJ
РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=852559

Конфликт интересов

Автор заявляет 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: 10.19.25 / Правовой режим информации, информационных систем и сетей
Специальность ВАК: 5.1.2 / Публично-правовые (государственно-правовые) науки

История статьи

Дата поступления – 9 сентября 2022 г.
Дата одобрения после рецензирования – 15 февраля 2023 г.
Дата принятия к опубликованию – 15 августа 2023 г.
Дата онлайн-размещения – 20 августа 2023 г.

Research article
DOI: https://doi.org/10.21202/jdtl.2023.36

Facial Recognition Technology and Ensuring Security of Biometric Data: Comparative Analysis of Legal Regulation Models

Dana Utegen ✉

M. Narikbayev KAZGUU University
Astana, Republic of Kazakhstan

Baurzhan Zh. Rakhmetov

M. Narikbayev KAZGUU University
Astana, Republic of Kazakhstan

Keywords

Biometric authentication,
biometric data,
digital technologies,
facial recognition,
technologies,
identification,
law,
legal regulation,
personal data,
privacy,
security

Abstract

Objective: to specify the models of legal regulation in the sphere of biometric identification and authentication with facial recognition technology in order to elaborate recommendations for increasing information security of persons and state-legal protection of their right to privacy.

Methods: risk-oriented approach in law and specific legal methods of cognition, such as comparative-legal analysis and juridical forecasting, are significant for the studied topic and allow comparing the legal regulation models used in foreign countries and their unions in the sphere of biometric identification and authentication with facial recognition systems, forecasting the possible risks for the security of biometric data, taking into account the prospects of further dissemination of the modern facial recognition technology, and to shape recommendations on legal protection of biometric data.

✉ Corresponding author

Results: the ways are proposed to further improve legislation of the Republic of Kazakhstan and other countries currently developing the legal regulation of biometric data, regarding the admissible criteria for using the facial recognition technology, the elaboration of categorization of biometric systems with a high and low risk levels (by the example of the experience of artificial intelligence regulation in the European Union), and the necessity to introduce a system of prohibitions of mass and unselective surveillance of humans with video surveillance systems, etc.

Scientific novelty: consists in identifying a positive advanced foreign experience of developing legal regulation in the sphere of facial recognition based on biometry (European Union, the United States of America, the United Kingdom of Great Britain and Northern Ireland), which can be used for further improvement of the national legislation in order to create more effective mechanisms of legal protection of personal data, including biometric information.

Practical significance: based on risk-oriented approach and comparative analysis, the research allows elaborating measures for enhancing the legal protection of biometric data and ensuring effective protection of civil rights and freedoms by forecasting further expansion of the modern facial recognition technology.

For citation

Utegen, D., Rakhmetov, B. (2023). Facial Recognition Technology and Ensuring Security of Biometric Data: Comparative Analysis of Legal Regulation Models. *Journal of Digital Technologies and Law, 1*(3), 825–844. https://doi.org/10.21202/jdtl.2023.36

Contents

Introduction

Most of the developed countries invest substantial funds into using facial recognition technology. This technology compares and analyzes two or more images of faces, identifies them using biometric data, and determines who the data belong to with

the available bases[1] (Gill, 1997). The biometric data used for facial recognition are stored in the biometric authentication system (Sarabdeen, 2022). The biometric authentication system is an information system that allows identifying a person based on some of their main physiological and behavioral characteristics[2]. The examples of biometric indicators are fingerprints, face, iris, palmprint, retina, hand geometry, voice, signature, and gait[3]. It is based on hardware systems of data collection, integrating software components which use mathematical algorithms to analyze data and identify a personality[4].

Considering various groups of legal relations in law-application and enforcement activity of executive authorities, chosen in this research for comparative analysis of the states, the implementation of which may use facial recognition technologies, one should distinguish the following objects, referred to vulnerable ones:

1) objects vulnerable in terms of terrorism;
2) critical state objects;
3) strategic objects of economic sectors having strategic significance;
4) hazardous industrial objects;
5) objects of mass gathering of people, etc.

Facial recognition technology is most often used by law enforcement bodies to identify people suspected in committing crimes. Analysis and identification takes places by obtaining photos, videos, driving licenses, public surveillance videos, photos from social networks, etc.[5]. Although facial recognition systems are used, in particular, for law and order protection and public safety provision, citizens are often surveyed without knowing about that, as there is no notification about surveillance. The use of facial recognition systems by law enforcement was criticized as biased, discriminating and lacking transparency.

International community generally supports the initiative of providing safety using digital technologies. According to the Resolution of the UNO Security Council, the member

---

1 Everything about facial recognition technology. *Www.cloudav.ru*. https://www.cloudav.ru/mediacenter/technology/facial-recognition-technology/ ; TAdviser – a portal for choosing technologies and suppliers. (2020). *TAdviser.ru*. https://www.tadviser.ru/index.php/

2 QUII. (2018). Biometric Recognition: definition, challenge and opportunities of biometric recognition systems. *IQUII*. https://medium.com/iquii/biometric-recognition-definition-challenge-and-opportunities-of-biometric-recognition-systems-d063c7b58209

3 Jain, A. (2008). Biometric authentication. *Scholarpedia*, 3(6), 3716. https://doi.org/10.4249/scholarpedia.3716

4 *Ibid*, *2*.

5 Resolutions of UNO Security Council S/RES/2396(2017). https://www.un.org/securitycouncil/ru/content/sres23962017

states call for active measures to combat terrorism threats and to prevent crime[6]. Due to the increased practice of fraud, falsification and forgery of personality identification documents, the recommendations of the UNO body in charge of global peace and safety referred to introducing systems of biometric data identification with a view of surveillance of terrorists or persons suspected in terrorist activity[7].

Besides ensuring safety, one should also mark the impact of the COVID-19 pandemic, which enhanced the use of facial recognition systems in struggling against the infection dissemination and controlling citizens' movement during the quarantine restrictions. The algorithms of facial recognition systems were used to control citizens' movements and wearing masks, checking body temperature in order to administer the measures of public healthcare provision (Chen & Wang, 2023; Johnson et al., 2022; Shore, 2022).

