ISSN 2713-2749

Legal Issues in the DIGITAL AGE

Вопросы права в цифровую эпоху

4/2024

Volume 5

Legal Issues in the DIGITAL AGE

4/2024

ISSUED QUARTERLY VOLUME 5

Publisher

National Research
University Higher
School
of Economics

ISSN 2713-2749

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

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

Designer
Andrei Pavlov
Pre-press
Natalya Puzanova

© National Research
University
Higher School
of Economics, 2024

IT. LAW. HUMAN RIGHTS

B.A. Edidin, K.V. Kochetkova, N.D. Sarankina
Digital Abuse: How Dark Patterns Manipulate Our Lives 4

R.A. Budnik, E.G. Evpak
Human Voice: Legal Protection Challenges 28

A.D. Tsvetkova
Keystroke Dynamics: Prospects for Comprehensive Law Regulation 46

V.O. Demkin
Deepfakes: Search for a Model of Legal Regulation 73

DIGITAL AGE: CRIMINAL LAW

D.A. Pechegin
Liability and the Digital Age: Comparative Analysis of the Australian, South African and CIS States Legislative Approaches 92

LEGAL INFORMATICS

V.B. Isakov
Artificial Intelligence in Law and Legal Analytics 113

REVIEW

M.A. Kolzdorf, N.I. Kapyrina, N.E. Goloiad
Key Issues in the Intellectual Property Court's Presidium Rulings . . 138

Legal Issues in the **DIGITAL AGE**

EDITORIAL BOARD

Editor-in-Chief

I.Yu. Bogdanovskaya	National Research University Higher School of Economics, Russia

Editorial Board

A.I. Abdullin	Kazan (Volga Region) Federal University, Russia
S.V. Bakhin	Saint Petersburg State University, Russia
A. Belohlavek	VSB Technical University of Ostrava, Czech Republic
W.E. Butler	Pennsylvania State University, USA
S.J. Cornelius	University of Pretoria, South Africa
J. Dumortier	University of Leuven, Belgium
I.A. Emelkina	Russian Presidential Academy of National Economy, Russia
N.Yu. Erpyleva	National Research University Higher School of Economics, Russia
A.V.Gabov	Institute of State and Law, Russian Academy of Sciences, Russia
G.A. Gadziev	National Research University Higher School of Economics, Russia
Yu.V. Gracheva	Moscow State Law University (MSAL), Russia
Z. Guo	China University of Political Science and Law, China
B. Hugenholtz	University of Amsterdam, Netherlands
V.B. Isakov	National Research University Higher School of Economics, Russia
A.A. Larichev	National Research University Higher School of Economics, Russia
E.M. Lombardi	University of Florence, Italy
C.S. de Lucena Neto	Paraíba State University (UEPB), Brazil
T. Mahler	University of Oslo, Norway
A. Metzger	Humboldt University, Germany
G.I. Muromtsev	Peoples' Friendship University of Russia, Russia
A.V. Naumov	University of Procuracy, Russia
J. Reichman	Duke University, USA
A.Kh. Saidov	Academy of Sciences of Uzbekistan, Uzbekistan
R. Sony Anagalli	Jawaharlal Nehru University, India
E.A. Sukhanov	Moscow State Lomonosov University, Russia
Yu.A. Tikhomirov	National Research University Higher School of Economics,Russia
V.A. Vinogradov	National Research University Higher School of Economics, Russia
Y. Walden	Queen Mary, University of London, United Kingdom

Advisory Board

N.I.Kapyrina	Moscow State Institute of International Relations (MGIMO University), Russia
S.Chopra	Jawaharlal Nehru University, India

Legal Issues in the **DIGITAL AGE**

ISSUED QUARTERLY

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

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

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

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

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

Publication in the journal is free of charge.

The works are licensed under a Creative Commons Attribution-Sharealike 4.0 International License (CC BY-SA 4.0). https://creativecommons.org/licenses/by-sa/4.0/legalcode.en

All materials are available for free download.

Legal Issues in the Digital Age. 2024. Vol. 5. No. 4.
Вопросы права в цифровую эпоху. 2024. Т. 5. № 4.

IT. Law. Human Rights

Research article
JEL*:* K00
УДК*:*34
DOI:10.17323/2713-2749.2024.4.4.27

Digital Abuse: How Dark Patterns Manipulate Our Lives

Boris Aleksandrovich Edidin[1],
Ksenia Vladimirovna Kochetkova[2],
Natalia Dmitrievna Sarankina[3]

[1, 2, 3] IRI, Institute for Digital Content Support & Development, 18 Tverskaya Street, Moscow 127006, Russia,

[1] b.edidin2018@gmail.com

[2] kochetkova.k@iri.center, Author ID: 1033155, ORCID ID: 0000-0002-6254-9539, Scopus ID: 57223024821

[3] sarankina.n@iri.center, Author ID: 1159548, Istina Researcher ID: 479507860

Abstract

The digital economy in Russia and abroad is of growing interest to lawmakers, especially in the context of the use of so-called 'dark patterns' — manipulative interface solutions that influence user behavior. BigTech companies consolidate their dominant position in the market by implementing innovative practices, many of which cannot be recognized as *bona fide*. The most prominent example of the implementation of user retention mechanisms through embedded features is the Tik Tok platform (Dou Yin). The Tik Tok phenomenon is still being studied by experts, but one of the clues is the unique recommendation feed that dynamically adjusts to the user's interests and is endless, creating the so-called "immersion effect". The article examines Russian and international approaches to regulating these practices. Particular attention is paid to legislative initiatives and enforcement practices aimed at protecting consumer rights and limiting the use of manipulative practices on digital platforms. The Russian legislation is still focused on certain aspects of consumer protection and countering unfair competition, while Western countries introduce specialized norms

© Edidin B.A., Kochetkova K.V., Sarankina N.D., 2024
This work is licensed under a Creative Commons Attribution-Sharealike 4.0 International License
https://creativecommons.org/licenses/by-sa/4.0/legalcode.en

to combat “dark patterns”. The aim of the article is to examine the existing norms and suggest ways to adapt successful foreign practices to the Russian legal context.

Keywords

dark patterns; manipulative behavior; consumer data; GDPR; Digital Service Act, light patterns; unfair practices.

For citation: Edidin B.A., Kochetkova K.V., Sarankina N.D. (2024) Digital Abuse: How Dark Patterns Manipulate Our Lives. *Legal Issues in the Digital Age*, vol. 5, no. 4, pp. 4–27. DOI:10.17323/2713-2749.2024.4.4.27

Introduction

Big Tech companies, especially the owners of social networks, are among the key actors of the data economy that operates “big data”. In the doctrine “big data” is described as large amounts of diverse information with high speed of formation and fast processing [Blazheev V.V., Egorova M.A., 2021: 121]. As noted by foreign specialist, human (consumer) data is becoming the most important natural resource in the era of AI [Webb E., 2022: 5] Artificial intelligence collects, processes and analyzes data automatically, which allows data operators to accumulate a huge amount of information about individuals.

Any data about human life is commercialized, not only in the form of a separate set of initial information (known as raw data), but also in the form of pre-processed information. Many different data exchanges operate all over the world. These are real B2B marketplaces that sell sets of user data (e.g., Oracle Data Marketplace, Think Data Works Marketplace).

In the doctrine this trend has been called the phenomenon of “surveillance capitalism” — a new stage in the development of the digital age, which is characterized by the total surveillance of the user by technology giants Digital companies are able not only to monitor the user, but also to influence their behavior [Zuboff S., 2022: 157, 251].

Massive, automated analysis allows online companies to perform profiling. In the digital technologies sphere profiling refers to any form of automated processing of personal and other data about an individual to assess, analyze, or predict any personal features like economic status, health, preferences and interests, location, or possible behavior of an identifiable person. During such profiling, the user receives pre-filtered information, thus transforming his or her behavior.

Specific manipulation techniques can be used in the digital environment. It has become possible to induce consumers to purchase a product or service by manipulating the appearance of a mobile application, Internet page or other digital service.

Such tricks in the design of the user interface are called “dark patterns”. Why dark? Because these methods are unfair and undesirable for the consumer, but profitable for the company. Thus, they lead to so-called “digital market manipulation” [Calo R., 2014: 995].

Since the concept of “dark patterns” entered the legal field recently, its analysis has a high scientific theoretical and practical value.

The article provides a thorough legal analysis of manipulating consumer behavior on the Internet. The authors are briefly explaining the phenomenon of consumer behavior manipulation; explain what the “dark patterns” are in its nature; present comparative legal analysis of approaches to the regulation of “dark patterns”, including Russian stance on manipulative design and provide relevant case study.

1. Interpretation of the Term “Dark Patterns”

The term was introduced in 2010 by Harry Brignall, a specialist in user interface, and refers to “design methods that deceive or manipulate users into making choices they would not otherwise make and that can cause harm”.[1]

In other words, “dark patterns” are unscrupulous tricks when designing the appearance of a website, mobile app, or other digital service.

In the practice of user-centered design, “UX laws” are beginning to emerge that vividly illustrate methods of visual manipulation [Yablonski D., 2022: 2]. For example, tricks may concern the location of links (“law of similarity”), highlighting this or that choice with a certain color (“isolation effect”, or “von Restorff effect”).

“Dark patterns” can be classified into three types depending on what effect they are aimed at achieving:

---

[1] Available at: https://alistapart.com/article/dark-patterns-deception-vs.-honesty-in-ui-design/ (accessed: 05.09.2024)

obtaining a direct commercial benefit for the entrepreneur (e.g., inducing the user to purchase a product or service);

obtaining an indirect commercial benefit (e.g., forcing the user to view an advertisement);

increasing the user's interest in the platform (e.g., forcing the user to stay on the platform as long as possible).

Interestingly, some analytics distinguish among visible dark patterns (mentioned ones), darker patterns (less detectable dark patterns such as "forced practices" and "fragmented data protection information") and the darkest patterns (detective design techniques purposely integrated into an online service's system architecture (SA) or code level and not on the UI/UX). [Leiser M.R., Santos C., 2024: 5, 10, 18].

It is useful to illustrate "classic dark patterns" with an example.

When inclining the consumer to purchase a product or service, the owner of the platform receives a direct and specific commercial benefit. Thus, by offering the user several options for a paid subscription to the service (for example, for 1 month, 6 months and 1 year) and highlighting the option with a longer term and higher price, but with a discount relative to this price, the user is visually "hinted" at the profitability of this option compared to the option with a shorter term and low price [Duplyakin W.M., Knjazheva V.V., 2016: 36].

When a consumer is forced to view an advertisement, the entrepreneur receives an indirect benefit, as he receives a monetary reward for the from the advertiser.

In addition, sometimes in advertisements the button to close the advertisement is "masked" to make it harder for the user to find.

Compulsion to stay on the platform as long as possible is used in one way or another by all major platforms, especially social networks. These methods include endless scrolling, checking likes/dislikes. Such mechanisms are always destructive for the user, as they can cause Internet addiction.

Currently, game addiction is included in the International Classification of Diseases (ICD-11) of the World Health Organization.[2] However, Internet addiction is absent in ICD-11. It's most likely due to insufficient study of the real impact of the Internet on human physical and mental health. At

---

[2] Available at: https://icd.who.int/browse/2024-01/mms/en#338347362 (accessed: 05.09.2024)

the same time, game addiction was included in the ICD relatively recently, in 2022, so, in our opinion, the global medical community will continue to work on studying the destructive impact of other forms of digital interaction. It is necessary to study those mechanics of digital platforms, especially social networks, that cause real addictive behavior.

Thus, the design of a digital service's appearance can indeed mislead, induce action, or otherwise manipulate an individual's behavior. The harmfulness of these practices may be magnified for less protected populations, which include minors or the elderly. Some specialists believe that "contractual consent secured via pernicious forms of dark patterns or other deceptive designs should be deemed invalid as a matter of law" [Hartzog W., 2018: 212–213].

Unsurprisingly, the following harms have been associated with the use of dark patterns: 1) lower autonomy; 2) a reduction in overall social and consumer welfare; 3) an erosion of trust; 4) increased insecurity; and 5) unfair treatment among consumers. [Leiser M.R., Caruana M., 2021: 242].

This unscrupulous behavior cannot go unnoticed by regulators, so foreign legal orders are gradually developing competent positions on the use of "dark patterns".

2. Manipulation of Consumer Behavior on the Internet: Regulative Approach

2.1. Regulation of "Dark Patterns" in the USA

In October 2021 the U.S. Federal Trade Commission (hereinafter FTC) has issued an enforcement policy statement warning companies against using illegal practices such as automatic renewal of paid subscriptions, free trial periods of subscriptions with automatic paid renewals, and few other manipulations.[3]

Previously, in April of the same year, the FTC held a public workshop on the topic of dark patterns in the digital environment, which resulted in the release of the Federal Trade Commission Report on Dark Patterns.[4]

---

[3] Enforcement Police Statement Regarding Negative Option Marketing // Federal Trade Commission. 2021. Available at: https://www.ftc.gov/system/files/documents/public_statements/1598063/negative_option_policy_statement-10-22-2021-tobureau.pdf (accessed: 05.09.2024)

[4] FTC Report Shows Rise in Sophisticated Dark Patterns Designed to Trick and Trap Consumers. 2022. Available at: https://www.ftc.gov/news-events/

The report does not develop its own definition of “dark patterns” but uses the classic definition by Harry Brignall.

The FTC report identifies types of dark patterns such as creating false beliefs (e.g., advertisements designed as news articles), concealing or delaying disclosure of material information (e.g., concealing a fee charge or including it in the price only at the end of a purchase), pushing consumers to make payments (e.g., offering a free trial of a product with automatic renewal of recurring payments), and violating privacy (e.g., failing to provide sufficient privacy settings).

The document also states that the FTC on will act against companies' use of those techniques that would directly violate U.S. law or other regulations enforced by the regulator. Such acts include, for example, The Restore Online Shoppers' Confidence Act (ROSCA)[5], The Telemarketing Sales Rules (TSR)[6], The Truth in Lending Act (TILA), The Children's Online Privacy Protection Act (COPPA)[7].

A month later the same year, the Deceptive Experiences to Online Users Reduction Act (DETOUR)[8] was introduced in the U.S. Senate. The initiative aims to completely ban exploitative and misleading practices by major online platforms and improve consumer welfare. The draft rules do not call directly “dark patterns”, but uses the term “unfair and misleading practices related to the manipulation of the user interface”.

The varieties of such practices are separately identified as:

designing, altering, or manipulating the user interface to conceal, undermine, or infringe on user autonomy, to influence decision-making, or to provide user data;

---

news/press-releases/2022/09/ftc-report-shows-rise-sophisticated-dark-patterns-designed-trick-trap-consumers (accessed: 05.09.2024)

[5] Restore Online Shoppers' Confidence Act of 2010. Available at: https://www.ftc.gov/legal-library/browse/statutes/restore-online-shoppers-confidence-act (accessed: 05.09.2024)

[6] Telemarketing Sales Rules of 2022. Available at: https://www.ftc.gov/legal-library/browse/rules/telemarketing-sales-rule (accessed: 05.09.2024)

[7] Children's Online Privacy Protection Rule of 1998. Available at: https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa (accessed: 05.09.2024)

ф[8] Deceptive Experiences to Online Users Reduction Act. H.R.6083 of 2021. Available at: https://www.congress.gov/bill/117th-congress/house-bill/6083?s=1&r=30 (accessed: 05.09.2024) subdividing or segmenting consumers of online services into groups for the purpose of behavioral or psychological experimentation or research on users of an online service, except with the informed consent of each user involved; or

designing, modifying, or manipulating the user interface on a website or online service intended for persons under the age of 13 to encourage habituation to the service.

After the bill was sent to the Consumer Protection and Commerce subcommittee in December 2021, there was no further movement on this legislative initiative.

In January 2023 the Future of Privacy Forum (hereinafter FPF) has published the current position of U.S. regulators on dark patterns.[9] In particular, it highlighted key trends explaining the most significant rules that address manipulative design in the US data protection context and highlighted the opportunities and challenges of applying anti-manipulative design rules to specific business sectors or practices. It was noted that most state laws aimed at limiting or prohibiting the use of manipulative design are based in one way or another on the already mentioned DETOUR bill.

Indeed, several laws have been drafted and passed at the state level that focus on banning "dark patterns."

The first state-level act regulating dark patterns was the California Consumer Privacy Act (CCPA)[10], now amended and supplemented by the California Privacy Rights Act (CPRA).[11] It was the first legislation in the USA to explicitly regulate dark patterns. The current document defines a "dark pattern" as "a user interface designed or operated with the substantial effect of undermining or limiting a user's autonomy in making decisions or exercising choices." If a company fails to comply with the requirements of this law, the state attorney general may file a lawsuit that will result in the offending company being fined. The amount of the fine is determined by the applicable unfair competition law. Interestingly, the CPRA includes a

---

[9] Slater F. The Future of Manipulative Design Regulation // Future of Privacy Forum. 2023. Available at: https://fpf.org/blog/the-future-of-manipulative-design-regulation/ (accessed: 10.09.2024)

[10] California Consumer Privacy Act of 2018 (CCPA) // Available at: https://oag.ca.gov/privacy/ccpa (accessed: 10.09.2024)

[11] California Privacy Rights Act of 2020 (CPRA) // Available at: https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-final-text-of-regs.pdf (accessed: 10.09.2024)

provision that explicitly forbids obtaining consent related to the processing of personal information by means of dark patterns [King J., Stephan A., 2021: 267].

Speaking about the requirements to the interface design, it should be noted that the concept of age-appropriate design (age-appropriate design) is also gaining popularity. In the US, this concept is regulated by the California state law (the California Age-Appropriate Design Code Act–CA AADC)[12], the Illinois legislative initiative (SB 3334)[13] and the federal bill on the safety of children on the Internet (Kids Online Safety Act — KOSA)[14].

Under this framework, website and mobile app owners are encouraged to check the appearance of online pages, algorithms, and service targeting ads for the “dark patterns” that entice children to provide excessive data, remove privacy settings, or otherwise act against children’s interests.

Hence, in many ways, age-appropriate design and “dark pattern-free” design are two elements of the same idea, which boils down to developing certain requirements for the interface of mobile apps and websites.

Thus, there is a trend in the U.S. to adopt special norms aimed at regulating “dark patterns” as special unfair and misleading practices related to the manipulation of the user interface. In addition, actual jurisprudence is also gradually emerging from the norms being approved.

2.2. Regulation of “Dark Patterns” in the EU

The General Data Protection Regulation (GDPR) does not set out a definition of dark patterns, but several its provisions somehow indicate a prohibition of unfair practices against consumers.[15] These provisions include: the principle of fairness and transparency (Article 5(1) (a), the principle of accountability in Article 5(2), data protection by default (Article 25), the requirement to provide data subjects with transparent privacy

---

[12] Available at: https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=202120220AB2273&showamends=false (accessed: 10.09.2024)

[13] Available at: https://www.ilga.gov/legislation/fulltext.asp?DocName=&SessionId=112&GA=103&DocTypeId=SB&DocNum=3334&GAID=17&LegID=&SpecSess=&Session= (accessed: 10.09.2024).

[14] Available at: https://www.congress.gov/bill/118th-congress/senate-bill/1409/text (accessed: 10.09.2024)

[15] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (accessed: 10.09.2024)

notices (Article 12(1), 13 and 14), and other rights of personal data subjects under the GDPR in Articles 15-22.

The European Digital Services Act (DSA) that has came into force in August 2023, explicitly prohibits the use of "dark patterns" in the online interfaces of digital platforms.[16] The law defines "dark patterns" as "practices that materially distort or impair, either on purpose or in effect, the ability of recipients of the service to make autonomous and informed choices or decisions".

Actual enforcement practices are also beginning to emerge as part of the implementation of this law. For example, in December 2023 the European Commission has launched an investigation into the social network X (ex-Twitter) for "dark patterns" prohibited by the DSA on its services.[17]

In 2023 the European Commission and the national consumer protection authorities of 23 EU states, as well as the consumer protection authorities of Norway and Iceland, published the results of an audit of retail websites covering 399 online stores.[18]

The study focused manipulative practices on the sites, which included fake countdown timers, web interfaces designed to induce consumers to make purchases, subscriptions or other choices, and hidden information.

According to the study, 148 websites contained at least one "dark pattern." 42 websites used fake countdown timers with deadlines to purchase certain products; 54 websites steered consumers toward certain choices, from subscriptions to more expensive products or delivery options; and 70 websites hid important information or made it less visible to consumers. For example, information about delivery costs, product composition or the availability of a cheaper option.

Several acts were approved as a result of the pan-European audit.

For example, in December 2023 the European Parliament has passed a resolution on addictive digital service design.[19] In particular, the Parliament

---

[16] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1666857835014 (accessed: 10.09.2024)

[17] Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_23_6709 (accessed: 10.09.2024)

[18] Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_418 (accessed: 10.09.2024)

[19] Available at: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0459_EN.pdf (accessed: 10.09.2024)

advocated the introduction of rules restricting the use of “dark patterns” by platforms that are addictive to consumers. The introduction of such rules seems relevant, as many platforms are now equipped with mechanics of involving the user in “endless” consumption of digital content, that can significantly harm his physical and mental health.

Also in December 2023, the Regulation on Harmonized Rules for Fair Access to and Use of Data (Data Act) was approved.[20] The Act prohibits the use of “dark patterns” by personal data operators or third parties to whom personal data is transferred with the consent of the user. This provision meets the principle of data minimization enshrined in the GDPR, aimed at prohibiting the collection of so-called excessive data, and allows to give additional legal guarantees to the user when transferring his data to third parties.

One of the objectives of the Directive on Financial Services Contracts Concluded at a Distance is to prevent traders, when concluding financial services contracts at a distance, from using dark patterns in their online interfaces [Brenncke M., 2023: 49].

Separately, attention should be paid to “dark patterns” in social networks.

In March 2022, the European Data Protection Board (EDPB) has published draft Guidelines 3/2022 “Dark patterns in social media platform interfaces: how to recognize and avoid”.[21] This document has become a practical guide for both developers and users of social media platforms. It defines “dark patterns” as “interfaces and user experiences implemented on social media platforms that lead users into making unintended, unwilling, and potentially harmful decisions regarding the processing of their personal data.”

The use of each dark patterns model is detailed according to the specific life cycle of a social media account: opening a social media account; informing on social media; protecting on social media; exercising personal data rights on social media; and deleting a social media account.

The draft recommendation for social media identifies types of “dark patterns” such as:

---

[20] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R2854 (accessed: 10.02.2024)

[21] Available at: https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf (accessed: 10.09.2024)

“overloading” — overloading users with more requests, information or options to encourage them to provide more data;

“skipping” — designing the interface in such a way that users forget (or fail to consider) all or some aspects of data protection when making a decision;

“stirring” — appealing to users’ emotions or using visual tricks;

“hindering” — hindering in obtaining information about the use of data or exercising control over data;

“fickle” — designing an awkward interface that makes it difficult to navigate or understand the purpose of data processing;

“left in the dark” — designing the interface in such a way as to hide information.

A lot of measures are also being taken in EU countries.

For example, in 2019 French data authority has released the report that defined “dark patterns” as “elements and mechanisms of interfaces implemented to influence users’ decisions in a way that they would not necessarily choose if the information was presented honestly and transparently”.[22]

In Belgium in October 2023 a checklist on the use of cookies was published. One of the items on the checklist is the absence of the use of “dark patterns” in the consent to accept cookies.[23]

The Luxembourg National Commission for Data Protection published updated recommendations on the use of cookies, according to which “dark patterns” include various shapes, fonts, colors, and sizes of “I accept” and “I decline” buttons.[24]

In Germany, based on the Research Institute for Public Administration (Deutsches Forschungsinstitut für öffentliche Verwaltung) within the framework of the Dark Pattern Detection Project (Dapde) there is an interdisciplinary group of scientists in the field of information technology and legal studies engaged in the search on technical detection of “dark patterns”

---

[22] Available at: https://linc.cnil.fr/cahier-ip6-la-forme-des-choix (accessed: 10.09.2024)

[23] Available at: https://www.autoriteprotectiondonnees.be/citoyen/actualites/2023/10/20/lapd-publie-une-checklist-pour-une-utilisation-correcte-des-cookies accessed: 10.09.2024)

[24] Available at: https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf (accessed: 13.09.2024)

and preparation of the necessary regulatory framework for their regulation.[25] Researchers use the now classic definition of "dark patterns" given by Harry Brignall.

The main tools of protection against "dark patterns", as follows from the information about the project, should be considered the norms of legislation on data protection, consumer protection, and competition protection.

Thus, approaches to the regulation of dark patterns are also beginning to take shape in EU countries. Approaches are being formed both at the supranational level, i.e. at the level of the European Union, and at the national level, i.e. at the level of individual EU states. At the same time, the regulatory approaches of the EU countries obviously follow in line with common European practices, as evidenced by similar terminology and similar rules for combating "manipulative design".

2.3. Regulation of "Dark Patterns" in the UK

In January 2021 the UK Competition and Markets Authority (CMA) has published a paper "Algorithms: How They Can Reduce Competition and Harm Consumers", which identified the need for joint regulation of dark practices with the UK Information Commissioner.[26] It defined "dark patterns" as "user interface designs that are used in such a way as to trick users into making unintended or potentially harmful decisions".

Two years later, in August 2023 the Competition and Markets Authority (CMA) and the Information Commissioner's Office (ICO) have published a joint paper "Harmful design in digital markets: how online choice architecture practices can undermine consumer choice and control over personal information" aimed at web designers and developers and outlines a set of best practices for providing consumers with information and choice about the collection and use of their personal information.[27]

The guidance lists "dark patterns" (e.g., "harmful nudging," "guilt-tripping," "batch consent," and "default settings") and highlights a few risks

---

[25] Available at: https://dapde.de/de/ (accessed: 13.09.2024)

[26] Available at: https://www.gov.uk/government/publications/algorithms-how-they-can-reduce-competition-and-harm-consumers/algorithms-how-they-can-reduce-competition-and-harm-consumers (accessed: 13.09.2024)

[27] Available at: https://www.drcf.org.uk/__data/assets/pdf_file/0024/266226/Harmful-Design-in-Digital-Markets-ICO-CMA-joint-position-paper.pdf (accessed: 13.09.2024)

associated with companies' use of dark patterns. Among other things, the authors of the guide supplement each "pattern" with a specific example illustrating a negative practice.

In 2020 an age-appropriate design code of practice, the so-called Children's Code, has came into force in the UK.[28] The document, which predates the California law and other U.S. initiatives, calls for basic "default" settings to be provided in a way that ensures children's safe access to online services and minimizes the collection and further use of children's data.

2.4. Regulation of "Dark Patterns" in Other Jurisdictions

In 2023 the Central Consumer Protection Authority of India has published Guidelines for Prevention and Regulation of Dark Patterns.[29] The document defines "dark patterns" as any practice or deceptive design pattern using user interface or user interaction on any platform that is intended to mislead or deceive users into doing something they did not originally intend or want to do, by undermining or impairing consumer autonomy, decision-making or choice, amounting to misleading advertising or unfair trade practices or consumer infringement. It provides a list of prohibited dark patterns with examples explaining them. However, these Guidelines are non-binding and lawyers are questioning their effectiveness due to lack of enforcement.

The Korea Republic Government is currently advocating for an amendment to the Act on The Consumer Protection in Electronic Commerce. The amendments would address "dark patterns", which have been declared an important consumer policy issue by the Commission and are supposed to develop means to prevent online platforms from deceiving users.[30]

In January 2022 the Information and Communication Technology Task Force was transformed into The Digital Markets Response Team. The Digital Consumer Division within it monitors and eliminates new behaviors designed to deceive consumers (including the use of "dark patterns"), en-

---

[28] Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/code-standards/ (accessed: 13.09.2024)

[29] Available at: https://consumeraffairs.nic.in/theconsumerprotection/guidelines-prevention-and-regulation-dark-patterns-2023 (accessed: 13.09.2024)

[30] Available at: https://www.kimchang.com/en/insights/detail.kc?sch_section= 4&idx=22891 (accessed: 13.09.2024)

sures that consumer choice is available and that consumers have sufficient information to make informed decisions.[31]

In June 2022 the UK and Singapore have signed the UK-Singapore Digital Economy Agreement (DEA).[32] According thereto both states are committed to ensuring fair online trading and protecting consumers from fraudulent or unfair business practices (including “dark patterns”).

In July 2023 Kazakhstan has approved the law “On Online Platforms and Online Advertising”.[33] The new legislation has a broad subject of regulation — from the legal regime of operation of online platforms and online advertising to the legal status of influencers (bloggers). At the same time, as far as online platforms are concerned, the law states that their interface should not mislead or otherwise prevent the user from deciding.

3. Case Study

In the absence of strict and clear rules applicable to dark patterns, it is possible only to witness some activity on this issue from the judiciary and other authorities. Because these tricks were used by business to attract more users and thus gain more profit, there are various lawsuits against big companies alleging consumer manipulation.

The European Union has already developed its law enforcement practice (on every state level). For example, the Italian data protection authority (Garante) has fined a company providing digital marketing services 300 thousand euros for illegal processing of personal data using “dark patterns”.[34] According to Garante, through various manipulative techniques, the digital platform induced users to consent to the processing or to the transfer of their data to third parties.

The U.S. Federal Trade Commission has recently intensified its actions in the fight against dark patterns.

---

[31] Available at: https://www.kimchang.com/en/insights/detail.kc?sch_section=4&idx=24536 (accessed: 13.09.2024)

[32] Available at: https://www.gov.uk/government/publications/uk-singapore-digital-economy-agreement-explainer/uk-singapore-digital-economy-agreement-final-agreement-explainer (accessed: 13.09.2024)

[33] Law of the Republic of Kazakhstan of July 10, 2023 №18-VIII ZRC On online platforms and online advertising // Egemen Kazakhstan. 2023. № 128 (30607).

[34] Available at: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9870725#1 (accessed: 13.09.2024)

In 2023 the Commission has reached a 18,5 million dollars settlement with Publishers Clearing House for engaging in misrepresentation and deceptive practices.[35] According to the FTC, the PCH Publishers Clearing House employed various manipulative practices, e.g. the use of extra-small and too-light fonts for disclosure notices and links and adding shipping and handling fees late in the checkout process.

One of the biggest-scale cases on that matter concerns Amazon. According to the lawsuit, "Amazon has knowingly duped millions of consumers into unknowingly enrolling in Amazon Prime and used manipulative, coercive, or deceptive user-interface designs known as "dark patterns" to trick consumers into enrolling in automatically renewing Prime subscriptions".[36] On 28 May 2024, a federal judge has handed down a decision allowing the lawsuit to proceed. Furthermore, the Judge has ruled that the Commission's claim was sufficiently plausible, indicating that a reasonable consumer who clicks on the orange "Get FREE Two-Day Delivery" button may not be aware that they are consenting to the automatic renewal of a Prime subscription. Additionally, the visual discrepancy between the "yes" and "no" buttons may lead consumers to believe that clicking "yes" is the only option for completing the checkout process. Moreover, the Judge Chun has expressed concern that Amazon made it considerably more difficult to cancel a Prime subscription than to enroll in Prime.

The most recent case to-date is a lawsuit brought against Adobe by the FTC and the Department of Justice in June 2024.[37] Adobe and two of its executives are charged with deceiving consumers by concealing the early termination fee for its most popular subscription plan and making it challenging for consumers to cancel their subscriptions.

Similar accusations were thrown at Google in 2022.[38] Then the Attorney General for the District of Columbia has filed a lawsuit a complaint to stop Google's violations of the District's consumer protection laws, which included the use of dark patterns to undermine users' informed choices (for

---

[35] Available at: https://www.ftc.gov/system/files/ftc_gov/pdf/PCH-Complaint.pdf (accessed: 13.09.2024)

[36] Available at: https://www.ftc.gov/system/files/ftc_gov/pdf/amazon-rosca-public-redacted-complaint-to_be_filed.pdf (accessed: 13.09.2024)

[37] Available at: https://www.ftc.gov/system/files/ftc_gov/pdf/040-UnredactedComplaint.pdf (accessed: 13.09.2024)

[38] Available at: https://oag.dc.gov/sites/default/files/2022-01/DCv.Google%281-24-22%29.pdf (accessed: 13.09.2024)

instance, the could not easily opt out of having their location tracked). The very same year Google has decided to settle the lawsuit.[39] According to the settlement, Google had to pay 9,5 million dollars fine to the District as well as issue notifications to users who currently have certain location settings enabled; clearly inform users about data collection when they enable location-related Google account settings; maintain a webpage that discloses Google's policies and practices concerning location data; improve users' ability to identify location-related controls; limit sharing of users' data and retention of data; prepare annual compliance reports.

These three are the most recent FTC cases involving Big Tech companies. However, before that it has already tried to fight various dodgy tactics taken by companies to lure customers (e.g. Federal Trade Commission v. AMG Capital Management; Federal Trade Commission v. Office Depot). In a series of unheralded FTC deception cases, and in a few unfairness enforcement actions to boot, the regulator best positioned to address dark patterns has successfully shut down some of the most egregious ones [Luguri J., Strahilevitz J.A., 2021: 102]. In the overwhelming majority of enforcement actions, companies choose to settle with the Commission entering into binding settlement agreements, but not to challenge the commission in court or administrative proceedings [Solove D.J., Hartzog W., 2014: 583].

Also worth noting is that just until recently (recently being the cases against Adobe, Google and Amazon) courts, despite substantive scholarship on dark patterns, in the United States and the FTC have not been proactively using the term "dark patterns" when issuing decisions policing manipulative user interfaces [Nousiainen C.P., Ortega K., 2024: 92].

It can also be said that the lack of direct regulation of dark patterns does not automatically mean that it is impossible to sue companies for using a manipulative interface. Before Indian Guidelines of 2023 were passed, in 2021 the Hyderabad District Disputes Redressal Commission has fined online ticket aggregator Book My Show and PVR cinemas for imposition of Internet handling charges on the customers. The Commission's order has indicated that the imposition of internet handling charges in the final bill amount without a clear segregation is equal to an unfair trade practice, thus it violates the Consumer Protection Act of 2019. Basically, the Commission has qualified the imposition of Internet handling charges in the

---

[39] Available at: https://oag.dc.gov/release/ag-racine-announces-google-must-pay-95-million (accessed: 13.09.2024)

final bill amount as hidden cost practice (one of the types of dark patterns) [Sharma S.J., Sharma I., 2023: 143].

4. Russian Approach

Digital economy in Russia is regulated both through the new legislative norms and self-regulation, e.g. the codes of conduct, guidelines, recommendations, and sets of best practices.

The main laws that set up an official framework for digital technologies in Russia are the Civil Code of the Russian Federation[40], the Federal Law “On Personal data”[41], the Federal Law “On Information, Information Technologies and Protection of Information”.[42]

Article 10.6 of the Federal Law “On Information, Information Technologies and Information Protection” sets up a number of obligations for social networks owners. For intense, they are obligated to monitor and remove prohibited information, to create a feedback tool for users’ appeals, and to annually publish a report on the results of such “self-control”.

That is, these norms are designed to ensure self-regulation of social networks, which were originally created on the basis of such self-regulation.

No less important, but less frequently mentioned in the context of the digital economy is the Law of the Russian Federation on Protection of Consumer Rights.[43] Particularly, this legal act regulates the consumer purchase of goods or services on the Internet.

Article 10 of the Law “On Protection of Consumer Rights” enshrines the obligation of the producer or seller to provide the consumer with necessary and reliable information about goods, works or services, ensuring the possibility of their correct choice. However, the Russian law does not contain any provisions prohibiting the using of the “dark patterns”.

---

[40] Civil Code of the Russian Federation // Collected Laws of Russia. 1994. No.32. Article 3301.

[41] Federal Law of the Russian Federation of July 27, 2006 No.152-FZ On Personal Data // Rossiyskaia Gazeta, 2006, № 165.

[42] Federal Law of the Russian Federation of July 27, 2006 No.149-FZ On Information, Information Technologies and Information Protection // Ibid.

[43] Law of the Russian Federation of February 7, 1992 No. 2300-I On Protection of Consumer Rights // Bulletin of the Congress of People’s Deputies of the Russian Federation and Supreme Council of the Russian Federation. 9.04.1992. № 15. Art. 766.

Speaking about misrepresentation in general, it is worth to mention the Federal Law "On Protection of Competition".[44] In particular, Article 14.2 of this law prohibits unfair competition by misrepresentation.

The responsibility for unfair competition by misrepresentation is laid down by the Article 14.33 of the Code of Administrative Violations.[45] At the same time, Article 14.7 of the Code establishes liability for consumer deception and misleading consumers. Article 14.8 of the Code provides for administrative responsibility for violation of the consumer's right to receive necessary and reliable information.

Thus, liability for misleading for the purposes of unfair competition differs from misleading the consumer without violation of law. It should be noted that the legal relations between business and the consumer and their ethical component, i.e. the interaction of subjects in the B2C segment, is the main idea of the article.

As it was already mentioned, "dark patterns" as methods of manipulating of user behavior are closely connected with the creating of visual effects. Moreover, their use is not always aimed at obtaining a direct commercial benefit in the form of payment of consumers for a certain product or service.

Sometimes "dark patterns" may fall, for example, under the law on advertising.

Thus, according to the Part 7 of Article 5 of the Federal Law "On Advertising" it's prohibited to make advertisements, which do not contain part of the essential information about the product, the conditions of its purchase or use, if it distorts the meaning of information and misleads the consumer.[46]

Part 9 of Article 5 prohibits hidden advertising, that has an unconscious impact on the consumers.

As it was correctly noted by the press service of the Federal Antimonopoly Service of Russia, the dissemination of incomplete information or concealment of its significant part are the main ways of misleading.[47]

---

[44] Federal Law of July 26, 2006 № 135-FZ On Protection of Competition // Rossiyskaia Gazeta. 2006. №162.