In this regard, of interest is the experience of legal regulation in the countries currently actively applying a system of biometric databases, aimed at simplifying the criminal investigation procedures and control over movement at borders.

1. United States of America: introduction and regulation of facial recognition technology

By the example of the United States of America, one should mark the practice of using surveillance cameras with facial recognition function in the context of antiterrorist measures after September 11, 2001. Based on the Border Security Act adopted by the US Congress, biometric identity documents were introduced[8]. Since 2004, the country introduced a system of taking fingerprints and including into a database of the images of people coming to the US. Checking biometric data with governmental databases is aimed at revealing the persons suspected in terrorism, wanted criminals or those previously violating the US immigration legislation. Thus, in less than half a year, a biometric database of over five million people was collected. Besides, the US security bodies took measures in relation to 3,800 foreigners based on the information obtained during biometric screening when visiting the USA[9]. The measures included detention of the suspects based on a warrant, refusal of acceptance at the border, or deportation to the country of last residence.

---

6 *Ibid*.

7 Resolution 2396 (2017), adopted by the Security Council on its 8148th session on December 21, 2017. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/460/27/PDF/N1746027.pdf?OpenElement

8 Markey, E. J. (2021, June 15). Text: S.2052 – 117th Congress (2021–2022): Facial Recognition and Biometric Technology Moratorium Act of 2021. https://www.congress.gov/bill/117th-congress/senate-bill/2052/text

9 Federal Register, Vol. 73, Iss. 245. (2008, December 19). https://www.govinfo.gov/content/pkg/FR-2008-12-19/html/E8-30095.htm

However, the tragic events of the 2001 terrorist attack did not cause but just facilitated the development of the previously existing fingerprints identification system.

In the US and other developed countries, facial recognition and facial expression analysis systems started to be developed in the 1960–1970-s in research laboratories funded by the Ministry of Defense and intelligence services. In 1990, new companies were created to commercialize the technology, which searched for target markets, in particular, among the institutions using their own computer networks, such as financial industry, business, large scale identification systems, passport services, public departments, law enforcement and penitentiary systems (Schweber, 2014). In 1999, he US Federal Bureau of Investigations developed and introduced an automated fingerprints identification system. This system combines records of fingerprints collected by federal law enforcement. It provides opportunities for automated search for fingerprints, electronic storage and exchange of images. In 2008, the system processes on average over 63,000 fingerprints a day, 91% of which scanned into the system in a digital form and the rest stored on a paper carrier[10].

In the recent years, the US practice accumulated a sufficient number of cases associated with the procedures of processing, storage and use of biometric data (Stepney, 2019). In this regard, it seems most important to study and analyze individual solutions in this category of issues, with a view of improving the legislation of the Republic of Kazakhstan.

In 2021, a case of Robert Williams was heard in the USA. The black man was arrested in 2020 for stealing watches from a shop in Detroit, Michigan. Although he had not visited that shop for several years, he was detained in the presence of his two daughters as a suspect of theft. The Detroit police department used facial recognition technology to identify a suspect by surveillance camera images. Thus, they used a database of driving licenses photos of the Michigan police department. However, facial identification appeared to be false, hence, an innocent person was kept in custody for 30 hours[11].

Unfortunately, this case is not the only one – the practice of holding innocent persons liable became frequent (Bowyer, 2004). In connection with the application of facial recognition technology, a research was carried out by the National Institute of Standards and Technology[12]. It showed that color bar takes place most often during facial

[10] FIRS IAFIS (Federal Bureau of Investigation). https://www.fbi.gov/how-we-can-help-you/need-an-fbi-service-or-more-information/freedom-of-informationprivacy-act/department-of-justice-fbi-privacy-impact-assessments/firs-iafis

[11] Harwell, D. (2021, April 13). Wrongfully Arrested Man Sues Detroit Police over False Facial Recognition Match. *Washington Post*. https://www.washingtonpost.com/technology/2021/04/13/facial-recognition-false-arrest-lawsuit/

[12] NIST (National Institute of Standards and Technology) (2000). https://www.nist.gov/

identification. Also, the facial recognition technology was widely used by law enforcement for identification of persons during meetings and demonstrations, investigations of misdemeanors, and arrests without any evidences of guilt (Buresh, 2021). As a result, the number of people who became victims of the unregulated surveillance and monitoring system is constantly growing[13].

After a number of consequences of faults of facial identification, the US civil society and international non-government organizations formed petitions calling for a mass prohibition of biometric recognition technologies allowing mass and discriminating surveillance[14]. Some of the American states initiated a Moratorium on the use of facial recognition technology. Later, a bill on facial recognition was proposed in the US, which restricts the application of this technology and its unethical use[15]. This document contains a list of restrictions of facial recognition technology application, including:

– immigration control,

– peaceful protests,

– establishing a personality of a criminal suspect.

According to the bill, law enforcement bodies are required to test the facial recognition system and submit annual reports on the efficiency of their implementation. One of the important criteria is deleting from the databases the images of minors, acquitted or released without charge[16].

Although most of the states initiated introduction and regulation of the facial recognition technology, one should highlight the experience of California, which became the first US state to ban the use of facial recognition technology by law enforcement. Later, this practice influenced the ban on using facial recognition technology not only by law enforcement, but also for private organizations[17].