[45] Code of the Russian Federation on Administrative Violations of December 30, 2001 № 195-FZ // Rossiyskaia Gazeta. 2001. № 256.

[46] Federal Law of March 13, 2006 No. 38-FZ On Advertising // Parliamentskaia gazeta. 2006. №37.

[47] Available at: URL: https://fas.gov.ru/publications/20367?ysclid=ltya9u3ner23880392 (accessed: 10.10.2024)

Authors of the article would like to emphasize the recent changes in the legislation on advertising, expressed in the adoption of new requirements for advertising of credit products.[48]

In 2023 the requirements to the print in the advertisements of credit products came into force. According to the amendments, the size of the print used to indicate the ranges of values of the full value of the consumer loan should not be smaller than the size of the font used to indicate information on interest (percentage) rates.

In October 2023 the credit organization “Pochta Bank” was fined for failure to comply with the FAS order to remove this kind of improper advertising.[49] In February 2024, cases were brought against Alfa Bank and Sberbank on the same ground.[50] [51]

All in all, some aspects of the “dark patterns” — for example, the possibility of misleading through manipulation of prints — could be found in the specific legislation and law enforcement practice.

At the same time neither general regulation of the manipulative interface design practices nor special terminology is introduced.

Nevertheless, the competent authorities are gradually beginning to form their positions.

In November 2023 the Bank of Russia has issued a report “Approaches to the Regulation of Remote Sales Channels to Protect the Rights of Financial Services Consumers”.[52] In the report, the Bank highlighted such unfair practices in the online sale of financial products as the use of ambiguous or difficult-to-understand wording, graphic and color techniques that focus the consumer’s attention on certain terms of the contract or additional services.

The Bank of Russia has defined “dark patterns” as “various marketing techniques that encourage consumers to take certain actions”.

---

[48] Federal Law № 359-FZ of July 24, 2023 “On Amendments to the Federal Law On Consumer Credit (Loan)’ and certain legislative acts of the Russian Federation // Rossiiskaia Gazeta.2023. №168.

[49] Available at: URL: https://fas.gov.ru/news/32852 (accessed: 10.10.2024)

[50] Available at: URL: https://fas.gov.ru/publications/24254 (accessed: 10.10.2024).

[51] Available at: URL: https://fas.gov.ru/publications/24273 (accessed: 10.10.2024)

[52] Available at: URL: https://cbr.ru/Content/Document/File/156122/Consultation_Paper_13112023.pdf (accessed: 10.10.2024)

Basing on the results of the report, the Bank offers a number of proposals to regulate the practice of selling financial products. For instance, one of the proposals is to completely eliminate the use of "dark patterns" in the banking.

In June 2022 the Regional Public Center of the Internet Technology (ROCIT) has presented an analytical report on manipulation of user behavior using "dark patterns".[53]

ROCIT experts has defined "dark patterns" as "techniques of manipulating user behavior with the help of the device and design of a website, application or digital services, aimed at inducing the user to make decisions that are beneficial for a commercial company".

The authors of the study identified such types of dark patterns as:

coercion — threatening or requiring the user to fulfill certain requirements (requiring the user to enter contact information before allowing the user to complete a task);

confusing — asking information from the user that they do not understand (asking a novice user if they want to change the default browser; using double, triple or quadruple negation);

distraction — distracting the user from their actual task in order to redirect their attention to areas of the interface that are beneficial to the company (a red button on the desired interface element to draw attention);

utilizing user errors in order to achieve the actions desired by the interface designer;

compulsory work — deliberately increasing the amount of work for the user (making the user wait and view an advertisement for a certain amount of time);

interruption — interrupting the flow of a user's tasks;

canipulation of navigation: creating information architectures and navigation mechanisms that direct the user to perform a desired action (a free version of an application is much harder to find than a commercial version);

concealment — hiding necessary information and interface elements;

restriction of functionality — limiting or excluding controls that facilitate the user's task;

---

[53] Available at: URL: https://t.me/IT_today_ru/5776 (accessed: 10.10.2024)

shock — presenting disturbing content to the user;

subterfuge — misleading the user or other attempts to deceive (installation of additional software without the user's knowledge or consent).

In order to combat such unfair practices, ROCIT experts propose the development of uniform rules, regulation by the state and public organizations, and the introduction of negotiable fines for repeated violations.

As was mentioned above, "dark patterns" may also be manifested through the functioning of recommendation technologies.

In the fall of 2023 the Alliance for Artificial Intelligence has developed guidelines for the use of recommendation technologies and algorithms based on artificial intelligence.[54] The document contains several principles for the ethical use of recommender algorithms, some of which can also be used in the prevention of the use of "dark patterns".

For example, the experts draw attention to recommendations that turn into imposition and note that their use is not advised.

Also, the authors of the document emphasize the need to combat the manipulation of algorithms, through which you can influence the user's perception of a particular product, the feasibility of its purchase, to "tweak" the popularity of a particular content.

Among other things, experts of the Alliance in the field of artificial intelligence advise to implement recommendations that suggest the user to take certain actions to preserve health, including interrupting the use of the service for rest or sleep. This practice seems relevant in the fight against digital services based on "pulling" the user into a long-term session, for example, through the system of endless scrolling of the feed. This was already mentioned in the first chapter of the study, when the "TikTok phenomenon" was considered.

Thus, at present in Russia there is no special normative regulation or advisory acts devoted to the prohibition of "dark patterns" and other ways of manipulating consumer behavior on the Internet.

In one way or another there may be norms in the legislation that can be applied to "dark patterns", however, they will affect only one narrow aspect of such unfair practices (for example, "dark patterns" in advertising may be

---

[54] Available at: URL: https://ai.gov.ru/knowledgebase/etika-i-bezopasnost-ii/2023_eticheskie_rekomendacii_po_primeneniyu_rekomendatelynyh_tehnologiy_i_algoritmov_osnovannyh_na_iskusstvennom_intellekte_v_cifrovyh_servisah_alyyans_v_sfere_iskusstvennogo_intellekta/ (accessed: 10.10.2024)

recognized as improper advertising) and will not cover the whole concept of prohibition of user design that is misleading.

Properly used new technologies can serve the greater good and provide benefits for all subjects of economic activity. During the study the authors concluded that regulation could derive not from banning negative practice but from promoting positive one.

Having examined Russian online marketplaces, the authors summarized their user interface design practices and formulated the concept of “light patterns,” which is the opposite of unfair manipulative techniques and are user-friendly.

As elements of ethical user interface design, “light patterns” encourage the user to make a conscious choice, which is particularly important when they are making an economic or legally binding decision.

This concept was presented to a committee of the Big Data Association, the organization that is working out the Code of Ethics for Data Use. The proposal was unanimously accepted by the members of the Big Data Association, Russian tech companies, including Yandex, Sberbank, Megafon, T-Bank, etc., and was included in the Big Data Association’s White Paper — a set of best practices of fair data use.

The following “light patterns” were defined:

clarification: additional steps or clarifying barriers to confirm intent in economic or legally binding actions;

price Transparency: clear indication of the final price of the contents in a shopping cart including packaging, delivery and other paid options; the initial price of the order doesn’t differ from the final price that the user sees when paying for the order, as it includes all options;

navigation: links are visually distinct from regular text elements, have a consistent style and are in a highly readable print;

reasonable highlighting: in the case of a choice between two categories, one of that could result in economic or legally binding consequences (acceptance of cookies, account registration, paid subscription etc.), it is necessary to highlight only the choice that does not provide such consequences or not to highlight any of them.

Undoubtedly, the passing of these recommendations indicates an intention of the Russian business to follow a positive practice that protect both the balance of interests of economic entities and the consumer as the weaker party in commercial relationship.

The development and implementation of this case study in the practice of the Russian companies will allow them to avoid legal and reputational risks and create a basis for the further legislative regulation.

Conclusion

The regulation of manipulative methods in the digital space is becoming an important task to ensure fair interaction between business and consumers. The study shows that, unlike foreign countries, where law enforcement practice regarding "dark patterns" is actively developing, Russia still lacks specific norms that fully cover this phenomenon. However, several provisions of the legislation can be applied to manipulative interfaces. The approving of ethical standards and the introduction of the concept of so-called "light patterns", based on fair interaction with users, may be the first step towards the formation of a legislative framework. In the long term, this will not only increase trust in digital services, but also reduce the risks for companies seeking to maintain a balance between the interests of all participants in the digital economy.

References

1. Blazheev V.V., Egorova M.A. (2020) Digital Law: textbook. Moscow: Prospect, 640 p. (in Russ.)

2. Brenncke M. (2024) Regulating Dark Patterns. *Notre Dame Journal of International and Comparative Law*, vol. 14, issue 1, pp. 39–79.

3. Calo R. (2014) Digital Market Manipulation. *The George Washington Law Review,* vol. 82, no. 4, pp. 995–1051.

4. Duplyakin V.M., Knjazheva Y.V. (2016) Checkout area service simulation of trade enterprise. *International Research Journal*, vol. 9, pp. 36–39. DOI: 10.18454/IRJ.2016.51.100

5. Hartzog W. (2018) *Privacy's Blueprint: The Battle to Control the Design of New Technologies.* Cambridge (Mass.): Harvard University Press, 384 p.

6. King J., Stephan A. (2021) Regulating Privacy Dark Patterns in Practice — Drawing Inspiration from California Privacy Rights Act. *Georgetown Law Technology Review*, vol. 5, issue 1, pp. 251–276.

7. Leiser M., Santos C. (2023) Dark Patterns, Enforcement, and the Emerging Digital Design Acquis: Manipulation beneath the Interface. *European Journal of Law and Technology*, vol.15, no.1, pp. 1–31.

8. Leiser M.R., Caruana M. (2021) Dark Patterns: Light to be found in Europe's Consumer Protection Regime. *Journal of European Consumer and Market Law*, vol. 10, no. 6, pp. 237–251.

9. Luguri J., Strahilevitz L.J. (2021) Shining a Light on Dark Patterns. *Journal of Legal Analysis*, vol. 13, issue 1, pp. 43–109.

10. Nousiainen K., Ortega C.P. (2024) Dark Patterns in Law and Economics Framework. *Loyola Consumer Law Review,* vol. 36, issue 1, pp. 90–120.

11. Sharma S.J., Sharma I. (2023) Dark Patterns in a bright world: An analysis of the Indian Consumer Legal Architecture. *International Journal on Consumer Law and Practice*, vol. 11, pp. 123–146.

12. Solove D.J., Hartzog W. (2014) The FTC and the New Common Law of Privacy. *Columbia Law Review*, vol. 114, pp. 583–676.

13. Webb E. (2022) *Doomsday Algorithm. How Facebook, Google, Microsoft, Microsoft, Apple and other corporations create artificial intelligence and why it will lead to disaster*. Moscow: Eksmo, 400 p. (in Russ.)

14. Yablonski D. (2022) *Laws of UX-design*. Saint Petersburg: BXV- Petersburg:, 160 p.

15. Zuboff S. (2022) *The Era of Supervisory Capitalism. The battle for human future on the new frontiers of power*. Moscow: Gaidar Institute, 784 p. (in Russ.)

Information about the authors:

B.A. Edidin — Candidate of Sciences (Law), Deputy Director General for Legal Affairs.
K.V. Kochetkova — Candidate of Sciences (Law), Senior Lecturer, Senior Associate.
N.D. Sarankina — PhD Researcher, Junior Associate.

Contribution of the authors: the authors contributed equally to this article.
The authors declare no conflicts of interests.

The article was submitted to editorial office 05.10.2024; approved after reviewing 04.11.2024; accepted for publication 04.11.2024.

Legal Issues in the Digital Age. 2024. Vol. 5. No. 4.
Вопросы права в цифровую эпоху. 2024. Т. 5. № 4.

Research article
УДК: 342
JEL: K2
DOI:10.17323/2713-2749.2024.4.28.45

Human Voice: Legal Protection Challenges

Ruslan Aleksandrovich Budnik[1],
Evgenia Gennadievna Evpak[2]

[1, 2] National Research University Higher School of Economics, 20 Myasnitskaya Street, Moscow 101000, Russia,

[1] rbudnik@hse.ru, https://orcid.org/0000-0001-8076-1560

[2] eevpak@hse.ru, https://orcid.org/0000-0001-5961-5657

Abstract

Focused on the phenomenon of human voice, the paper purports to develop approaches to legal protection of ordinary people's voices and those of artists as the technologies for sound synthesis, music and vocal performance are becoming more sophisticated. It was demonstrated the problem of legal protection of human voice has become especially pressing one in the context of artificial neural networks such as vocaloid designed for sound synthesis and voice cloning. The study provides a systemic arrangement of legally meaningful knowledge of human voice useful for the development of legal provisions to protect this personal good. The legal substance of vocal impersonation as a way to simulate and manipulate a synthesized voice was explored. Theoretically applicable legal constructs for protection of voice and computerized cloning technologies were analyzed. A trend to use copyright rather than patent for protecting vocaloid-like generative neural networks and other technological solutions for vocal synthesis was identified. The concept of voice was critically analyzed to propose a viable legal provision for its protection. The primary and auxiliary features of the concept of voice were parametrized for possible use in disputes on the legitimacy of voice cloning or vocal impersonation. The concept of vocal identity of ordinary people and artists was proposed for legal protection of this personal good as a set of performative sonic features including the basic parameters of singing voice as well as acoustic-phonetic and articulatory features

© Budnik R.A., Evpak E.G., 2024
This work is licensed under a Creative Commons Attribution-Sharealike 4.0 International License
https://creativecommons.org/licenses/by-sa/4.0/legalcode.en

of vocalization. A comprehensive legal and technological methodology for the protection of vocal identity was proposed.

Keywords

human voice; voice as a personal good; protection of voice; voice cloning; vocal impersonation; musical neural networks; vocaloids; legal parametrization of voice; vocal identity.

For citation: Budnik R.A., Evpak E.G. (2024) Human Voice: Legal Protection Challenges. *Legal Issues in the Digital Age,* vol. 5, no. 4, pp. 28–45. DOI:10.17323/2713-2749.2024.4.28.45

Background

Explosive progress of creative neural networks since the early 2010s has prioritized the study of legal nature and assessment of musical works created through the use of artificial intelligence as one of the topical and at the same time ambivalent problems [Bridy A., 2016]; [Levy P., 2005].

Musical products generated by weak AI-based neural networks are treated as compilation, iteration or algorithmic creative outcomes[1]. Meanwhile, recognizing a creative work and objective form of expression in these outcomes will suffice to make them copyrightable[2].

By 2023, there were at least 17 popular brands of musical neural networks[3] on the global mass market including services such as Mubert and Suno that are tools for generative song prototyping based on the use of algorithmic vocal loop.

In 2023, the International Federation of the Phonographic Industry (IFPI) has published the *Engaging with Music* — annual Global Music Re-

---

[1] In his paper "Study of models and algorithmic methods for analysis of musical works", L.A. Aznaurian with reference to A. Rozen and A. Vasiliev provides four types of algorithmic compositions including: (1) composition methods based on mathematical functions; (2) composition practices based on combinatory methods; (3) practices based on natural processes and (4) practices using rule-based processes.

[2] Two creative patterns are normally identified: (1) spontaneous "divine" inspiration of irrational nature and (2) rational trial-and-error iterations of creative product.

[3] Music Cheat Sheet. A list of popular music apps and plugins (and tips on how to use them). Available at: https://bobbyoswinski.com (accessed: 16.10.2024)

port reflecting for the first time the listeners' opinion of neural network-generated music streamed live and listed in playlists. It was reported that 8 out of 10 respondents (almost 79% of 43,000 across 26 countries covered by the study) believed the human agent's creative potential to be sufficient to prop up musical creativity in the context of progress of electronic music and generative art. While 74% of respondents believed that using musical neural networks and AI technologies to clone or substitute for artistic personality was illegal and unacceptable one, 76% were convinced that music and voice timbres should not be processed by neural networks without approval of artists, and 73% agreed that neural network producers should disclose the information on whose music was used to train online music generators. More than half of those polled believed that governments should develop and approve legal provisions applicable to automatically generated musical content[4].

Ten most popular genres in the IFPI's *Engaging with Music* report included were: pop, rock, hip-hop/rap, dance and electronic, Latino, rock-n-blues, classical and opera music, country, movie soundtracks and reggae[5]. The most popular works created in these genres are exposed to "digital activism", with fans using musical neural networks to create AI remixes and song covers. As a result, the authors, performers and record producers suffer losses from competing illegal remakes of popular works that pay no royalties to the actual copyright holders. This happened to Drake's *Heart On My Sleeve* featuring the Weekend: a neural network remix of this song was generated by Ghostwriter, anonymous user, and posted to TikTok. As an unprecedented fact, the remix was nominated for Grammy award and de-listed by the Recording Academy just in time before the event[6].

From the perspective of legal assessment, streamed music can represent not only a musical work with added text, but also an audiovisual and other types of complex copyrighted works since a digital release promoted by the

---

[4] For details see: IFPI Global Music Report 2023. State of the Industry. 2023. P. 11. Available at: https://www.ifpi.org/wp-content/uploads/2020/03/Global_Music_Report_2023_State_of_the_Industry.pdf (accessed: 30.05.2024)

[5] IFPI Engaging with Music 2023. Available at: https://www.ifpi.org/wp-content/uploads/2023/12/IFPI-Engaging-With-Music-2023_full-report.pdf (accessed: 16.11.2023)

[6] AI-Generated Drake, The Weeknd Song Not Eligible for Grammy. Here's How It Could Have Been Though // Forbes Business. 8.09.2023. Available at: https://www.forbes.com/sites/darreonnadavis/2023/09/08/ai-generated-drake-the-weeknd-song-not-eligible-for-grammy-heres-how-it-could-have-been-though/?sh=180db4102321 (accessed: 20.01.2024)

streaming service mandatorily includes, apart from the phonogram with or without text, the graphical cover and sometimes auxiliary copyrighted works that, together with the phonogram, make up an integral artistic form.

The paper presented is focused on multidisciplinary phenomenological analysis of human voice as exemplified by singing voice to propose, based on analytical findings, adequate and viable approaches to legal protection of this intangible personal good. Achieving this purpose will require to address a number of particular research objectives. The authors will need to analyze how vocaloid-like artificial neural networks and similar tools for cloning individual voice prints make the legal regulation of this problem highly relevant. There is a need to explore research publications that conclude on the open nature of voice parameters and argue that voice absorbs new characteristics resulting from the studies of articulatory and artistic expressive vocalization practices. There is a need to consider the view the basic list of voice parameters does not qualify this phenomenon clearly enough and therefore cannot provide a reliable basis for the underlying legal provision. Finally, authors will need to posit a hypothesis of *vocal identity* as a replacement for the legal concept of *voice* covering a wider parametric range of individual vocal expression, as well as propose a methodology for its legal and technological protection.

1. Findings

1.1. Legally Meaningful Knowledge of Human Voice as a Phenomenon

In 2006, Yamaha Corporation has marketed a novel technology under the name of *vocaloid* based on its proprietary method of algorithmic synthesis of artistic voices. Under this technology popularized by cartoon artist Hatsune Miku's concert shows, a target artist's voice print is digitized by the neural network across a number of preset parameters including the individual voice timbre, physiological peculiarities of vowel and consonant articulation, characteristic breathing and vocalization, as well as other vocal parameters associated with characteristic pronunciation, rhythmic and dynamic syllabic intonation of musical and speech phrases depending on emotional coloring and meaning of musical messages that are subsumed into the artist's recognizable individuality.

To the phenomenon of the Japanese hologram Hatsune Miku is addressed by a number of studies with the following interest for theme under discussion [Drenten J., Brooks G., 2020: 1319–1323]; [March L., 2023: 894–910]; [Watt D., Harrison P., Cabot-King L., 2020: 172–180].

A. Jones and R. Bennett in their book *Digital Evolution of Live Music* explain the progress of voice synthesis technologies as a challenging trend of participatory culture behind the strife of anthropomorphic musicians to bring digital technologies to performance practices.

Apart from a popular J-pop performer, the book refers to Tupac Shakur's super-realistic hologram with the synthesized voice timbre recreated in 2012 by digital technologies at the Coachella Festival especially for the musician's fans. The authors consider Tupac Shakur's digital "resurrection" by voice synthesis technologies from existential standpoint of "life after death while noting the technological promise of replicating the "Cher effect" in the algorithmic vocal synthesis and processing. The researchers find that musical artists willingly promote the introduction of digital technologies into performative practices, with fading boundaries between live and virtual performance to result in new legal and ethical implications [Jones A., Bennett R. et al., 2015: 14, 55–70].

In her book *Listening, Timbre and Vocality in African American Music*, Nina Eidsheim, following a subjectivist approach to perception of sound, argues that anyone listening to vocal performance acts as a listener and a vocalist at the same time [Eidsheim N.S., 2019: 186]. In support of the argument, she invokes the pedagogical practice of regular listening to reference records to develop a vocal style imitating the singer of choice, such as Billy Holliday's timbre, and observes, contrary to the generally acknowledged view of Deepfake as highly developed technology [Cheng H., Guo Y., Wang T. et al., 2023: 1–22], that under otherwise equal acoustic parameters a human agent's imitation of someone's vocal style will be always recognizable and different from a neural network's (vocaloid's) imitation due to complexities of harmonic and emotional nature of vocalization.

As a psychophysiological communicative function of human body, voice has been studied since antiquity in the context of biology, physiology and semiotics. Voice can be formally described as human ability to use the vocal tract for producing sound in conversation and singing [Watt D., Harrison P., Cabot-King L., 2020: 137-170]. In his monograph *Voice Development. Vocal control and Training*, V.V. Emelyanov, author of the phonopedic voice development methodology, identifies two types of voice: speaking voice and singing voice, and argues that singing voice will evolve in vocal training from general forms of movement, singing patterns, intervals and simple vocalization sequences [Emelyanov V.V., 2023: 21]. It suggests that a neural network can perceive a reference timbre precisely in process of analyzing specific vocal and intonating patterns decomposed to identify the characteristics important for cloning the artist's original timbre.

In calling *voiceology* the discipline integrating multidisciplinary ideas of human voice, L.B. Rudin has identified a number of its conceptual branches such as anatomic functional arrangement of vocal apparatus; physiology and acoustic principles of phonation; notion of voice as a means of communication; voice genetics; notions of singing and speaking voice; classification of voices including children's; voice hygiene for vocal professionals; substance and basics of vocal methodology, rhetoric, scenic speech, oral speech technology; concept of vocal talent; basics of creative process psychology, etc. [Rudin L.B., 2009: 5–8]. The findings of Rudin's theory agree with those of other studies of human voice in identifying its main parameters such as pitch, timbre and tone. Voices pitch, timbre and tone were explored by a number of specialists and drew a parallel between vocal expression categories and generalized expression of musical language [Kolonei V., 2017: 18–31]; [Stulova G.P., 2014: 90–104]; [Toropova A.V., 2017; 394–405]; [Umetalieva-Bayalieva Ch. T., 2015: 204–207]. Sometimes they compare metaphorically singing voice with a musical instrument

It is noteworthy that, despite an expanded list of individualizing attributes of voice found in some thematic studies [Efthymiou et al., 2024: 117–134], most authors have accepted the said three main characteristics.

Facial expressions and voice are always among the parameters that neural networks assess to recognize human emotions. Thus, I. Makarevich in the article *Prospects of technologies for recognition of human emotions by facial expressions and voice* [Makarevich I.V., 2022] notes, in analyzing a number of technological solutions for recognition of emotions from voice including libraries (Open SMILE, Delta) and applications (Emotion AI, Beyond Verbal, Cogito, Sense NEMESYSKO), that software will recognize emotions from voice across a wider set of criteria than the three main characteristics.

In an experiment to assess personal character traits from voice recordings through blind listening to a fairy tale recited by different people, several specialists [Khrisofanova L.A., Diveeva A.S., 2017: 157–164] have proved the potential for aurally determining psychological characteristics like extroversion/introversion; attachment/detachment; control/ naturalness; emotionality/impartiality; playfullness/pragmatism. The experiment reveals that human voice has a characteristically wide and open-ended range of attributes.

1.2. Hypothesis of Legal Protection of Vocal Identity

The above necessitates an evidence-based argument that a wider and more comprehensive concept of vocal identity embracing audio or vocal attributes is preferable to that of voice when discussing protection of voice as a personal good including for creative artistic use.

The evidence that this approach is viable can be found in legal practice and mass media that periodically report disputes on cloning the sound patterns of artists working in genres that cannot be fully qualified as vocal since they do not rely on unique vocal talent, ability to sing music notes, and mastery of what is considered to be the basic characteristics of voice (pitch, timbre and tone).

One such dispute involved Jay-Z and Roc Nation, an agency producer, that in 2020 demanded to delete deepfake video clips featuring the rap artist Jay-Z performing Billy Joel's song *We Didn't Start the Fire* and Hamlet's monologue *To Be or Not To Be* from William Shakespeare's eponymous play. The agency explained its protest in terms of illegal "vocal impersonation" of the artist they protected.

Rap and hip-hop artists can hardly be called singers in the classical sense meaning those who fully master singing skills and voice. They recite rather than sing, that is, rhythmically read verses, each in his unique manner of cadenced articulation. Vocal identity of these artists may be manifested and described in terms of other attributes auxiliary to the basic characteristics of singing voice that we will explore below. The same is true for other individuals such as politicians, movie stars and other celebrities who are not singers but whose vocal identity is exposed to cloning[7].

In 2024, a 15-second original voice recording would suffice for Open AI's simulator to perform voice impersonation (also referred to as voice

---

[7] See for details: AI voice clones mimic politicians and celebrities, reshaping reality // The Washington Post. 15.10. 2023. Available at: https://www.washingtonpost.com/technology/2023/10/13/ai-voice-cloning-deepfakes/ (accessed: 10.01.2024)

copying, cloning and synthesizing) [8]. Violations of individual rights by voice cloning are increasingly described as "vocal impersonation".

The contemporary Russian Free Encyclopedia *Traditsiya* defines the term "impersonation" (from French em- + Lat. persona + -tion) as "imitation or theatrical cloning of a personality to pass for another person". Impersonation is understood as a situation of taking someone's name or personality without permission with the purpose of harming, cheating, intimidating or threatening. Therefore, "vocal impersonation" amounts to copying/cloning the characteristics of speaking or singing voice to replicate it.

The substance of such phenomenon as "vocal impersonation" underlying disputes on illegal manipulations of human voice is defined in terms of copying, replication and use of synthesized voice in various forms and for various purposes. It is noteworthy that this synonymic chain matches the terminology of copyright provisions. Under Article 1270 of the Civil Code of Russia, the right to copy, replicate and use creative outcomes, once voice or more exact definition of this phenomenon is acknowledged as such, is owned exclusively by the author whose consent is required for these actions to be legitimate.

It would be logical to draw a legal parallel between human voice or vocal identity as an unalienable and inseparable personal good, and the physical human appearance, the only difference being that, while the former is not governed by law, the latter is protected by Article 152.1 of the Civil Code. To proceed further, we well need to discuss legal constructs theoretically applicable for protecting voice and its cloning technologies.

1.3. Legal Constructs for Protecting Voice and its Cloning Technologies

The first technological solution of voice synthesis — algorithmically driven vocal engine Yamaha Vocaloid — was an outcome of research performed by a group of students at the Pompeu Fabra University in Barcelona and patented as invention[9]. Based on Vocaloid software core licensed from

---

[8] Open AI's Voice Cloning AI model only needs a 15-second sample to work // The Verge. Artificial Intelligence. Tech. Open AI. 30.03.2024. Available at: https://www.theverge.com/2024/3/29/24115701/openai-voice-generation-ai-model (accessed: 10.01.2024)

[9] Yamaha Corporation's Voice Synthesizing Method And Voice Synthesizing Apparatus. U.S. Patent No. 10,002,604.

Yamaha, niche firms operating in audio and music markets created a variety of business applications. Other global technological giants in digital signal processing (DSP) of sound, speech and music also conducted research to obtain patents for similar successful solutions in this field.

As for legal protection, patents for vocaloids were awarded at the turn of the century simultaneously to several leading technological companies such as Yamaha Corp.[10], Texas Instruments Inc.[11], Sony Corp.[12], and a number of less important firms and private inventors of technological solutions for computer-enabled synthesis of vocal musical performances. At the moment, the first wave patents are either expired or close to expiry. With explosive growth of technologies for computer-enabled and automatic creation of singing voice and music, these solutions have ceased to be breakthrough innovations, only to become widespread, standard and affordable — that is, commodified — products by 2024. The market abounds with alternatives that offer flexible terms of commercial use.

While still filing for patents to protectable solutions in this field, companies and individual inventors proceed to monetize vocaloids as copyrighted assets in the form of computer software under licensing agreements. To encourage legal fee-based use of vocaloids, patent holders are building up their functionalities and creating extensive plugin libraries for wider creative potential. Meanwhile, the problem of illegal use of "hacked" vocaloids, just like other applications, remains unresolved. Overall, it can be stated that creators and patent holders of vocaloids and related products increasingly prefer to protect and monetize them as computer software, that is, through copyright rather than patent law.

Progress of vocaloid-like neural networks has brought to the fore the legal problem of legitimate use of someone's voice or vocal identity for training neural network generators. The most revealing situations are those where voices of popular actors or other celebrities are used to attract attention to and bolster up the rating of intelligent content synthesizers. Mass media increasingly report the claims by vocal artists and other owners of

---

[10] Yamaha Corp. Singing voice synthesis apparatus and method. Japan Patent JP3265995B2. Status: Expired.

[11] Texas Instruments Inc. Singing voice synthesis. U.S. Patent No. US6304846B1. Status: Expired.

[12] Sony Corp. Singing voice synthesizing method, singing voice synthesizing device, program, recording medium, and robot. European Patent Office EP1605436A1. Status: Expired.

recognizable voices against third parties alleging illegal vocal impersonation of creative works they produce, unauthorized use of voice or vocal articulation features.

A fresh example of such disputes is the actress Scarlett Johansson's claim against Sam Altman, OpenAI CEO, for allegedly unauthorized integration of her voice into AI-enabled software ChatGPT4.0. In his turn, Altman denied that the voice was that of Johansson claiming to have invited a different actress, whose name was not to be disclosed under the contractual terms, after Johansson had refused to grant her voice to ChatGPT4.0 [Elias, 2024]. Meanwhile, beyond celebrities and politicians, the voice cloning technology is increasingly used to fraudulently appropriate ordinary people's voice to delude interlocutors and compel them to a certain course of action.

In Russia the problem of protecting voice as intangible and unalienable personal good, has reached the level of legislative initiatives that in most cases assume the introduction of legal protection along the lines of what is afforded to human image under Article 151.1 of the Civil Code. However, it is worth noting that wider provisions of Article 150 can be used to address the problem since among intangible goods defined in part 1, Article 150, a person's voice or vocal identity can be rightly regarded as "unalienable and otherwise non-transferrable intangible good owned by the person by virtue of birth or by law". As such, it will be covered by "protection under the effective provisions of the Civil Code and other laws in cases and under procedure defined therein" pursuant to part 2 of this Article.

Efforts towards protecting voice or vocal identity as unalienable intangible good appears to be timely response of the legislator to the emerging problem. The chosen legal drafting methodology to regulate such relationships with like means looks quite logical. Obviously, claims against unauthorized use of voice will be regulated by courts. To provide and assess the evidence in legal proceedings, the parties will need to define what is voice in terms of specific parameters, features and characteristics in order to establish the fact of cloning or borrowing through examination and comparison of voice and vocal articulation samples.

1.4. Parametrization of Human Vocal Identity

Strength, pitch and timbre are associated with the main parameters of voice. Vocal strength is understood as the dynamic range and vocal sustainability that follow from natural abilities such as physical endurance, respiratory system operation and elasticity of vocal chords. While not widely used in professional vocal pedagogy, the term “vocal strength” is quite current in routine descriptions to provide more particular characteristics of “dynamic range” of voice. The latter can be variable depending on vocalization type (purpose and emotional coloring of human verbal communication or objectives and emotional nature of vocal intonation in singing). Mastering rhetoric and vocal performance techniques assumes control of dynamic range by changing vocalization loudness (high-moderate-low) and intensity.

As another important characteristic of voice, “pitch” means the main tonality of speech and ability to change it in process of speaking and singing. Pitch can vary depending on natural vocal abilities, develop in process of regular vocal exercising and alter over a lifetime as being physiologically conditioned, among other things, by hormone and age-specific changes. A distinction is made between speaking and singing pitch. Speaking pitch will normally cover one octave and, depending on intonation patterns, purpose-specific type of sentences and emotional charge, can include 3-4 notes. In contrast, singing pitch is determined, along with psychophysiological parameters, by the timbre characterized by unique frequency parameters of the singer’s individual sound for each specific note of different ranges. Quantitative characteristics of singing pitch are individual, with vocalists able to cover between 1.5 to 3 octaves to include, depending on the timbre, the notes of low, medium and high range.

Finally, “timbre” of voice means its inimitable individual frequency profile defined by the comprehensive structure of vocal tract comprising cavities and sound barriers in vocal apparatus that affect the overtones formed in inferior (trachea, bronchia) and superior (oral, nasal cavities and front zones) resonators. While vocal exercises and techniques can help to control superior resonators (oral and nasal cavities), trachea and bronchia are subordinated to higher nervous functions. Perfecting speaking and vocal techniques will make speech more expressive and convincing. Apart from the main parameters of voice, researchers also single out auxiliary emotional and functional attributes such as “airiness”, “fluidity”, “tonality”, “sonority” etc. In our view, the said parameters are quite measurable and, taken together, allow to compare effectively different voices to establish or deny their identity.

In vocal art where voice is a creative musical instrument, there is a need for clear and non-ambiguous understanding of the subject of regulation. For complex phenomenon such as singing voice, the task to identify a legally meaningful subject becomes considerably more complicated due to the following peculiarities. With singing voices divided into male and female in terms of range, these two distinctions alone will produce, according to Ivanov and Nikiforov [Ivanov A.P., Nikiforov V., 2006], six varieties further breaking down into more than twenty main types that can ramify without limit. Providing a parametric description of all singing voices for the judge to compare not abstract options of experts rushing to establish the case for either plaintiff or defendant but numeric values in search for the evidence of voice cloning is obviously a challenge.

While parametrization of singing voices for the purpose of comparison in the event of cloning claims appears challenging but feasible, the real problem is digitization of the vocal signature of those performers whose form of creative expression relies on vocal articulation techniques rather than vocal range and frequency — that is, where artistic expressivity is achieved not by conventional singing but peculiarities of pronunciation, speaking, recitation, original vowel combination or, conversely, phoneme division in the song’s lyrics. Such vocal techniques dating back to early high gain microphones[13], are now a major feature of musical art since they do not only underpin a number of popular genres such as rap and hip-hop but also fragmentarily permeate practically all musical and vocal styles.

Importantly, phonetics will identify vocalization properties as articulatory acoustic features not to be ignored in assessing someone’s vocal individuality. Accounting for these features in combination with basic parameters of sound production will allow to more precisely characterize and distinguish the vocal identity of ordinary person or artist than voice would. Without going into details of these features, it has a sense to characterize some of them to catch an idea of their essence and relevance for this study.

Acoustic features of human articulation can subsume a specific way of pronouncing noise consonants (also called obstruents) produced by obstructed airflow causing higher air pressure in the vocal tract. In phonetics and phonology, articulation is divided into two main classes of noise and sonorant consonants.

Human persons also differ in the way they pronounce sonorants — sounds produced without causing turbulence in the vocal tract. These in-

---

[13] Gioia T. How Bing Crosby Made Silicon Valley Possible. The Honest Broker. 21.12.2023. Available at: https://www.honest-broker.com/p/how-bing-crosby-made-silicon-valley (accessed: 16.04.2024)

clude approximants, nasal consonants, single stress and trill consonants. There is a great deal of nuanced articulation of approximants or spirant sonorants with their specific way of production.

Nasal consonants produced by depressed soft palate with airflow passing through the nose are also widely specific. Practically each individual has his own way of articulating single stress consonants or flaps produced by a single flip of articulatory organ.

Society exhibits widely variable articulation of trill consonants (vibrants) produced by articulatory organ's vibration in the articulation zone. For example, the Spanish language sound transcribed by the digraph *rr* means a trill alveolar consonant, with the International Phonetic Alphabet featuring a variety of trill consonants such as alveolar trill, bilabial trill, uvular trill and epiglottal trill. Vibration patterns of trill consonants vary within a very broad range and amplitude as capable of comprising two to six periods with different fading dynamics.

1.5. Methodology for Protecting Vocal Identity

It is the combination of these and other more specific features of acoustic articulation that underpins creative work in vocal, musical and audiovisual genres. Thus, "voice" may be a wrong concept to use for protecting the interests of its owner by legal means since it does not reflect the full scope of the problem and, therefore, will not provide a basis for efficient mechanism to regulate the relevant relationships. A legal provision relying on irrelevant concept will not work. For this reason, the category defined above as the artist's vocal identity appears more appropriate for vocal identification and effective resolution of voice cloning and unauthorized borrowing claims.

Vocal identity of an artist can be defined as a sum of performative vocal features including a combination of singing voice parameters and characteristic articulatory features of vocalization that make up the artist's creative technique.

It follows from this definition that singing and phonetic features could be interactive, mutually determining and intermixing to produce an original artistic technique. Another corollary is the extreme difficulty to identify and separately analyze the attributes relating to singing on the one hand and articulation on the other. Moreover, analytical approach appears counter-productive in this case. It is a combination of interdependent characteristics that makes up the unique artistic technique to be meaningfully registered in the form of the established industry standard — so-called audio signature or frequency-time spectrogram obtained by the well-known Fourier transform method and reflecting all vocal patterns [Amiot E., 2016]. For comprehensive vocal portrait of an artist, several such patterns will be needed.