---

13 Rauenzahn, B., Chung, J., & Kaufman, A. (2021, March 20). Facing Bias in Facial Recognition Technology. *The Regulatory Review*. https://www.theregreview.org/2021/03/20/saturday-seminar-facing-bias-in-facial-recognition-technology/#:~:text=According%20to%20the%20researchers%2C%20facial

14 The Computer Got It Wrong: Why We're Taking the Detroit Police to Court over a Faulty Face Recognition "Match". (2021, April 13). *American Civil Liberties Union*. https://www.aclu.org/news/privacy-technology/the-computer-got-it-wrong-why-were-taking-the-detroit-police-to-court-over-a-faulty-face-recognition-match

15 Paul, K. (2019, May 15). San Francisco Is First US City to Ban Police Use of Facial Recognition Tech. *The Guardian*. https://www.theguardian.com/us-news/2019/may/14/san-francisco-facial-recognition-police-ban

16 Ban Biometric Surveillance. *Access Now*. https://www.accessnow.org/ban-biometric-surveillance/

17 California Law Enforcement Prohibited from Using Facial Recognition Technology in Body Cameras under Ting Bill Signed by the Governor. Assemblymember Phil Ting Representing the 19th California Assembly District. https://a19.asmdc.org/press-releases/20191008-california-law-enforcement-prohibited-using-facial-recognition-technology

Following the example of California, there were established the grounds in terms of providing a search warrant and a requirement to present sufficient evidences of committing a crime. Besides, restrictive measures referred to using the facial recognition technology during protests and meetings in order to prevent violation of civil rights and freedoms. The bill was widely supported by international non-government organizations controlling the government activity, civil freedoms groups and the law enforcement[18]. Large companies like IBM, Amazon and Microsoft especially supported the decision on suspending selling facial recognition tools to governments[19].

As a result, the adopted act on facial recognition prohibits coincidence to be single evidence establishing sufficient grounds for arrest, this being the most adequate protection measure to prevent mistakes in an indictment order (Gates, 2002).

Illinois also adopted a law on regulating facial recognition systems, namely, Biometric Information Privacy Act[20] (Zuo et al., 2019). It stipulates prohibitions on exchange, transfer without consent, trading or deriving profit from selling biometric data[21] (Hill et al., 2022).

Based on the analysis of various US states, one may notice a certain fragmentation of approaches. While not all states restricted the use of surveillance cameras with the facial recognition function, most of the states have adopted laws restricting the use of such cameras by law enforcement[22]. Not all US citizens and foreigners residing in the US may reckon on safety in case of faults in identification. The bill provides just a basic protection for the Americans, allowing the civil society to promote initiatives on limiting the uncontrolled use of such systems.

According to the drafters, the formulated approach to restricting the use of facial recognition function and regulating collection and processing of data will allow reducing the

---

18 Use of facial recognition systems by police will be restricted in the US. (2022, September 30). *ForkLog*. https://forklog.com/news/v-ssha-ogranichat-ispolzovanie-politsiej-sistem-raspoznavaniya-lits

19 Muravyev, D. (2020, June 19). Why IT companies rejected the facial recognition technology and what this has to do with protests in America. *Teplitsa sotsialnykh tekhnologiy*. https://te-st.ru/2020/06/19/why-it-companies-against-facial-recognition/

20 740 ILCS 14/ Biometric Information Privacy Act. *Www.ilga.gov*. www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57

21 Deadline for filing a lawsuit in a multimillion-dollar settlement with Snapchat is approaching. (2022, October 13). *Chicago24online*. https://chicago24online.com/news/priblizhaetsya-krajnij-srok-podachi-iska-v-mnogomillionnom-uregulirovanii-processa-so-snapchat/ ; Thornley v. Clearview AI, Inc., No. 20-3249 (7th Cir. 2021). *Justia Law*. https://law.justia.com/cases/federal/appellate-courts/ca7/20-3249/20-3249-2021-01-14.html

22 Face Off: Law Enforcement Use of Face Recognition Technology. (2018, February 23). *Electronic Frontier Foundation*. https://www.eff.org/wp/law-enforcement-use-face-recognition

probability of abuse caused by discriminative monitoring and ensuring measures for privacy protection[23].

Thus, one may conclude that facial recognition and surveillance technologies allow faults and enhance discrimination, especially when police continue to make decisions on arrests and detention without additional means of crime investigation (Givens et al., 2004). If restriction measures are taken, the facial recognition system will be used only for necessary and justified purposes, and will restrict the broad discretion powers of the law enforcement (Nissenbaum, 2004). Besides, it will enhance the right to delete one's information in case of an acquitting judgment. The legislator's initiative on restricting the facial recognition system is also due to the privacy protection, preventing bias and discrimination of citizens by color and race.

2. European Union: risk-oriented approach in legal regulation

Regarding the practice of the European Union (further – EU), one should pay attention to adoption of the legislation restricting the use of facial recognition systems in real time. Beside misuse by law enforcement, detaining citizens without due reasons, it was found that the artificial intelligence and facial recognition tools can be used for surveillance of migrants, religious groups and minorities[24]. The established position of the members of European Parliament associates the surveillance methods with threats to privacy and civil freedoms, and considers them to be enhancing bias and discrimination.

A prerequisite to taking restrictive measures is the vast practice of using automated facial recognition technology by police for searching people in public places. These technologies used in street surveillance cameras to ensure public safety caused uproar of civil society activists, who demanded accounts of actual facts of crime prevention with the help of surveillance (Kuteynikov et al., 2022). In their protests, the human rights community emphasized the freedom of speech and the right to peaceful assembly, which are the essential civil freedoms. It was highlighted that the use of facial recognition system by the government hinders expression of opinions, harms entire communities and violates individual freedoms[25].

---

23 Turner, N. L, & Chin, C. (2022, April 7). Police Surveillance and Facial Recognition: Why Data Privacy Is an Imperative for Communities of Color. *Brookings*. https://www.brookings.edu/research/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/

24 Review of ECHR decisions as of September, 2018 (2018, September 14). Assistance to those wishing to apply to the European Court of Human Rights in Strasburg. https://european-court-help.ru/obzor-reshenii-espch-za-sentiabr-2018-goda/ ; Face off Report. (2018). *Big Brother Watch*. bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/report/

25 Guariglia, Paige Collings, & Matthew. (2022, September 26). Ban Government Use of Face Recognition in the UK. *Electronic Frontier Foundation*. https://www.eff.org/deeplinks/2022/09/ban-government-use-face-recognition-uk

A remarkable case heard by a high court in Cardiff was a suit by Ed Bridges supported by a Liberty civil rights group. Bridges claimed that the use of facial recognition technology by police when he was shopping and later during a peaceful protest against weapon sales violates his right to privacy and peaceful protests.

The high court in Cardiff stated that, although the mass surveillance system violates the right to privacy of those scanned by surveillance cameras, automatic facial recognition was performed on legal grounds[26] (Begishev & Khisamova, 2018).

In 2022, the legislative initiatives in Great Britain, regarding the restriction of facial recognition systems were reviewed[27]. According to the Data Protection Act of 2018, biometric and medical data are sensitive data; hence, their collection and processing can be performed only after obtaining an explicit consent[28]. Information Commissioner's Office in Great Britain also informed about an investigation in relation to the organizations introducing the facial recognition systems which carry the risk of using emotion analysis algorithm.

Emotion analysis technologies process such data as glance tracing, mood analysis, facial movements, analysis of pace, heartbeat, facial expression[29] (Begishev & Khisamova, 2018).

Emotion analysis implies collection, storage and processing of a range of personal data, including subconscious behavioral or emotional reactions. Such use of data is much more risky than traditional biometric technologies used for facial identification (Sprokkereef, 2007).

The emerging problems of applying identification systems influences the thorough analysis of legal regulation of authentication systems in the European Union. In April 2021, the European Data Protection Supervisor, having analyzed the current risks and concerns about the use of systems with facial recognition function, called for banning the use of artificial intelligence for automatic identification of persons in public places. Similarly, in January 2021, the Council of Europe called for strict regulation of technologies and marked in its new guidelines that facial recognition must be prohibited if they are used exclusively for determining the skin color, religious or other convictions, gender, racial

---

26 Bowcott, O. (2019, September 4). Police Use of Facial Recognition Is Legal, Cardiff High Court Rules. *The Guardian*. https://www.theguardian.com/technology/2019/sep/04/police-use-of-facial-recognition-is-legal-cardiff-high-court-rules

27 Kaminskiy, B. (2022, July 27). Britain attempted to ban facial recognition in shops. *ForkLog*. https://forklog.com/news/v-britanii-potrebovali-zapretit-raspoznavanie-lits-v-magazinah

28 Data Protection Act 2018. (2018). *Legislation.gov.uk*. https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

29 "Immature Biometric Technologies Could Be Discriminating against People" says ICO in Warning to Organisations. (2022, October 27). *Ico.org.uk*. https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/10/immature-biometric-technologies-could-be-discriminating-against-people-says-ico-in-warning-to-organisations/

or ethnic origin, age, state of health or social status of a person. Civil rights groups also urged the EU to ban biometric surveillance on the grounds of incompliance with human rights[30].

The European Commission included into the EC act on artificial intelligence restrictions on using the facial recognition system in public places and for private companies, but left the opportunity of police using it for exclusive purposes. The security agencies may use this technology in such cases as searching for missing children, preventing terrorist attacks and identification of armed and dangerous criminals.

The draft EU act on artificial intelligence presented in April 2021 is aimed at restricting the use of biometric identification systems, including facial recognition technology. Within the project, it is proposed to introduce new requirements regulating the use of technology depending on the criteria – "high" or "low" risk[31].

High risk artificial intelligence systems will include:

– critically important objects which may inflict harm to life and health of citizens;

– biometric identification and categorization of physical persons;

– education and vocational training (for example, calculating scores at exams);

– components of product safety (for example, using artificial intelligence in robotized surgery);

– employment, personnel management and access to self- employment (for example, software for sorting CVs at admission);

– access to the key private and public services and benefits (scoring crediting system, which limits the ability of citizens to obtain credit);

– data of law enforcement;

– data of migration and border forces (verifying the passing documents);

– data of the institutions of justice and democratic procedures (applying of law to a specific set of evidences)[32].

High risk systems will be prohibited for purposeless use or will have to comply with the strict rules of supervisory bodies, and used in serious cases for safety provision. A wide range of facial recognition technologies, used for law enforcement purposes, during border control, in public places, educational establishments, public transport, can be allowed only on the condition of assessing the compliance and observance of safety requirements (Sprokkereef, 2007). The low risk facial recognition technologies will be

30 *Ibid*, 20.

31 Kasparyants, D. (2021, October 7). Standardization of artificial intelligence in the EU. *"GRChTs" scientific-technical center.* https://rdc.grfc.ru/2021/10/ai-standards/

32 Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence. (2021, April 21). *European Commission*. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682

restricted to the criteria of transparency and requirements to the rules of information storing and processing[33].

Regardless of the proposed projects of artificial intelligence regulation, there are still serious concerns in Europe about using such categorization and regulation without due public control. Most of the EU member states still advocate for stricter rules, including complete prohibition of such technologies. In particular, the system of remote biometric identification and the facial recognition technology are referred to high risk systems (Firc, 2023). One of the main requirements is complete prohibition of their use in public places for law enforcement purposes.

3. Republic of Kazakhstan: on the way to regulating biometric data

Republic of Kazakhstan faces the trend towards using the foreign experience in biometric authentication in various spheres, such as state governance, banking, medicine, law enforcement, education, etc.

A number of amendments were introduced into the current legislation[34], including a definition of biometric data; the rules of processing and storing biometric data when rendering state services were adopted. The provisions of these rules stipulate the procedures of biometric data processing when rendering state services; such data are submitted voluntary and can be at any time deleted from databases upon a written application of the data subject[35].

In compliance with the Law "On personal data and their protection", the notion of biometric data is defined as a category of personal data characterizing physiological and biological features of the subject, based on which his or her personality may be identified[36].

The definition establishes the belonging of biometric data to personal data, while the process of biometric data identification is qualified as "biometric authentication". According to the Law on informatization, biometric authentication is defined as

---

33 Filipova, I. A. (2022). *Legal regulation of artificial intelligence: tutorial* (2nd ed., renewed and complemented). Nizhniy Novgorod: Nizhniy Novgorod State University. https://www.researchgate.net/publication/359194516_Legal_Regulation_of_Artificial_Intelligence/citation/download ; Madiega, T., & Mildebrath, H. (2021, September). *In-Depth Analysis*. https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf

34 On personal data and their protection. *Adilet IPS*. https://adilet.zan.kz/rus/docs/Z1300000094/z13094.htm

35 Rules of collection, processing and storage of biometric data of physical persons for their biometric authentication when rendering state services. *Adilet IPS*. https://adilet.zan.kz/rus/docs/V2000021547#z14

36 *Ibid*., 22.

a complex of measures, identifying a personality based on physiological and biological unchangeable features[37].