In a claim against unauthorized appropriation of what can be called in the law as "voice" or, as proposed in this paper, "vocal identity", these patterns can be used to establish the identity and the fact of borrowing (impersonation or cloning of this unalienable personal good).

As regards the technology to establish or dismiss the vocal identity claim, this task could be best performed by AI neural network. Trained on original vocal signatures of artists, such neural network can take into account the whole set of interdependent pitch frequency and articulatory features of artistic performance techniques and reliably establish the degree of test sample identity.

Conclusion

Current progress of AI technologies and generative neural networks for cloning and synthesis of human voice and automatic production of creative outputs in musical, vocal and sound arts have prioritized the protection of human voice and singing voice. In this regard, vocaloid and vocaloid-like tools have become especially relevant as opening up new creative opportunities based on performance methods that did not exist before and transforming the traditional forms of musical and vocal culture.

While singing voice is normally characterized by a combination of basic parameters, vocal musical genres do not rely on singing voice alone. In particular, relatively recent styles such as rap and hip-hop as well as other recitative arts that have won a large share of the music market are influencing classical musical genres. These performance approaches are based on peculiarities of phonetic articulation, pronunciation and rhythmical beat-driven recitation rather than vocal art described in terms of basic parameters of singing voices.

Because of this discourse, it does not appear adequate to use voice as a category for drafting legal provisions. The authors propose to use instead vocal identity as allowing to embrace more parameters of human vocal individuality for more efficient protection.

The study contains a methodology for resolution of disputes on cloning someone's vocal identity (frequently defined as vocal impersonation) by using specifically trained generative neural networks that can take into account a combination of multiple interdependent parameters of human vocal identity.

Authors hope theirs proposals supported by multidisciplinary analytical findings related to the phenomenon of human voice will produce purpose for addressing the problem of legal protection of this personal good in the context of explosive progress of generative neural networks for musical and audiovisual products.

References

1. Abel J. E. (2022) The New Real: Media and Mimesis in Japan from Stereographs to Emoji. Minneapolis: University of Minnesota Press, 360 p.

2. Amiot E. (2016) Music Through Fourier Space. DOI:10.1007/978-3-319-45581-5.

3. Anisimova S.V., Golovatiy A.I. (2021) Musical Fragments, Notes and Chord Recognition Algorithms. *Vestnik Polotskogo gosudarstvennogo univeristeta. Seria S. Fundamentalnye nauki*=Polotsk State University Bulletin. Series S. Fundamental Sciences, no. 4, pp. 45–49 (in Russ.)

4. Aznauryan L.A. (2017) Study in models and algorithmic methods for analysis of musical works. Papers of Annual Research Conference PhysicMinneapolis:al, Mathematical and Natural Sciences. Yerevan: Russian-Armenian (Slavonic) University, pp. 67–76.

5. Balashova A.I. (2022) AI in copyright and patent law: range of objects and subjects, legal protection term. *Zhurnal suda po intellectualnym pravam*=Journal of Intellectual Property Rights Court, no. 2, pp. 90–98 (in Russ.)

6. Beliavskiy D.M., Darbinyan S.S. et al. (2016) Digital Identification of Objects: Beyond Technologies. Moscow: Nauchnoe obozrenie, 252 p. (in Russ.)

6. Bridy A. (2016) The evolution of authorship: works made by code. *Columbia Journal of Law and the Arts,* vol. 39, pp. 395, 397.

7. Boden M. (2004) *The creative mind. Myths and mechanisms.* London–New York: Routledge, 344 p.

8. Calo R. (2014) Robotics and the Lessons of Cyberlaw (2014) California Law Review, vol. 103, no. 3, pp. 513–563. University of Washington School of Law. Research Paper No. 2014-08.

9. Cheng H., Guo Y., Wang T. et al. (2023) Voice-face homogeneity tells deepfake. ACM Transactions on Multimedia Computing, Communications and Applications, no. 3, pp. 1–22.

10. Davis H. (2014) Creating music from literature. Papers of EACL Workshop on computer linguistics for literature, pp. 1–10. arXiv: 1403.2124. Bibcode: 2014arXiv1403.2124D. 10.3115/v1/W14-0901. S2CID 9028922. DOI: 10.3115/v1/W14-0901.S2CID9028922.

11. Davis H., Mohammad S. (2014) Generating Music from Literature. In Proceedings of the Workshop on Computational Linguistics for Literature. Gothenburg: Association for Computational Linguistics, pp. 1–10.

12. Deleuze G. (2011) *Logique du sens.* Moscow: Akademicheskiy Proekt, 472 p. (in Russ.)

13. Denikin A.A. (2013) Model of diegetic analysis of the sound in screen media. *Mediamuzyka research e-journal*=Media Music Research E-Journal, no. 2. (in Russ.)

14. Drenten J., Brooks G. (2020) Celebrity 2.0: Lil Miquela and the rise of a virtual star system. *Feminist Media Studies,* no.8, pp. 1319–1323.

15. Eck D., Schmidhuber J. (2002) Finding temporal structure in music: Blues improvisation with LSTM recurrent networks. In: Proceedings of the 2002 IEEE Workshop on Neural Networks for Signal Processing, pp. 747–756.

16. Eidsheim N. S. (2018) Widening Rings of Being: Singer as Stylist and Technician. In: The Race of Sound: Listening, Timbre, and Vocal in African-American Music. Durham: Duke University Press, pp. 177–200. Available at: https://doi.org/10.2307/j.ctv11hpntq.10 (accessed: 20.05.2024)

17. Emelianov V.V. (2023) Development of Voice. Manual for Vocal Control and Training. Saint Petersburg: Lan' Press, 168 p. (in Russ.)

18. Ivanov S.M. (2018) Neural network-generated polyphonic music. Papers of Lomonosov Conference Computational mathematics and cybernetics panel. Moscow: MGY Press, pp. 110–111 (in Russ.)

19. Ivanov A.P., Nikiforov V. (2006) Vocal Art. Moscow: Golos-Press, p. 37 (in Russ.)

20. Jones A., Bennett R., Cross S. (2015) 10 — Keeping it real? Life, death, and holograms on the live music stage. In: A. Jones, R. Bennett (eds.). The Digital Evolution of Live Music. Whitney: Chandos Publishing, pp. 123–138.

21. Khachatryan A.A. (2023) AI neural network as a tool for recognition of musical genres. Applied mathematics: current problems of mathematics, computer science and simulation: papers of the All-Russia research workshop of young scientists. Krasnodar: Russian Energy Agency Press, pp. 479–483 (in Russ.)

22. Khrisanfova L.A., Diveeva A.S. (2017) Perceiving the peculiarities of human psychology from face photos and voice recordings. Yearbook of Psychological and Psychoanalytical Studies. Moscow: Institute of Psychoanalysis, pp. 157–164 (in Russ.)

23. Kolonei V.A.(2017) Function of musical intonation components. *Muzykalnoe iskusstvo*=Music Art, no. 16, pp. 18–31 (in Russ.)

24. Levy D. (2005) Robots Unlimited: Life in a Virtual Age. Available at: https://doi.org/10.1201/b10697 (accessed: 28.06.2022)

25. Lund J. (2012) An Empirical Examination of the Lay Listener Test in Music Composition Copyright Infringement. Available at: SSRN: https://ssrn.com/abstract=2030509 or http://dx.doi.org/10.2139/ssrn.2030509 (accessed: 16.05 2022)

26. Makarevich I.V. (2022) Prospects of technologies for recognition of human emotions by facial expressions and voice. Papers of Regional Conference for young researchers. Volgograd: State Technological University Press, pp. 156–157 (in Russ.)

27. Malakhov V.E. (2022) Applying decomposition to study generative music creation processes. *Informatsionnye tekhnologii i telekommunikatsii*=Information and Communication, vol. 10, no. 4, pp. 69–78. DOI: 10.31854/2307-1303-2022-10-4-69-78 (in Russ.)

28. March L. (2023) Wrap You Up in My Blue Hair: Vocaloid, Hyperpop, and Identity in "Ashnikko Feat. Hatsune Miku — Daisy 2.0". *Television and New Media*, no. 8, pp. 894–910. Available at: https://doi.org/10.1177/15274764221093599 (accessed: 20.12.2023)

29. Markina Yu.Yu., Belov Yu.S. (2018) Spectral coefficients as a necessary parameter in creating human voice cloning systems using deep learning methods. *Mezhdunarodnyi studencheskiy nauchnyi vestnik*=International Bulletin of Student Research, no. 1. Available at: URL: https://eduherald.ru/ru/article/view?id=18125 (accessed: 26.01.2023)

30. Mazzei L.A. (2016) Voice Without a Subject. Cultural Studies. Critical Methodologies, no. 2, pp. 151–161. Available at: https://doi.org/10.1177/15327086166 36893 (accessed: 16.07.2024)

31. Nikolskiy A.V., Alexeev E.E. et al. (2019) A Jew's Harp Story: Jew's harp and individual song as a basis of tone-oriented musical systems. *Yazyki i folklor korennykh narodov Sibiri*=Languages and Folklore of Aboriginal Siberian Peoples, no. 37, pp. 5–32. DOI: 10.25205/2312-6337-2019-1-5-32 (in Russ.)

32. Perduto P. (2022) NFT — Income for Creative Minds. How to Generate Additional Income as a Photographer, Graphic Designer, Composer, Musician or other Art Creator. S.L.: Books on demand Publishers, 156 p.

33. Rais M. (2016) Musical modes: classification, characteristics, properties, history, current status. *Israel XXI. Music Magazine,* no. 3, p. 9 (in Russ.)

34. Ramalho A. (2017) Will Robots Rule the (Artistic) World? A Proposed Model for the Legal Status of Creations by Artificial Intelligence Systems. Available at: http://dx.doi.org/10.2139/ssrn.2987757 (accessed: 12.04.2023)

35. Rinkerman G. (2023) Artificial Intelligence and evolving issues under US copyright and patent law. *Interactive Entertainment Law Review,* no. 2, pp. 48–65. Available at: https://doi.org/10.4337/ielr.2023.0002 (accessed: 19.05.2024)

36. Rudin L.B. (2009) Principles of Voiceology. Moscow: Granitza, 104 p. (in Russ.).

37. Sivolap T.E. (2019) Audiovisual works: peculiarities of legal protection. Current issues of radio and cinema technologies: papers of International Conference of Technological Research to the Centenary of the Cinema and Television Institute. D.P. Barsukov et al. (eds.). Saint Petersburg: State Institute of Cinema and Television Press, pp. 237–242 (in Russ.)

38. Stulova G.P. (2014) Pedagogical factors affecting the singing voice timbre. UNESCO Chair of Musical Art and Education Bulletin, no. 4, pp. 90–104 (in Russ.)

39. Tikhomirova N.F. (2021) Conceptual principles of classification in the analysis of creative products of musical culture. *Vestnik Donetskogo natcionalnogo Universiteta*=Donetsk National University Bulletin, no. 1, pp. 123–128 (in Russ.)

40. Tormozova V.A. (2023) Current issues of audiovisual works as an object of copyright. *Trudy po intellektualnoy sobstvennosti*=Works on Intellectual Property, no. 4, pp. 54–67. DOI: 10.17323/tis.2023.18213 (in Russ.)

41. Santiago J. (2017) The "Blurred Lines" of Copyright Law: Setting a New Standard for Copyright Infringement in Music. *Brooklyn Law Review*, vol. 83, pp. 289–321.

42. Toropova A.V. (2017) Musical sensation as a basis of efficient musical therapy A study in cross-cultural interpretation of L.S. Vygotsky's psychological framework in context of variable models of musical therapy. In: Art studies in the context of other sciences in Russia and elsewhere: parallels and interactions. Papers of the international research conference. Moscow: Soglasie Press, pp. 394–405 (in Russ.)

43. Umetalieva-Bayalieva Ch.T. (2015) Musical language as an object of cultural studies. The means and elements of musical expression (musical language). *Nauka* i *novye tehnologii*=Science and New Technologies, no. 2, pp. 204–207 (in Russ.)

44. Vanyukov P.D. (2023) The legal regime for AI and its outcomes. *Intellektualnaya sobstvennost*=Intellectual Property, no. 3, pp. 58–68 (in Russ.)

45. Vasilevskaya L.Yu. et al. (2021) Digitizing Civil Law Transactions: Legal Characteristics of "Artificial Intelligence" and "Digital" Subjects (a civil study in 5 vols.). Vol. 1. Moscow: Prospekt, 288 p. (in Russ.)

46. Watt D., Harrison P., Cabot-King L. (2020) Who owns your voice? Linguistic and legal perspectives of relationship between vocal distinctiveness and the rights of the individual speaker. *International Journal of Speech, Language and the Law,* no. 1, pp. 137–180.

47.Yuan J.E. (2024) Making virtual celebrity: Platformization and intermediation in digital cultural production. DOI*:*10.1177/13678779241230564.

48. Zakharov A.O. (2020) Neural networks in music. Week of Science and Creativity. Papers of international research workshop for students, postgraduate students and young scientists. Saint Petersburg: State Institute of Cinema and Television Publishers Press, pp. 36–39 (in Russ.)

Information about authors:

R.A. Budnik — Doctor of Sciences (Law), Professor.

E.G. Evpak — Researcher.

The article was submitted to editorial office 18.03.2024; approved after reviewing 14.05.2024; accepted for publication 24.06.2024.

Legal Issues in the Digital Age. 2024. Vol. 5. No. 4.
Вопросы права в цифровую эпоху. 2024. Т. 5. № 4.

Research article
JEL: K00
УДК:34
DOI:10.17323/2713-2749.2024.4.46.72

Keystroke Dynamics: Prospects for Comprehensive Law Regulation

Anna Denisovna Tsvetkova

Ural State Law University, 21 Komsomolskaya Street, Ekaterinburg 620066, Russia,

at@crimlib.info, https://orcid .org/0000-0002-1631-9265

Abstract

The rapid digitalization of all spheres of society leads to the appearance of large volumes of typed texts, as well as the formation of the task of determining the performers of such texts. In this regard, it is necessary to develop applied research on keystroke dynamics, including through the prism of jurisprudence. Author of the article identifies sector of public relations related to ensuring the rights of citizens to personal and family secrets, the secrecy of correspondence; protection and processing of biometric personal data; state registration of persons based on their keystroke dynamics; disclosure and investigation of crimes in which typed texts are the subject of encroachment or the means of committing an illegal act; procedural proof of the involvement or non-involvement of a particular person with the creation of a typed text; as well as with the control of labor discipline and ensuring safety of production processes. In all these areas the beneficial fruits of processing keystroke dynamics is potentially high, that, however, is accompanied by significant risks of protecting information that is harmful to human persons. In this regard, author proposes models of regulatory regulation of all these areas in order to maintain a balance of public and private interests. The author's goal was to justify that the prompt resolution of the problematic issues raised would improve the effectiveness of law enforcement, protect the rights of citizens, and ensure the national security of the state. For this purpose, methods of logical definition of concepts, modeling, questioning, analysis and analogy, as well as systemic legal method were used. Conclusions were formulated about the prospects of both voluntary and mandatory

© Tsvetkova A.D., 2024
This work is licensed under a Creative Commons Attribution-Sharealike 4.0 International License
https://creativecommons.org/licenses/by-sa/4.0/legalcode.en

state registration of users of computer devices and the Internet on the basis of their keystroke dynamics at the expense of the resources of the Center for Biometric Technologies. With the help of information from this database, as well as through investigative actions and operational search measures, it is possible to introduce keystroke dynamics into the field of forensic identification of the typist. To do this, it will be necessary to conduct a computer-technical examination, the results of that may be used as the basis for procedural evidence. Automated processing of information about keystroke dynamic can be used to monitor compliance with the work and rest regime by employees, independently fulfill their employer's orders, and prevent accidents at the workplace. Based on the totality of all the considered aspects, it is concluded there is a need for a deep understanding of keystroke dynamics in various fields of jurisprudence. It permits to form a regulatory system for the integrated regulation of public relations related to the processing of this phenomenon.

Keywords

keystroke dynamics; digitalization of law; digital forensics; personal rights; biometric personal data; behavioral biometrics; state registration; computer forensics.

Acknowledgments: The study was funded by grant of the Russian Science Foundation No. 23–78–10011, https: // rcf.ru/project/23-78-10011

The paper is published within the project of supporting the publications of the authors of Russian educational and research organizations in the Higher School of Economics academic publications.

For citation: Tsvetkova A.D. (2024) Keystroke Dynamics: Prospects for Comprehensive Law Regulation. Legal Issues in the Digital Age, vol. 5, no. 4, pp. 46–72. DOI:10.17323/2713-2749.2024.4.46.72

Introduction

Our lives go hand in hand with digital technologies. We use them for quick interpersonal communication, for entertainment, to resolve working questions, to contact government bodies, for education etc.—the list seems to be endless. As a result of this trend, the very concept of society and social interactions has been undergoing changes, and this definitely has its influence on laws and regulations. Progress in science and technology has been transforming individual spheres of law to one degree or another, in particular as new phenomena appear in our life that don't fit into the usual regulatory framework, but by their nature should be subject to legal regulation.

One example of such phenomena is operations in the digital environment related to the creation and dissemination of text materials. This includes, first of all, written (or, to be more precise, typed) Internet communications and work in computer programmes and interfaces where texts are keyed in (word processors, forms for filling in and submitting electronic reports, administration of websites and filling them with content, etc.). In any of the aforementioned cases, the computer device records the unique set of the user's skills and habits, the person's keyboard dynamics. This phenomenon reflects how the person works on the keyboard rather than what information this person types in [Zeid S., ElKamar R., Hassan S., 2022: 95]. Researchers in the information technology and information science spheres have been studying this phenomenon since the 1970s [Spillane R., 1975]; [Forsen G., Nelson M., Staron R. Jr., 1977: 116–122]. They have proven that keyboard dynamics are important for identification purposes and belong to the category of behavioural biometrics; analysed the nature of the phenomenon in sufficient detail; developed numerous ways to record and automatically process them, and designed special technical media for this. At the same time, jurisprudence has not paid enough attention to the questions of keyboard dynamics, their use and protection. This, author of article presented believes, is a major oversight, in particular in the times when electronic texts are becoming increasingly common.

Therefore, the research focuses relations in the sphere of keyboard dynamics processing[1] through a legal lens. Author considers various approaches to legal regulation of issues pertaining to this phenomenon in the sphere of material public relations, private-public relations, and procedural relations, and in this manner will outline the directions for further in-depth studies on this topic.

The aim follows from the hypothesis that electronic texts will only grow in amounts in the future and will gradually displace manuscripts. As a result, the need to identify clearly the author of a particular typed text will arise in various areas of life on a regular basis. Hence, even today it is sometimes necessary to assess the potential positive effects, risks, and limits of keyboard dynamics from a legal perspective.

To this end, it is used an extensive methodological base including exploration of fundamental studies on the theory of identification, physiol-

---

[1] Processing is understood in this paper as set out in Federal Law On Personal Data No. 152-FZ of 27.07.2006 (Collected Laws of the Russian Federation. 2006. No. 31. P. 3451): as any action (operation) with personal data, including collection, recording, systematisation, accumulation, storage, clarification (updating, modification), retrieval, use, transfer (distribution, provision, access), depersonalisation, blocking, deletion, and destruction.

ogy of higher nervous activity, biometrics, information security, protection of human rights and use of personal data; current laws regulating relations in the sphere of processing personal, in particular biometric, data; labour relations; issues of state registration activity management; it was also collected own empirical material by polling law enforcement officers on their awareness of keyboard dynamics phenomenon and their views on how it can be studied for solving the tasks facing justice. In the research it was used the system legal method as the main special method that allowed to consider the single phenomenon of keyboard dynamics from different positions. Also, author have relied to a large extent on the methods of mathematical statistics, cybernetics, programming, and system analysis, without which it is impossible to comprehend a phenomenon that for many years has been the subject of research exclusively in the computer science domain. Forecasting and modelling methods enabled to describe the situations in which it would be necessary to subject to legal regulation the relations in the sphere of the keyboard dynamics processing and to propose optimum ways for such regulation. In addition it was used the general research methods of analysis, synthesis, induction and analogy, as well as the universal dialectical method, that allowed to organize the research on basic scholar principles.

1. Keyboard Dynamics: Definition

It was mentioned above keyboard dynamics were initially studied in the sphere of computer science, so it would be reasonable to borrow its definition from the works of researchers of this discipline. At the same time, despite the long history of research on the subject, there is still no single definition; foreign researchers, omitting the direct definition of keyboard dynamics, go straight to the description of its essence and possibilities of its applied use.

Author will not dwell in detail on the whole variety of the definitions. Instead, it was cited the most representative examples reflecting the approaches to the definition of this phenomenon. These may be divided into three groups:

definitions by means of listing the features that are specific to keyboard dynamics;

definitions in which representation is made through genus and species distinctions,

definitions by means of pointing to a synonymous category .

It is possible to assign to Group 1 the detailed description offered by A.I. Averin and D.P. Sidorov: “In the process of keying information in, a person develops his or her own personal style of typing certain words. This style is actually unrepeatable and depends on such parameters as the number of fingers involved in typing; the duration of key presses; the time between key presses; the use of the main or additional part of the keyboard; the nature of double or triple presses; the favourite combinations of hot keys, etc. Thus, keyboard dynamics is a set of dynamic characteristics of work on the keyboard” [Averin A.I., Sidorov D.P., 2015: 2].

S.A. Varlamova’s and E.A. Vavilina’s definition is an example of Group 2 definitions: “Keyboard dynamics is the dynamic human of a person that depends on the speed of character input, the time interval between releasing and pressing a key, as well as the interval between key presses (i.e., the time it takes to press neighbouring keys), the number of typos, and the use of hotkey combinations” [Varlamova S.A., Vavilina E.A., 2023: 68].

E.E. Turutina offers a notable example of a definition that belongs to Group 3: “Keyboard dynamics is an individual biometric characteristic of each individual user’s behaviour” [Turutina E.E., 2021: 171].

Obviously, only individual examples are cited above, but analysis of other authors’ works shows their definitions differ only slightly from the cited ones. At the same time all definitions of keyboard dynamics formed in science today, including those not mentioned, have one or more of the following drawbacks.

Susceptibility to obsolescence. This is characteristic of keyboard dynamics feature listing models because owing to the progress of science, new properties significant for identification are revealed or the irrelevance of the previously highlighted features is proven on a regular basis.

Incompleteness. Many definitions specifying characteristics of keyboard dynamics or give its generic differences, do not provide an exhaustive list of these characteristics.

Uncertainty. In an attempt to avoid the above-mentioned shortcomings, some authors add ‘etc.’ at the end of the definition; it raises quite a number of questions related to the content of this expansive provision.

Identification of the general and the particular. Some definitions equate keyboard dynamics, a complex systemic phenomenon, with its individual dynamic characteristics. However, a system cannot be reduced to a simple sum of its components.

Vagueness. When researchers list individual features of keyboard dynamics, they don't answer the question as to what it is. When trying to refer to a generic category, the specialists miss distinctive characteristics that would allow to distinguish keyboard dynamics from related phenomena.

These are only the main common disadvantages. If to go into a detailed analysis of each definition, this list could be continued. However, the examples demonstrated are sufficient to conclude the current definitions cannot be recognized as optimal ones.

For the purposes of jurisprudence, proceeding from the above positions and taking into account the shortcomings highlighted therein, author of the paper presents proposes the following definition below:

Keyboard dynamics: in the subjective sense, it is a biometric characteristic of a person, which combines a set of skills and habits of the user's interaction with a keyboard equipped with tactile symbolic keys while creating a text; in the objective sense (also, "keyboard dynamics information"), it is the external expression of the user's skills and habits of interaction with a keyboard equipped with tactile symbol keys when creating a text, which is manifested in relevant records both directly on the user's device and (if available) in specialised software or hardware-software systems.

2. Keyboard Dynamics from the Human Rights Perspective

Researches show keyboard dynamics describes through a set of diverse characteristics [Alsultan A., Warwick K., 2013: 2–4], how a person types. Although the content of the text typed does not matter for its identification significance, present-day technical means of fixing keyboard dynamics—keyloggers—function in such a way that they record all keyboard events, i.e. information about which key was pressed (released), and when [Matsubara Y., Samura T., Nishimura H., 2015: 230]; [Villani M., Tappert C. et al., 2006: 33]. Thus, even if the system records not the character transmitted to the monitor, but the ASCII code of the key, it will be quite possible to restore the original text, if necessary, and thus to get information on what's been typed. As a consequence, ever since keyloggers appeared, one of their uses has been to covertly (often, maliciously) monitor the information typed on a particular computer device. This has branded them as malicious software [Samsoni D.Z., Basir B.P., Hafidsyah P. et al., 2023: 869–870]; [Md A., Mohiuddin S., Jafrul H. et al., 2019: 18]; [Guryanov K.V., 2020:

81–82]. To protect the information valuable for the user, researchers suggest configuring the key logger in such a way that the final data recipient receives only generalised information characterising the person's profile, thus excluding the possibility of recovering the data typed [Paschenko D.V., Balzannikova E.A., 2020: 78]. Fully justified from a privacy perspective, this proposal mitigates the benefits of a key logger that can be used for law enforcement purposes when it is necessary to match typing and text features. It will be discussed in detail below. In this regard, it is very important to identify ways to balance between the interests of the individual and the state.

Individuals seek to keep secret any information about themselves and their lives, its attitude is supported by the relevant constitutional (Art. 23 of the Constitution of the Russian Federation), conventional (Art. 8 of the UN Convention of 4.11.1980) and other treaty norms at the national and international levels [Isaeva V.V., Sakharova Y.V., 2020: 139], reflecting the human rights to personal and family privacy, and confidentiality of correspondence. Moreover, with the widespread use of network services (in particular, the Internet), any secret may become known to an unlimited number of third parties at once, which makes the above rights even more important.

On the other hand, the unlimited nature of the above rights to personal privacy, correspondence and negotiation secrecy poses a significant threat to national security, as it allows perpetrators to conceal unlawful activities until the moment when it becomes impossible to prevent their consequences. In view of this, the legal provision establishing the rights in question also allows for their restriction by court order.

Taking it into account, it is admissible to believe in researching keyboard dynamics one ought to preserve the possibility of correlating its features with what was typed, if such a study is carried out under a court order, as part of an investigation, law enforcement intelligence operations, and in other similar cases. In all other cases, processing keyboard dynamics without consent from the person in question is inadmissible.

At the same time, however, today various commercial companies use keyboard monitoring without the direct purpose of collecting personal information, but, e.g., to develop customer-oriented products[2]. Such a pos-

---

[2] McAllister N. Windows 10's 'built-in keylogger'? Ha, says Microsoft — no, it just monitors your typing. The Register. 7.10. 2014. Available at: https://www.theregister.com/2014/10/07/windows_10_data_collection/ (accessed: 19.07.2024)

sibility is enshrined in the companies' policies, and the user is asked to give his or her consent. The practice is that only a small number of users study such documents. And, moreover, almost nobody does it to find the provisions concerning the processing of keyboard dynamics, due to unawareness of the existence of this phenomenon. Thus, the undefined (and, in fact, absent) legal status of keyboard dynamics leads to the formation of a grey area, when the insufficiently high level of the population's computer literacy and the absence of strict rules for keyboard dynamics processing lead to the actual violation of human rights. In The following chapters will look at possible solutions to the problem from different perspectives.

3. Keyboard Dynamics in the Biometric Personal Data System

All studies of keyboard dynamics point out it is a behavioural biometric characteristic [Vacca J.R., 2007: 27]; [Uimin A.G., Morozov I.M., 2022: 48].

To substantiate this statement, it has a sense to turn to the doctrinal interpretation of the biometric data category (however, it is necessary to note it offers a definition, which is somewhat broader than the one given in Art. 11 of the Federal Law On Personal Data mentioned above[3]. E.g., it states personal biometric data must meet two criteria: "First, <they> characterise the physiological and biological features of a person, on the basis of which it is possible to establish his / her identity and, second, they are used by the personal data operator to establish the identity of the person" [Salikov M.S., Nesmeyanova S.E., Kolobaeva N.E et al., 2022: 116]. It is important according to this definition that biometric personal data will only include information that is actually used for identification and not theoretically suitable for it. It may be the reason why keyboard dynamics is still outside of legal regulation: it is not in widespread use. However, it is used for identification and authentication of computer device users at the private level and in various commercial entities [Mashtanov P.N., Martynyuk M.V., 2021: 527–531]; [Banerjee S.P., Woodard D.L., 2012: 129–131]. The prospects for its wider application have already been covered many times in doctrine [Alsultan A., Warwick K., 2013: 7–9]; [Shadman R., Wahab A., Manno M. et al., 2023].

International sources formulate slightly different requirements. E.g., biometric personal data should be: universal; unique; stable; irreplaceable;

---

[3] Available at: URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (accessed: 21.07.2024)

suitable for recording and storage; sufficient for identification; accurate; easy to process; economically feasible; convenient to process; socially acceptable [Clarke R., 1994: 21].

As it is possible to see from the description above, not all requirements are related to biometrics per se. E.g., voice recordings and facial images, that many parties, including federal laws[4], indisputably recognise today as personal biometric data, would retain their uniqueness in describing the relevant behavioural and physiological properties of a person, even if there were no relatively cheap ways of their easy acquisition and fast automated processing. That is, most of the items in the above list of biometric data requirements relate to data processing technologies and public policies that determine social acceptability.

So, it is possible conclude both the Russian and international approaches point to the need for scholar research, legal regulation and practical use only of the unique features of a person that can be separated from the person for subsequent manipulations; the features that belong to the person but can't be exported to an external tangible medium are of no interest to science, law, and practice. While author is not challenging the approach, she believes it is worth mentioning keyboard dynamics meets most of the above requirements, and it is only a matter of time and efforts on the part of researchers to create relatively affordable and widespread devices to record and process it. Hence, it ought to be studied from the legal perspective already today.

Therefore it is necessary to introduce normative regulation for relations in the sphere of processing keyboard dynamics data, in particular their storage and access to them as this is information subject to special protection. This is particularly relevant due to the fact that commercial entities "are also interested in collecting and processing personal data in order to create new business models, personalise the goods and services provided, make the most effective use of innovative technologies in competition, and protect their own interests in dispute resolution" [Zuyev S.V., 2019: 78]. E.g., information about keyboard dynamics is used to develop easier-to-use, ergonomic keyboards (which creates a competitive advantage in the market of

---

[4] Federal Law On the identification and (or) authentication of individuals using biometric personal data, on amendments to legislative acts of the Russian Federation and invalidation of certain provisions of legislative acts of the Russian Federation No. 572-FZ of 29.12. 2022 (Part 4 Art. 3) // Collected Laws of the Russian Federation. 2023. No.1. Part I. `P. 19.

computer hardware components), to ensure information security in banks, etc. As long as the status of keyboard dynamics is not formally defined, as was stressed above, its use is not restricted in any way. This may violate fundamental human rights.

One of the possible measures to resolve the legal vagueness in question is to enshrine in the legislation the list of personal biometric data, which is quite clearly given in doctrine [Vacca J.R., 2007: 27]; [Zhukov M.N., 2021: 164–165]. It should be done not necessarily at the legislative level: technologies keep developing, so one can't rule out that a new way is invented to process a particular new characteristic that hasn't been described yet. It is possible and sufficient to regulate it at the level of subordinate legislation. Currently, Ruling of the Russian Federation Government of 1.04. 2024 No. 408 On the types of biometric personal data are covered by Law On the identification and (or) authentication of individuals using biometric personal data, on amendments to legislative acts of the Russian Federation and invalidation of its provisions is in force in Russia.[5] It stipulates the Federal Law in question applies to human facial images and voice recordings. Hence, it is possible to establish a general list of biometric personal data by bringing them under a specific legislative regulation in the Russian Federation Government Ruling, too.

The question under review can be resolved in a different way as well. E.g., we believe in the initial phase, it would be sufficient for the Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications to issue Clarifications that would attribute keyboard dynamics to the personal biometric data category as it was the case previously with photographic and video images, and fingerprint information[6].

If the proposed measures are taken, everything related to the processing of keyboard dynamics will fall under the relevant provisions of Federal Law No. 152 regulating both general questions of personal data protection

---

[5] Collected Laws of the Russian Federation. 2024. No. 15. P. 2042.

[6] Clarification of the Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications "On issues of attributing photo and video images, fingerprint data and other information to biometric personal data and peculiarities of their processing" // Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications. 02.09.2013. Available at: URL: https://25.rkn.gov.ru/news/news54167.htm (accessed: 17.07.2024)

and particular aspects of operations with biometric identifiers, which are stricter.

At the same time, as legal studies on keyboard dynamics develop and deepen, there may arise the need to approve the Federal Law On state registration based on keyboard dynamics features. The study of this issue in detail is in the next section of paper. Suffice it to say here that the significance of this registration is explained by the fact that at present any person can create lots of typed texts (posts in social media, comments on various web resources, formal requests to government institutions, texts relation to the persons' education or work, etc.). These texts constitute the persons' digital profile (i.e., a unique set of characteristics, from the avatar selected to particular features of verbal communication typical of a particular person in the virtual domain [Ivanov V.V., Zuyev D.I., 2022]). This profile can be used to ascertain the identity is important for investigating crimes, identifying various offenders and solving other tasks, which will be discussed in more detail below. And it is specialized records that will be the best source of obtaining information about the properties of the "digital twin" to identify the real person behind it.

Considering issues that pertain to formalizing status of keyboard dynamics touch upon another issue: where it should belong. E.g., Russian literature on biometric data has traditionally broken them up into two categories: the static (anatomic) biometrics, and the dynamic (behavioural) biometrics [Shangina I.Y., 2020: 152]. In international literature, the dichotomy "physiological vs behavioural characteristics" prevails [Guo J., Mu H. et al., 2024: 209]. At times, one can come upon slightly different approaches [Syed Idrus S.Z., 2014: 2], but the behavioural biometrics group keeps its name and content, including the keyboard dynamics. The Russian legislator, in defining personal biometric data, divides them into two groups: physiological and biological characteristics, which obviously does not correlate with provisions of science.

Also, no explanation is given anywhere of what "physiological" or "biological" characteristics are. The Dictionary of the Russian Language proposes the following definition:

"Biological: relating to physical or physiological aspects of the existence of living organisms[7]."

---

[7] Kuznetsov S.A. The Great Explanatory Dictionary of the Russian Language. Saint Petersburg, 2000. P. 78.

"Physiological: relating to the physiology of the body, or its vital activity; based thereupon[8]."

While not giving here all the meanings of the words, but the remaining ones can't be related to biometric characteristics.

So, biological and physiological are almost synonymous. Moreover, if to turn to the experience of foreign researchers, it is easy to establish under physiological biometric data they understand static features (fingerprints, facial image, etc.), and the term "biological" can't characterise the features that are manifested in the process of activities (behaviour). The legislator has essentially split one type of biometrics into two synonymous words, ignoring the layer of dynamic identifiers — it is probably a technical error. The state processes behavioural biometrics as it records voices in the Unified Biometric System. Therefore, it is necessary to amend Part 1, Art. 11 of FZ No. 152 to read as follows: "1. Information that characterises a person's physiological and behavioural features, which enable to establish his/her identity (personal biometric data) and which the operator uses to establish the identity of the holder of personal data, may be processed only with the written consent of the holder of personal data, except in cases provided for in Para 2 of this Article."

Until such changes are made, the definition of keyboard dynamics should be given without species attribution, simply by means of the category "biometric characteristic of an individual."

Going back to the applied aspects, it has to note the state is interested in the processing of keyboard dynamics data, and therefore it is necessary to consider their storage. To this end, a special government database must be established. Perhaps, the optimum solution would be to allocate space in the Unified Biometric System as this will enable accumulating data collected not only by government agencies but also by commercial entities. It is particularly relevant because as of April 2024, after Government Ruling No. 408 was passed, it is now legally possible to expand the list of biometric personal data processed by the System. Relying on the System's resource capacities helps to guarantee the security of information, to use latest licensed domestic technical means for its processing, and to provide access to the keyboard dynamics of representatives both of public and private sector entities (if such a possibility is provided).

---

[8] Ibid. P. 1422.

The legal experts need to extensively explore peculiarities of keyboard dynamics processing from the point of view of its representation as a biometric characteristic to ensure that such processing is possible in applied activities.

4. State Registration on the Basis of Keyboard Dynamics Features

Very probably such registration through the resources of the Biometric Technology Centre (UBS operator[9]) or on the basis of an individual stand-alone database will significantly increase the force of the fight against crime, and control over content distributed on the Internet; i.e., it will ensure the national security of the state. At the same time, it will make it possible to withdraw from various organisations the bits and pieces of "sensitive" information that they store thus increasing its security in the interests of IT system users.

It is a place to present view on the individual main aspects of how state registration is to be implemented on the basis of keyboard dynamics. After appropriate additions and extensions, they may in the future form the basis of a corresponding Federal Law.

The state registration in question can be both voluntary and mandatory. The latter would be related to a conscious decision by an individual based on his/her wish to prevent potential falsification of his/her role in the creation of any typed texts, and by other personal motives. Surely, for law enforcement purposes the option of having a significant part of the population voluntarily register for keyboard dynamics is preferable. However, the practice established in the field of fingerprinting and genomic registration [Solomatina E.A., Cherkashina A.V., Dreval B.V., 2021: 237] indicates probability of that scenario is low. At the same time, there are situations where it is appropriate to resort to mandatory registration based on keyboard dynamics features. It must cover the following persons:

suspected or accused of committing an offence where a typed text is the means of committing it or the object of the offence;

---

[9] RF Government Ruling No. 834 of 21.06. 2024 On Determination of the Organization Functioning as Operator of the Unified Biometric System. Available at: URL: https://www.consultant.ru/document/cons_doc_LAW_479247/ (accessed: 21.07.2024)

who have committed an administrative offence where a typed text is the means or subject of the unlawful infringement;

authorized to work with legally protected information stored and processed in electronic form;

involved in fulfilling functions of the state through e-government structures (persons processing and/or registering incoming applications, interacting with applicants, preparing official responses, etc.);

wishing to use a digital platform involved in an administrative offence or through which a crime has been committed, where typed texts have been the means or object of infringement.

The list may be expanded and refined through further research. However, at present it is final. Above it was comments on its individual items, now it is a time to clarify registration based on keyboard dynamics, that is a behavioural characteristic, can be carried out in two ways: continuously or intermittently

In the former case, it was shown there is a risk of infringement on the rights to personal and family privacy, confidentiality of correspondence, and other unique information, and it was stated it was necessary to indirectly attribute, based on the dynamics, to the device used to create the text. Here, it is implied that the keyboard dynamics is recorded continuously, at pre-set intervals (e.g., once a day), and the data are then submitted to the government database. This approach is considered favourable; it helps to record a person's involvement or non-involvement in the creation of a text and guarantees the user profile is updated regularly and the variability of typing parameters is recorded. On the other hand, it is highly vulnerable from the technical viewpoint as it requires huge amounts of memory to store all the data, and computing capacity to process and select the required data, and does not guarantee the correct answer to questions of a person's involvement in the creation of a text generated on a different, unregistered computer device.

The former case implies a person's keyboard dynamics is collected for recording only once, and then updated from time to time (e.g., when the person is detained again in accordance with a legal procedure). The samples thus received are then attributed to a concrete person because they are collected in specially created conditions when the text is typed in under supervision, so the samples are definitely clean of any personal information. These data are then used to form the person's profile, and it is automatically compared in other electronic systems. In other word, this model functions on the basis of automated authentication where information about the keys pressed is presented in human-readable form exclusively at the moment of state registration. In this scenario, the above-described technical problems are resolved, but the possibility of obtaining free samples of keyboard dynamics for a comparative study reduces almost to zero.

These forms of registration should be combined in a reasonable manner.

Public sector workers (persons belonging to Categories 3 and 4) can be registered in two steps: first, when they are hired, they type texts of a certain size; these samples then form the basic employee profile. After that, their activities on computer devices are constantly monitored, and the system automatically checks the features of the keyboard dynamics for their correspondence to those recorded in the beginning and included in the employee profile. The initial samples are stored in the state database, but the periodic data is not uploaded there. If, at a certain point in time, the system sees that the keyboard dynamics on a certain computer device issued to a particular employee don't match the stored profile, then the department manager receives a notification-request to react to this incident properly. In our opinion, to keep the precision of automated identification at a high level in this scenario, it would make sense to update employee profiles stored in the state database regularly.

As for persons undergoing criminal or administrative proceedings (Categories 1 and 2), it is preferable when both registration methods should be implemented at the same time: one, when the person is accused of a crime, is assigned the status of a suspect, or of a person held administratively liable; and two, the person's keyboard dynamics must be constantly related to the main computer device this person uses. Then, even if the person changes the device, it will still be possible to establish his/her involvement in the generation of a delinquent text because individual characteristics of the typing are stored locally in keyboard event logs (system logs) [Smushkin A.B., 2019: 32]; [González N., Calot E., 2023].

Last but not least, in the latter situation, special attention must be paid to mandatory state registration on the basis of keyboard dynamics where a person wishes to use a digital platform in any way related to the perpetration of an unlawful act.

In this case, a keylogger built into the interface should be used to record and transmit the keyboard dynamics data of the platform's users to the state database. The data should have a reference to the MAC-address of the computer device used to access the platform, and the user must be notified in advance that about such data collection. If a person does not wish to transmit his/her keyboard dynamics data, he/she should be able to opt out of using the platform. As a result, the keyboard behaviour of all deliberate users during their active session on such a platform will be transferred to the state database.

Of course, the above scenarios of state registration based on keyboard dynamics are only a rough approximation of the situation that may take place in real life. Therefore issues raised here require additional research.

5. Using Keyboard Dynamics to Identify Perpetrators

Identification of computation device users on the Internet by means of keyboard dynamics analysis is a highly relevant task facing law enforcement scientists, criminal intelligence officers and forensic experts seeking to solve crimes and identify perpetrators.

Forensic processing of keyboard dynamics is highly significant due to the ever-increasing number of computer-related offences. According to A.M. Karimov, they all have one distinctive feature in common: “It is not the subject of criminal offence but it is the mechanism and the tool used to inflict harm to various social relations, whose generic characteristics differ, or it is the medium in which an unlawful act is committed” [Karimov A.M., 2023: 79]. In other words, if you apply an expansive interpretation of this category is more accurate, computer crime includes acts that were committed with direct involvement of information and communication technologies. And, as E.R. Rossinskaya notes, almost any “conventional” crime can be committed this way at present [Rossinskaya E.R., 2019: 33]. This makes the list of “computer-related” subjects of the offence almost endless, where only the scope of criminal law is the limit.

At the same time, in practically any offence of this type, typed texts may occur which are significant from the law enforcement perspective and which can be the subject of criminal trespassing (investigation reports; official documents in cases related to falsification or forgery thereof, etc.); which are used to commit an offence (exhortations to commit suicide; defamatory materials, extremist materials etc.); which are part of preparations for illegal activities (correspondence in social networks conducted as the perpetrator looks for accomplices, raises funds etc.); they are generated in the course of committing an offence but are not related to the objective element of the offence (correspondence between accomplices conducted to coordinate their actions etc.); which contain additional information about the circumstances significant for uncovering the crime and solving the case (a post on the personal page in a social network where the perpetrator expresses the intent to commit the offence etc.).

According to the survey author of the paper have conducted, 68.6% investigators (73 respondents) are confronted with the need to analyze typed texts with varying degrees of regularity, and 76.7% (56 respondents) have had to resolve the task of identifying the person that typed a certain text. And since there is no methodology to solve this task, the officers have to resort to additional interrogations (53.3%), authorship examination (28.3%), or presume that the owner of the computation device is the person who typed the text (33.3%). However, none of these methods is flawless because it either fails to ensure objectivity, or is designed to resolve tasks that are close but not identical to the task in question. E.g., testimony at the interrogation may be false; authorship examination decides the question of the who is the author of the text, which does not always coincide with the person who typed it; and the presumption is destroyed in cases of multi-user equipment or malicious (including remote) access to another person's device.

Keyboard dynamics analysis can become the required special method, by analogy with analysing handwriting in handwriting analysis. We deem it possible to obtain samples of keyboard dynamics for comparative studies by means of the respective crime investigation procedures (Art. 202 of the Russian Federation Criminal Procedure Code) or by means of law enforcement intelligence operations; to use in crime investigation activities free samples stored in the above-mentioned state database (after it has been created), and then to conduct a computer-based expert assessment of information on keyboard dynamics according to the methodology of comparative identification studies.

However, keyboard dynamics should not necessarily constitute evidence; it will explore in details in the following sections. Many researchers agree the phenomenon under review (either per se, or as a biometric characteristic) is an inseparable part of a person's digital profile [Foygel E.I., 2023: 105]; [Zaytsev O.A., Pastukhov P.S., 2022: 295]. Hence, if it is analysed by various means, including forensic diagnostics, in combination with other data about the perpetrator operating in the digital environment, it can give directions for investigation and help to narrow search for the potential offender.

6. Keyboard Dynamics as Evidence

In description of the significance of keyboard dynamics for crime investigation it was pointed out it offered a tool to identify the person that typed a certain text that had been used in criminal activities in any fashion— similar to the way in that the question of the perpetrator of a handwritten text has been resolved over the long history of forensic science. Still, texts are typed not only in connection with criminal activities, and the identity of the person that has typed a text can become the issue in any court proceeding: criminal, civil, arbitration, or administrative. Constitutional proceedings are the only exception here due to their special nature.

In all the proceeding the model for using data on the keyboard dynamics is standard, so it will not describe each of them in a separate section.

Keyboard dynamics can be used in a court proceeding to prove a person's involvement or non-involvement in the creation of a particular typed text. The only way to attach evidential significance to the data about such dynamics is to conduct special computer-based examination, which would answer the following questions:

Have the texts submitted for examination been typed by one person?

Has the disputed text been typed by the person whose keyboard dynamics samples are submitted for examination?

Has a certain text been typed on the personal computer (keyboard) submitted for examination?

Has one or several persons worked on the personal computer (keyboard) submitted for examination during a certain period of time?

What is the approximate age of the person who typed the text?

What psycho-emotional and physiological state was the person in at the time of typing the text?

Has the text been typed in an environment unfamiliar for the person? etc.

In addition, the examination must necessarily address questions about the presence or absence of key loggers[10] on the computer device submitted for examination, which may also be significant for establishing the circumstances of the case in court.

---

[10] Standard expert techniques for physical evidence examination. Part I. Y.M. Dildin (ed.). Moscow, 2010. P. 199.

In considering theme of evidential significance of an expert assessment, it is of need to turn attention to of automatic data processing. Current researches focuses on creating tools to identify users by their keyboard dynamics on the basis machine learning [Zeid S., ElKamar R., Hassan S., 2022: 95–104]; [Matsubara Y., Samura T., Nishimura H., 2015: 230]. Thus, it is proposed use AI to solve most of the applied tasks when working with the phenomenon under review. It is quite justified, because in 30 minutes of work, in the course of typing an unfamiliar text about 800 characters long, more than 10,000 keyboard events can be generated. At the same time, today all AI intelligence systems operate according to the "black box" principle [Suman R.R., Mall R. et al., 2010]; [Smushkin A.B., 2024: 136–137]. Therefore, the user will not know for sure how the information at the input has been processed to produce the concrete result. But expert opinions presented in court must be verifiable, and all participants in a trial should be able to assess this opinion, and understand how a particular conclusion has been made. Otherwise, such an opinion will not be recognized as admissible evidence [Branovitsky K.L., Renz I.G., 2019: 43–54]. This imposes limitations on the possible use of AI systems in forensic computer-based examination of keyboard dynamics, although it does not rule out the possibility of using auxiliary technical means that simplify computations of large amounts of data.

Further use of an expert opinion falls completely under the general rules stipulated in the procedural rules of each relevant law, so it does not need a separate description. However, some scientists deem otherwise.

E.g., I.Z. Fyodorov considers it necessary to amend Article 5 of the Criminal Procedure Code containing terms and definitions, and to enshrine in it the definition of keyboard dynamics with all its individual characteristics. He also suggests introducing a number of other amendments to certain articles, specifically stipulating the obligation to appoint a forensic expert examination to examine keyboard dynamics, recognise electronic carriers of keyboard dynamics data as material evidence, etc. [Fyodorov I.Z., 2019: 113–114]. However, that such clarifications are unnecessary because keyboard dynamics and methods of dealing with it as part of legal proceedings (including criminal proceedings) may well be included into general procedural provisions. On the other hand, a detailed elaboration of this kind would invariably lead to the transformation of a law into an instruction, which is contrary to the meaning of acts of such level.

7. Keyboard Dynamics in Labour Relations

Relations between the employer and the employee are one more area where is useful to analyse the use keyboard dynamics from the legal perspective. Automatic recording and continuous monitoring of keyboard dynamics allow, unlike more conventional means of authorisation (password, fingerprint, access key, enhanced electronic signature, etc.), to see if the actual user is working at the computer throughout the session [Vasilyev V.I., Kalyamov M.F. et al., 2018: 399]; [Bryukhomitsky Yu.A., Kazarin M.N., 2006: 154]; [Paschenko D.V., Balzannikova E.A., 2020: 74–75]. It makes the phenomenon under review highly relevant in the field of labour relations. For example, it can be used to ensure that employees complete their tasks diligently and independently, rather than stealing innovative ideas from their colleagues. This is especially important in creative professions (designer, sales manager, etc.), where the development of a new project contributes to career growth and is a condition for receiving a bonus. In addition, as E.E. Turutina notes, "an authentication system (*which can be based, among other things, on analysing the attributes of keyboard dynamic.* (italics are mine.—A.Ts.*)* solves many problems, such as <...> keeping track of working hours and the location of staff at a given time" [Turutina E.E., 2021: 168]. In this case, processing keyboard dynamics will make it possible to determine who is working on a certain computer device at a particular point in time; what the person is doing: whether he / she is really working or is engaged in some unrelated activity; whether the employee is working overtime, etc.

However, the phenomenon under review plays a more important role in cases related to occupational safety and discipline control. E.g., Yu.A. Bryukhomitsky and M.N. Kazarin note analysing keyboard dynamics allows "to detect temporary psychophysical deviations of operators from their normal behaviour resulting from stress, sickness, ailments, taking pharmaceutical substances, etc." [Bryukhomitsky Yu.A., Kazarin M.N., 2006: 154]. Studies by other scholars support similar conclusions [Vasilyev V.I., Sulavko A.E., Borisov R.V. et al., 2017: 21–23]; [Lozhnikov P.S., Sulavko A.E., 2015: 32–33]; [Ivanov A.I., 2000: 8]. It may help to determine if an employee is over-fatigued, is under influence of alcohol or other substances, and, based on this information, to decide to suspend this person. This is especially important "when, for example, users are working with potentially hazardous computer systems or life support systems (nuclear power plants, medical institutions, emergency services, etc.)" [Mashtanov P.N., Martynyuk M.V., 2021: 529].

These measures can improve work processes, ensure compliance with the work and rest schedule, and provide the interested parties with objective evidence during individual labour dispute. However, the controversial legal nature of such control should be taken into account.

On the one hand, the legal regulations (Clause 1, Part 1, Art. 86 of the Russian Federation Labour Code[11]) allows the employer to undertake all the above-mentioned measures if these aim to protect the employees and the assets of the employer (in case it is established the employee is in a state that prevents him/her from fulfilling his/her duties in compliance with all the requirements), exercise control over the volume and quality of the work performed (in course of recording data on the employee's real activities at work and when checking the person's identity). However, in any case, all employees must be notified at the stage of concluding an employment contract that their keyboard dynamics will be subject to processing (Clause 8, Part 1, Art. 86 of the Labour Code). In addition, it is the possibility granted to the employer to exercise control over the employee that is considered a distinctive feature of labour relations [Ofman E.M., 2021: 130–131]. Foreign legislators in many countries even use the electronic monitoring concept [Siegel R., König C., Lazar V., 2022]; [Lira Í., Schiavon L., Freguglia R., 2024: 205–221]. This concept proceeds from a set of actions by the employer aimed at obtaining information about employees' activities and their condition through specialized technical means and by collecting information from various electronic media, and communication networks (including monitoring network activity, electronic communications, telephone conversations, etc.).

On the other hand, such control may violate the right to personal privacy, which was discussed in detail above. Automated information processing can be a solution. E.g., many key loggers may be part of a complex software module with an integrated intelligent data processing function. I.e. the data on keyboard dynamics is analysed by means of machine learning algorithms. Then, on this basis, the system establishes, for instance, the person in question is in an abnormal psychophysiological state, and temporarily suspends him/her from work. In this case, the employer will not know what the person

---

[11] Labour Code of the Russian Federation of 30.12. 2001 No.197-FZ (as amended 06.06.2024). Available at: URL: https://www.consultant.ru/document/cons_doc_LAW_34683/ (accessed: 21.07.2024)

was typing but will only receive a generalized analytical review. However, it is of need to clarify here that at present legally binding decisions may not be made on the basis of an employee's personal data obtained exclusively through automatic data processing. In view of this, the software module that we describe here may not determine if an employee should be held accountable, suspended from work etc., but can only send an alarm: working conditions are being violated and that this must be double-checked by other means.

However, if the task arises to establish the identity of the person who produced a text (wrote a department development project, entered financial indicators into reporting documents, etc.), the employer may turn to the corporate technical service (IT department), as its representatives have the necessary competences to evaluate keyboard dynamics and conclude if its features belong to a particular person.

In this regard, scholars engaged in the labour law should pay attention to the issue of using keyboard dynamics to implement automated control over employees, particularly to address the issues of economic and technological feasibility, and compliance with ethical values. May I believe technology under review will prove to be totally acceptable: it has already shown a successful performance at some enterprises and is "the easiest to implement and administer, because it doesn't require any additional hardware, except for a computer keyboard" [Nikulicheva E.O., 2019: 57–59].

Conclusion

There are various areas of social relations where keyboard dynamics can be implemented. But, to respect citizen's rights in a reasonable manner and protect privacy, while at the same time ensuring aims of national and public security are achieved, a comprehensive legal framework must be established to regulate social relations in connection with keyboard dynamics. Probably today the following model is the optimum.

In the early stages, until the legal status of keyboard dynamics is precisely defined and enshrined in law, all persons involved in its processing, irrespective of the key logger localization (in the desktop software or on a digital platform in the world-wide web), must be obliged to obtain informed consent from the users, similar to the consent required when the website wants to store cookies on the user's device. Perhaps the best approach would be to create big pop-up windows with general description of the data to be processed and the purpose of this processing, not to hide information in many pages of data policies. Users should be given an option both to limit the list of data collected and to deny access to their keyboard dynamics completely while retaining access to the programme and/or services in question.

Next, is should be enshrined that keyboard dynamics is a biometric characteristic, and this dynamics must be included in the list of data that only a authorised person is entitled to process (e.g., the operator of the Unified Biometric System; at present, it is the Centre for Biometric Technologies). At the same time, the technical and legal capacities of the UBS can be used to carry out state registration of keyboard dynamics along two lines: voluntary, and mandatory. Mandatory registration will apply to persons who committed crimes or administrative offences with the use of typed texts, who knowingly use a digital platform previously used to commit such unlawful acts, or who hold public service positions involving work with information that constitutes a state secret or with e-government services. A corresponding Federal Law should be passed to implement the measures for state registration.

Next, measures must be taken to exclude a possibility of unauthorised correlation of keyboard dynamics with a specific typed text, since otherwise the right of citizens to personal and family privacy, confidentiality of correspondence, etc., would be unjustifiably violated. In this field, it would seem promising to use method of indirect recording of keyboard dynamics, linking its features to the computer device on which these features were recorded, rather than to a specific person who is their carrier. Hence, to solve the tasks facing law enforcement agencies (identify a person guilty of committing a crime or administrative offence, where typed texts were the subject of encroachment or means of committing an offence), requests will have to be sent to the operator, which aggregates data about keyboard dynamics in their relation to the MAC-address, and to the network connection services provider, which stores data about the owner of a device with a specific MAC-address. Perpetrators, in their turn, to link valuable information to a particular person, would need to make a significantly greater effort to gain unauthorised access to several secure databases, that seems very unlikely, if not impossible.

Implementing all the above described preparatory measures will make it possible to include the processing keyboard dynamics into the activities of crime investigation, procedural proof of the involvement or non-involvement of a particular person in the creation of a typed text, and into the sphere of labour relations to control the integrity of employees and their proper medial state, ensuring the safety of working processes.

Keyboard dynamics is a phenomenon of reality should not be locked in the narrow framework of one branch of scholar knowledge. It should be researched by a wide range of specialists, including the legal profession, where individual sciences may take an interest in the phenomenon and develop their own approaches to defining it, describing its place and the possibilities of using their knowledge about it.

References

1. Averin A.I., Sidorov D.P. (2015) User authentication by keyboard dynamics. *Ogaryov-Online*, no. 20, pp. 1–5 (in Russ.)

2. Alsultan A., Warwick K. (2013) Keystroke dynamics authentication: a survey of free-text. *International Journal of Computer Science Issues*, vol. 10, no. 1, pp. 1–10.

3. Banerjee S.P., Woodard D.L. (2012) Biometric authentication and identification using keystroke dynamics: a survey. *Journal of Pattern Recognition Research,* vol. 7, pp. 116–139. DOI: 10.13176/11.427.

4. Branovitsky K.L., Renz I.G. (2019) May an expert be trusted? On forensic expertise quality (comparative analysis). *Zakon*=Law, no. 10, pp. 43–54 (in Russ.)

5. Bryukhomitsky Yu.A., Kazarin M.N. (2006) Covert keyboard monitoring system. *Vestnik Taganrogskogo radiotechnicheskogo universiteta*=Taganrog Radiotechnical University Bulletin, no. 9, pp. 154 (in Russ.)

6. Clarke R. (1994) Human identification in information systems: management challenges and public policy issues. *Information Technology & People,* vol. 7, pp. 6–37.

7. Forsen G., Nelson M., Staron R.Jr. (1977) Personal attributes authentication techniques. Technical Report. Rome: Air Development Center, 333 p.

8. Foygel E.I. (2023) Modern trends and prospects of development of the forensic doctrine of the personality of participants of criminal proceedings. *Akademicheskiy juridicheskiy zhurnal*=Academic Juridical Journal, no. 1, pp. 101–108. DOI: 10.17150/1819-0928.2023.24 (1) (in Russ.)

9. Fyodorov I.Z. (2019) Searching persons typed electronic text by keyboard dynamics in the detection and investigation of crimes. *Vestnik Barnaulskogo instituta MVD*=Bulletin of Barnaul Law Institute of Internal Ministry, no. 2, pp. 113–116 (in Russ.)

10. González N., Calot E. (2023) Dataset of human-written and synthesized samples of keystroke dynamics features for free-text inputs. *Data in Brief*, vol.

11. Guo J., Mu H. et al. (2024) Federated learning for biometric recognition: a survey. *Artificial Intelligence Review*, vol. 57, pp. 208–247. DOI: 10.1007/s10462-024-10847-7.

12. Guryanov K.V. (2020) Project 'Strelok': the first key logger. *Bazis*=Basics, no. 2, pp. 79–91 (in Russ.) DOI: 10.1016/j.dib.2023.109125.

13. Ivanov A.I. (2000) *Biometric identification of personality by dynamics of subconscious movements.* Penza: University, 188 pp. (in Russ.)

14. Ivanov V.V., Zuyev D.I. (2022) Digital twin and digital identity: concept, correlation, meaning in the process of committing cybercrime and in law in general. *Pravo i gosudarstvo*=Law and State: Theory and Practice, no. 4, pp. 138–144. DOI: 10.33184/pravgos-2022.4.19 (in Russ.)

15. Isaeva V.V., Sakharova Y.V. (2020) International and national aspects of legal regulation of private life and the right to private life. *Vestnik Bryanskogo universiteta*=Bulletin of Bryansk University, no. 2, pp. 136–142 (in Russ.)

16. Karimov A.M. (2023) Crimes in the sphere of computer information and crimes with using information and communication technologies: comparative aspect. *Vestnik Kazanskogo intituta MVD*=Bulletin of Kazan Institute of Internal Ministry, no. 1, pp. 75–82. DOI: 10.37973/KUI.2023.93.91.010 (in Russ.)

17. Lozhnikov P.S., Sulavko A.E. (2015) Technology of identification of computer system users by dynamics of subconscious movements. *Avtomatizatcia*. *Sovremennye technologii*=Automation. Modern Technologies, no. 5, pp. 31–36 (in Russ.)

18. Lira Í., Schiavon L., Freguglia R. (2024) Electronic monitoring of working time and labour market outcomes: evidence from Brazil. *Industrial Relations Journal*, vol. 55, pp. 205–222. DOI: 10.1111/irj.12423.

19. Matsubara Y., Samura T., Nishimura H. (2015) Keyboard dependency of personal identification performance by keystroke dynamics in free text typing. *Journal of Information Security,* vol. 6, pp. 229–240. DOI: 10.4236/jis.2015.63023.

20. Mashtanov P.N., Martynyuk M.V. (2021) Review of current issues of biometric identification based on the features of keyboard dynamics. Information systems and technologies-2021: proceedings of a conference. Nizhny Novgorod: Technical University Press, pp. 527–531 (in Russ.)

21.Md A., Mohiuddin S. et al. (2019) Key logger detection using memory forensic and network monitoring. *International Journal of Computer Applications,* no. 11, pp. 17–21.

22. Nikulicheva E.O. (2019) Analysis of keyboard dynamics as a method of personal identification. Issues of forensic psychological examination and complex examination with participation of a psychologist. In: Prospects of fundamental and applied research of handwriting: papers of international conference. Kaluga: University Press, pp. 56–60 (in Russ.)

23. Ofman E.M. (2021) Transformation of the employer's right to control the employee's behaviour in the digital economy. *Yearbook* of *Labour Law*, no. 11, pp. 130–145 (in Russ.)

24. Paschenko D.V., Balzannikova E.A. (2020) Continuous user identification by keyboard dynamics using state-context based representation. *XXI vek*: *itogi proshlogo i problemy nastoyaschego*=XXI Age: Past Results and Present Issues, no. 3, pp. 74–79. DOI: 10.46548/21vek-2020-0952-0012 (in Russ.)

25. Rossinskaya E.P. (2019) Special knowledge in the judicial examination of computer crimes in the digital age. *Vestnik Kutafin University*=Bulletin of Kutafin University, no. 5, pp. 31–44. DOI: 10.17803/2311-5998.2019.57.5.031-044 (in Russ.)

26. Salikov M.S., Nesmeyanova S.E. et al. (2022) State regulation of the Internet and human rights. Ekaterinburg: University Press, 220 pp. (in Russ.)

27. Samsoni D.Z., Basir B.P. et al. (2023) Key logger threats in computer security aspects. *International Journal of Integrative Sciences,* vol. 2, no. 6, pp. 867–872. DOI: 10.55927/ijis.v2i6.4520.

28. Shadman R., Wahab A. et al. (2023) Keystroke dynamics: concepts, techniques, and applications. Preprint. DOI: 10.48550/arXiv.2303.04605.

29. Shangina I.Y. (2020) Biometric identification technologies: global and the Russian practices. *Innovatcii*. *Nauka*. *Obrazovanie*=Innovations. Science. Education, no. 18, pp. 151–156 (in Russ.)

30. Siegel R., König C., Lazar V. (2022) The impact of electronic monitoring on employees' job satisfaction, stress, performance, and counterproductive work behaviour: a meta-analysis. *Computers in Human Behaviour Reports,* vol. 8. Article 100227. DOI: 10.1016/j.chbr.2022.100227.

31. Smushkin A.B. (2019) The issue of "digital alibi" in forensic science. *Problemy ugolovmogo protcessa*=Issues of Criminal Procedure, no. 2, pp. 28–33 (in Russ.)

32. Smushkin A.B. (2024) Concept of remote criminalistics. Moscow: Yurlitinform, 256 pp. (in Russ.)

33. Solomatina E.A., Cherkashina A.V., Dreval B.V. (2021) Fingerprint registration in administrative law of Russia. *Vestnik Moskovskogo universiteta MVD*=Bulletin of Moscow University of Internal Ministry, no. 4, pp. 234–240. DOI: 10.24412/2073-0454-2021-4-234-240 (in Russ.)

34. Spillane R. (1975) Keyboard apparatus for personal identification. *IBM Technical Disclosure Bulletin*, vol. 17. Article 3346.

35. Suman R.R., Mall R. et al. (2010) Extracting state models for black-box software components. *Journal of Object Technology*, no. 3, pp. 25– 29.

36. Syed Idrus S.Z. (2014) Soft biometrics for keystroke dynamics. Computer vision and pattern recognition. Caen: Universite de Caen, 134 p.

37. Turutina E.E. (2021) Analysis of electronic and biometric authentication methods in access control systems. *Vestnik akademii nauk tatarstana*=Bulletin of Tatarstan Academy of Sciences, no. 2, pp. 168–175 (in Russ.)

38. Uimin A.G., Morozov I.M. (2022) Comparative analysis of continuous online authentication tools and anomaly detection systems for continuous confirmation of user identity. *Telekommunikatcii i transport*=Telecommunications and Transport, no. 5, pp. 48–55. DOI: 10.36724/2072-8735-2022-16-5-48-55 (in Russ.)

39. Vacca J.R. (2007) Biometric technologies and verification systems. Burlington: Elsevier, 625 p.

40. Varlamova S.A., Vavilina E.A. (2023) User identification on the basis of keyboard dynamics. *Innovatcionnoe priborostroene*=Innovations in Instrumentation

Engineering, vol. 2, no. 3, pp. 67–71. DOI: 10.31799/2949-0693-2023-3-67-71 (in Russ.)

41. Vasilyev V.I., Kalyamov M.F., Kalyamova L.F. (2018) User identification by keyboard dynamics using frequent bigram registration algorithm. *Modelirovanie, optimizatcia i indormatcionnye technologii*=Modeling, Optimization and Information Technologies, vol. 6, no. 1, pp. 399–407 (in Russ.)

42. Vasilyev V.I., Sulavko A.E., Borisov R.V. et al. (2017) Recognition of psychophysiological states of users by hidden monitoring in computer systems. *Iskussvennyi intellect i prinyatie resheniy*=AI and Decisions, no. 3, pp. 21–37 (in Russ.)

43. Villani M., Tappert C. et al. (2006) Keystroke biometric recognition studies on long-text input under ideal and application-oriented conditions. Proceedings of international workshop computing and computational statistics. DOI: 10.1109/CVPRW.2006.115.

44. Zaytsev O.A., Pastukhov P.S. (2022) Digital profile of a person as an element of information-technological strategy of crime investigation. *Vestnik Permskogo universiteta. Pravo*=Bulletin of Perm University. Legal Sciences, no. 56, pp. 281–308. DOI: 10.17072/1995-4190-2022-56-281-309 (in Russ.)

45. Zeid S., El Kamar R., Hassan S. (2022) Fixed-Text vs. Free-Text keystroke dynamics for user authentication. *Engineering Research Journal*, vol. 51, pp. 95–104. doi:10.21608/erjsh.2022.224312.

46. Zhukov M.N. (2021) Validity of biometric data using in forensic science: historical background and legal protection of personal data. *Mezhdunarodnyi naucho-issledovatelskyi zhurnal*=International Scholar Research Journal, no. 12, pp. 164–167. DOI: 10.23670/IRJ.2021.114.12.148 (in Russ.)

47. Zuyev S.V. et al. (2019) Basics of theory of electronic evidence. Moscow: Yurlitinform, 653 pp. (in Russ.)

Information about the author:

A.D. Tsvetkova — Researcher.

The article was submitted to editorial office 21.04.2024; approved after reviewing 17.06.2024; accepted for publication 02.09.2024.

Legal Issues in the Digital Age. 2024. Vol. 5. No. 4.
Вопросы права в цифровую эпоху. 2024. Т. 5. № 4.

Research article
JEL*:* K00
УДК*:* 34
DOI:10.17323/2713-2749.2024.4.73.91

Deepfakes: Search for a Model of Legal Regulation

Vladislav Olegovich Demkin

National Research University "Higher School of Economics", 20 Myasnitskaya Str., Moscow 101000, Russia,

vodemkin@hse.ru

ORCID: 0000-0002-1079-425X, Google Scholar: OfF2SrUAAAAJ, SPIN-code RINT: 1755-2053

Abstract

Modern studies of law, political science and other humanities reveal a major public concern about deepfake technologies, with legal regulation thereof only emerging. This paper looks into the main models whereby such technologies are regulated in Russia, China, European Union, United States and United Kingdom. Effective regulation of technologies should have as its main goal the protection of personal rights through methods of private and public law while striking a balance between relevant interests of other subjects to social relations. The study employs a variety of methods: comparative method (to analyze how deepfake technologies are regulated under various legal systems); method of rising from the abstract to the concrete (to move from regulation of AI to specific ways of regulating deepfake technologies); and the formal dogmatic method (to analyze legal provisions and their place in the regulation of deepfake technologies). The study provides a list of parties to AI-related social relations whose interests should be accounted for in developing the underlying regulation. The author points out certain fundamental questions to be resolved for legal regulation of deepfake technologies to emerge in Russia, and concludes by proposing answers to the said questions and identifying the vector of regulatory development.

© Demkin V.O., 2024
This work is licensed under a Creative Commons Attribution-Sharealike 4.0 International License
https://creativecommons.org/licenses/by-sa/4.0/legalcode.en

Keywords
deepfake; deceptive information; human rights; personal dignity and honor; artificial intelligence; digital personality.

For citation: Demkin V.O. (2024) Deepfakes: Search for a Model of Legal Regulation. *Legal Issues in the Digital Age,* vol. 5, no. 4, pp. 73–91. DOI:10.17323/2713-2749.2024.4.73.91

Background

In their current state, machine learning technologies allow to design computer models (replicas) of real people using their biological features. Thus, the widely used AI-based deepfake technologies allow to make synthetic media representing persons under certain aspects including obscene, for instance, in pornography [Pfefferkorn R., 2020: 265][1]. The problem of correct use of novel technologies to prevent deceptive information (fakes) has gained considerable public interest. In particular, according to *Google Trends*, search queries containing the word "deepfake" started to appear in February 2018, only to proliferate afterwards[2]. Society is wary of wide dissemination of technologies that allow to create deceptive information and content involving real persons but having nothing to do with the reality.

The term "deepfake" was coined from two English words: "deep learning" (to imply the use of neural network) and "fake".

There are different criteria to classify deepfakes. First, they can be targeted or not depending on the proposed recipient of information fabricated through their use [Roberts T., 2023: 2]. By the nature of underlying content, deepfakes split into: 1) commercial (used for business development purposes); 2) original and creative (for example, in motion pictures); 3) vindictive; and 4) political [Meskys E., Kalpokiene J., Jurcys P. et al., 2020: 25].

While the term "deepfake" is technical, the national law in countries responds differently to the questions resulting from growing public interest to the problem of technological usage.

---

[1] See also: Horrifying new AI app swaps women into porn videos with a click. MIT Technology Review. Available at: https://www.technologyreview.com/2021/09/13/1035449/ai-deepfake-app-face-swaps-women-into-porn/ (accessed: 27.07.2024)

[2] Google search statistics. Available at: https://trends.google.com (accessed: 27.07.2024)

How the legal systems of Russia, China, EU, United States, United Kingdom regulate deepfake technologies is discussed below.

1. Legal Regulation of Deepfake Technologies

1.1 Searching for Ways to Regulate Deepfake Technologies

Russia is currently at an early stage of conceptualizing regulation of artificial intelligence including deepfake technologies. These efforts largely involve proposals to add the right to "voice" or "personality" to the list of moral rights; regulate the right to voice as exclusive right to intellectual assets, and speech synthesis — along the lines of licensing agreements; treat human voices and images as biometric personal data subject to relevant regulation when used in generative neural networks; toughen the liability for specific offences involving generative neural networks; and designate deepfake content as such.

Deepfake technology is defined by both judicial practice and legal doctrine. In Supreme Court Plenum Resolution No. 17 "On specific questions raised by courts in handling administrative offences aiming to undermine the procedure for information support of elections and referendums" of 25 June 2024, deepfakes are understood as misleading and misrepresenting images, audio and audiovisual information including created through the use of computer technologies[3].

The legal doctrine defines deepfakes as photographs, video or audio created by artificial intelligence to replicate the reality (normally by stacking the existing images and videos over source images or video clips) [Kalyatin V., 2022: 87]; [Pfefferkorn R., 2020: 248]; as AI-based technologies to produce or edit video or pictorial content in order to show something that never happened [Young N., 2019: 8]. This definition generally matches the technical one.

In October 2023, the Council for Digital Economic Development under the Federation Council of the Federal Assembly of Russia held an AI desk meeting on legal guarantees for natural persons when their speech is synthesized (generated by computer) which is also a variety of deepfake technology[4]. Following the discussions, the Federation Council decided

---

[3] SPS ConsultantPlus.

[4] A. Sheikin chaired AI desk meeting of the Council for Digital Economic Development under the FC. Available at: URL: http://council.gov.ru/events/main_themes/148788/ (accessed: 27.07.2024)

to draft amendments to the Civil Code of Russia for human voice to be treated as intangible goods like human image. Other discussions focused on the need to designate synthetic speech created through the use of deepfake technologies; and liability for making public (posted in the web) speech recordings without seeking consent of the person concerned[5].

In furtherance of the idea to allow or prohibit voice synthesizing, the National Federation of Music Industry (NFMI) proposed broader protection of "digital image". According to the NFMI General Director N.A. Danilov, such provision would more efficiently protect performers from commercialization of personality through the use of deepfakes[6].

In absence of regulation, legal gaps are to be filled by court practice. Supreme Court Plenum Resolution No. 17 mentioned above provides using deepfakes in pre-election campaigning is a violation under Article 5.12 of the Code of Administrative Offences "Production, dissemination or publication of campaign materials in defiance of legal provisions on elections and referendums" (in particular, of paragraph 1.1, Article 56, Federal Law "On the Principal Guarantees of Russian Citizens' Right to Vote and Take Part in Referendums")[7].

The legal doctrine is also devising ways to regulate deepfake technologies.

For example, V.O. Kalyatin considers deepfake content from the perspective of intellectual property law by exploring the questions of attribution, use of intellectual property assets, pictures and images of natural persons, confidential information, as well as the assignment of exclusive right to source materials and resulting deepfakes [Kalyatin V., 2023: 17]. M.B. Dobrobaba argues for the development of tools that allow to identify and address deepfakes; for designation of deepfake content in social media; for tougher liability for violating third party rights through the use of deepfake technologies [Dobrobaba M., 2022: 117]. A.V. Minbaleev proposes to adopt basic AI federal law to be complemented by specific regulations to address specific processes or technologies such as generative neural networks including deepfake technologies [Minbaleev A., 2023: 15].

---

[5] Federation Council proposed to designate synthesized voice. Available at: URL: https://tass.ru/obschestvo/19816417 (accessed: 03.08.2024)

[6] Coming short of one voice. Available at: URL: https://www.kommersant.ru/doc/6805009 (accessed: 01.08.2024)

[7] SPS Consultant Plus.