Besides the said definitions, Republic of Kazakhstan has adopted the Law on dactyloscopic and genome registration. The goals of the Law are determined by the requirements of obligatory collection of fingerprints to create a common database of biometric data. The database of fingerprints will be used during border control, for anti-terrorism measures, criminal investigations, order and safety provision[38].

As for data processing, in 2022 the Program of developing a national payment system in the Republic of Kazakhstan up to 2025 was adopted[39]. The Program stipulates the introduction of biometric authentication during payment operations; as part of the initiative of its implementation, it is stated that it is aimed at increasing the personal data security through introducing a mechanism of the subjects' consent for data processing. As a result, a subject must be aware of the procedure of their application for a state service, the goal of their application, and have an opportunity to give or withdraw consent for access to their data[40].

Besides the procedures of common use of biometric data, the Program of Almaty development up to 2025 and 2030 establishes installing of surveillance cameras with facial recognition function[41]. In 2027, it is planned to broaden surveillance systems by installing cameras on all terrorist-vulnerable objects and in residential quarters[42]. The topicality of installing surveillance cameras increased after mass unrest which took place in January 2022, when in several large cities of Kazakhstan, especially in Almaty, law enforcement and security bodies failed to control mass unrest, looting and public order offenses[43].

Initiatives on installing surveillance cameras with facial recognition function were stipulated by a law draft on digital technologies regulation, according to which, amendments

---

37 Law of the Republic of Kazakhstan No. 418-V of November 24, 2015 "On informatization" (with amendments as of 03.09.2022). *PARAGRAF Information system*. https://online.zakon.kz/document/?doc_id=33885902

38 Raisova, Z. (2021, January 6). Obligatory dactyloscopy of Kazakhstaners: what is it for and how does it work? *CABAR.asia*. https://cabar.asia/ru/zachem-vvoditsya-obyazatelnaya-daktiloskopiya-kazahstantsev

39 On adopting the National development plan of the Republic of Kazakhstan up to 2025 and recognizing invalid certain orders of the President of the Republic of Kazakhstan: Order of the President of the Republic of Kazakhstan No. 636 of February 15, 2018. *Adilet IPS*. https://adilet.zan.kz/rus/docs/U1800000636

40 On adopting the Program for creating the National platform of digital biometric identification for 2021–2024 (2021). *Otkrytye NPA*. https://legalacts.egov.kz/npa/view?id=13895562

41 *Program of Almaty development up to 2030 is socially oriented*. (2022, June 28). https://www.gov.kz/memleket/entities/almaty/press/news/details/394216?lang=ru

42 Alkhabaev, Sh. (2022, September 12). Facial recognition system will be introduced in Almaty. *Tengrinews.kz*. https://tengrinews.kz/kazakhstan_news/sistemu-raspoznavaniya-lits-vnedryat-v-almatyi-477602

43 Kazakhstan: victims of January protest do not find justice. (2022, May 9). *Human Rights Watch*. https://www.hrw.org/ru/news/2022/05/09/kazakhstan-no-justice-january-protest-victims

were made in the current Law on informatization[44]. To ensure national safety and public order, it is planned to introduce a national system of video monitoring as a complex of hardware and software means for collection, processing and storage of video images database[45].

At the same time, the analyzed documents and normative legal acts, referring to personal data protection in the Republic of Kazakhstan, are currently only partially comply with the international standards of human rights protection. Besides, the presence of laws does not provide a substantial guarantee of their protection. Special attention should be paid to the rules of collection, processing and storage of biometric data [46].

Using the cameras with facial recognition function and citizens' collecting fingerprints may allow privacy violation. That is why, for legal regulation of biometric data it is necessary to thoroughly study the international experience of the states which already implement the practice of biometric data collection, in order to avoid the risks associated with personal data leakage (Raissova & Mukhamejanova, 2021).

In the law enforcement practice, it is recommended that biometric data processing complies with the established techniques of using the facial recognition technology in law enforcement and law application activity, which exclude or significantly reduce the possibility to violate privacy, human rights and freedoms:

The use of facial recognition system must comply with the legal goals and be reasonably necessary.

The use of facial recognition system must be open and transparent, which implies reporting to citizens in the form of statistical data and disclosing materials on crime solving using the facial recognition technology.

Possibility to apply to authorized bodies in case of claims and to obtain the information of interest.

The presence of clear rules, policies and procedures for security of biometric data and means of their processing.

Observing the rules of minimization of biometric data collection.

Restriction of access of the third persons not involved into data processing and surveillance.

Compliance with the requirements of laws and safety measures for protection against unsanctioned access and use of biometric data.

Regular implementation of scheduled and unscheduled inspections to provide the quality of biometric data protection and exclude their illegal use or granting access to them.

---

44 On the draft Law of the Republic of Kazakhstan "On making amendments in certain legislative acts of the Republic of Kazakhstan on the issues of digital technologies regulation": Decree of the Government of the Republic of Kazakhstan No. 1001 of 28.12.2019. *Adilet IPS*. https://adilet.zan.kz/rus/docs/P1900001001

45 On adopting the Rules of functioning the National video monitoring system. *Adilet IPS*. https://adilet.zan.kz/rus/docs/V2000021693

46 Research of the probable economic, social and legal consequences of the Law of the Republic of Kazakhstan "On dactyloscopic and genome registration" (2021, June 23). *Soros Kazakhstan Foundation*. www.soros.kz/ru/study-of-the-law-of-the-republic-of-kazakhstan-on-fingerprint-and-genomic-registration/

Conclusion

This research describes the experience of using facial recognition technologies and biometric identification as a tool to ensure safety. Description of state restrictions allowed formulating the approaches to the legal regulation of the sphere under study, the advantages and risks of their implementation.

To prevent any violations of privacy, discrimination, limitation of rights and freedoms by the government or private organizations, it is necessary, based on the carried out analysis of the experience of the states which have implemented national projects on biometric data regulation, to identify the guarantees and increase the level of state-legal protection. Analysis of the experience of the states showed that adoption of the respective laws, regulating the biometric data protection, is inevitable, as the current legislation does not fully comply with the criteria of the safe use of facial recognition technology by governmental and private organizations.

As a result of the carried out analysis and the studied experience of foreign states, one may highlight the following important proposals to further improve legislation in the Republic of Kazakhstan:

– to complement the current legislation in terms of defining the admissible criteria of using facial recognition technology;

– to introduce a prohibition of mass and unselective surveillance using video surveillance systems;

– to ban the use of images of the citizens of the Republic of Kazakhstan, taken from publicly accessible sources, to complete databases of biometric data;

– to elaborate categorization of biometric systems with high and low risk level by the example of artificial intelligence regulation in the European Union;

– to introduce a prohibition of using the biometric identification system in real time by all users except law enforcement.

Based on the studied experience of the European Union and the US, the said proposals may be taken into account both in the Republic of Kazakhstan and in other countries, which are currently developing biometric data and their legal regulation. When using facial recognition systems, state bodies must promote the implementation of the principles of transparency, legitimacy and necessity, as well as to formulate the policy of the third persons' data processing.

References

Begishev, I. R., & Khisamova, Z. I. (2018). Criminological risks of using artificial intelligence. *Russian Journal of Criminology*, *12*(6), 767–775. (In Russ.). https://doi.org/10.17150/2500-4255.2018.12(6).767-775

Bowyer, K. W. (2004). Face recognition technology: security versus privacy. *IEEE Technology and Society Magazine*, *23*(1), 9–19. https://doi.org/10.1109/mtas.2004.1273467

Buresh, D. L. (2021). Should Personal Information and Biometric Data Be Protected under a Comprehensive Federal Privacy Statute that Uses the California Consumer Privacy Act and the Illinois Biometric Information Privacy Act as Model Laws? *Santa Clara High Technology Law Journal*, *38*(1). https://digitalcommons.law.scu.edu/chtlj/vol38/iss1/2

Chen, W., & Wang, M. (2023). Regulating the use of facial recognition technology across borders: A comparative case analysis of the European Union, the United States, and China. *Telecommunications Policy*, *47*(2), 102482. https://doi.org/10.1016/j.telpol.2022.102482

Firc, A., Malinka, K., & Hanáček, P. (2023). Deepfakes as a threat to a speaker and facial recognition: An overview of tools and attack vectors. *Heliyon*, *9*(4), e15090. https://doi.org/10.1016/j.heliyon.2023.e15090

Gates, K. A. (2002). Wanted Dead or Digitized: Facial Recognition Technology and Privacy. *Television & New Media*, *3*(2), 235–238. https://doi.org/10.1177/152747640200300217

Gill, P. (1997). Technostalgia: Making the future past perfect. *Camera Obscura: Feminism, Culture, and Media Studies*, *14*(1–2), 161–179. https://doi.org/10.1215/02705346-14-1-2_40-41-161

Givens, G., Beveridge, J. R., Draper, B. A., Grother, P., & Phillips, P. J. (2004). How features of the human face affect recognition: a statistical comparison of three face recognition algorithms. In *Proceedings of the 2004 IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 2004. https://doi.org/10.1109/cvpr.2004.1315189

Hill, D., O'Connor, C. D., & Slane, A. (2022). Police use of facial recognition technology: The potential for engaging the public through co-constructed policy-making. *International Journal of Police Science & Management*, *24*(3), 325–335. https://doi.org/10.1177/14613557221089558

Johnson, Th. L., Johnson, N. N., McCurdy, D., & Olajide, M. M. (2022). Facial recognition systems in policing and racial disparities in arrests. *Government Information Quarterly*, *39*(4), 101753. https://doi.org/10.1016/j.giq.2022.101753

Jones, C. (2021). Law Enforcement Use of Facial Recognition: Bias, Disparate Impacts to People of Color, and the Need for Federal Legislation. *NCJL & Tech.*, *22*(4), 777. https://scholarship.law.unc.edu/ncjolt/vol22/iss4/6

Kuteynikov, D. L., Izhaev, O. A., Lebedev, V. A., & Zenin, S. S. (2022). Privacy in the realm of Artificial Intelligence Systems Application for Remote Biometric Identification. *Lex Russica*, *75*(2), 121–131. (In Russ.). https://doi.org/10.17803/1729-5920.2022.183.2.121-131

Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review*, *79*, 119. https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10

Raissova, G., & Mukhamejanova, D. (2021). Nondiscrimination Policy and Privacy Protection in Case of Genetic Passport for Soldiers. *South Asian Journal of Social Sciences and Humanities*, *2*(3), 140–150. https://doi.org/10.48165/sajssh.2021.2309

Sarabdeen, J. (2022, March 11). Protection of the rights of the individual when using facial recognition technology. *Heliyon*, *8*(3), e09086. https://doi.org/10.1016/j.heliyon.2022.e09086

Schweber, H. (2014). Lochner v. New York and the Challenge of Legal Historiography. *Law & Social Inquiry*, *39*(1), 242–274. https://doi.org/10.1111/lsi.12062

Shore, A. (2022). Talking about facial recognition technology: How framing and context influence privacy concerns and support for prohibitive policy. *Telematics and Informatics*, *70*, 101815. https://doi.org/10.1016/j.tele.2022.101815

Sprokkereef, A. (2007, August). Data Protection and the Use of Biometric Data in the EU. In *The Future of Identity in the Information Society* (pp. 277–284). Boston, MA: Springer. https://doi.org/10.1007/978-0-387-79026-8_19

Stepney, Ch. (2019). Actual Harm Means it is too Late: How Rosenbach v. Six Flags Demonstrates Effective Biometric Information Privacy Law. *Loyola of Los Angeles Entertainment Law Review*, *40*(1). https://digitalcommons.lmu.edu/elr/vol40/iss1/2