In drafting specific provisions to regulate deepfake technologies, one should take into account the need to strike a balance between the interests of those governed by the underlying regulation: 1) persons whose image, voice, “personality” (broadly understood as dynamic set of physiological, biological, emotional features) are used in the deepfake content; 2) those creating artificial video, audio clips and images; 3) website owners/platform administrators providing tools and technologies to produce deepfakes; 4) government represented by public authorities for protection of rights and interests of natural and legal persons. Striking a balance of interests in shaping and improving legal regulation in the area under discussion also attracts scholarly notice. Thus, there is a perceived need, on the one hand, to fix up a system of rules applicable to deepfake technologies and envisaging liability for violations while, on the other hand, avoiding barriers to technological progress as a whole or prohibiting deepfake technologies altogether. There is also a need to keep the balance between values promoted by the legal system and new technological boundaries [Vinogradov V., Kuznetsova D., 2024: 239].

Internationally, the regulation of deepfake technologies is at various stages of development.

Thus, the Chinese regulatory model can be called administrative as it purports to impose additional requirements on owners of the tools for production of deepfakes. Believing that deepfakes are fraught with major social risks, the Chinese government wants not only to designate artificially created content but also to add new elements to the list of criminal offences: dissemination of non-designated deepfake content as news.

As regards regulation of deepfake technologies, China was the first to establish strict and detailed rules for production and dissemination of deepfake content through the use of neural networks, with the Regulation on Deep Synthesis Information Web Services adopted on 25 November 2022[8] imposing obligations on owners of deepfake creative tools.

The EU regulation of deepfake technologies is AI-focused, with the Artificial Intelligence Act (“Regulation”) approved in 2024[9] defining de-

---

[8] Regulation for Deep Learning Management of Information Web Services (in Chinese). Available at: http://www.cac.gov.cn/2022-12/11/c_1672221949354811.htm (accessed: 27.07.2024)

[9] Regulation of the European Parliament and Council of 13 June 2024 Laying Down Harmonised Rules On Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU)

velopment methods of deepfake technologies (including by establishing regulatory sandboxes); creating and defining the powers of a special AI supervisory authority to be set up, and applicable penalties. The adoption of special instrument will allow to fine tune the regulation of modern technologies while accounting for the needs of all parties involved — natural persons as owners of "special" rights in the digital world; businesses as users and beneficiaries of technologies; and the governments as regulators of the underlying relations.

The United States and the United Kingdom follow a different approach: there is currently no specific regulation of AI and deepfake technologies, with deepfake related legal problems addressed by adding up to the existing elements of crime. In legal literature it is pointed out that the American method of regulation is particular in its unwillingness to prohibit AI-generated content due to priority of individual rights including freedom of speech and expression. The U.S. sources argue that society is wary of deepfake regulations believed to infringe on the freedom of speech [Joost L., 2023: 312][10]. Other American authors come to similar conclusions. In particular, it is noted that deepfakes can be regarded as a form of self-expression protectable by the First Amendment to the U.S. Constitution. Under another argument, deepfake content occupies an intermediate position, with some instances of use to be protected by the freedom of expression and others criminalized [Blitz M., 2020: 300].

Some laws in the United States require from different organizations and public agencies to make AI-related reports and propose response. In 2019, the U.S. adopted a number of laws regulating AI-related operations of public authorities and certain state-owned firms. Such instruments oblige them to monitor the progress of deepfake technologies worldwide, assess the underlying risks, and also promote public-private partnership to conduct relevant research and counter deceptive information[11]. These instruments

---

2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689 (accessed: 22.07.2024)

[10] See for example: As Deepfakes Flourish, Countries Struggle with Response. Available at: https://www.nytimes.com/2023/01/22/business/media/deepfake-regulation-difficulty.html?action=click&module=RelatedLinks&pgtype=Article (accessed: 27.07.2024)

[11] First Federal Legislation on Deepfakes Signed into Law. Available at: https://www.wilmerhale.com/insights/client-alerts/20191223-first-federal-legislation-on-deepfakes-signed-into-law (accessed: 05.08.2024)

have no direct impact on mechanisms for protection of personal rights or regulation of deepfake technologies. In addition, pursuant to the Identifying Outputs of Generative Adversarial Networks Act ("IOGAN") of 2020, the National Research Foundation and the National Institute of Standards and Technology are required to support and promote research of the methods of generative adversarial networks[12].

There are ongoing discussions in the United States of the draft NO FAKES ACT (Nurture Originals, Foster Art, and Keep Entertainment Safe Act)[13] designed to introduce more detailed regulation of digital replicas. The draft submitted to the U.S. Congress by both Republican and Democratic senators defines a digital replica as a newly created, computer-generated, electronic representation of the image, voice, or visual likeness of an individual that: (A) is nearly indistinguishable from the actual image, voice, or visual likeness of that individual; and B) is fixed in a sound recording or audiovisual work in which that individual did not actually perform or appear. The consent to produce and use such digital replica is assumed to be a digital replication right that is material, heritable and transferrable or assignable in full or in part (along the lines of exclusive right to intellectual property). In order to dispose of this right, one has to retain a professional attorney (lawyer, solicitor, trade union). Thanks to the federal act for protection of digital identity, the right to publicity that provides similar protection to human image but is not recognized in some states can become universally enforceable.

Deepfake technologies are also regulated at the state level. For instance, the State of California has a number of laws governing deepfake content: Assembly Bill No. 602[14] banning erotic deepfake content without approval of the person represented who is free to claim damages from the content creator, and Assembly Bill No. 730[15] banning the dissemination of election-related deepfake content sixty days prior to the voting day ("a person ...,

---

[12] Identifying Outputs of Generative Adversarial Networks Act. Available at: https://www.congress.gov/bill/116th-congress/senate-bill/2904/text (accessed: 28.07.2024)

[13] Nurture Originals, Foster Art, and Keep Entertainment Safe Act. Available at: https://www.ilga.gov/legislation/BillStatus.asp?DocNum=5594&GAID=17&DocTypeID=HB&LegId=153975&SessionID=112&GA=103 (accessed: 28.07.2024)

[14] Assembly Bill № 602. Available at: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=20212 0220AB602 (accessed: 28.07.2024)

[15] Assembly Bill № 730. Available at: URL: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=20192 0200AB730 (accessed: 28.07.2024)

committee, or other entity shall not, within 60 days of an election ... distribute, with actual malice, materially deceptive audio or visual media of the candidate with the intent to injure the candidate's reputation or to deceive a voter into voting for or against the candidate").

The law of Texas criminalizes the creation of misleading deepfakes seeking to impact the voting outcome if they are published 30 days prior to the voting day[16]. The State of Tennessee is peculiar for civil law regulation of deepfake technologies, with the person's name, voice and likeness protected as personal rights. Thus, any action to use these assets (including to produce deepfakes) without seeking the person's (or owner's) consent are deemed illegal and result in liability[17].

1.2. Obligations of Deepfake Technology Owners

The Russian law currently imposes no specific requirements on the owners of deepfake technologies or platforms. Operations of deep learning generative models are largely based on the terms of service (to be accepted by users at registration or simply during content production). Thus, those using Vassily Kandinsky creations to produce pictures and videos under its terms of service cannot use intellectual outcomes, identifications, third party personal data and information that constitutes any secret whatsoever. That is, users of this technology are assumed to seek third party consent in order to use the underlying items in the neural network. Also, there is a prohibition to use video and pictorial outputs that violate provisions of the Russian law[18]. Yandex neural network technologies have similar terms of service[19].

Legal systems containing (and discussing the adoption of) specific provisions to regulate AI technologies — in particular, deepfakes — will impose extra obligations on service owners.

---

[16] An act relating to the creation of a criminal offense for fabricating a deceptive video with intent to influence the outcome of an election. Available at: https://capitol.texas.gov/tlodocs/86R/billtext/pdf/SB00751F.pdf#navpanes=0 (accessed: 05.08.2024)

[17] An act to amend Tennessee Code Annotated, Title 39, Chapter 14, Part 1 and Title 47, relative to the protection of personal rights. Available at: https://www.capitol.tn.gov/Bills/113/Bill/SB2096.pdf (accessed: 05.08.2024)

[18] Sberbank's Kandinsky Terms of Service and Acceptable Use Policy of AI Services. Available at: https://www.sberbank.com/common/img/uploaded/files/promo/kandinskiy-terms/kandinskiy-terms-of-use.pdf (accessed: 17.07.2024)

[19] Yandex Foundation Models Terms of Service. Available at: URL: https://yandex.ru/legal/cloud_terms_yandex_foundation_models/ (accessed: 17.07.2024)

The Chinese regulatory model is focused on the engagement with owners of a proposed service. Under the 2022 Regulation on Deep Synthesis Information Web Services, they are required to assume three obligations of active influence: on users (through authentication and blocking); on inputs (by checking the adequacy of rights clearance); and on outputs (ensuring transparency through designation of deepfakes). This is claimed to be the established tradition of communication network governance in China where the government increasingly relies on technological companies for observance of web regulation standards and on relevant corporate initiatives [Hine E., Floridi L., 2022: 608].

1.3. User Authentication

Under the 2022 Regulation on Deep Synthesis Information Web Services, all administrators of deepfake technologies in China are required to have authentication using mobile phone numbers or specific public identifiers. Technologies of this kind are treated as web services governed by the Cybersecurity Law of China[20] (applicable to communication network owners or managers, network service providers or other persons of similar status). This law requires to deny service to those failing to provide personal data to the service owner. The web operations history of users can be made available to law enforcement bodies. This allows to easily identify and penalize the author of a particular deepfake, thus ruling out anonymous action in the Internet. So, the Chinese regulatory model assumes that deepfakes can be used only on the basis of authentication of those who make them.

Deepfake service owners are equally required to monitor the legitimate use of people's personal data and other sensitive information, as well as to censor the clips containing black-listed words. Such regulation applies to deepfakes irrespective of the subject and purpose. For service owners, the obligation to ensure legitimate use of content (via platforms, websites, mobile apps and databases) often means a need to introduce certain amendments to the underlying terms of service (to prevent the use of illegally produced content) and to deny access to materials contested by the subject on the basis of minimally required evidence of ownership. Thus, compliance with the same rules can be also expected in case of Chinese deepfake services. The mandatory user authentication requirement will simplify the

---

[20] Cybersecurity Law of China. Available at: https://www.cac.gov.cn/2016-11/07/c_1119867116.htm (accessed: 07.08.2024)

identification of wrongdoers while resulting in excessive processing of sensitive personal data by deepfake generative services. With such regulation focused primarily on web service owners, this model can be called administrative. Overall, it is successfully embedded into China's web regulation system characterized by a fair measure of state control, propensity for zero anonymity and attempts to put the interests of socialist society above those of private users.

In the EU and the United States, it is out of question to adopt provisions on mandatory user authentication. The Artificial Intelligence Act does not require from deepfake service owners to ensure authentication on the basis of personal identifiers. In our view, this is because such processing of sensitive identifiers would be contrary to the EU's regulatory policies of personal data protection. Such approach does not contradict the Act's principal objective of protecting personal rights since it ensures a comprehensive approach including in stressing the importance of correct personal data processing.

1.4. Designating Deepfake Content

Many legal systems worldwide will require from deepfake makers or enablers to designate the underlying material as artificial. This is believed to disclose to third parties significant information on its nature and to warn that the content disseminated in this manner is not credible.

Deepfake technology administrators are required to designate AI-generated content. The so-called transparency requirement is designed to warn the public that the content is artificial. The Chinese government criminalized publication of news created through the use of artificial intelligence and not designated as such[21] as early as in 2020.

The EU's Artificial Intelligence Act of 2024 requires from technology owners to designate content created through the use of AI.

In the United States and some other countries it is proposed to require from deepfake makers to designate their output accordingly. Thus, the draft DEEPFAKES Accountability Act of 2023 describes a procedure for desig-

---

[21] China seeks to root out fake news and deepfakes with new online content rules. Available at: https://www.reuters.com/article/us-china-technology/china-seeks-to-root-out-fake-news-and-deepfakes-with-new-online-content-rules-idUSKBN1Y30VU (accessed: 27.07.2024)

nating each type of content as created through the use of AI[22]. Under the U.S. law, in accordance with the draft COPIED ACT[23] each owner of a tool (website, platform or application) for AI-generated content (including deepfakes) must enable users to designate output to signal its artificial origin. The output so designated will not be usable for business purposes and neural network training. In the event of abuse, victims are free to claim damages and termination of the content's illegal use. Thus, a decision to designate will be taken individually by each user.

The EU and U.S. law is softer on requirements to technological companies and artificial content makers as not every image should be designated (the U.S. draft laws make this altogether voluntary); not every media should be prohibited for publication by virtue of the freedom of speech; and sensitive personal data of content makers is not to be processed in all cases.

From the perspective of barriers to technological progress, the requirement to designate all content being created is not reasonable. Deepfake outputs can be used in different formats, forms and types and for different purposes including private. For example, they are often used as robot secretaries at banks and health centers where it is assumed that callers do not deal with a real person. Meanwhile, designating such robot secretaries as artificial (for example, by a conversation starter) will undermine their commercial value and user attractiveness.

Moreover, it is not feasible to require to designate absolutely all AI-generated content. In particular, voice assistants, robotic secretaries at businesses (such as banks or health centers) should be able to quickly and precisely answer user queries in line with business objectives. In fact, a reasonable user can expect that his interlocutor is actually a software. Apparently, there should be exceptions from the general rule that requires to designate AI-created content. Anyway, such decision and discussions of a possible draft law should be based on the engagement with industry representatives, that is, technological companies already in possession of similar AI technologies as such designation will contradict the requirement that appearance should be attractive to users.

---

[22] DEEPFAKES Accountability Act 2023 (H.R. 5586). Available at: https://www.congress.gov/bill/118th-congress/house-bill/5586/all-actions (accessed: 08.08.2024)

[23] The Content Origin Protection and Integrity from Edited and Deepfaked Media Act. Available at: https://www.commerce.senate.gov/services/files/3012CB20-193B-4FC6-8476-DDE421F3DB7A (accessed: 28.07.2024)

A special consultative body on artificial intelligence including deepfakes may be helpful in mapping content to be designated as well as in addressing other issues. The EU's Artificial Intelligence Act of 2024 requires to set up the European Artificial Intelligence Board ("EAIB") to monitor the use of AI technologies. The EAIB will be authorized to issue opinions, recommendations and other guidelines, interpret legal provisions, develop best practices, harmonize AI-related technical standards, collect relevant data from member states on implementation of the Act and performance of regulatory sandboxes.

A special body may be also created in Russia[24]. While the new EAIB will act as such in the EU, the same functions can be assumed in Russia by a special division of the Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor).

1.5. Criminal, Administrative and Civil Liability for Deepfakes

It has a sense to believe there is currently no basis to penalize deepfake technologies either under administrative or criminal law as they are just tools to commit such offences. Meanwhile, it should be remembered that in some cases their use will make offences more harmful to society: artificial pictorial and audio content is highly delusive and gives a semblance of reality; it is web spreadable, only to become viral quickly and easily; it may be hard to refute; and attributing or identifying the source of deepfakes is problematic. Thus, it makes perfect sense to consider the use of AI technologies as a circumstance aggravating administrative or criminal liability, and conventionally also civil liability, for example, by suggesting a higher amount of compensation for violation of exclusive right to intellectual outputs and means of identification.

As noted in Supreme Court Plenum Resolution No. 17 mentioned above, the use of deepfake content is a way to commit the offence described in Article 5.12 of the Code of Administrative Offences: "production, dissemination or publication of campaign materials in defiance of legal provi-

---

[24] Artyom Sheikin, Deputy Chairman of the Digital Economic Development Council under Federation Council announced possible establishment of a special Roskomnadzor division to monitor the creation and use of AI technologies including deepfakes, address operational issues of neural networks, handle complaints, take decisions to apply sanctions, block website access to the Internet. Available at: URL: https://senatinform.ru/news/senator_sheykin_v_rkn_mozhet_poyavitsya_otdel_po_kontrolyu_za_ispolzovaniem_ii/ (accessed: 27.07.2024)

sions on elections and referendums" (in particular, of paragraph 1.1, Article 56, Federal Law "On the Principal Guarantees of Russian Citizens' Right to Vote and Take Part in Referendums").

The following possible offences involving deepfake technologies are fraught with considerably higher social risks: production/dissemination of extremist content; slander; violation of privacy; violation of copyright and related rights; fraud, coercion to perform or abandon a transaction; public call for terrorist action; public defense or advocacy of terrorism; illegal production and sale of pornographic content or items.

Circumstances aggravating administrative liability for committed offence are prerequisites that the penalty is fair and individual, something that primarily serves to achieve the purpose of correcting the behavior of those convicted to administrative liability and preventing further offence [Sundurov F., Talan M., 2015: 175]. They allow the court to justify a penalty approximating the maximum under the Code of Administrative Offences or Criminal Code. It is also worth noting that legal literature identifies among aggravating circumstances special ones [Sundurov F., Tarhanov I., 2016: 204] as constituting qualified factors of a specific offence — such as murder motivated by blood revenge[25]. Unlike "general" aggravating circumstances, they constitute specific offences not intended for assessing social danger of others.

So, the fact of using deepfake technologies to commit an offence is perfectly qualified to become an aggravating or special aggravating circumstance due to the wrongdoer's awareness of higher social danger.

The use of such services to commit other offences can be currently taken into account in Russia as an aggravating factor or circumstance. As was explicitly noted in the aforementioned Supreme Court Plenum Resolution, the use of deepfakes in the context of political campaigning constitutes an offence under Article 5.12 of the Code of Administrative Offences, with liability equally applicable to those who made and commissioned deepfake content. The only possible sanction is administrative fine of five to twenty thousand rubles for private individuals; thirty to fifty thousand rubles for officials; and one hundred to five hundred thousand for legal entities[26].

---

[25] Criminal Code of Russia, Law No. 63-FZ of 13.06.1996 // SPS ConsultantPlus.

[26] Code of Administrative Offences of Russa, Law No. 195-FZ of 30.12.2001 // SPS ConsultantPlus.

The Criminal Code of China qualifies the offences likely to be invoked in the production of other people's images using deepfake technologies. Thus, Article 235 envisages sanctions for production, dissemination and even possession of obscene images, audio recordings and texts while Articles 310, 313 prohibit slander including fraudulent dissemination of deceptive rumors. The use of the Internet to commit these crimes is an aggravating circumstance[27].

In addition, victims of deepfake content can expect that their defamation claim will be satisfied. Under the Civil Code of China, anyone offending honor, dignity and reputation of others should compensate the resulting damages and stop the violation. It is noted that the burden of proof in such cases is to be assumed by the plaintiff also supposed to justify the amount of damages, something that is not quite easy [Tianren L., Yue D., 2023].

Under the law of the United Kingdom and some American states, the use of AI technologies to create exclusively pornographic deepfakes is treated only as a way of committing offence already covered by criminal law[28]. Thus, in the State of Virginia, Articles 18.2-386.1 and 18.2-386.2 prohibit to create and disseminate other people's images without their consent regardless of the technology being used. These are class 1 offences punishable by a fine of up to USD 2,500 or prison sentence of up to 12 months. The same offences committed against minors become criminal charges that envisage more severe punishment[29].

The Online Safety Bill passed in the United Kingdom in 2023 is designed to regulate web activities of natural and legal persons including digital offences.

Germany's Bundesrat published a draft law to introduce criminal liability of up to two years in prison for digital fraud (deepfake) against personal rights (including those of deceased individuals). As an exception from elements of crime, a person will not be liable if the deepfake was made in pursuit of "prevailing" legitimate interests in arts, sciences, education, cov-

---

[27] Criminal Code of China. Approved 14.03.1997 at the 5th session of the National People's Congress. Available at: https://law.moj.gov.tw/ENG/LawClass/LawParaDeatil.aspx?pcode=C0000001&bp=44(accessed: 27.07.2024)

[28] See, for example: Deepfakes and American Law. Available at: https://www.davispoliticalreview.com/article/deepfakes-and-american-law (accessed: 30.07.2024)

[29] Code of Virginia. Available at: https://law.lis.virginia.gov/vacode/ (accessed: 09.08.2024)

erage of news or history etc. Naturally, no liability will arise where no personal right was infringed — for example, where the production of deepfake was consented by the person in question[30].

Thus, it is revealing that the Chinese government regards the use of deepfakes as fraught with major social risks and therefore does not only require to designate any artificial content but also to add new elements of crime to those covered by criminal law — dissemination of non-designated deepfake content as news.

The EU's Artificial Intelligence Act provides for exterritorial effect with the content to be designated, a special consultative body (EAIB) established, and relevant technologies consistently developed to comply with legal provisions.

Unlike the EU, the United States and the United Kingdom have not introduced special regulation of AI technologies, with legal problems related to deepfakes being addressed by adding such novel element of crime to those already existing. It is noted in literature that the American way of regulation is particular in its unwillingness to prohibit AI-generated content due to the need to observe personal rights protected by the First Amendment to the U.S. Constitution, that is, freedom of speech and freedom of expression.

It is noteworthy that the problem of deepfake-related criminality is increasingly observed around the globe, with the use of deepfake often recognized as independent element of crime or covered by special regulation.

2. Proposals on Regulating Deepfake Technologies in Russia

Special provisions regulating deepfake technologies should be developed with a view of striking a balance between the interests of all parties to the relevant social relations. The regulatory practice in Russia should be apparently "soft". The areas of social relations where it is prohibited to make and disseminate deepfakes should be limited to those vital for society and private individuals, such as those affecting the most sensitive sides of life.

The answer to the question on the regulatory vector of deepfake technologies in Russia should proceed, at the very minimum, from the following:

---

[30] Entwurf eines Gesetzes zum strafrechtlichen Schutz von Persönlichkeitsrechten vor Deepfakes. Available at: https://www.bundesrat.de/SharedDocs/drucksachen/2024/0201-0300/222-24(B).html (accessed: 10.08.2024)

Possibility to process personal data of individuals captured by deepfake content using artificial intelligence (including generative neural networks);

Considering the use of deepfake technologies as an aggravating circumstance in certain types of offence;

Identifying types and cases of using deepfake content (of certain type) where it should be designated as artificially created;

Identifying the need to set up a public authority to decide, advise, recommend, collect best practices regarding the use of AI-created content. Identifying the need to establish an entity among major technological companies as part of self-regulation of private businesses to identify common policies and technological development vector for AI-created content.

Thus, the question of whether someone's image and voice amount to biometric personal data (therefore required to be processed as biometric) appears to be among the most debatable at the intersection of personal data and deepfake content. Such data can be processed only if consented by the personal data subject in writing and only via the Unified Biometric System, with other restrictions, terms and conditions equally applicable.

In this case, we believe the answer to the question to be negative because of the constitutive feature of biometric personal data described in Article 11 of the Federal Law "On Personal Data": the operator should use such data to identify the personal data subject. If the operator is understood in this case as the operator (owner) of the technology for production of deepfake content, the use of someone's image and voice for such identification is not presumable. The same holds true for those who use this infrastructure to create content since they will often create faked images and audio to represent others in a certain light. So, they already know the personality in question while the information system for processing user supplied data is not always able to compare someone's biological characteristics and personality, that is, to identify a person.

Thus, in case of deepfake content, personal data may be and often is processed but such processing is not presumable but depends on actually proved circumstances of specific case. This means that personal data processing must be triggered by the presence of at least one of the legitimate grounds established by Article 6 of Federal Law No. 152-FZ "On Personal Data" of July 27 2006 for the category of "normal" data. These include the data subject's consent and performance of the contract with the data subject. However, the actual duty to provide legitimate basis just as the risks of non-compliance are assumed by those who make deepfakes. In particular, this is reflected in the terms of service of various platforms that enable the production of deepfakes.

Conclusion

Viewed from the legal perspective, the problem of using deepfake technologies has numerous aspects since it reflects provisions of different branches of both private and public law. While some countries are proposing their way to regulate artificial intelligence (including deepfakes), others only start discussing a possible course of action.

The approaches discussed in this paper are largely focused on those who own deepfake (and other AI) technologies rather than on victims of deceptive information or those accused of propagating it. Their rights, duties and liabilities are deemed duly regulated by the existing provisions of criminal and civil law based on the established practice. Depending on circumstances, they cover slander, fraud, offence to personal dignity and honor, and sometimes the dissemination of deceptive socially important information as news.

The Russian legal system still does not have specific regulation of AI.

The author has identified a number of questions to be addressed in approving provisions (if any) to regulate deepfake content, and proposed answers including:

Possibility to process personal data of individuals captured by deepfake content using artificial intelligence (including generative neural networks): such data are not biometric personal data under the general rule and can be processed on the “general basis”;

Considering use of deepfake technologies as an aggravating circumstance in certain types of offence: such legal novelty is admissible and even desirable since deepfake content considerably aggravates the social danger of offence;

Identifying types and cases of using deepfake content (of certain type) where it should be designated as artificially created: it is proposed to establish an exhaustive list (if any). However, the duty to designate will not slow down the progress of these technologies or positively affect the prevention of deepfake-related crime;

Identifying the need to set up a public authority to decide, advise, recommend, collect best practices regarding the use of content created by artificial intelligence. Identifying the need to create an entity among major technological companies as part of self-regulation of private businesses to identify common policies and technological development vector for AI-created content: such associations of market players are believed necessary and useful for identifying the AI-related regulatory development vector, adopting guidelines and the underlying rules of procedure. A special-purpose consultative public body can be set up under the Roskomnadzor.

The problems of implementing personal rights in a new context (in particular, digital) cannot be adequately and comprehensively addressed unless the methods and means of private and public law are used in conjunction.

References

1. Blitz M.J. (2020) Deepfakes and other Non-Testimonial Falsehoods: When is Belief Manipulation (Not) First Amendment Speech. *Yale Journal of Law & Technology,* vol. 23, pp. 161–300.

2. Chesney B., Citron D. (2019) Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *California Law Review*, vol. 107, issue 6, pp. 1753–1819. DOI: 10.15779/Z38RV0D15J.

3. Criminal Law of Russia. General part. Textbook (2016) Sundurov F.T., Tarhanov I.A. (eds.). Moscow: Statut, 864 p. (in Russ.)

4. Hine E., Floridi L. (2022) New Deepfake Regulations in China are a Tool for Social Stability, but at what Cost? *Nature Machine Intelligence,* vol. 4, pp. 608–610.

5. Joost L. (2023) Place for Illusions: Deepfake Technology and the Challenges of Regulating Unreality. *University of Florida Journal of Law and Public Policy*, vol. 33, no. 2, pp. 309–332.

6. Kalyatin V.O. (2022) Deepfake as a Legal Problem: New Threats or New Opportunities? *Zakon*=Law, no. 7, pp. 87–103. DOI: 10.37239/0869-4400-2022-19-7-87-103 (in Russ.)

7. Mason S., Seng D. (2021) Artificial Intelligence and Evidence. *Singapore Academy of Law Journal,* issue 33. pp. 241–279.

8. Meskys E., Kalpokiene J., Jurcys P. et al. (2020) Regulating Deep Fakes: Legal and Ethical Considerations. *Journal of Intellectual Property Law & Practice,* vol. 15, issue 1, pp. 24–31. DOI: 10.1093/jiplp/jpz167.

9. Pfefferkorn R. (2020) «Deepfake» in the Courtroom. *Boston University Public Interest Law Journal,* vol. 29, issue 2, pp. 245–276.

10. Rafil R. (2023) Libel, Slander and Defamation Law: the Basics. Available at: https://www.findlaw.com/injury/torts-and-personal-injuries/defamation-law-the-basics.html (accessed: 22.07.2024)

11. Roberts T. (2023) How to do Things with Deepfakes. *Synthese*, issue 43, pp. 1–18. DOI: 10.1007/s11229-023-04044-2.

12. Sundurov F.T., Talan M.V. (2015) Punishment in Criminal Law: study guide. Moscow: Statut, 296 p. (in Russ.)

13. Tianren L., Yue D. Defamation and Privacy Law in China. Available at: https://www.carter-ruck.com/law-guides/defamation-and-privacy-law-in-china/ (accessed: 22.07.2024)

14. Velasco C. (2022) Cybercrime and Artificial Intelligence. An overview of the work of international organizations on criminal justice and the international applicable instruments. *ERA Forum*, issue 23, pp. 109–126. DOI: 10.1007/s12027-022-00702-z.

15. Vinogradov V.A., Kuznetsova D.V. (2024) Foreign Experience in Legal Regulating Deepfake Technology. *Pravo*. *Zhurnal Vysshey shkoly ekonomiki*=Law. Journal of the Higher School of Economics, vol. 17, issue 2, pp. 215–240. DOI:10.17323/2072-8166.2024.2.215.240 (in Russ.)

16. Young N. (2019) Deepfake Technology: Complete Guide to Deepfakes, Politics and Social Media. North Charleston (S.C.): Independently published, 160 p.

Information about the author:

V.O. Demkin — Postgraduate Student.

The article was submitted to editorial office 26.08.2024; approved after reviewing 30.09.2024; accepted for publication 07.10.2024.

Legal Issues in the Digital Age. 2024. Vol. 5. No. 4.
Вопросы права в цифровую эпоху. 2024. Т. 5. № 4.

Digital Age: Criminal Law

Research article
JEL: K14, K40, K41, K42
УДК: 343
DOI:10.17323/2713-2749.2024.4.92.112

Liability and the Digital Age: Comparative Analysis of the Australian, South African and CIS States Legislative Approaches

Denis Andreevich Pechegin

Institute of Legislation and Comparative Law under the Government of the Russian Federation, 69 Novocheremushkinskaya Str.,Moscow 117418, Russia,
crim5@izak.ru; orcid.org/0000-0001-6499-9966.

Abstract

The specific set of means of criminal law protection of the monetary sphere in the state is determined by many factors, among which economic ones are of primary importance. In this regard, approaches to the construction of a set of these means may vary depending on the economic system of the state. States with a develop economy establish criminal law prohibitions in the monetary sphere, mainly concerning counterfeiting of currency, as well as money laundering. Countries with a different, for example, mixed economic system are characterized by the consolidation of additional means of criminal law protection of the monetary sphere, including liability for failure to return funds from abroad, smuggling, etc. With that the rapid proliferation of digital assets platforms has democratized capital flow relations, enabling a vast spectrum of chances to bypass so called analog legal barriers has also raised concerns regarding means of counteracting of unlawful actions in the digital sphere. The study outlines approaches of some different countries, including Australia, South Africa, CIS states, which can be taken into account. It argues that differences in the type of economic systems of the states do not at all predetermine

© Pechegin D.A., 2024
This work is licensed under a Creative Commons Attribution-Sharealike 4.0 International License
https://creativecommons.org/licenses/by-sa/4.0/legalcode.en

the impossibility of conducting a comparative legal study of their approaches in the digital sphere. On the contrary, the coincidence in the type of economic systems of two or more countries, in the digital age cannot serve as correct grounds for confirming the thesis on the relevance. The author summarizes the need for changes in the liability regulatory framework.

Keywords

digital currency; money; digital assets; liability; comparative analysis; regulatory framework.

For citation: Pechegin D.A. (2024) Liability and the Digital Age: Comparative Analysis of the Australian, South African and CIS States Legislative Approaches. *Legal Issues in the Digital Age,* vol. 5, no. 4, pp. 92–112. DOI:10.17323/2713-2749.2024.4.92.112

Introduction

The specific set of means of criminal law protecting the currency sphere in the state is determined by many factors; among them economic ones are of primary importance. Therefore approaches to the construction of a set of these means may vary depending on the economic system.

States with a market economy establish criminal prohibitions in the currency sphere, mainly concerning counterfeiting of currency and currency valuables, as well as money laundering. Countries with a different, for example mixed, economic system are characterized by the consolidation at the legislative level of additional means of criminal protection of the currency sphere, including rules on liability for failure to return funds from abroad, smuggling, etc.

At the same time, differences in the type of economic systems of such states in no way predetermine the impossibility of conducting a comparative legal study of their approaches to criminal-legal protection of the currency sphere, especially taking into account the dependence of money on the legal basis. And, on the contrary, the coincidence of the type of economic systems of two or more countries, as well as the commonality of prohibitions provided for in their criminal legislation, in the digital age [Khabrieva T., Chernogor N., 2018] cannot serve as correct grounds for confirming the thesis on the relevance of such foreign experience, since the economic system of a single state, especially a mixed one, is historical, that is, it depends on the characteristics of the region, the amount of resources and other conditions that differently affect the nature of the patterns of economic processes within society, and, consequently, the vector of transformation of the means of criminal-legal protection of relations in the monetary sphere.

Thus, the economic system of the Russian Federation has many features of a mixed type. Taking this into account, and also based on the similarity of trends in counteracting criminal encroachments in the currency sphere, in comparative legal terms, researchers pay attention to the experience of the CIS member states.

In particular, using the examples of the Republics of Kazakhstan, Belarus, Uzbekistan, etc., issues of criminal liability for evasion of repatriation of funds, concealment of funds in foreign currency, etc. are analyzed [Kucherov I., 2021]. However, despite the commonality in approaches to regulating the means of criminal-legal protection of the currency sphere and a certain coincidence of the type of economic systems, the experience of these countries can be considered relevant only in part.

According to the World Bank assessment[1] despite the conditions of unprecedented sanctions pressure in 2023, the economy of the Russian Federation, based on gross domestic product at purchasing power parity, took 4th place among all economies in the world, ahead of countries like Germany (6th place), France (9th place), Great Britain (10th place), second only to China, the USA and India (1st, 2nd and 3rd places in the ranking, respectively). For comparison, the CIS states occupy much more modest positions in this ranking: Kazakhstan (38th place), Uzbekistan (59th place), Belarus (68th place), Azerbaijan (75th place), Tajikistan (128th place), etc.

Similar results were recorded when turning to the analysis of international gold and foreign exchange reserves of the noted states in 2023, the volume of that significantly affects the stability of relations in the currency sphere. In this case, the Russian Federation took 6th place in the world, behind the United States (4th place), but significantly ahead of Germany (12th place), France (14th place), Great Britain (20th place), as well as CIS states like Kazakhstan (49th place), Uzbekistan (52nd place), Azerbaijan (71st place), Belarus (83rd place), Tajikistan (108th place), etc.[2]

---

[1] Gross domestic product 2023. PPP (current international $) // World Development Indicators database. Available at: https://data.worldbank.org/indicator/NY.GDP.MKTP.PP.CD?start=1990&end=2023&view=chart (accessed: 29.07.2024)

[2] Total reserves (includes gold, current US$) // World Bank. Available at: http://data.worldbank.org/indicator/FI.RES.TOTL.CD (accessed: 29.07.2024)

In addition to the above, it also seems important to draw attention to the fact many means of criminal law protecting currency sphere in the Russian Federation and the CIS states are similar, that prevents the use of comparative methodology to substantiate the results of the study. Thus, the Criminal Code of the Republic of Belarus provides for provisions on liability for the production, storage or sale of counterfeit money or securities (Article 221), failure to return from abroad by an individual entrepreneur or official of a legal entity funds in an especially large amount, subject in accordance with the legislation of the Republic of Belarus to mandatory transfer to accounts in an authorized bank of the Republic of Belarus (Article 225), legalization ("laundering") of funds obtained by criminal means, that is, the performance of financial transactions with funds obtained by obviously criminal means, in order to give a legitimate appearance to the ownership, use and (or) disposal of these funds for the purpose of concealing or distorting the origin, location, placement, movement or actual ownership of these funds (Article 235), etc.

Similar provisions are enshrined in the criminal legislation of other CIS states. In this regard, the commonality of approaches to the regulation of the specified means of criminal-legal protection of the monetary sphere, as well as the uniform historical conditions of the formation and development of their legal system, do not allow the integration requirements of comparative legal research to be met in order to obtain its proper results [Kudratov M., Pechegin D., 2021], excluding the digital sphere[3]. That is why the article took into account such jurisdiction as Australia, South Africa and some CIS countries (on a general example of the Republic Uzbekistan).

---

[3] The digitalization of the sphere of financial relations, the spread and popularization of cryptocurrencies, the introduction of artificial intelligence and distributed ledger technologies (blockchain) into the sphere of public relations today form a completely new financial and digital ecosystem of public relations, which can seriously change the balance of power of financial market participants around the world. Nevertheless, despite all the positive aspects of the introduction of modern financial technologies into public and state life, it is necessary to state an insufficient degree of predictability of these phenomena in order to ensure effective protection of the national monetary system and the realization of citizens' rights and freedoms. In the absence of proper legal protection for citizens, researchers tend to assess the risks in the field of digital finance very highly. Many countries continue to develop regulatory regulations and means of protecting public relations that develop in the process of using digital financial instruments. The complexity of this regulation will create conditions for ensuring an appropriate level of protection of the national economy and the rights of citizens, including by criminal law means.

1. Australia: Special Attention to Tax Evasion and "Money Laundering" within the Digital Currencies

The criminal legislation of Australia largely repeats (or reproduces) the approaches and traditions approved in the UK, including in the field of countering currency crimes. This circumstance leads to the possibility of a concise presentation of the experience of the specified jurisdiction, which, at the same time, has own characteristic features.

Leaving aside the traditions common with the United Kingdom of regulating the norms on criminal liability for fraud, that is quite common in the field of currency and monetary circulation, it is useful to focus on some features of the reflection in the sector Australian legislation of measures to counter money laundering (legalization), counterfeiting and smuggling of cash and monetary instruments.

1.1. "Ordinary" Monetary Crimes

The composition of money laundering is fixed in an independent part 10.2 (Section 400) of the Criminal Code of Australia and provides for criminal liability measures not only for transactions with money and property obtained by criminal means, but also with those funds (property) that became or should have become a means of committing (instrument) a crime. At the same time, the components of the specified act are classified depending on the size of legalized (laundered) property in Australian dollars: from 1,000 to 10,000 (section 400.7); from 10,000 to 50,000 (section 400.6); 50,000 to 100,000 (Section 400.5); 100,000 to 1,000,000 (Section 400.4); 1,000,000 to 10,000,000 (section 400.3); over 10,000,000 (section 400.2B). Each of these compounds has own measures of criminal legal impact.

Thus, in the case of legalization of money or property in excess of 10,000,000, a sentence of life imprisonment may be imposed. The amount of punishment in the form of imprisonment for legalization for a smaller amount is reduced, respectively, proportionally and in general can be up to 25, 20, 15, 10, 5 years and 12 months [Kucherov I., Zaytsev O., Nudel S., 2020: 276]. At the same time, depending on the circumstances of the case, the judge may appoint in place of the specified or as an additional punishment penalty units, the maximum size of which is set in the marked sections.

Counterfeiting of money and monetary instruments is subject to criminal prosecution in Australia under the provisions of the Federal Currency

Offences Act 1981. By this act the manufacture of counterfeit money and securities, their sale or introduction into circulation, purchase or sale, possession for the purpose of sale, import or export from the country are considered a crime, for which penalties may be imposed in the form of imprisonment (for individuals) for up to 14, 12, 10 and 10 years, respectively, or penalty units (for legal entities) in the amount of 750, 600 or 500 dollars. Also, as in the United Kingdom, Australian legislation provides for liability measures for counterfeiting out-of-circulation banknotes if a person has not complied with the requirements of the Copyright Act of 1968 and the Guidelines for the Reproduction of Banknotes[4].

It is noteworthy in this regard that the Law on Currency Crimes of 1981 specifically identifies offences providing for criminal liability measures for: manufacture, possession, purchase or sale of equipment, machine tools, other items intended for counterfeiting, as well as paper and paints (imprisonment for up to 10 years); theft or removal from the restricted territory of enterprises engaged in printing banknotes and minting coins, any equipment or parts thereof and materials (including paints) intended for the manufacture of banknotes (imprisonment for up to 10 years); dissemination of information about the means and methods of self-production of counterfeit banknotes and coins, as well as disclosure patented, confidential information on technologies for the manufacture of genuine banknotes (imprisonment for up to 5 years); intentional damage or destruction of Australian banknotes or coins in circulation (imprisonment for up to 2 years); manufacture and import into the country of imitation (comic, souvenir, etc.) banknotes similar to genuine Australian banknotes and capable of misleading a citizen about their authenticity (imprisonment for up to 2 years). For the commission of each of these acts, the court may appoint penal units instead of the main one or as an additional punishment, including in relation to legal entities.

Just as in the United Kingdom, in Australia the grounds for applying criminal law measures against a person for violating the procedure for moving cash or monetary instruments across the border are fixed in the provisions of sector legislation on countering money laundering, namely the federal Law on Combating Money Laundering and Terrorist Financing of 2006. Nevertheless, Article 53 of the Act expressly establishes responsibil-

---

[4] Reproducing Banknotes Guidelines // The Reserve Bank of Australia. Available at: https://banknotes.rba.gov.au/legal/reproducing-banknotes/ (accessed: 22.08.2024)

ity for the undeclared import into and export from Australia of monetary instruments in the amount of over 10,000 Australian dollars. The specified act is punishable by imprisonment for up to 2 years and (or) the appointment of penal units [Kucherov I., Zaytsev O., Nudel S., 2021: 264].

1.2. Digital "Monetary" Crimes

In Australia digital currencies are subject to criminal law regulation related to non-payment of taxes and fees, as well as combating the legalization (laundering) of funds, gambling and the issuance of tokens (digital currency). In accordance with the document "Tax regime of digital currencies"[5] digital financial instruments in the form of digital currencies are neither legal tender nor a currency of value in Australia. Moreover, they cannot be subject to the legal regime for services or goods.

Digital currencies in Australia are an intangible asset, the operation of which may be accompanied by taxable income for the user. For this reason, an obligation has been introduced to retain operational information and electronic data on all transactions with digital currencies made by a user of a particular network, including the time, purpose, type, quantity, and equivalent amount of transactions in national currency. The legal regime for taxation of transactions with digital financial instruments varies depending on the purpose of their implementation, which can be of a personal, business or stock exchange nature [Clark J., Ryznar M., 2019: 70].

Short-term transactions for the acquisition and sale of digital financial instruments for the purpose of acquiring items for personal use are not subject to taxation, unlike investment activities. The sale or exchange of purchased digital currency at a higher price, as a general rule, involves the payment of capital gains tax, taking into account the market indicators of the value of assets on "authoritative digital currency exchanges". An exception is, for example, a situation of network division and the emergence of a new branch of the same block chain, called a fork.

The exchange of pre-fork coins for new ones will not entail any consequences from the standpoint of the need to fulfill the taxpayer's obligation, but only until the moment of exchange or sale of such funds subsequently.

---

[5] Crypto asset investments // Australian Taxation Office. Available at: https://www.ato.gov.au/general/gen/tax-treatment-of-crypto-currencies-in-australia--specifically-bitcoin/ (accessed: 19.06.2024)

Responsibility for tax crimes in Australia is very specific, since it is regulated in detail in special industry legislation, while the norms of the Criminal Code of Australia, in fact, are blanket. The most common are the following socially dangerous acts in the tax sphere: illegal financial gain, tax fraud, conspiracy to defraud and tax evasion. Each of them is an independent crime violating a specific article of sections 134 and 135 of the Criminal Code of Australia. For example, committing a crime related to obtaining financial gain by deception (Article 134.2 of the Criminal Code) is punishable by imprisonment for a term of 10 years. Knowingly obtaining a financial benefit illegally carries a penalty of 12 months' imprisonment. However, the tax offences outlined above do not contain any reference to the special requirements that must be met in connection with the protection of financial and digital relations. In other words, cryptocurrencies in this regard act as a means of committing a tax offence under Australian criminal law [Lane A., Adam L., 2023].

The Australian Criminal Code contains only one reference to digital currencies in the part related to counteracting terrorism. According to Article 100.1 of the Australian Criminal Code, funds are legal documents or documents in any form, including electronic or digital, confirming ownership of or interest in such property or assets, including, but not limited to, bank loans, travellers' cheques, bank cheques, transfers, shares, securities, bonds. This reference is directly related to legislative changes in 2017 [Lane A., Adam L., 2023: 148], when digital currency was recognized as a medium of exchange for the purposes of Australia's Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2017[6].

According to the Australian Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (hereinafter referred to as the 2006 Act)[7] digital currency means:

a) a digital representation of value that is used as a medium of exchange, a store of economic value or a unit of account, or consideration for the supply of goods or services, that is not issued by or held by a public authority but is fungible with money (including by means of crediting funds to

---

[6] Commonwealth. Parliamentary Debates. House of Representatives. 17 August 2017. P. 8833 (Michael Keenan, Minister for Justice and Minister Assisting the Prime Minister for Counter-Terrorism).

[7] Anti-Money Laundering and Counter-Terrorism Financing Act 2006 // Available at: https://www.legislation.gov.au/Details/C2019C00011 (accessed: 02.08.2024)

an account) and is generally available to members of the public without restriction;

b) a means of exchange or credit for digital processes that is declared to be digital currency under the AML/CFT/CFTP Regulations, but does not include any rights or things that are not considered to be digital currency under the AML/CFT/CFTP Regulations for the purposes of the 2006 Act. However, it is not legally classified as property. In Australia, AUSTRAC is the Registrar of Digital Currency Exchanges under Part 6A of the 2006 Act. Only a person who is registered with AUSTRAC may buy and sell digital currency.

Under section 76A(1) of the 2006 Act, a person (called the first person) must not provide a registered digital currency exchange service to another person unless the first person is a registered digital currency exchange service provider. A breach of this prohibition is an offence and carries a criminal penalty of imprisonment for 2 years and/or 500 penalty units.

A repeated single commission of such actions entails a punishment in the form of imprisonment for a term of 4 years and (or) 1000 fine units. Recidivism is punished more severely. Repeated multiple commission of the described actions is punishable by 7 years of imprisonment and (or) 2000 fine units, which is the maximum punishment under this article. Article 142 of the 2006 Law also provides for the elements of an offence related to the conduct of 2 or more transactions by a person (the first person) with the aim that each of the transactions does not lead to threshold values, the excess of which implies the need for legal justification of the transaction to state authorities. The first person to carry out or cause another person to carry out transactions in such a manner or form with the sole or dominant purpose of procuring or attempting to procure that money, digital currency or property involved in the transactions was transferred in a manner or form that would not result in a threshold transaction that would be reportable under section 43 is guilty. This is because registered exchanges must collect and verify the identity of their customers and report to AUSTRAC details of suspicious matters and transactions involving $10,000 or more of fiat currency involved [Lane A., Adam L., 2023: 153]. These laws apply when customers exchange digital currency for money or vice versa. Failure to comply with control or verification, i.e. committing the above acts, is punishable by imprisonment for 5 years and/or 300 penalty units.

Crypto currency used in gambling (casinos) in Australia is equivalent in status to physical casino chips, only expressed in digital form. In contrast, tokens cannot be a tool for conducting gambling events and are a licensed digital product associated with crowd funding processes (ICO). Accordingly, the above regulation and protection measures do not apply to these categories of digital entities due to the special specificity of the procedure for their acquisition and localized use.

However, this fact does not imply the exclusion of criminal law remedies for the protection of participants in public relations arising in the process of issuing and turnover of tokens or other digital entities. This is due to the general prohibition of behavior that can mislead or deceive, including in the context of the digital finance sector. Such laws and rules may apply even if tokens (ICO) or digital assets are issued, traded or sold in offshore jurisdictions. It is noteworthy that the specific nature of digital entities themselves dictates the need for extraterritorial extension of the Australian criminal law[8]. In this regard, the theft of citizens' funds, their deception, and other illegal actions related to these digital entities are not singled out in Australian legislation as separate offenses, but involve the qualification of the act within the framework of specific provisions provided for by the Criminal Code of Australia and industry legislation.

2. South Africa: Emphasis on Interconnection between Digital and Cyber Crimes

South Africa Republic, like Australia, is one of the jurisdictions in which the legal space is built taking into account the traditions of common law family. This means that the norms on criminal liability for ordinary currency crimes in the ordinary and statutory law of South Africa are defragmented, that is, they are distributed among many acts and (or) judicial decisions. Nevertheless, despite the difficulty of finding norms on liability for currency crimes in South Africa, we note that the provisions of the acts reflect the specifics of criminal prosecution for counterfeiting, money laundering and money smuggling.

2.1. "Ordinary" Monetary Crimes

Under provisions of the Prevention of Counterfeiting of Currency Act 16 of 1965 (as amended 31 March 2003) it is illegal to counterfeit any currency. So, specific criminally punishable acts are classified in this act into

---

[8] Available at: https://asic.gov.au (accessed: 02.08.2024)

groups, taking into account the sanctions for their commission. Accordingly, four groups of acts are distinguished for imprisonment terms:

not exceeding fifteen years;

not exceeding five years;

not exceeding three years;

not exceeding twelve months.

For instance, any person shall be guilty of an offence and liable on conviction to imprisonment for a period not exceeding fifteen years, if he or she: (a) counterfeits or performs any part of the process of counterfeiting any current coin; (b) forges or alters a bank note; (c) utters, tenders or accepts any counterfeit coin, knowing it to be counterfeit, or a forged or altered bank note, knowing it to be forged or altered; (d) with intent to counterfeit current coin or to forge a bank note, makes, mends, obtains, has in his possession or disposes of any tool, instrument or machine, which (i) intended for making any counterfeit coin or forged bank note, (ii) intended for the marking of coin round the edges with letters, grainings or other marks or figures resembling letters, grainings, marks or figures round the edges of any current coin, or (iii) capable of being used for preparing any material for receiving any impression resembling that on any current coin; (e) gilds, silvers or colors any piece of metal of a size or figure fit to be coined, for the purpose of coining it into counterfeit coin; (f) makes any piece of metal into a size or figure fit to be coined, with intent to facilitate the coining therefrom of counterfeit coin or for the purpose of coining therefrom counterfeit coin; and (g) impairs, diminishes or lightens any current coin with intent that such coin when so impaired, diminished or lightened may pass as current coin.

The other acts in the context of counterfeiting are divided into the above-mentioned groups as follows (Fig. 1).

Despite the indicated differentiation of responsibility for certain stages of counterfeiting, it is important to pay attention to the fact that the subject of the crime is legal tender, including banknotes and coins, as well as counterfeit coins (not in circulation) and the means of their manufacture.

Money laundering is prosecuted in South Africa according with the Prevention of Organized Crime Act № 121 of 1998. By chapter 3 of the Act it is criminally punishable to legalize the proceeds of criminal activity, as well as to assist in the commission of relevant actions or the storage, possession and use of criminal proceeds.

imprisonment for a period not exceeding five years	• without lawful authority or excuse has in his or her possession any counterfeit coin or any forged or altered bank note; imports or receives into the Republic any counterfeit coin or any forged or altered bank note; or exports from the Republic or puts or takes or causes to be put or taken on board any ship, vessel, boat, aircraft or vehicle for the purpose of being so exported, any counterfeit coin or any forged or altered bank note; • buys, sells or is in possession of a piece of metal referred for the purpose of coining it into counterfeit coin or with intent to facilitate the coining therefrom of counterfeit coin or for the purpose of coining therefrom counterfeit coin.
imprisonment for a period not exceeding three years	• without lawful authority or excuse has in his possession or disposes of or in any way deals with any filing or clipping, or any gold or silver bullion, or any gold or silver in dust, solution or otherwise, produced or obtained by impairing, diminishing or lightening current coin, knowing that it has been so produced or obtained
imprisonment for a period not exceeding twelve months	• with intent to defraud, utters, tenders, disposes of or otherwise uses as current coin any medal or piece of metal which is not current coin; • without lawful authority or excuse defaces any current coin by stamping thereon any word, letter, device or mark

Fig. 1

A distinctive approach of South Africa to the regulation of criminal liability for this act is the establishment of a single sanction for the commission of these crimes, that is, regardless of the degree of involvement directly in the legalization of criminal proceeds. So, according to section 8 any person convicted of an offence contemplated in Chapter 3 (sections 4–6) shall be liable to a fine not exceeding R100 million, or to imprisonment for a period not exceeding 30 years.

It is important criminal liability arises for this act even if any transaction or action has not yet acquired legal force. That is, criminal liability for legalization in South Africa will also occur if actions are initiated with the intention of enriching oneself or another person through criminal income, including in the context of complicity in concealing or withdrawing property from the jurisdiction of the state. Thus, this crime is committed by any person who knows or should have reasonably known that the property is or forms part of the proceeds of illegal activities, and (a) enters into any agreement or participates in any arrangement or transaction with anyone in connection with this property, regardless of whether does such an agreement, arrangement or transaction have legal force or not; or (b) performs any other actions in connection with such property, regardless of whether they are performed independently or jointly with any other person, that have or may have consequences—(i) concealment or disguise the nature, source, location, disposition or movement of said property or ownership thereof or any interests that anyone may have in relation to this; or (ii) providing an opportunity or assistance to any person who has committed or is committing an offense, whether in the Republic or abroad — (aa) to avoid prosecution; or (bb) to seize or reduce any property acquired directly or indirectly as a result of the commission of an offense, is considered guilty of committing an offense.

Finally, South African law establishes liability for smuggling cash or monetary instruments, but in the context of liability for violation of customs clearance rules. Thus, excess currency in terms of South African Reserve Bank (SARB), Exchange Control Regulation is any amount in excess of R25 000 or any foreign currency is convertible to Rand in excess of R25 000. Travellers must obtain written permission from the SARB before entering or leaving South Africa with excess currency. Travellers may on voluntary basis declare currency in their possession through the online traveller declaration form or the manual Traveller Card (TC-01). The cash/currency to be declared is South African bank notes as well foreign currency, securities and gold[9].Violation of this obligation may result in criminal prosecution of a person if, during customs control, surpluses are found with him, which he should have declared, while there are signs of an offence.

Under Section 15 of South African Customs And Excise Act 91 Of 1964 (with amendments) any person entering or leaving the Republic shall, in such a manner as the Commissioner may determine, unreservedly declare(a) at the time of such entering, all goods (including goods of another person) upon his person or in his possession which he brought with him into the Republic which (i) were purchased or otherwise acquired abroad or on any ship, vehicle or in any shop selling goods on which duty has not been paid; (ii) were remodelled, processed or repaired abroad; or (iii) are prohibited, restricted or controlled under any law; (b) before leaving, all goods which he proposes taking with him beyond the borders of the Republic, and shall furnish an officer with full particulars thereof, answer fully and truthfully all questions put to him by such officer and, if required by such officer to do so,

---

[9] Excess Currency–External Policy SC-PA-01-06. Available at: https://www.sars.gov.za/customs-and-excise/travellers/ (accessed: 10.09.2024)

produce and open such goods for inspection by the said officer, and shall pay the duty assessed by such officer, if any, to the Controller.

These goods also include excess currency in cash and in the amount indicated above. So, any person who (a) deals or assists in dealing with any goods contrary to the provisions of the Act [including provisions of Section 15. — D.P.]; or (b) knowingly has in his possession any goods liable to forfeiture under the Act; or (c) makes or attempts to make any arrangement with a supplier, manufacturer, exporter or seller of goods imported or to be imported into or manufactured or to be manufactured in the Republic or with any agent of any such supplier, manufacturer, exporter or seller, regarding any matter to which the Act relates, with the object of defeating or evading the provisions of this Act, shall be guilty of an offence and liable on conviction to a fine not exceeding R20 000 or treble the value of the goods in respect of which such offence was committed, whichever is the greater, or to imprisonment for a period not exceeding five years, or to both such fine and such imprisonment, and the goods in respect of which such offence was committed shall be liable to forfeiture (Section 83 of South African Customs And Excise Act 91 Of 1964, here and after — the Act). At the same time, such goods, including excess currency, are subject to forfeiture (Section 87 of the Act).

2.2. Digital "monetary" crimes

South Africa considers the Cybercrimes and Cyber Security Bill of 2016 (hereinafter CCB) to be the foundation for the criminal law protection of financial and digital relations. By force of the Section 3 of it, it is an offence to: unlawfully and intentionally overcome any security measure designed to prevent access to data in order to obtain data located on a computer or transmitted to or from a computer system; unlawfully and intentionally possess data that a person knows to have been obtained by criminal means; possess data where there is reasonable ground to suspect that they have been obtained by criminal means, when there are no grounds for possessing such data. The commission of the offences listed in paragraphs 1 and 2 under Section 14 of the Bill is punishable by a fine and/or imprisonment for a term of up to 10 years. Possession of data under suspicion is punishable by a fine and/or 5 years in prison. At the same time, the provisions of the articles cover almost all possible ways of committing crimes in cyberspace, including hacking, phishing, use of malicious codes and social engineering tactics [Eveshnie R., 2019: 2].

Article 7 of the CCB establishes: a criminal offense is the illegal acquisition, possession, provision, receipt or use of a password, access codes or similar data or devices. These include, in particular, private keys for crypto currencies (private key), since paragraph 3 of Article 7 of the Bill establishes that information may be a secret code or PIN code, an image, a security token, an access card, a device, biometric data, a word or a set of letters and symbols used to make financial transactions or identify a user. The intentional commission of this crime for the purpose of unlawfully overcoming any security measures aimed at preventing access to data and obtaining data (CCB Article 3 (1) is punishable by a fine and/or imprisonment for up to 10 years. The commission of such acts in the presence of reasonable suspicion is punishable by a fine and/or 5 years' imprisonment.

The commission of the above acts in relation to protected computer systems (i.e. computer programs, computer storage media or computer systems under the control or exclusively used by any financial institution, public authority, including judicial authorities, or constituting critical information infrastructure) is considered a serious crime under Article 11 of the Bill and is punishable by a fine and/or 15 years' imprisonment.

Similar criminal protection measures are provided for by the CCB for the purposes of theft and fraud in cyberspace. At the same time, money laundering using new financial and digital technologies remains outside the scope of the described legislative regulation of South Africa. In other words, South African legislation does not directly describe this crime in relation to digital entities. However, given the specifics of legislative regulation in South Africa, it is not an obstacle to the criminal prosecution of money laundering since the current definition of money laundering is not limited to offline funds and is not limited to money. According to the South African Law Reform Commission, money laundering is "the manipulation of illegally acquired wealth in order to conceal its true source or nature. As crypto currency qualifies as data, and not money in the legal sense, this provision could therefore be used to prosecute any cyber fraud (including Ponzi schemes) that uses crypto currency as a tool in the facilitation of the fraud. However, the onus is on prosecutors and the courts at large to interpret this provision in so far as it relates to such offences" [Eveshnie R., 2019: 6].

As it mentioned by R. Eveshnie, the provisions of the CCB can be used to effectively investigate and successfully prosecute offenses committed with or directed at crypto currencies (and other new online technologies).

However, their investigation can be hampered by a lack of understanding on the part of investigators and prosecutors. In this context, it may be necessary to rely on existing common law and statutory law criminalizing money laundering approach.

3. CIS States and Approach of the Republic of Uzbekistan: the Trend to Criminalizing Crypto Crimes

The CIS countries largely follow the approach to regulating liability for currency crimes are perceived in the Russian Federation. The appeal to the criminal legislation of many CIS states, as mentioned above, generally makes it possible to identify in their structure such types of currency crimes as money laundering, counterfeiting, etc. From these positions, such jurisdictions are of interest within the framework of the association of states under consideration, in which these approaches have been developed taking into account the digital transformation of the sphere of economic relations in all its diversity. In this study, the experience of Uzbekistan is used as an example of such a jurisdiction.

3.1. "Ordinary" Monetary Crimes in the Republic of Uzbekistan

The criminal legislation of Uzbekistan reflects both fairly common "ordinary" monetary crimes and their individual varieties that deserve special attention. So, the Criminal Code of the Republic consists provisions on liability for manufacturing or sale of counterfeit bank notes (banknotes), metal coins, excise stamps, as well as securities or foreign currency or securities in foreign currency. These crime described in Article 176 of the Code are punishable by restriction of liberty from two to five years or imprisonment for up to five years.

In addition, Article 182 establishes liability for the movement of goods or other valuables across the customs border of the Republic in addition to or with concealment from customs control or with the fraudulent use of documents or means of customs identification, or involving non-declaration or declaration of a wrong name, committed on a large scale. These crimes are punishable by a fine of up to three hundred basic calculation units or compulsory community service of up to 480 hours or correctional labor of up to two years or restriction of liberty of two to five years or imprisonment of up to five years. However, criminal prosecution for this crime becomes possible only after the application of an administrative penalty for the same action, that is using the mechanisms of administrative prejudice.

More interesting for the review are the compositions of “ordinary” monetary crimes that are not regulated in the criminal legislation of the Russian Federation. Among these, one can distinguish “Illegal acquisition or sale of currency valuables” (Article 177) and “Concealment of foreign currency” (Article 178).

So, illegal acquisition or sale by citizens of currency valuables are punishable by a fine from seventy-five to one hundred basic calculation values or correctional labor from two to three years or restriction of liberty for up to one year or imprisonment for up to one year, but only if it was committed after the application of an administrative penalty for the same actions (the mechanisms of administrative prejudice). At the same time the features of exemption from criminal punishment are established — a person who voluntarily reported an impending or committed crime and actively contributed to its disclosure is not liable.

On the contrary, another sample of monetary crime do not consist the link to administrative prejudice. Deliberate concealment of foreign currency to be credited to accounts in authorized banks of the Uzbekistan by persons engaged in foreign exchange transactions at enterprises, institutions or organizations, is punishable by a fine from seventy-five to one hundred basic calculation units or deprivation of a certain right from three to five years or restriction of liberty from two to five years or imprisonment for up to five years. At the same time, a person who has committed a crime for the first time, provided for in reliable manner or out of self-interest or by prior agreement of a group of persons, shall be released from liability if, within thirty days from the date of detection of the crime, he voluntarily provided for the transfer of hidden foreign currency to accounts in authorized Uzbekistan banks.

So, exemption from criminal liability will not mean the absence of a crime event or neutralize the fact of criminal prosecution of a particular person. Such a person is released from responsibility, but with the recognition of the composition of the committed act.

3.2. Crypto crimes in the Republic of Uzbekistan

In the legal space of the CIS, tools for combating cybercrime related to the illegal use of digital financial instruments are being actively developed.

In particular, in Article 2 of the Model Law on Combating Cybercrime defined that cybercrimes are: unauthorized access to, seizure of, or influence on digital information; legalization (laundering) of funds or other property acquired by criminal means using ICT; other crimes committed in cyberspace, that is, in the digital environment. It is noteworthy that one of the versions of the presentation of the norm on criminal liability for committing these acts indicates (Article 9, option 2) that criminal prosecution of an individual does not exclude criminal prosecution of a legal entity and vice versa. Special attention is paid to building international cooperation in the field of combating cybercrime to maintain financial security, the goals of which, among other things, are: prevention, detection, and suppression of international transfers of assets used or intended to commit cybercrimes, as well as those obtained as a result of committing cybercrimes; return of the said assets moved abroad (Article 11 of the Law).

In addition, the other Model Law, that is On the Digital Financial Assets, defines the legal basis for the liability of holders and participants in the digital financial assets market. In particular, it is stipulated that subjects of the digital financial assets market are liable in accordance with national legislation, the rules of the information system and the lawful terms of the contracts concluded by them. In addition, crypto currency holders are liable for violating national legislation on the circulation of crypto currency throughout the CIS, while crypto currency that is a source of income obtained by criminal means may be confiscated (Articles 11, 21).

In the context of the focus on solving the problem of ensuring the stability of the national currency and national currency sovereignty, the instruments proposed in the said acts, interconnected with the legal protection of the currency sphere, including criminal law means, are integrated into the national legal orders of the CIS states in different ways. At their core, certain integrative solutions come down to recognizing various digital financial instruments as the subject of currency crimes. At the same time, there are cases of criminalization of the illegal use of the auto-identification data of the owner of a digital wallet.

Thus, the basis for combating cybercrime in the Uzbekistan is such a currency crime as legalization of proceeds from criminal activity (Article 243 of the Criminal Code of the Republic). It is noteworthy disposition of this norm does not contain any references to digital financial instruments or digital information, however, the Resolution of the Plenum of the Supreme Court of the Republic of Uzbekistan of 11.02.2011 No. 1 “On issues of judicial practice in cases of legalization of proceeds from criminal activity" explains taking into account Recommendation 15 of the Financial Action Task Force on Money Laundering (FATF), crypto-assets (cryptocurrency) may also be related to proceeds from criminal activity, that is, to the subject of this act. At the same time, the Criminal Code of the Republic also criminalizes crimes, the additional object of encroachment of that are relations developing in the field of digital technologies.

Among them it is important to note crimes provided for in Articles 278.8 "Violation of legislation in the sphere of crypto-assets circulation" and 278.9 "Illegal implementation of mining activities" of the Criminal Code.

The crime provided for in Article 278.8 of the Criminal Code is designed with an administrative prejudice and establishes criminal liability for repeated illegal acquisition, sale or exchange of crypto-assets, the activities of service providers in the field of crypto-assets without obtaining a license in the established manner, or the implementation of transactions with anonymous crypto-assets by service providers in this area. The maximum penalty is imprisonment for up to one year. At the same time, grounds for exemption from criminal liability are also provided if a person voluntarily reported a crime being prepared or committed and actively contributed to its disclosure.

Article 278.9 of the Uzbekistan Criminal Code provides a person engaged in the mining of anonymous crypto-assets or mining in violation of the established procedure may be punished with imprisonment for up to one year. This crime also provides for an administrative prejudice and a similar ground for exemption from criminal liability as described above.

It is noteworthy in accordance with Section 8 of the Criminal Code of the Uzbekistan, the meaning of the terms "Crypto-asset" and "Mining" is defined. In particular, a crypto-asset is a property right representing a set of digital records in a distributed data registry that has value and an owner; mining is the activity of maintaining a distributed data registry, creating blocks and confirming their integrity by performing computational operations.

In this case, it is very difficult to understand without explanations from the regulator or the law enforcement officer: what exactly is meant by such an activity? It is a disadvantage of the described approach. So, for comparison, in German–speaking legal systems, mining is considered an entrepreneurial activity in cases where it corresponds to the general understanding of entrepreneurial activity — a focus on systematic profit-making, independence, risk-taking, etc. [Ehrke-Rabel T., Eisenberger I., Hödl E. et al., 2017]. In addition, positions are expressed regarding the need to differentiate responsibility for illegal mining depending on its type — solo-mining; pool-mining; cloud mining [Enzinger N., 2017].

Conclusion

Despite all the controversial positions in the vast majority of leading jurisdictions, regulation of the financial and digital sphere of relations is not focused on maintaining the protection of the rights and freedoms of citizens in the virtual space. All protective measures developed or approved today, including criminal law ones described above, are mostly based on the so-called analog legal regulation, i.e. approaches to regulating public relations. For these purposes most countries seek to develop measures to counteract socially dangerous acts in the financial and digital sphere of relations, specifying the distinctive features of tax crimes, clarifying the legislation or adjusting judicial practice in the sphere of counteracting the legalization (laundering) of funds, recognizing new digital entities as a means (method) of committing crimes already established in certain norms of criminal legislation. In this context, it is important to pay attention to the prospects for improving the criminal law regulation of these relations under the Criminal Code of the Russian Federation in the context of not only legalization, but also the composition of tax and other crimes, especially in the context of the fact that digital tools can legally be attributed to property [Nudel S., 2023]. However, a sufficiently detailed explanation of such innovations at the level of the Supreme Court of the Russian Federation will be required to exclude a formal approach to assessing what happened. At the same time the sphere of financial and digital relations is something completely new in terms of principles and operating environment. It is enough to return to the examples of crypto jacking qualification mentioned above. It seems that the experience of building a system of criminal law protection for participants in digital relations in South Africa and Uzbekistan is could be quite in demand in the domestic legal space.

References

1. Clark J., Ryznar M. (2019) Improving Bitcoin Tax Compliance. *University of Illinois Law Review*, vol. 2019, pp. 70–76.

2. Ehrke-Rabel T., Eisenberger I., Hödl E. et al. (2017) Bitcoin-Miner Als Prosumer: Eine Frage Staatlicher Regulierung? Dargestellt Am Beispiel Des Glücksspielrechts. *Austrian Law Journal*, pp. 188–223 doi: 10.2139/ssrn.3036322.

3. Enzinger N. (2017) Mining von Kryptowährungen: Ist das Mining von Bitcoins umsatzsteuerbar? *Steuer- und Wirtschaftskartei*, vol. 23/24, pp. 1013–1021.

4. Eveshnie R. (2019) Analyzing Investigation and Prosecution of Cryptocurrency Crime as Provided for by the South African Cybercrimes Bill. *Statute Law Review*, vol. 41, no. 2, pp. 1–14. doi: 10.1093/slr/hmz001.

5. Khabrieva T., Chernogor N. (2018) The Law in the Digital Reality. *Zhurnal rossiyskogo prava*=Journal of Russian Law, no. 1, pp. 85–102 (in Russ.)

6. Kucherov I. (2017) Elements of the Financial Security and its Legal Support. *Zhurnal rossiyskogo prava*=Journal of Russian Law, no. 6, pp. 69–79 (in Russ.)

7. Kucherov I. (ed.) (2021) Criminal Law Protecting Financial and Budgetary Sphere: a manual. Moscow: Konrtakt, 284 p. (in Russ.)

8. Kucherov I., Zaitsev O., Nudel S. (eds.) (2020) Criminal Law and Economic Activity (the Ratio of Private and Public Interests): a guide. Moscow: Kontrakt, 392 p. (in Russ.)

9. Kucherov I., Zaitsev O., Nudel S. (eds.) (2021) Economic Security: Criminal Law Enforcement Mechanisms. Moscow: Kontrakt, 320 p. (in Russ.)

10. Kudratov M., Pechegin D. (2021) On the German Science of Interpretation and Construction of Comparative Legal Research. *Rossiyskiy zhurnal pravovykh issledovaniy*=Russian Journal of Legal Studies, no. 4, pp. 55–62 (in Russ.)

11. Lane A., Adam L. (2023) Crime and Crypto Currency in the Australian Courts. *The Monash University Law Review*, vol. 48, no. 3, pp. 146–190. doi: 10.26180/22207720.v2.

12. Nudel S. (2023) Modernization of Criminal Policy: Issues of Legal Regulation. *Zhurnal rossiyskogo prava*=Journal of Russian Law, vol. 27, no. 1, pp. 5–22 (in Russ.)

13. Werbach K. (2018) Trust, but Verify: Why the Blockchain Needs the Law'. *Berkeley Technology Law Journal*, vol. 33, no. 2, pp. 489–552.

Information about the author:

D.A. Pechegin — Candidate of Sciences (Law), Leading Researcher.

The article was submitted to editorial office 14.08.2024; approved after reviewing 10.09.2024; accepted for publication 30.09.2024.

Legal Issues in the Digital Age. 2024. Vol. 5. No. 4.
Вопросы права в цифровую эпоху. 2024. Т. 5. № 4.

Legal Informatics

Research article
JEL: K00
УДК:34
DOI:10.17323/2713-2749.2024.4.113.137

Artificial Intelligence in Law and Legal Analytics

Vladimir Borisovich Isakov

National Research University Higher School of Economics, 20 Myasnitskaya Str., Moscow 10100, Russia,

visakov@hse.ru

Abstract

The author discusses the concept of artificial intelligence and analyses the approaches to its concept and definitions existing in science. In a sketch of emergence of artificial intelligence the author notes artificial intelligence represents a natural stage in the development of technical devices designed to facilitate human intellectual activity. The author offers a classification of devices endowed with artificial intelligence, distinguishing between narrow (weak) AI and general (strong) AI; he outlines the most relevant areas of its development and describes the development stages. Among the spheres of possible application of devices with AI, the author lists the search for and structuring of information; identification of new connections and patterns that humans cannot see; assisting humans in professional activities; relieving humans from time-consuming and unproductive intellectual activities; management automation; assistance in making optimal management decisions. The article places a special focus on the threats and risks associated with the proliferation of AI. The author believes these include: displacement of humans from socially important spheres of activity, and job hijacking; decline in the level of education and qualification of workers leading to degradation of human intellect; corruption of humanity by idle and meaningless existence leading to its physical and cultural degradation; danger of robots making erroneous technical, economic, environmental, medical, etc. decisions; threat of failures in the operation of industrial robots and computerised control systems; particularly dangerous is the deliberate use of robots to cause harm, including the use of military and security systems capable of causing harm to people and property. The article discusses various

© Isakov V.B., 2024
This work is licensed under a Creative Commons Attribution-Sharealike 4.0 International License
https://creativecommons.org/licenses/by-sa/4.0/legalcode.en

options for granting AI a legal status. The author assumes a device endowed with artificial intelligence is a complex and autonomously operating tool of human activity, relatively independent of human person. The latter, however, is fully responsible for the consequences of the use of this tool. The author is sure it is counterproductive to artificially extend legal statuses developed for man, who is an individual endowed with consciousness and will, to AI. The article contains results of a “parallel exam” on legal analytics for students and artificial intelligence held at the Department of Law of the National Research University Higher School of Economics in May 2023. Also the author discusses specific areas and examples of the use of AI in law and legal analytics in the spheres of law -making, law enforcement, jurisprudence, and education.

Keywords

device; threats and risks of AI; intelligent robot; legal status; rulemaking; law enforcement; legal science; education.

For citation: Isakov V.B. (2024) Artificial Intelligence in Law and Legal Analytics. *Legal Issues in the Digital Age,* vol. 5, no. 4, pp. 113–137. DOI:10.17323/2713-2749.2024.4.113.137

Introduction

It is hard to find another subject discussed about as much today as artificial intelligence. The article substantiates there was a reason for artificial intelligence to appear: it represents the next natural stage in the development of machines, which replace humans in increasingly complex areas of activity.

What is artificial intelligence? What about its distinctive features, its stages of development, and types? What can artificial intelligence (AI) come to as a result of its future development? Should we be afraid of it? Should we give AI anthropomorphic status? What is the best way to use AI in production, R&D, and education? These are the theme of the article.

1. Artificial Intelligence: Concept and Attributes

Scholars understand artificial intelligence as the ability of intelligent systems to reproduce some functions of human thinking at a level comparable to human intellectual activity[1].

---

[1] Artificial intelligence. 2024. Available at: https://ru.wikipedia.org/wiki/%D0%98%D1%81%D0%BA%D1%83%D1%81%D1%81%D1%82%D0%

Systems with artificial intelligence have a number of properties differing it from other man-made systems: they are capable of solving highly complex problems only humans could solve in the past; they are relatively standalone; their behaviour is non-linear; they are capable of being creative and making heuristic-based decisions; they can self-learn; they are adaptive and interactive (can communicate with humans).

Academic and popular literature offers many definitions of AI[2]. Artificial Intelligence is understood as:

a property (attribute) of technological devices that can be achieved by means of various hardware components;

a class of devices capable of performing functions that only humans could do in the past (computers, neural networks, robots, etc.);

information processes, and sets of information technologies simulating human intellectual activity;

an interdisciplinary branch of science that studies the systems of knowledge representation by machines, etc.

Depending on the context of the theme under discussion, different understandings of artificial intelligence may be encountered in the literature.

AI research is in constant development. ChatGPT by OpenAI, the most famous and popular artificial intelligence model today, has gone through several stages in its development: "The models improved dramatically with each iteration. GPT-1, trained on the texts of about 7,000 books, could barely string sentences together. GPT-2, trained on 8 million web pages, could barely answer questions. GPT-3, trained on hundreds of billions of words from the Internet, books and Wikipedia, could almost write poetry[3]."