Zuo, K. J., Saun, T. J., & Forrest, C. R. (2019). Facial Recognition Technology: A Primer for Plastic Surgeons. *Plastic and Reconstructive Surgery*, *143*(6), 1298e–1306e. https://doi.org/10.1097/prs.0000000000005673

Authors information

Dana Utegen – Deputy Director, Senior Lecturer of KAZGUU Law School, KAZGUU University Astana
Address: 8 Korgalzhinskoye shosse, 010000 Astana, Republic of Kazakhstan
E-mail: d_utegen@kazguu.kz
ORCID ID: https://orcid.org/0000-0001-5296-7916

Baurzhan Zh. Rakhmetov – PhD in Politics and International Relations, Assistant Professor of International School of Economics, KAZGUU University Astana
Address: 8 Korgalzhinskoye shosse, 010000 Astana, Republic of Kazakhstan
E-mail: b_rakhmetov@kazguu.kz
ORCID ID: https://orcid.org/0000-0003-3948-9977
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/record/32537389
Google Scholar ID: https://scholar.google.com/citations?user=hanfRwoAAAAJ

Authors' contributions

Dana Utegen made the manuscript draft and critically reviewed it, inserting valuable comments of intellectual contentя; developed the methodology design; performed comparative analysis; collected literature; analyzed legislation of the United States of America and the Republic of Kazakhstan; prepared and edited the manuscript; formulated the key conclusions, proposals and recommendations; formatted the manuscript.
Baurzhan Zh. Rakhmetov formulated the research idea, goals and tasks; participated in research design; analyzed and summarized literature; analyzed legislation of the European Union and the Republic of Kazakhstan; interpreted the specific research results; critically reviewed and edited the manuscript; interpreted the general research results; approved the final version of the article.

Conflict of interest

Rakhmetov B. Zh. 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
ASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – November 7, 2023
Date of approval – April 23, 2023
Date of acceptance – August 15, 2023
Date of online placement – August 20, 2023

Научная статья
УДК 34:342.721:004:004.8
EDN: https://elibrary.ru/drgddj
DOI: https://doi.org/10.21202/jdtl.2023.36

Технология распознавания лиц и обеспечение безопасности биометрических данных: компаративный анализ моделей правового регулирования

Дана Утеген ✉

Университет КАЗГЮУ имени М. С. Нарикбаева
г. Астана, Республика Казахстан

Бауржан Жанатович Рахметов

Университет КАЗГЮУ имени М. С. Нарикбаева
г. Астана, Республика Казахстан

Ключевые слова

Безопасность,
биометрическая аутентификация,
биометрические данные,
идентификация,
неприкосновенность частной жизни,
персональные данные,
право,
правовое регулирование,
технологии распознавания лиц,
цифровые технологии

Аннотация

Цель: выявление моделей правового регулирования в сфере биометрической идентификации и аутентификации технологией распознавания физических лиц для выработки рекомендаций по повышению информационной безопасности человека и государственно-правовой охраны его права на неприкосновенность частной жизни.

Методы: рискориентированный подход в праве и такие специально-юридические методы познания, как методы сравнительно-правового анализа и юридического прогнозирования, имеют для исследуемой проблематики определяющее значение и позволяют сопоставить применяемые в зарубежных странах и их объединениях модели правового регулирования в сфере биометрической идентификации и аутентификации системами распознавания физических лиц, спрогнозировать возможные риски для безопасности биометрических данных с учетом перспективы дальнейшего распространения современной технологии распознавания лиц, сформулировать рекомендации по правовой охране биометрических данных.

✉ Контактное лицо

Результаты: предложены пути дальнейшего совершенствования законодательства Республики Казахстан и иных стран, находящихся в процессе развития правового регулирования биометрических данных, в части определения допустимых критериев использования технологии распознавания лиц, разработки категоризации биометрических систем с высоким и низким уровнем риска (по примеру опыта регулирования искусственного интеллекта в Европейском союзе), необходимости введения системы запретов массовой и неизбирательной слежки за человеком с помощью систем видеонаблюдения и др.

Научная новизна: заключается в выявлении положительного зарубежного передового опыта по развитию правового регулирования в сфере распознавания физических лиц на основе биометрии (Европейский союз, Соединенные Штаты Америки, Соединенное Королевство Великобритании, Северная Ирландия), который может быть использован для дальнейшего совершенствования национального законодательства в целях создания наиболее эффективных механизмов правовой защиты персональных данных, включая биометрическую информацию.

Практическая значимость: основанное на рискориентированном подходе и компаративистском анализе исследование позволяет выработать меры по усилению правовой охраны биометрических данных, обеспечению эффективной защиты гражданских прав и свобод на неприкосновенность частной жизни на основе прогноза дальнейшего распространения современной технологии распознавания лиц.

Для цитирования

Утеген, Д., Рахметов, Б. Ж. (2023). Технология распознавания лиц и обеспечение безопасности биометрических данных: компаративный анализ моделей правового регулирования. *Journal of Digital Technologies and Law*, *1*(3), 825–844. https://doi.org/10.21202/jdtl.2023.36

Список литературы

Бегишев, И. Р., Хисамова, З. И. (2018). Криминологические риски применения искусственного интеллекта. *Всероссийский криминологический журнал*, *12*(6), 767–775. https://doi.org/10.17150/2500-4255.2018.12(6).767-775

Кутейников, Д. Л., Ижаев, О. А., Зенин, С. С. (2022). Неприкосновенность частной жизни в условиях использования систем искусственного интеллекта для удаленной биометрической идентификации личности. *Lex Russica*, *75*(2), 121–131. https://doi.org/10.17803/1729-5920.2022.183.2.121-131

Bowyer, K. W. (2004). Face recognition technology: security versus privacy. *IEEE Technology and Society Magazine*, *23*(1), 9–19. https://doi.org/10.1109/mtas.2004.1273467

Buresh, D. L. (2021). Should Personal Information and Biometric Data Be Protected under a Comprehensive Federal Privacy Statute that Uses the California Consumer Privacy Act and the Illinois Biometric Information Privacy Act as Model Laws?. *Santa Clara High Technology Law Journal*, *38*(1). https://digitalcommons.law.scu.edu/chtlj/vol38/iss1/2