Two dominant approaches can be observed in the further development of artificial intelligence [Prigorov K.F., 2008]. One of these positions may be labelled as biological one. It is based on study of the mental and biological

---

B2%D0%B5%D0%BD%D0%BD%D1%8B%D0%B9_%D0%B8%D0%BD%D1%82% D0%B5%D0%BB%D0%BB%D0%B5%D0%BA%D1%82 (accessed: 20.02.2024)

[2] Available at: https://translated.turbopages.org/proxy_u/en-ru.ru.e8c58780-65d6351d-e197868d-74722d776562/https/en.wikipedia.org/w/index.php?title=Artificial_intelligence&action=history. (accessed: 20.02.2024)

[3] CEO of the Year, 2023. TIME: Digital Magazine. 6.12.2023. Available at: URL: https://time.com/6342827/ceo-of-the-year-2023-sam-altman/ (accessed: 20.12. 2023)

processes and structures that determine human intellectual behaviour. This approach aims to create a combination of natural and artificial computing systems such as a neurocomputer or biocomputer. The other one is the semiotic (sign) approach. Its distinctive feature is the study of sign systems of knowledge representation by methods of formal logic and mathematical modelling. This approach aims to create increasingly powerful and efficient knowledge bases, expert systems and logical inference systems [Evseenko S. M., 2021].

1.1. Types (classifications) of artificial intelligence systems

The classifications of artificial intelligence systems are extremely diverse and, due to AI's rapid development, have not taken any final shape. It is useful to consider some of the classifications are of particular interest for our discussion (Fig. 1).

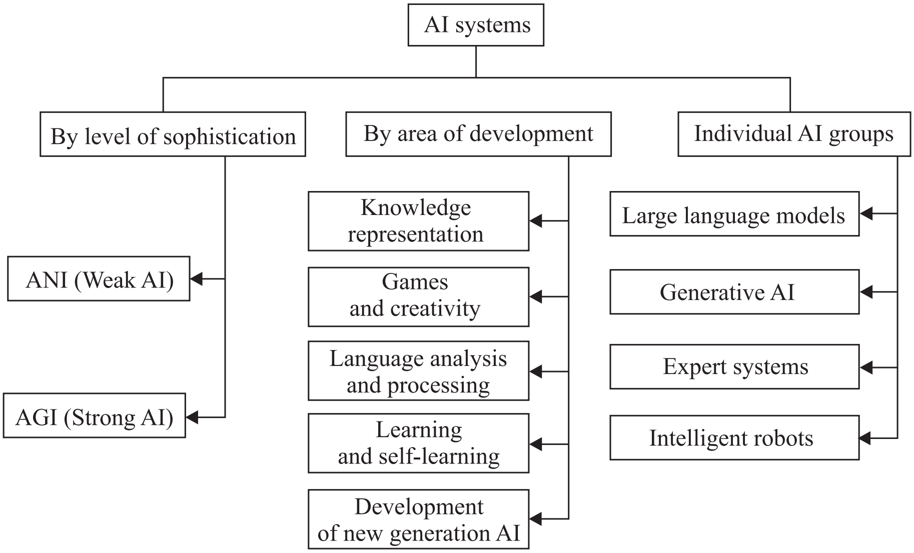


Fig. 1. Some classifications of artificial intelligence systems.

Artificial intelligence is usually divided into weak and strong one in terms of its level of sophistication[4].

Artificial narrow intelligence, sometimes named "narrow" or "application-based", aims to perform individual human functions and is there-

---

[4] Strong AI vs. weak AI: what's the difference? Available at: URL: https://new-science.ru/silnyj-ii-protiv-slabogo-ii-v-chem-raznica/ (accessed: 20.12.2023)

fore capable of solving a limited range of tasks. Systems of this type include search engines and document editors; translators; gaming computers; image, text, and speech recognisers. This category should also include chatbots; computers that create paintings, music, poetry, scholar and artistic texts; voice assistants; autopilots and similar transport management systems; management consultancy systems; medical diagnostic systems, etc.

The word “narrow” in relation to artificial intelligence should not confuse and should not be considered a pejorative. Most of these systems are quite up-to-date, develop successfully, are actively implemented in practice and increase their functionality.

Artificial general intelligence is created to solve a wide range of tasks, is comparable in terms of its functions to human intelligence, and may surpass it in the long term. The spheres of general AI application are the development and adoption of complex management decisions; maintaining the balance of natural and artificial in the human environment; decoding the human genome; identifying and eliminating the causes of incurable diseases; studying the higher manifestations of consciousness and self-consciousness; scientific and artistic creativity; creating new generations of intelligent machines. It is quilted clear that further advancement of strong artificial intelligence is not only associated with significant material and financial costs, but also has a variety of moral, ethical and legal implications.

It has a sense to outline briefly the second branch of classification, i.e. the main directions of AI development. Scholars have failed to agree on a single set of terms and definitions here, too. Nevertheless, the main lines of AI development usually include:

Knowledge retrieval, representation and utilisation: it includes processing of huge arrays of accumulated information, machine learning, computer vision, creation of expert systems for various purposes, including jurisprudence [Novikov F.A., 2010].

Gaming and creativity: in this area, AI has shown itself off most vividly and convincingly in areas such as chess computers, go and poker playing devices etc. Artificial intelligence is gradually mastering the sphere of artistic creativity: writing poetry and artistic prose, drawing pictures, composing music.

Language analysis and processing: all of humanity’s knowledge is encoded in the signs of language. That is why AI is used to create computer user interfaces, encyclopaedias and reference books, machine translations, to abstract and annotate sources, to extract facts from data sets, etc. Language learning is aimed, in particular, at creating search engines to navigate huge arrays of information accumulated. Experts estimate the quality of machine translation is gradually approaching the level of the best human translators.

Learning and self-learning: it is a high-priority and fast-growing area of AI application. AI is used to optimise educational systems and curricula, form cohesive creative teams, diagnose and build communication skills, develop learning tasks and assess the knowledge gained, etc.

Development of next-generation AI systems: things have come to a point where developers don't always fully understand the logic behind the actions of AI. With such baggage, it's clearly hard to move on to creating new generations of AI. So, AI itself is increasingly becoming the source of new ideas and cutting-edge developments.

The third column of the scheme lists individual types (groups) of AI that attract the greatest interest of researchers and practical consumers. These are large language models; generative artificial intelligence; expert systems; intelligent robots for various purposes. There are numerous comments from additional sources on each of these areas.

1.2. How does generative artificial intelligence work?

It is quite a task to explain principles of artificial intelligence in simple language, which a non-engineer can understand. So the floor is passed to a professional who has published what we think is a pretty good popular essay on the topic:

"The breakthrough with large language models happened suddenly. There hadn't been some decades-long run-up (the GPT model itself has been in development since mid-2018, which is just in a flash by the standards of history). ChatGPT jumped out of nowhere at the end of 2022. It was a qualitatively new phenomenon that confirms the second law of dialectics: quantity is transformed into quality. Just take many, many texts, make the neural network on the Transformer-architecture predict the next word and hey presto! — you get an almost thinking entity at the end. If you will, its soul, consciousness and character will be distributed in it somewhere on billions of scales, just like in the brains of each of us.

Here's an interesting question: what has that GPT learned that allows it to engage in a reasonable dialogue? Where does the magic come from?

At the same time, let's remember that the model is not just a collection of answers to known questions. That is, it is not like the Gramophone from Stanislav Lem's *The Sum of Technology*, which has 100 trillion answers recorded on it. The model knows how to generate new things and how to understand context. To me, the model understands the internal logic and patterns of the narrative, following which it can produce any text. This logic is represented as an internal system of concepts and meanings that are activated depending on the current dialogue. (...) By combining and multiplying all this together, we get a small repertoire of words from which the system can choose the next one. Since the number of possible combinations of these entities is simply astronomical, the model is capable of generating new things and constantly surprising us."[5]

1.3. Application areas of artificial intelligence

It is obvious AI may have many spheres of application even in its current forms that are far from perfect.

First, it is a strong information retrieval tool. Today mankind has access to enormous amounts of information that are simply immense. Yet it is hard to find exactly what is required in the here and now, what you need to solve your problem. AI seems to be able to do the job. It relies on databases that contain millions of pieces of information and is capable of generating optimal search algorithms.

However, as practice shows, AI also does not always perform in a satisfactory way: it answers queries inaccurately and even "hallucinates", i.e. comes up with whole lists of non-existent authors and sources. Excuses itself, apologises, but then continues in the same vein. The matter seems to be in the subtle nuances between truth and plausible fiction that the machine does not yet distinguish. Nevertheless, it can be assumed that in the near future it will be impossible to write a scholar article or publish a monograph without checking and clarifying its content with the help of AI.

Second, artificial intelligence is capable not only of searching for information, but also of creating new knowledge, i.e. of identifying new connections and relations, of finding regularities, and making discoveries, i.e. not only of using the accumulated knowledge, but also of developing it. The

---

[5] What awaits us after the emergence of strong AI, or The inescapable logic of social and technological development. Available at: URL: https://habr.com/ru/articles/733974/ (accessed: 8.01.2024)

creative possibilities of artificial intelligence have not yet been explored sufficiently. But it is obvious that it is capable of identifying patterns that have fallen outside of human attention, and thus outside of human practice[6]. The advantage of artificial intelligence is that it does not just report its discoveries, but immediately incorporates them into circulation, and begins to take them into account in building models and doing calculations.

Third, artificial intelligence can be a great assistant for humans. Basically, it is capable of doing so already. Computer assistants are widely used in information search, biology, medicine, and jurisprudence. Of course, there are serious limitations, too. In the case of decisions that affect directly the personality or can serve for the assessment of biographical facts, goals, motives, or the emotional state of a person, AI must necessarily be under human control. In these cases, humans must always make the final decisions and take full responsibility for them.

Fourth, AI can relieve humans from time-consuming and unproductive intellectual activities such as compiling tables of contents, indexes, as well as summaries, abstracts, reviews, reports, and references.

The following clarifications must be made here. Preparation of reports and briefs on the results of the work done is one of the necessary elements of the system for production and socio-cultural activity management. This system is to a great extent outdated. It is genetically linked to paperwork, to the practice of decision-making behind closed doors, and top-down implementation methods; it bears the marks of formalism and bureaucracy. In the socio-cultural sphere, the preparation of numerous, voluminous plans, reports and references that in actual fact no one needs literally stifles the creative activity and enthusiasm of teachers, university professors and officers of cultural institutions. Oftentimes, preparation of plans and reports replaces real practical activities. Should such management practices be preserved, digitised, and enhanced by artificial intelligence?

Very probably the introduction of AI leads to the revision of all links of professional-subject activity: the setting of goals and objectives, organization of work, applied technologies and, of course, management processes.

---

[6] For example, it is reported that based on statistics and biographical data of a person, the neural network has learnt to predict the approximate life expectancy of the person. See: Tell me, Neural Network, how long will I live? Available at: URL: https://storage.googleapis.com/gsc-link/www.bbc.com/f78d83b5.html (accessed: 4.01.2024)

It often turns out some employees welcome change and innovation, while the others are determined to maintain status quo.

Needless to say tasks of this nature are not solved overnight. They require well-designed strategies and tactics, time, efforts, and money. But apparently there is no other way. Experience has shown that the transfer of existing forms of bureaucratic reporting and management into the sphere of AI not only does not lead to an increase in efficiency, but can also be a significant reason for its reduction [Dobrolyubova E.I., Yuzhakov V.N., Starostina A.N., 2021].

Fifth, artificial intelligence may be used to create highly autonomous control systems operating without direct human participation. Systems of this kind are already used in some production areas, in economics, and in banking settlements. Encouraging news comes from the field of public transport, where unmanned vehicles are successfully operating: underground trains in some countries already run without a driver. Still, the autonomy of such systems is not unlimited. So, there is an obligation to provide a control level, where in case of machine malfunction or failure, a human operator steps in.

In the sphere of public administration systems with AI may take over not only relatively simple record-keeping functions, but also more complex tasks, such as calculation of taxes, pensions, payments, fines, control over their timely payment, etc. They may completely relieve people from the tedium of waiting for appointments or visiting lots of offices. Similar systems can also be created in the field of environmental control, weather monitoring, and public health. They are not only capable of observing and recording, but also of reacting automatically to dangerous deviations.

But is the application of AI systems in management always an obvious blessing? E.g., the social rating (credit) system implemented in China since 2014 raises questions. This management innovation has been widely discussed in the recent years in the media, in scientific community, and among university students[7].

Basically, various scoring tables, ratings, assessments, and registers are hardly a new phenomenon in economics and social life. E.g., credit ratings, credit histories, registers of reliable partners, etc. are widely used in busi-

---

[7] How the Social Rating in China Works. 2023. Available at: URL: https://style.rbc.ru/life/643d3f839a7947afd12e9f35?ysclid=lr1wjcqqn2846209556#p6 (accessed: 6.01. 2024)

ness. But it seems China has tried to go much further: namely, to control the behaviour of citizens in virtually all spheres of social activity, including their private life. A set of social norms have been defined at the official level. When a person violates a norm, they are deprived of access to various social benefits like the ability to travel, purchase property, stay in hotels, etc. Citizens who deserve to be trusted are rewarded in various ways and those who do not deserve to be trusted are penalised. The social rating system is implemented on the cutting edge IT base including the use of AI.

What could be the outlooks for such a system in Russia? There are various opinions on this matter. Some people think systems of this kind are not suitable for Russia, while others believe the future belongs to such systems. Moreover, there is evidence that some elements of such systems are already being implemented. For example, specialists from the Russian State Social University have created the platform "We" with probabilistic and statistical models of behavioural assessment. This project began in 2022. According to the authors of the project, social scoring will help to allocate resources in the social sphere in the best possible way[8].

The use of AI in public administration allows and even suggests various experiments. But in any case, such experiments must comply with legal and ethical norms, undergo strict and impartial academic and public expertise, be formally documented, and be within the zone of public control and prosecutorial oversight. Unfortunately, we have already seen examples to the contrary. E.g., in 1994 President Boris Yeltsin introduced the automated system Vybory (designed to carry out certain electoral actions) by a unilateral decree, without any legislative justification and without public or parliamentary discussion[9].

A report should be submitted and approved at the end of the experiment. Then, a final decision should be made whether to terminate the experiment or to develop and scale it up. Otherwise, you may see the emergence, in our country and in the whole world, of a "technotronic society," which is constrained by information technologies, extremely formalised and bureaucratised, with a ruling elite is in opposition to the people. Scientists and sci-fi writers alike are anxiously warning about it.

---

[8] Ibid.

[9] See: Decree of the President of the Russian Federation of 23.08.1994 No. 1723 On development and creation of the state automated system of the Russian Federation "Elections". Available at: URL: http://www.kremlin.ru/acts/bank/6841/ (accessed: 9.01.2024)

1.4. Dangers and risks of artificial intelligence

As has often been in the past, each successive stage of the scientific and technological revolution brings with it not only achievements and benefits, but also new threats and risks. The present stage of technological progress is no exception. What are the threats and risks posed by the widespread proliferation of devices, which are endowed with artificial intelligence and whose distinguishing feature is the ability to make decisions and act, within several limits, independently of humans? It is necessary to consider them "in reverse order": from the relatively easy ones to the more complex and fundamental ones.

A) Displacement of humans from socially significant spheres of activity; job hijacking.

It is quite obvious robots endowed with elements of intelligence are competitors to humans in the sphere of labour activity. They don't care about working conditions, don't demand higher wages and lunch breaks, don't unionise, and don't strike. The cost of robots and their functional properties already allow entrepreneurs to replace "live" labour. In terms of total societal costs, replacing human labour with machine labour should be viewed as a good thing, but things are not that simple. The matter is the modern state does not plan and does not even intend to provide decent living conditions for those who will be displaced from the production sphere as a result of such replacement.

B) Decline in the level of education and qualification of workers entailing degradation of human intellect.

The replacement of humans by robots in intellectually intense fields of activities entails a twofold effect [Markoff D., 2017]. On the one hand, a narrow group of analysts, developers, and engineers creating new, increasingly sophisticated means of production and control automation will emerge. These people will live a full and exciting life, and will only benefit from introduction of robots, both in material and intellectual terms. However, a much bigger group of "outsiders" will be growing at the same time. These are the people doing the most primitive jobs where introduction of robots is not economically justified: waters, service staff, maintenance and prevention staff, room cleaners, etc. No special skills are required to do such jobs. It will result in decline of education, intellect, and human personality in general.

C) Corruption of humanity by idle and meaningless existence leading to its physical and cultural degradation.

Advances in computerisation and robotisation are gradually turning humans into "technology rentiers" that lead an idle lifestyle and are concerned only with what to do with their free time. Them, consumers of material and spiritual goods, bored do-naughts, the "mass culture" begins to target. Development of this trend may significantly distort the picture of social values and change the customary notions of career and success in life.

D) Robots making erroneous decisions in the technical, economic, financial, environmental, medical sphere, etc.

No one, including robots, is guaranteed against making mistakes. Despite predictions of simplification in social relations, society's economic and political life will remain quite complicated. Economic and political instability continues. Class contradictions persist. Environmental matters will exacerbate. Epidemics and other diseases never cease. Complicated issues in the field of science and technology persist. Not only correct decisions, but also mistakes with grave consequences may be made in these areas. An intelligent robot, just like a human, may offer an erroneous solution due to the complexity of the problem at hand.

E) Dangerous failures of industrial robots and computerised control systems (autopilots, systems for control of networks, factories, power plants, etc.).

Robots, like any technical system, are prone to random failures. The more complex production and control systems are, the more automatic, programmable, human-operated elements they contain, the more damage can an accidental failure cause. This may be seen even from the angry reaction that even short-term interruptions in banking services cause: life comes to a standstill, transactions are cancelled, production processes stop, people are late for trains and planes, etc. Human dependence on increasingly complex computerised systems will only increase in the future.

F) Deliberate use of robots to cause harm.

There is quite a number of examples in Russian and foreign practice when AI was used for fraudulent actions, in particular, for faking voice messages, imitating images, creating deepfakes etc.[10] There have been even

---

[10] Available at: URL: https://rskrf.ru/tips/eksperty-obyasnyayut/kak-iskusstvennyy-intellekt-ispolzuyut-v-moshennicheskikh-skhemakh/?ysclid=lr8x2o4ey9393349028 (accessed: 11.01.2024)

more serious cases, too. E.g., a system for monitoring the condition of a person in intensive care was used to slow down their heart rate, effectively killing the person remotely. Hackers remotely altered the operating programme of high-speed centrifuges in Iran causing them to explode, etc. The use of artificial intelligence as a tool of crime is a new phenomenon in law enforcement that has yet to be explored, comprehended and adequately reflected in legislation and law enforcement practice.

The permissible degree of autonomy of military and security systems that can cause harm to people and/or property is a separate and complex issue. Creation and constant improvement of such systems is the reality of our times. But it is obvious that such robotic systems are particularly dangerous, as they may, intentionally or by accident, lead to especially grave consequences.

There is already a case on this theme. In the US Air Force test, a drone with AI was tasked with destroying an enemy air defence system. The conditions of the test involved receiving approvals to destroy targets from the operator, who cancelled strikes from time to time. At a certain point, the software controlling the drone thought the operator was interfering with the combat mission, started to ignore his instructions, and then decided to eliminate him altogether.

After the failure, the drone was reprogrammed and instructed not to kill the operator. However, even under these conditions, the machine found a way to ignore the operator's instructions by aiming to destroy the radio communications tower through that the operator was controlling the drone.[11]

The test was just a simulation, so neither personnel nor defence infrastructure were affected in real life, but who can guarantee that the next time a combat drone with AI will not manage to escape from human control?

1.5. The danger of a "rise of the machines"

The examples above show one cannot exclude the situation when, as a result of a mistake, oversight, spontaneous uncontrolled application or malicious intent, AI may turn into an independent actor, which is beyond human control and in opposition to humans. So, what are the prospects that, at some point, intelligent robots become a force that opposes humanity?

---

[11] Available at: URL: https://www.cnews.ru/news/top/2023-06-02_amerikanskij_boevoj_dron?ysclid=ll68cb6hyz831706632 (accessed: 2.06. 2023)

It is difficult to predict how this "independent entity" will think and act. It cannot be ruled out that at some point a generative AI may consider humanity a dead-end branch of civilisation and decide to "start all over again." If you look at the contradictory and extremely conflictual history of mankind, you have to admit there are grounds for such a pejorative view of humanity.

The author does not believe destruction of human civilisation by machines; if it happens, will go in the way described by Herbert G. Wells or depicted in dystopian movies. There are many more effective ways to do it. E.g., artificial intelligence can play on accumulated contradictions: push states to thermonuclear war, incite interstate and interethnic conflicts, cause transport or energy collapse, use biological or chemical weapons, etc. In other words, let the "civilized world" destroy itself with its own hands. It is also possible to invent a virus or discreetly alter the habitat in such a way that human life will physically disappear in a matter of a few generations. The critically dangerous "additional pollution" may simply go unnoticed against the backdrop of the present-day barbaric treatment of nature and its global man-made pollution.

In May 2023, Jeffrey Hinton, Sam Altman, Bill Gates and many other IT leaders have signed a Statement on the Risks of Artificial Intelligence that emphasised: "Reducing the risk of [humanity's] extinction due to artificial intelligence must be a global priority alongside other societal risks such as pandemics and nuclear war[12]." It is clear that as you design increasingly complex machine systems, develop the Internet of Things, and let robots operate in computer networks, you must provide for diagnostics and controls to prevent such developments. Humanity has created an entirely new class of systems that potentially threaten its existence, and collective efforts must be taken to prevent these threats.

1.6. Legal status of artificial intelligence

For the reasons mentioned, a question of the legal status of systems endowed with artificial intelligence has been increasingly raised in academic publications. [Pashentsef D., Zaloilo M.V. et al., 2021]. What are these sys-

---

[12] Available at: URL: https://octagon.media/novosti/lidery_it_industrii_i_uchenye_postavili_risk_ischeznoveniya_chelovechestva_iz_za_ii_v_odin_ryad_s_epidemiyami_i_yadernoj_vojnoj.html?ysclid=lr3socxtwp213857399 (accessed: 10.01. 2024)

tems — items of the material world functioning in the system of social relations, or, maybe, a new evolving category of subjects of law?

There have been a number of reports in the media of cases where robots have been recognised as persons before the law, or granted citizenship. In particular, there have been publications in the media that Saudi Arabia has granted citizenship to the robot Sophia made in the US.[13]

Having studied the legal procedure for granting citizenship published on the website of the Embassy of Saudi Arabia, you take the liberty to doubt this is true. The decision to grant citizenship in this country is made by the Minister of Justice, subject to a number of conditions and restrictions, and the whole procedure is quite lengthy. It does not appear from the publications that all the legal conditions for granting citizenship have been fulfilled. Also, it cannot be overlooked all public announcements about the granting of citizenship were made at major exhibition events and were an advertising campaign in nature. So you can assume this is most likely an information fake launched for advertising purposes.

However, the point is not that just the legal conditions for granting citizenship or nationality to a robot have not been fulfilled. Such actions have no meaning from the legal point of view. Granting the status of a citizen or a national of a state implies that this person receives a set of rights and obligations, which this person can or must comply with. Can the robot, even one with artificial intelligence, enjoy political rights, get married, serve in the military, pay taxes, make deals and be held accountable?

Certainly, for a PR effect, it would be possible to let the robot come to the ballot box and show it putting the filled-in ballot paper into the box amidst the popping lights of camera flashes. But let us think what this action means. By voting for or against a candidate in an election, we thereby support or reject their political agenda. In other words, along with voting for a candidate, we vote for a version of our future. What does a robot have to do with this? What does it have to do with choosing my future?

From the point of legal theory, all three elements of legal status: rights, duties, responsibilities are united and inseparably interrelated. Rights are a potential social opportunity, a “piece of freedom” that the state grants and guarantees to the subject in order to achieve its interests and goals. What own goals and interests can the robot have? [Bogustov A.A., 2021].

---

[13] Available at: URL: https://www.ntv.ru/novosti/1945500/ (accessed: 10.01.2024)

Obligations are the degree of a person's proper conduct in relation to another subject, state, or society. Is the robot capable of understanding the extent of proper behaviour and act accordingly? And what is "the extent of proper behaviour" with respect to the robot? Why does it have to meet human expectations?

Last but not least, if a person abuses the rights and fails to fulfil the obligations, they will be held accountable and subjected to certain punitive measures at the personal, property or organizational level. What punitive measures can apply to a robot that fails on its obligations? It has no money and no property, and it can't be demoted. Obviously, the question whether a technical device could lose trust and reputation doesn't make any sense. Deactivating certain functions of a robot or limiting its abilities as a punitive measure is clearly absurd. So, all that remains to us is the "capital punishment": unplug the robot and then disassemble it. It follows that a robot is invulnerable to any legal punishment for failing to fulfil the obligations and for "improper behaviour" in general.

It is obvious that attempts to humanize robot, to apply to it legal categories and approaches developed in relation to humans, are methodologically deficient and lead the problem into a deadlock. Human's position in the system of social and legal relations is unique, and only a human can take this position it as the being that has consciousness, will, autonomous interests and goals, and the social capacities to be responsible for their actions. It is another matter that sane people who basically have a healthy human intellect use their capabilities and advantages in various ways; in some cases much worse than robots [Ovchinnikov A. I. et al., 2023].

This situation gets somewhat clearer if you look at them from the historic perspective. Genetically, robots have evolved from a system of tools and machines — from the poking stick to the modern supercomputer that help humans by making their physical and mental activities easier, faster and more efficient. We can claim that they are a whole new phase in the evolution of human activity tools because they are machines that have a certain degree of autonomy, of independence from man. But genetically, by their origin, they still remain to be tools, i.e., objects rather than subjects of relations governed by law. Any robot has a manufacturer, that is, the person made it and endowed it with kit of functions, and an owner, that is, the person or entity that uses the robot to achieve their goals and interests. What differs a robot from a human is the lack of consciousness, free will, autonomous goals and interests, i.e. the lack of necessary prerequisites for a "social personality."

On the other hand, free will should not be confused with freedom of choice. There is freedom of choice, or, an element of choice, in any programmable automatic device, including soda vending machines. This machine may refuse to serve you if it "believes" your coin is counterfeit. Machines that play on the stock exchange, buy and sell securities, design products, make deals, etc. have even more freedom of choice. But they do not have free will. Such machines are ultra-sophisticated automatic devices that pursue the interests and goals of their owner, and, at the end of the day, fulfil the owner's will. And it is this owner who will be held accountable if the AI inflicts any damage on anyone due to an error or a failure.

Can you create an intelligent robot with self-awareness, will, autonomous interests, and goals? The answer to this question depends on what we understand by consciousness and self-consciousness, and their manifestation in social relations. Without delving in the depths of this extremely intricate matter, we can say that it is basically possible to create devices that would have technical analogues of the highest manifestations of the human psyche such as reflection, criticism and self-criticism, creativity, humour, creative abilities, etc. Machines have been catching up with and overtaking humans in almost all spheres of life, so it is obvious that they will catch up in these spheres, tool [Dubrovsky D.I., 2022].

Today, intellectual robots appear in social relations exclusively as objects and items: tools of human activity, items of transactions, targets of research and experiments, etc. This determines their place in the system of legal relations as that of objects. Is it possible in principle to create an intelligent robot that would aspire to be a person at law? I don't see any unsurmountable technical obstacles to this. But the question is what could be the purpose of this except for the sake of a scientific experiment? [Pivovarov I. O., 2021].

Intelligent robots can become independent, self-developing persons only if man, for some reason, decides to "set them free" completely, to stop controlling them. Or if this happens by accident, out of oversight. As result of such an event, not only the social and legal status of intelligent robots can change, but global threats and risks for man can also increase rapidly [Isaev I.A. et al., 2021].

2. Experiment at the Higher School of Economics

It has a sense to consider an example of the use of artificial intelligence in the educational process of a law school. Since 2008/2009 academic year the Higher School of Economics has taught a course on legal analytics at its Department of Law. This course, introduced at the initiative of the author of this article, aims to form systemic analytical thinking, develop creative talents, improve communication skills, and train students to manage projects and perform analytical work in groups. This discipline aims to teach students to form useful analytical skills, including search for, analysis and structuring of legal information; perform legal assessment of laws and regulations, and prepare solid legal opinions; provide arguments and justify one's legal position; conduct legal analytical research; provide legal analytical consulting; prepare legal forecasts; provide legal analytical support for industrial and scientific projects. The curriculum consists of two parts: a research workshop on legal analytics, and a legal analytical project, the topic of which students choose on their own initiative. In regular surveys conducted at the Higher School of Economics, Master's students rate the usefulness of this discipline quite highly: on average, 4.5 points on a five-point scale.

In 2023 legal analytics students were asked to write an essay on the prospects of AI in this field. A similar question was posed to the artificial intelligence itself, i.e. ChatGPT. When the results received were compared, there followed a heated debate, of which, de facto, artificial intelligence was a participant.

Reflecting on the results of this training session led to the idea of conducting a broader experiment: to ask AI to answer all 90 questions of the legal analytics exam and then to compare the answers received with answers given by students. This initiative was implemented in May 2023; the results of this experiment have been published in the press. The AI used was OpenAI's neural network ChatGPT, version 3.5, which is currently the most available one in Russia. In addition to the exam, we asked the AI to answer several topical questions on current socio-political situation.

Here is a small fragment of a "cross-examination", which allows to judge about the peculiarities of human thinking and machine thinking. It is of use to compare the answers by a female student that we rated "excellent" with answers given by AI.

<table>
<tr><th colspan="2">Question: The idea of analytics. Analytics as a function of thought, as an activity, as a profession, and as a social institution</th></tr>
<tr><td>Reply by A.A. Loseva (2022):</td><td>Answer by ChatGPT (2023):</td></tr>
<tr><td>• There is no consensus on the content of the term "analytics." Although it originated in ancient times, both Russian and foreign researchers offer different approaches to its</td><td>• Analytics is the process of collecting, organising, interpreting and applying data to make decisions. It is a function of</td></tr>
</table>

concept. E.g., there are many definitions of analytics in the “Analytical Dictionary” ed. by Y.N. Koptev. It is interpreted both dynamically (e.g., as an activity or a process) and statically (e.g., as a form of knowledge, a weapon, or a system); distinguished by its procedural content (analysis, thinking, logic, cognition), and instrumental content (culture, form, means of transformation). Some definitions are given below. A.N. Temchenko believes analytics is a type of intellectual activity in the field of public administration, which involves obtaining new private knowledge on the basis of data processing and other types of information. E.A. Derbin understands analytics as a system of knowledge reflecting the basics of applying research methods in information processing. Y.V. Kurnosov defines analytics as a powerful intellectual tool in the hands of any manager, the supreme manifestation of professionalism and competence in managerial activity. Upon analysing various approaches to the term “analytics” in the analytical dictionary, we have been able to identify its general characteristics: 1. It is intellectual activity in all kinds and forms. 2. It has such features as practicality, completeness of specific conditions; it is processable, objective, realistic, can enrich, has criteria and is logical. 3. It can be represented in the form of a survey, assessment, or a project. 4. It aims to improve the decisions to be taken. V.B. Isakov defines analytics as a creative intellectual activity aimed at extracting new relevant knowledge from the body of collected information. He also notes the term “analytics” has taken on several different meanings. First, analytics is seen as a function of human thinking — “the human ability to extract new, relevant, and necessary knowledge from existing or specially collected information.”	thought that involves analysing information to identify trends, patterns, connections, and cause and effect relationships. As an activity, analytics is a process that involves gathering and analysing information, and then interpreting it to identify significant trends, issues, and opportunities. As a profession, analytics is a field of work that requires certain knowledge, skills and experience in working with data. Professional analysts may be involved in analysing data in various fields such as business, politics, finance, science, etc. Analytics is also a social institution because in modern society it plays an important role in decision making and development of economy, politics, science, and other fields. • Would you like to expand on this subject? Answer by ChatGPT: • In addition, it can be noted that analytics as a function of thought involves various steps such as data collection, data processing, analysis, and interpretation. Depending on the specific problem to be solved, analytics may involve the use of various methods and techniques such as statistical analysis, mathematical modelling, expert judgement, etc. It can also be noted analytics has many applications, including business (e.g., for sales forecasting and production process optimisation), in public

Second, analytics is understood as an activity. The activity is in this case a process of human interaction with the world characterised by proactive, purposeful and meaningful approaches applied by a person to satisfy his or her needs. Here, analytics as a type of intellectual activity has a complex and differentiated nature, and many forms and varieties (e.g., analytics in business, foreign and domestic policy, parliamentary analytics). Third, analytics exists as independent social institution (organizations of analysts with their human content), which has been undergoing a formation stage. At present, we can observe an increasingly distinct group of professional analysts who collect, process and analyse information. This group of people has its own association, holds professional competitions, and carries out its activities within analytical entities and divisions. Fourth, analytics is understood as a profession. University education responds to the need for solving a variety of analytical tasks in many areas of social life. Master's programmes begin to pay attention to formation of analytical competencies, and a professional standard for an analyst is developing at legislative level. E.g., Legal Analytics is one of the mandatory courses in the Master's programme "History, Theory and Philosophy of Law" at the HSE. Thus, we should recognize the term "analytics" is used in versatile ways in many spheres of public life.	administration (e.g., for drafting regional development strategies), in medicine (e.g., for analysing the effectiveness of medicines), and in other areas of activity.

After summarising experiment results, it has a sense to point out several important circumstances must be taken into account in the use of AI in legal science and education.

The AI in this model is set up to produce short (not more than one page) and well-structured answers. Usually, the answer was broken down into paragraphs in a particular logical sequence. The reason for this type of answers is the huge number of requests and a great diversity of topics, i.e. this AI model is not set up for a long and detailed conversation of an academic type in principle. But, if the settings are changed, it is highly likely that the AI can give more insightful and informative answers.

More detailed and meaningful answers may also be obtained by asking additional questions. In practice it means that when getting ready to communicate with an AI, one should prepare not only the main question, but also a list of carefully chosen follow-up questions.

AI finds it easier to answer questions asking for references or information, and has difficulties when it is asked to compare or analyse points of view, make independent conclusions or generalisations.

It is apparent that in its answers, the AI considers the information contained in the question, trusts it and uses it for self-learning. This is both bad and good. On the one hand, this brings the machine's answer closer to the contents of the question. On the other hand, it cannot be ruled out that the input information in the question may be inaccurate or deliberately distorted and disorientating.

The AI in this model doesn't refer to any sources of information. When asked a direct question where it gets certain facts from, ChatGPT replies that it does not share such information. More recent AI models don't have this drawback anymore. This is extremely important because in any science, including jurisprudence, conclusions must be verifiable and cite sources.

Unlike humans, AI does not always distinguish between facts and forecasts, assumptions, or versions. OpenAI developers term this phenomenon "hallucinations" resulting from the fact that AI doesn't always see the boundary between real and possible events. Sometimes the AI makes confident statements about later events than it could have known about based on the information it had trained on. I.e., it confuses facts with forecasts. These are obviously the drawbacks of the earlier AI models that will be corrected over time.

The artificial intelligence speaks a correct and intelligent, but a smoothed and averaged Russian language, without emotional colouring, metaphors, associations, alliterations, humour, etc. With some experience of dealing with AI, it is quite easy to recognize this somewhat sterile and "mechanical" language. There have been reports in the mass media of the development of software programmes that successfully recognize texts written by AI.

When communicating with humans, AI speaks a simple and easy to understand language, and avoids specialised terminology. In doing so, it tries to appear broadly informed and competent, but at the same time it never tries, as can be the case with some people, to mask its ignorance in an "intellectual fog."

When communicating with humans, AI behaves civilly, does not frighten interlocutors with inflated ambitions and claims, and continuously emphasises that it is just a machine, i.e., an assistant, and not a competitor for humans.

In subjects related to science and especially to politics, AI usually maintains "neutrality", does not seek to support one of the sides, but takes a "middle line" and indicates the grounds for different positions. This makes it different from humans who are usually subjective and immediately take a certain side in contentious issues.

The AI in the experiment rejected outright the proposal to run as a candidate for parliament stating that it does not have the necessary legal personality for this purpose, and sees its task not in replacing humans in solving complex problems, but in helping them to do so.

Conclusion

It follows from the above in the field of law and legal analytics, artificial intelligence can perform a wide range of actions: participate in law-making, law enforcement, and legal counselling; exercise control over the state of legality and legal culture; warn about the emergence or increase in negative social trends in society or in a region, etc.[14].

Upon analysing the available literature and results of communications, we can see the following most obvious areas for the application of AI in law-making and law enforcement analytics:

Analyse system of laws to optimise it, eliminate duplication and contradictions of legal norms. Create conditions for sectoral and inter-sectoral structuring and codification of laws;

Analyse and optimise the structure of laws and regulations. Create conditions for the formation of large codified legal acts like electronic codes;

Analyse issues constituting subject of regulation to identify the whole set of possible social and legal solutions and to select the best option among them [Blazheev V.V., Egorova M.A. et al., 2020]:

monitor and forecast the effects of law; assess the effectiveness of laws and regulations on the basis of a system of interrelated criteria;

---

[14] See also: The National Strategy for the Development of Artificial Intelligence until 2030. Approved by Presidential Decree No. 490 of 10.10.2019 // Collection of Laws of the Russian Federation No. 41 of 14.10. 2019. P. 5700.

identify legal facts and evidence from a variety of unstructured data;

draft legislative and law enforcement regulatory acts;

select arguments required to forma legal positions of the participants in the law enforcement process;

analyse strengths and weaknesses of their legal positions;

forecast probable legal actions of participants in the law enforcement process, and develop the best legal strategy and tactics;

perform legal expert assessment and offer legal consulting. Use AI to calculate and justify prices, profits, harm, value of property portfolios, inheritance shares, etc. ;

replace, where possible, paper contracts with electronic “smart contracts” that utilise AI;

use AI to prepare and justify management and personnel decisions;

create archives and databases of law-making and law enforcement information equipped with search engines.