Chen, W., & Wang, M. (2023). Regulating the use of facial recognition technology across borders: A comparative case analysis of the European Union, the United States, and China. *Telecommunications Policy*, *47*(2), 102482. https://doi.org/10.1016/j.telpol.2022.102482

Firc, A., Malinka, K., & Hanáček, P. (2023). Deepfakes as a threat to a speaker and facial recognition: An overview of tools and attack vectors. *Heliyon*, *9*(4), e15090. https://doi.org/10.1016/j.heliyon.2023.e15090

Gates, K. A. (2002). Wanted Dead or Digitized: Facial Recognition Technology and Privacy. *Television & New Media*, *3*(2), 235–238. https://doi.org/10.1177/152747640200300217

Gill, P. (1997). Technostalgia: Making the future past perfect. *Camera Obscura: Feminism, Culture, and Media Studies*, *14*(1–2), 161–179. https://doi.org/10.1215/02705346-14-1-2_40-41-161

Givens, G., Beveridge, J. R., Draper, B. A., Grother, P., & Phillips, P. J. (2004). How features of the human face affect recognition: a statistical comparison of three face recognition algorithms. In *Proceedings of the 2004 IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 2004. https://doi.org/10.1109/cvpr.2004.1315189

Hill, D., O'Connor, C. D., & Slane, A. (2022). Police use of facial recognition technology: The potential for engaging the public through co-constructed policy-making. *International Journal of Police Science & Management*, *24*(3), 325–335. https://doi.org/10.1177/14613557221089558

Johnson, Th. L., Johnson, N. N., McCurdy, D., & Olajide, M. M. (2022). Facial recognition systems in policing and racial disparities in arrests. *Government Information Quarterly*, *39*(4), 101753. https://doi.org/10.1016/j.giq.2022.101753

Jones, C. (2021). Law Enforcement Use of Facial Recognition: Bias, Disparate Impacts to People of Color, and the Need for Federal Legislation. *NCJL & Tech.*, *22*(4), 777. https://scholarship.law.unc.edu/ncjolt/vol22/iss4/6

Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review*, *79*, 119. https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10

Raissova, G., & Mukhamejanova, D. (2021). Nondiscrimination Policy and Privacy Protection in Case of Genetic Passport for Soldiers. *South Asian Journal of Social Sciences and Humanities*, *2*(3), 140–150. https://doi.org/10.48165/sajssh.2021.2309

Sarabdeen, J. (2022, March 11). Protection of the rights of the individual when using facial recognition technology. *Heliyon*, *8*(3), e09086. https://doi.org/10.1016/j.heliyon.2022.e09086

Schweber, H. (2014). Lochner v. New York and the Challenge of Legal Historiography. *Law & Social Inquiry*, *39*(1), 242–274. https://doi.org/10.1111/lsi.12062

Shore, A. (2022). Talking about facial recognition technology: How framing and context influence privacy concerns and support for prohibitive policy. *Telematics and Informatics*, *70*, 101815. https://doi.org/10.1016/j.tele.2022.101815

Sprokkereef, A. (2007, August). Data Protection and the Use of Biometric Data in the EU. In *The Future of Identity in the Information Society* (pp. 277–284). Boston, MA: Springer. https://doi.org/10.1007/978-0-387-79026-8_19

Stepney, Ch. (2019). Actual Harm Means it is too Late: How Rosenbach v. Six Flags Demonstrates Effective Biometric Information Privacy Law. *Loyola of Los Angeles Entertainment Law Review*, *40*(1). https://digitalcommons.lmu.edu/elr/vol40/iss1/2

Zuo, K. J., Saun, T. J., & Forrest, C. R. (2019). Facial Recognition Technology: A Primer for Plastic Surgeons. *Plastic and Reconstructive Surgery*, *143*(6), 1298e–1306e. https://doi.org/10.1097/prs.0000000000005673

Сведения об авторах

Утеген Дана – заместитель директора, старший преподаватель Высшей школы права, Университет КАЗГЮУ имени М. С. Нарикбаева
Адрес: 010000, Республика Казахстан, г. Астана, Коргалжинское шоссе, 8
E-mail: d_utegen@kazguu.kz
ORCID ID: https://orcid.org/0000-0001-5296-7916

Рахметов Бауржан Жанатович – PhD в области политики и международных отношений, ассистент-профессор Международной школы экономики, Университет КАЗГЮУ имени М. С. Нарикбаева
Адрес: 010000, Республика Казахстан, г. Астана, Коргалжинское шоссе, 8
E-mail: b_rakhmetov@kazguu.kz
ORCID ID: https://orcid.org/0000-0003-3948-9977
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/record/32537389
Google Scholar ID: https://scholar.google.com/citations?user=hanfRwoAAAAJ

Вклад авторов

Д. Утеген осуществляла составление черновика рукописи и его критический пересмотр с внесением ценных замечаний интеллектуального содержания; разработку дизайна методологии; проведение сравнительного анализа; сбор литературы; анализ законодательства Соединенных Штатов Америки и Республики Казахстан; подготовку и редактирование текста статьи; формулировку ключевых выводов, предложений и рекомендаций; оформление рукописи.
Б. Ж. Рахметов осуществлял формулирование идеи, исследовательских целей и задач; участие в научном дизайне; анализ и обобщение литературы; анализ законодательства Европейского союза и Республики Казахстан; интерпретацию частных результатов исследования; критический пересмотр и редактирование текста рукописи; интерпретацию общих результатов исследования; утверждение окончательного варианта статьи.

Конфликт интересов

Б. Ж. Рахметов 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: 10.19.61 Правовое регулирование информационной безопасности
Специальность ВАК: 5.1.2 / Публично-правовые (государственно-правовые) науки

История статьи

Дата поступления – 7 ноября 2022 г.
Дата одобрения после рецензирования – 23 апреля 2023 г.
Дата принятия к опубликованию – 15 августа 2023 г.
Дата онлайн-размещения – 20 августа 2023 г.