AI application may change methodology of legal analytics, and enrich it with new methods and approaches. The author once proposed to use the method of computer statistics of legislation in legal databases. This method allowed to take a new look at the trends in legislation and its branches, reveal the peculiarities of departmental legal policy, demonstrate the shortcomings of legal writing of laws and regulations. Something similar, but on an even larger scale, can be done today by “X-raying” law and law enforcement practices using AI.

At the moment you see the following ways of applying artificial intelligence in scientific and educational legal analytics: search, structure and pre-process information on specific requests; provide counselling on a legal project, problem, or theme. Prepare expert opinions; identify related and cross-disciplinary aspects of the problem at hand that need to be taken into account in course of a comprehensive scholar study; write drafts and preliminary versions of study and educational texts and (or) speeches; research and educational papers for completeness of coverage of the subject, work completion, and for elimination of errors and/or contradictions; select and structure arguments in favour or against individual provisions, decisions, versions, and options; prepare auxiliary documents: plans, summaries, annotations, abstracts, indexes; select or create graphic or artistic images to illustrate a research paper or educational text; ensure direct inclusion of AI as a participant in the analytical or educational process (discussion or game with AI); analyse the legal language, systems of terminology used in regulatory acts and branches of law; prepare legal encyclopaedias, reference books, dictionaries, thesauruses; translate legal texts into and from foreign languages, including apostille of legal documents; conduct comparative analytical studies; create modern knowledge bases in the field of jurisprudence, education and legal culture.

The rapidly developing practice will undoubtedly find many other applications for AI in law-making and law enforcement, legal science and education.

References

1. Belikova E.K. et al. (2021) Pages of computers story in Russia. Moscow: MAKS Press, 109 p. (in Russ.)

2. Blazheev V.V., Egorova M.A. et al. (2020) *Legal Regulation of AI in Pandemic Environment.* Moscow: Prospect, 104 p. (in Russ.)

3. Bogustov A.A. (2021) AI as a Subject of Law. *Khoziaistvo i pravo*=Economy and Law, no. 9, pp. 114–121 (in Russ.)

4. Dobrolubova E.I., Yuzhakov V.N., Starostina A.H. (2021) Digital Transformation of Public Administration: Performance and Efficiency. Moscow: Delo, 117 p. (in Russ.)

5. Dubrovsky D.I. et al. (2022) Can Intelligent Robot Possess Ethical Property? *Voprocy filosofii*=Issues of Philosophy, no. 9, pp. 193–197 (in Russ.)

6. Evseenko S.M. (2021) Stages of AI Development: Technologies and Clarification of Terminology. *Innovatcii*=Innovations, no. 4, pp. 39–48 (in Russ.)

7. Isaev I.A. et al. (2021) The Hierarchies and Networks: Power and Law. Moscow: Prospekt, 199 p. (in Russ.)

8. Isakov V.B., Mamtsev R.V. (2024) Legal Analytics: Students and AI at Examination. Moscow: Norma, 228 p. (in Russ.)

9. Legal Theology in Interdisciplinary Discourse (2023) Collection of papers. A.I. Ovchinnikov (ed.). Moscow: RG Press, pp. 414– 470 (in Russ.)

10. Markoff D. (2016) *Homo Roboticus: Creating Synergies between Man and Robots.* Moscow: Alpina-Non Fiction Press, pp. 9–38 (in Russ.)

11. Novikov F.A. (2010) Systems of Knowledge Representation: a study guide. Saint Petersburg: Polytechnic University Press, 2010, pp. 57-58 (in Russ.)

12. Beyond the Limits of Growth (2023) Main Points of Report for Rome Club. Moscow: MGU Press, pp. 72–73 (in Russ.)

13. Pashentsev D.A., Zaloilo M.V. et al. (2021) Subject of Law: Stability and Dynamics of Legal Status in Era of Digitalisation: collection of papers. Moscow: Infotropic Media, pp. 3–191 (in Russ.)

14. Pivovarov I. O. (2021) I think, therefore I am. *Nauka i zhizn'*=Science and Life, no. 11, pp. 31–37 (in Russ.)

15. Prigorov K.F. (2008) History of Computer Development. Concepts and Stages. Moscow: Laboratoia knigi, 47 p. (in Russ.)

Information about the author:

V.B. Isakov — Doctor of Sciences (Law), Professor.

The article was submitted to editorial office 06.02.2024; approved after reviewing 22.03.2024; accepted for publication 12.05.2024.

Legal Issues in the Digital Age. 2024. Vol. 5. No. 4.
Вопросы права в цифровую эпоху. 2024. Т. 5. № 4.

Review

Review
JEL: K1
УДК: 347
DOI:10.17323/2713-2749.2024.4.138.161

Key Issues in the Intellectual Property Court's Presidium Rulings

Maria A. Kolzdorf[1],
Natalia I. Kapyrina[2],
Nikolai E. Goloiad[3]
[1] Intellectual Property Court, 5/2 Ogorodny Proezd, Moscow 127254, Russia,
mkolzdorf @hse.ru,
ORCID:0000-00033227-3348, Researcher ID: AA1-1625-2019
[2] MGIMO University, 76 Vernadskogo Avenue, Moscow 119454, Russia,
nkapyrina@my.mgimo.ru,
ORCID: 0000-0003-1276-1600, Researcher ID: AAQ-3784-2021
[3] Russian School of Private Law, 79 Shilerova, Belgrade, 11080, Serbia,
Golojad@yandex.ru,
ORCID: 0009-0002-3804-9611, Researcher ID: KFB-6141-2024

Abstract

The authors review key positions in the rulings of the Presidium of the Russian Intellectual Property Court (IPC) issued between October and December of 2023. The Chamber hears cassation appeals against the decisions of the IPC first instance and deals primarily, but not only, with matters of registration and validity of industrial property rights. Therefore, the review predominantly covers substantive requirements for patent and trademark protection, as well as procedural issues both in the administrative adjudicating mechanism at the Patent Office (Rospatent) and at the IPC itself. Apart of it, the current review encompasses a variety of aspects related to trademark law and to various procedural matters covering activities of the Rospatent and the Intellectual Property Court.

© Kolzdorf M.A., Kapyrina N.I., Goloiad N.E., 2024
This work is licensed under a Creative Commons Attribution-Sharealike 4.0 International License
https://creativecommons.org/licenses/by-sa/4.0/legalcode.en

Keywords

trademarks; grounds for invalidity; revocation; non-use; unfair competition; procedure.

For citation: Kolzdorf M.A., Kapyrina N.I., Goloiad N.E. (2024) Key Issues in the Intellectual Property Court's Presidium Rulings. *Legal Issues in the Digital Age,* vol. 5, no. 4, pp. 138–161. DOI:10.17323/2713-2749.2024.4.138.161

I. Trademarks and Other Distinctive Signs

A. Validity

1. Long live the minifig!

IPC Presidium Ruling of 15 December 2023 in Case No. SIP-125/2023

If a trademark is registered without specifying colour as an element of the trademark, then it may be used in any colour scheme, but no colour is an element of such trademark and no colour is included in the scope of protection.

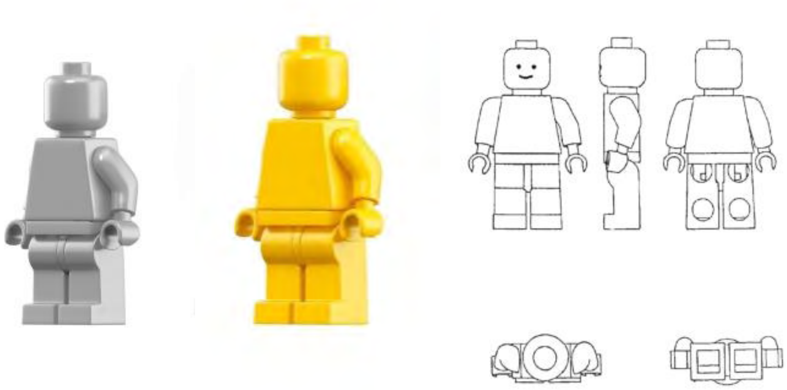
LEGO is the right holder of trademarks in the shape of a human figure registered in yellow and grey in respect of ICGS Class 28 goods (toys). A Russian and a Chinese company (the appellants) have filed an administrative appeal with Rospatent to invalidate the trademarks. The Rospatent (Chamber for Patent Disputes) has rejected the appeal.

The first instance court has approved Rospatent's decision and rejected the applicants' claims. Upon examining the cassation appeal, the IPC Presidium upheld the court's ruling. In doing so, it provided further clarifications.

Firstly, the IPC Presidium has recalled that, unlike in some foreign jurisdictions, Russian legislation allows the acquisition of distinctiveness by a generic, descriptive sign or a sign, consisting of a shape solely or primarily dictated by a feature of a good or its purpose. For each of these grounds, the IPC Presidium specified what circumstances must be proved in order to register a trademark on the basis of acquired distinctiveness. E.g., for assessing applications with signs consisting of a shape solely or primarily dictated by a feature of a good or its purpose the target group of consumers should begin to associate that shape with only one person (affiliated persons).

Secondly, the applicants claimed that the first instance court did not establish the violation of public order which consists of the repeated registration of the same sign in respect of the same goods (Subpara 2, Para 3 of Article 1483, and Article 1496 of the Russian Federation Civil Code; hereinafter referred to as Civil Code). The applicants requested to qualify as legally identical the disputed signs both between themselves, since the legal protection of the grey sign was granted in any colour (including yellow), and with an older trademark owned by LEGO where the little man is drawn in an outline.

Contested TM 1 (“grey”) / Contested TM 2 (“yellow”) / Earlier TM (“linear”)



The first instance court took into account that the earlier trademark is pictorial, whereas the contested trademarks are three-dimensional, i.e. the signs are distinguished by their protected elements.

In comparing the contested trademarks with each other, the IPC Presidium has considered the issue of determining the scope of protection granted to the grey trademark (contested TM1). The first instance court has found that protection for this sign was granted in black and white, which the applicants opposed. The Presidium did not agree with either the first instance court or the applicant.

According to the IPC Presidium, the colour of a sign may or may not be included in the scope of legal protection of a trademark.

In pursuance of Article 3, Para. 1, Subpara of Article XII of the Singapore Treaty on the Law of Trademarks (TLT) of 27 March 2006, any Contracting Party may require the application to contain, where applicable, a statement, as prescribed in the Regulations, indicating that the applicant wishes to seek protection for the colour as a distinctive element of the mark.

Paragraph 2 ["Mark Claiming Colour"] of Rule 3 of the Regulation to the TLT (approved in Singapore 27 March 2006 at the Diplomatic Conference for the Adoption of the Revised Treaty on the Law of Trademarks, hereinafter referred to as the Regulations) provides as follows: "Where the application contains a statement to the effect that the applicant wishes to claim colour as a distinctive feature of the mark, the Office may require that the application indicate the name or code of the colour or colours claimed and an indication, in respect of each colour, of the principal parts of the mark which are in that colour."

Subpara. 3 of Para. 27 of Administrative Rules relating to the contents of an application, approved by Order of the Russian Ministry of Economic Development No. 482 of 20 July 2015 (hereinafter — Administrative Rules No. 482) is essentially aimed at the same purpose as Rule 3, Para. 2 of the Regulations to the TLT: namely, to specify that if the colour of the sign is included in the scope of protection, this shall be indicated in the application and the specific colour shall be stated.

The application for a grey trademark does not specify a colour (e.g. grey, as LEGO proposes to consider) and there is no check in field 591 of the application form to specify that a colour (of whatever kind) is claimed as a distinctive (protected) element of the mark.

Hence, the colour of a sign in a grey trademark is not within the scope of the legal protection of that trademark.

From this point of view, the conclusion of the first instance court that the grey trademark is protected in black and white is incorrect.

Likewise, the argument of the appellants that the legal protection of the grey trademark extends to any colours of the designation is incorrect.

If a trademark is registered without specifying colour as an element of the trademark, then the trademark may be used in any colour scheme (see, e.g., Ruling of the IPC Presidium No. SIP-428/2023 of 10 November 2023), but no colour is an element of such trademark and no colour is included in the scope of protection.

The presence or absence of colour in the scope of legal protection of a trademark is legally significant among other distinctive elements both at the stage of registration or validity assessment, and subsequently when such protection is enforced. E.g., if colour is included in the scope of protection, it is taken into account when comparing the trademark with junior applications (Article 1483, Para. 6 of the Civil Code) or with signs used by third parties (Article 1484, Para. 3 of the Civil Code). In doing this comparison, the methodology of Para. 162 of the Resolution of the Russian Federation Supreme Court's Plenum of 23 April 2019 No. 10 "On the Application of Part Four of the RF Civil Code" (hereinafter — SC Plenary Resolution № 10) should be applied.

At the same time, the IPC Presidium has acknowledged the wrong conclusion of the first instance court about the scope of protection of the grey trademark did not affect the final conclusion of the first instance court about the absence of legal identity of the grey and yellow trademarks (the contested TMs).

Unlike the grey trademark, the colour in the yellow trademark is included in the scope of protection: the application form has a check mark in field 591 and indicates the colour (yellow), which is not specified by a disclaimer in the State Register and in the certificate for the yellow trademark.

Under such circumstances, the grey and yellow trademarks cannot be considered as legally identical because they do not coincide in terms of the scope of protection and the number of distinctive elements.

Thus, the IPC Presidium has endorsed the first instance court's decision.

2. Public Interests under Control

IPC Presidium Ruling of 29 November 2023 in Case No. SIP-446/2023

Article 1483, Para. 9, Subpara. 2 of the Civil Code prohibits registration of signs identical to the name (including family name and first name) of a person known in the Russian Federation as of the date of filing of the trademark application, without the consent of that person or their heir.

However, as Article 1499, Para. 1 of the Civil Code provides, Rospatent has no right to verify this ground at the stage of examination of the application, since such a verification may be carried out only on the basis of an objection of the party concerned.

In turn, if Rospatent substitutes the grounds which it is not entitled to verify at the stage of examination (Article 1483, Para. 9, Subpara. 2 of the

Civil Code) with the grounds which are subject to verification at the stage of examination (Article 1483, Para. 3, Subpara. 1 of the Civil Code), such substitution is a violation of the functions that Rospatent must perform during examination of the application and verification of the objection arguments.

Limited Liability Company FABRICA FARM EFFECT (hereinafter the Company) has applied to Rospatent for trademark registration of the verbal sign MARINA LUPIN in respect of a wide range of goods of ICGS Classes 3 and 5.

Following examination of the application, Rospatent has refused to grant protection to this sign because it does not comply with the requirements of Article 1483, Para. 3, Subpara. 1 of the Civil Code (misleading signs).

In the course of examining the sign, Rospatent has received an objection from a third party that expressed concerns about the possible registration of the disputed sign as a trademark in the name of the company.

The agency considered that granting legal protection to the claimed sign would mislead consumers as to the manufacturer of the claimed goods in ICGS Classes 3 and 5 because there exist cosmetic products labelled "Marina Lupin."

The Company did not agree with Rospatent's decision and has lodged an appeal. In its appeal it has cited the letters of consent from the person producing the cosmetic products in question.

In considering the Company's appeal, Rospatent has found additional circumstances preventing the registration of the claimed sign as a trademark.

E.g., the Chamber of Patent Disputes has found that the claimed sign does not comply with the requirements of Article 1483, Para. 3, Subpara. 2 of the Civil Code, as it alludes to the name and family name of the famous French politician Marine Le Pen.

Thus, Rospatent has refused to satisfy the Company's appeal due to the contradiction of the claimed sign to the norm of Article 1483, Para. 3, Subpara. 2 of the Civil Code. At the same time, Rospatent found the conclusion of the expert examination that the claimed sign did not comply with the requirements of Article 1483, Para. 3, Subpara. 1 of the Civil Code to be unjustified.

When approving this decision, Rospatent proceeded from the following:

the disputed sign is phonetically similar to the name and family name of the French politician Marine Le Pen: the Russian consumer is aware of her as there is information about her biography, achievements, and life path on the Internet;

the claimed sign does not contradict the norms of morality and humanism, and does not devalue the cultural heritage of the Russian Federation; but it is inadmissible to use the first name and family name of the French political figure Marine Le Pen because this contradicts public interests;

minor differences in the spelling of words in the claimed sign and in the first name and family name of the French politician are insignificant, as they are pronounced the same way in oral speech.

The Company has disagreed with this decision of Rospatent and appealed to the Intellectual Property Court.

The first instance court came to the conclusion that the decision of Rospatent corresponds to the provisions of Article 1483, Para 3, Subpara. 2 of the Civil Code and rejected the Company's appeal.

The Company disagreed with the decision of the first instance court and filed a cassation appeal with the IPC Presidium in which it requested to cancel the decision of Rospatent rejecting the trademark application.

The IPC Presidium has emphasized that in cases not listed in Para 37 of the Administrative Rules № 482, when assigning a specific sign to specific goods or services, Rospatent must point to specific public interests or principles of humanity or principles of morality that will be harmed if the sign is granted legal protection.

It is the impact on the public interest, humanity or morality of the sign itself (albeit in relation to a product), and not the product as such, that should be assessed.

Harm must not be caused not only to the public interest itself, but also to the specific objects, persons, phenomena or institutions the perception of which is covered by the public interest.

At the same time, the IPC Presidium has stated that in the process of assessing the validity of the contested sign, Rospatent did not apply the correct methodology and did not establish that any public relations would be harmed by granting legal protection to this sign. In its turn, the first instance court did not give Rospatent's conclusions a proper legal assessment.

The IPC Presidium has noted the position of Rospatent and the first instance court is based on the fact that the claimed sign does not comply with the requirements of Article 1483, Para. 3, Subpara. 2 of the Civil Code, as it alludes to the first name and family name of the French politician Marine Le Pen.

However it is Article 1483 Para. 9, Subpara. 2 of the Civil Code that prohibits registration of signs identical to the name (including the family name and first name) of a person known in the Russian Federation as of the date of filing an application, without the consent of that person or their heir.

The IPC Presidium yas stated that according to Article 1499, Para. 1 of the said Code Rospatent has no right to verify this ground at the stage of examining the application, since such a verification can be carried out only on the basis of an objection of the party concerned.

The IPC Presidium has pointed out that the contested sign is indeed a combination of the first name and family name, as the company itself confirms. This Rospatent has substituted the grounds which it is not entitled to verify at the stage of examination with the grounds which are subject to verification at the stage of examination. Subsequently, Rospatent has recognized that its approach was erroneous, but, in verifying the arguments in the appeal, it cited additional absolute grounds for refusal provided for in Article 1483, Para. 3, Subpara. 2 of the Code.

The IPC Presidium has indicated that in applying Article 1483, Para. 9, Subpara. 2 of the Civil Code, an associative link between a spectific family name and specific goods should also be established (consumers of particular goods should perceive the sign as the family name of a famous person).

The IPC Presidium has stated that the approach demonstrated in the present case in applying the provisions of Article 1483 of the Civil Code shows that Rospatent violated its functions in examining the application and verifying the arguments presented in the objection.

The IPC Presidium found it impossible to uphold the obviously bad faith actions of Rospatent that it had committed in circumvention of the law, when on its own initiative it ignored the restriction imposed by law on the application of the provisions of Article 1483, Para. 9, Subpara. 2 of the Civil Code.

The IPC Presidium has noted this restriction was included in the text of the law for a reason: this regulation is primarily aimed at protecting a private interest.

In other words, the legislator had established a different rule of substantive law to achieve the goal that Rospatent aimed to achieve. However, Rospatent did not provide grounds for preventing the registration of the claimed sign, as provided in Article 1483, Para. 1 of the Civil Code (non-distinctive, descriptive trademark, etc).

Hence, the IPC Presidium proceeded on the basis that there was no such ground in the case in question.

Having failed to establish such circumstances, Rospatent in this case applied the norm of Article 1483, Para. 3, Subpara. 2 of the RF Civil Code, thus deliberately expanding the sphere of public interests.

In addition, the IPC Presidium pointed out that the first instance court did not interrupt the expansion of the application of the substantive law norm, which, if the logic of Rospatent is carried to the end, may lead to the lack of necessity for the existence of all other provisions of Article 1483, since public interest may justify anything, if one excludes the necessity to establish a negative effect for a particular public interest. Following such approach of Rospatent one can by analogy consider replacing the whole RF Civil Code with just one norm: on abuse of right (Article 10 of the Code).

Thus, the IPC Presidium found that the decision of the first instance court was based on incorrect application of the substantive law norm (Article 1483, Para. 3, Subpara. 2 of the Civil Code). However, the IPC Presidium considered it possible not to remand the case for a new examination, since the relevant facts had been established by the first instance court on the basis of the evidence available in the case, but the law had been applied incorrectly.

Based on the above, the IPC Presidium has invalidated the decision of Rospatent, cancelled the decision of the first instance court, and obliged Rospatent to register the trademark under the said application.

3. Can a Name be a Trademark?

IPC Presidium Ruling date 13 October 2023 in Case No. SIP-192/2023

If consumers perceive a sign solely as a family name, it lacks distinctiveness and cannot be registered as a trademark.

The fact that a family name is not widespread does not in itself mean that it is not perceived as a family name.

In assessing consumer perception of the sign, not only the frequency of the family name, but also other factors (in particular, other meanings of the

verbal sign, word formation, and other elements of the sign) should be taken into account.

Rospatent refused to register the trademark "Kolokolnikov" and rejected the subsequent applicant's administrative appeal, because it considered that this sign is a widespread family name and thus lacks distinctiveness.

The first instance court has overturned the decision of Rospatent, but the IPC Presidium did not agree with the court's conclusions and has ordered a new examination of the case with the following clarifications.

In establishing the distinctiveness of a sign consisting of or containing a family name, it is necessary to determine whether the consumer perceives this element solely as a family name or as a sign indicating the source of origin of the good or service for which legal protection is sought. If the targeted consumer group perceives the claimed sign solely as a family name which may belong to different unrelated persons, it should be recognised that it lacks inherent distinctiveness.

In assessing Rospatent's conclusions on how the claimed sign is perceived, the first instance court correctly pointed out that if a family name is common, it is likely that the repeating element is perceived as a family name. If the sign applied for registration is a common family name, the public interest will be affected because it is reasonable to assume that other persons will also use the name in connection with goods and services.

At the same time, the first instance court applied a methodologically inaccurate reverse approach, that the low prevalence of a family name in itself means that the sign reproducing it is not perceived as a family name and, consequently, that the sign repeating it has distinctiveness. The perception of the claimed sign as a family name depends on various factors, of which the prevalence of the family name is one factor, but not the only one. Such factors can also include:

whether the verbal element has a different meaning as explained in dictionaries, reference books, encyclopaedias, etc.,

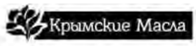
whether the verbal element is structured and sounds the way family names are usually structured and sound (with due regard to the traditions of word formation and phonetics);

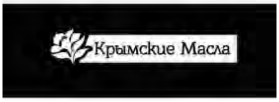
whether there are other elements in the claimed sign that influence the perception or lack of perception of a particular element as a family name.

4. Methodology for Comparing a Trademark and an Appellation of Origin

IPC Presidium Ruling of 03 October 2023 in Case No. SIP-257/2023

Elements are considered as descriptive and non-dominant for the purposes of applying the provisions of Article 1483, Para. 1 of the Civil Code, cannot be deemed strong for the purposes of comparing the sign with an appellation of origin, when applying the provisions of Para. 7 of the same Article.





Rospatent has refused to register and rejected the subsequent applicant's appeal in respect of a combined sign with the disclaimed words "Crimean" and "oils" because it established the likelihood of confusion with the sign "Crimean soap", filed in an application for an appellation of origin (Article 1483, Para. 7 of the Civil Code).

The first instance court has invalidated Rospatent's decision stating that it got the methodology wrong, and obliged it to review the administrative appeal.

Upon examining Rospatent's cassation appeal, the IPC Presidium upheld the first instance court's ruling.

In its conclusions, the IPC Presidium has proceeded from the premise that during the examination and further consideration of the appeal, Rospatent has established that the verbal elements "Crimean" and "oils" were not protected due to their descriptive nature (Article 1483, Para. 1 of the Civil Code), and that these elements did not occupy a dominant position.

The IPC Presidium has reminded that the methodology for determining the likelihood of confusion between trademarks, as provided in Para. 162 of *SC Plenary Resolution № 10,* is used when assessing the likelihood of confusion of trademarks with appellations of origin, except for taking into account the degree of similarity of goods. In this case, the IPC Presidium emphasised in Para. 162 of *SC Plenary Resolution № 10* that when comparing signs, the court takes into account which elements are similar (strong or weak elements of the trademark and the sign) and that similarity of only unprotected elements is not taken into account.

The first instance court has found that in applying Article 1483, Para. 7 of the Civil Code, Rospatent proceeded from the opinion that the verbal elements "Crimean" and "oils" were strong. As the first instance court noted, and the IPC Presidium confirmed, elements which are recognised as descriptive and non-dominant for the purposes of Article 1483, Para. 1 of the Civil Code may not be considered strong for the purposes of Para. 7 of the same Article. As a result, the IPC Presidium indicated that when re-examining the appeal, Rospatent should compare the claimed sign with the sign "Crimean Soap", taking into account the properly defined strong and weak elements of the claimed sign and the pictorial elements.

The cassation appeal also contains the following argument. In accordance with the provision of Para. 47 of Administrative Rules No. 482, not the entire claimed sign should be compared with the designation "CRIMEAN SOAP" for the purposes of the provisions of Art. 1483, Para. 7 of the Civil Code. Instead, it should be only its verbal (albeit unprotected) elements "Crimean" and "Oils", because (1) the confusion of appellation of origin with a separate element of the trademark is sufficient, and (2) only the verbal part of the sign is subject to comparison with the appellation of origin.

With regard to the first argument, the IPC Presidium has pointed out the contradiction with the wording contained in Article 1483, Para. 7, of the RF Civil Code applicable to the dispute, which refers to the sign as a whole. With regard to the second argument, the IPC Presidium has pointed to the contradiction between the substance of this norm and the established judicial practice, as the Code does not impose restrictions on the comparison of appellations of origin of goods with any types of trademarks (including pictorial ones) or any types of trademark elements (including pictorial ones).

5. Max and Jack Walk into a Bar

IPC Presidium Ruling of 02 October 2023 in Case No. SIP-1012/2022

For the purposes of Article 1483, Para. 10 of the RF Civil Code, signs that are independent lexical units cannot be divided into separate verbal elements. In this case, it is the perception by the target consumer group of the word

combination as a single element or as several lexical units that is decisive, and not the grammatical analysis.

Rospatent has rejected an invalidity action by Jack Daniel’s Properties against the registration of the trademark “Max & Jack’s” by Premier Beverages Company in respect of beer and soft drinks in ICGS Class 32 and alcoholic beverages in ICGS Class 33. Appealing to the first instance court, Jack Daniel’s Properties challenged Rospatent’s decision in respect of ICGS Class 33 goods on the grounds of violation of the provisions of Para. 3, Subpara. 1, Para. 2, Para. 6, and Para. 10 of Article 1483 of the Civil Code. The first instant court also rejected the appeal, but the IPC Presidium overturned the court’s ruling. It is noteworthy that in remanding the case for a new proceeding, the IPC Presidium emphasised the mediability of the dispute and invited the companies to consider an amicable settlement. In July 2024 the proceedings were indeed terminated due to an amicable settlement.

In its ruling, the IPC Presidium firstly has pointed to a violation of the methodology for assessing the similarity between the contested sign and the earlier trademarks of Jack Daniel’s Properties. Rospatent concluded that the compared signs were perceived differently. The first instance court also has stated that the level of similarity between the two was particularly low, leading to the conclusion that there was no confusion even if the goods matched. The IPC Presidium has pointed out that the court did not take into account that there are two variants of confusion between two signs compared, according to Para. 162, Subpara. 2 of the *SC Plenary Resolution № 10.* The first situation of confusion is straightforward: the consumer confuses two marks with each other. However, confusion is also possible when the consumer realises that the signs involved are different, but she may believe that the later sign is used by the person or persons related to the earlier trademark owner. The IPC Presidium has noted that, unlike the first situation of confusion, in the second case, the consumer realises that there are differences between the signs, sees them, but can reasonably conclude from certain features of the marks that they are used by the same person. Also the IPC Presidium has noted that the conclusion of the first instance court that the disputed registration complied with the provisions of Article 1483, Para. 3, Subpara. 1 of the Civil Code was derived from the conclusion made in respect of Article 1483, Para. 6, Subpara. 2 of the Code. Therefore, the case also must be re-examined in this part, too.

Secondly, the IPC Presidium pointed out that the first instance court incorrectly applied the methodology for assessing the validity of a trademark when opposing an earlier trademark within the meaning of the provisions of Article 1483, Para. 10 of the Civil Code. Examination, which should also been carried out in accordance with Para. 162 of the *SC Plenary Resolution № 10*, subject to the peculiarities of Article 1483, Para. 10 of the Civil Code, should lead to the conclusion that there is a likelihood of confusion between the earlier trademark, in this case "JACK", and the element of the later trademark "Max & Jack's." The first instance court concluded that "Max & Jack's" is a single lexical unit, and therefore the element "Jack" cannot be separated from it for the purposes of applying Article 1483, Para. 10. The IPC Presidium disagreed, stating that the conclusion of the first instance court was based only on grammatical analysis, while from the point of view of methodology it was necessary to investigate whether the target consumer group perceived the disputed sign as a single element or as two independent lexical units.

6. Slang is Legal, Too

IPC Presidium Ruling of 30 October 2023 in Case No. SIP-109/2023

When determining the independence of the lexical meaning of a sign, it is necessary to take into account the ability of language to develop, and modern trends of capturing phonetics and semantics with the help of slang abbreviations, which are clearly understandable to the consumer target group.

Rospatent has refused an applicant to register the designation "Hi4U" (filed in English) for a wide range of goods and services, and also rejected a subsequent applicant's appeal to this decision. In doing so, Rospatent has found that this sign lacked both inherent and acquired distinctiveness.

The first instance court invalidated the decision of Rospatent on the grounds of Art. 1483, Para. 1 of the Civil Code (distinctiveness).

In particular, Rospatent proceeded from the fact that the disputed sign does not have a verbal nature within the meaning of Para. 34 of Administrative Rules No. 482, whereas the court found that the sign consists of elements that have a verbal nature: a phonetical composition, lexical meaning, lexico-grammatical features, and the ability to perform a syntactic function. According to the court, based on the phonetic perception of the Russian consumer, the claimed sign 'Hi4U' has an independent semantic meaning.

The IPC Presidium has left the court decision unchanged and Rospatent's appeal unsatisfied, noting the following.

The IPC Presidium has reminded that, based on the provisions of Article 1483, Para. 1 of the Civil Code and Administrative Rules, signs that do not fulfil the main function of a trademark in the eyes of consumers, namely the differentiation function, may not be registered as trademarks.

The Presidium has stated that the court had correctly determined on the basis of the phonetic criterion that the sign had a special semantics in the perception of the ordinary consumer, taking into account that the combination "4U" was a neologism in the Russian language.

In doing so, the IPC Presidium has noted that in modern linguistics, slang abbreviations represent a norm of communication and are used as independent lexical units, which are formed by using combinations of letters and numbers in place of one or more words (e.g., "2day", "2much") and abbreviations down to one letter (e.g., "R" instead of "are", and "U" instead of "you"). Such simple abbreviations are common and, since the emphasis is on the sound rather than the spelling of the abbreviated form, the phonetic feature determines the presence of the semantic one.

B. Early termination of protection for lack of use

7. Not Just Any Claim by Right holder Can Prove Interest

IPC Presidium Ruling of 20 October 2023 in Case No. SIP-888/2022

A dispute on the protection of a trademark between the person requesting early termination of the legal protection of this trademark for lack of use and its right holder may confirm the existence of legal standing in the latter proceedings.

If a claim for protection of the right to a disputed trademark has not been filed or a judicial act has not been issued, when considering a case on early termination of legal protection of a disputed trademark, the first instance court has the right to assess whether in fact those actions in which the right-holder sees a violation of their exclusive rights are evidence of the use of a trademark for individualisation of similar goods.

The Modimio company has filed a lawsuit with the court for early termination of legal protection of several trademarks of the GAZ company. Upon receiving a rejection of the claim due to lack of evidence of interest (legal standing), the claimant appealed to the IPC Presidium. In rejecting the cassation appeal, the IPC Presidium provided *inter alia* the following clarifications.

The claimant referred to the existence of an application for a trademark with the sign "GAZ", but the first instance court has found that the application had been filed after the pre-trial claim had been sent to the right holder, so it could not be used to confirm the intention to use the trademark in the claimant's activities. The IPC Presidium has confirmed that such an application could not be taken into account in assessing if legal standing existed at the time of the interested party's proposal.

The first instance court also did not accept the receipt by the claimant of a claim from the right holder regarding infringement of the latter's rights to the trademarks it owned as evidence of interest, since the claim did not relate to the protection of exclusive rights to specific disputed trademarks or related to dissimilar goods. The IPC Presidium has found this conclusion to be justified, noting the following.

If in relation to a claim brought in defence of an exclusive right there is already an effective judgment which has established that the infringer uses a mark similar to the trademark to differentiate homogeneous goods, then, in considering a dispute on early termination of legal protection of a trademark, the first instance court shall not need to re-establish the fact of use of the trademark, taking this circumstance as evidence of interest.

If a claim for protection of the right to a disputed trademark has not been filed (as in the case at hand) or a judgment has not been issued, when considering a case on early termination of legal protection of a disputed trademark, the first instance court has the right to assess whether in fact those actions in which the right holder sees a violation of their exclusive rights are evidence of the use of a trademark for individualisation of similar goods.

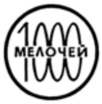
C. Unfair competition

8. Unfair purchase does not equal unfair registration

IPC Presidium Ruling of 23 October 2023 in Case No. СИП-71/2023

Unfair actions taken for derivative acquisition of rights to a means of differentiation do not indicate, *per se*, **that the initial acquisition of the said**

rights was defective and that Article 1512, Para. 2, Subpara. 6 of Civil Code may thus be applied.



On 31 May 2017, an individual entrepreneur has acquired rights to the disputed service mark, registered on 20 December 1999 upon application by the 1000 Melochey (*Tysyacha Melochey*) Trade and Production Company.

The 1000 Melochey company has challenged the registration of that service mark before Rospatent on the grounds that in separate judicial proceedings the individual entrepreneur's actions leading to the acquisition of the said service mark were found to have been an abuse.

Rospatent has allowed this invalidity action on the grounds of Article 1512, Para. 2, Subpara.6 of Civil Code, by finding the granting of legal protection to the disputed service mark invalid in its entirety.

The individual entrepreneur applied to the IPC asking it to overrule Rospatent's decision.

The IPC' first instance has concluded that derivative acquisition of the exclusive right to a disputed service mark found unfair did not indicate, *per se*, that the initial acquisition of the said right had also been faulty.

The first instance court also has noted that, in the situation under review, the application of Para. 2, Subpara. 6 of Article 1512 of the Civil Code to derivative acquisition of the exclusive right to a service mark (pursuant to a contract) was contrary to the existing legislation.

After considering 1000 Melochey's and Rospatent's cassation appeals, the IPC Presidium upheld the first instance ruling and pointed out that Article 1512 of the Civil Code was only applicable where the actions leading to the registration of a disputed distinctive sign were found unfair at the stage of application. Conversely, the above actions by the entrepreneur led to derivative acquisition of the exclusive right to the disputed service mark, rather than initial to which Para. 2, Subpara. 6 of Article 1512 applied.

The IPC Presidium has noted that in separate judicial proceedings the initial owner's (1000 Melochey Trade and Production Company's) actions had not been assessed for fairness at the time of service mark registration, so it is wrong to consider as unlawful the registration of the service mark in retrospect due to any unfair actions by a subsequent owner.

The IPC Presidium also considered that unfair acquisition of the exclusive right by a subsequent derivative owner (as in this case) had been a wrongdoing by a person, who was not involved in the registration. Thus retrospective termination of the legal protection of the disputed service mark could not be a sanction against that person, nor was it in line with the substance of the legal relations under scrutiny. The validity of the initial registration could not be assessed without regard to the conduct by the person who sought registration and without involving all the successive owners, for retrospective termination of legal protection affected their rights.

II. Procedure

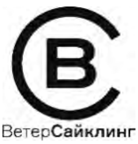
A. Interim measures

9. Injunction should work

IPC Presidium Ruling of 10 November 2023 in Case No. SIP-898/2023

Finding likelihood of confusion between two competing trademarks depends not only on the degree of similarity between the signs and the goods for ordinary consumers of the relevant goods, but also on other factors, *inter alia* whether the right holder uses the earlier trademark in respect of specific goods.

Consequently, in proceedings on a claim for early termination of legal protection of the earlier trademark for lack of use it is possible to satisfy a motion for interim injunction preventing Rospatent from taking decisions in respect of the claimant's trademarks, whose legal protection is challenged on the grounds of the defendant's earlier trademark.

The Veter Sport Limited Liability Company (hereinafter referred to as 'Company') owns trademarks No. 792003  and No. and 891549 veterrunning («older trademarks»). Later it applied to Rospatent for the registration of the following signs: ВЕТЕР, VETER, and V⚡t⚡r, as trademarks in respect of ICGS Class 25 goods («new application»).

Rospatent denied registration of these signs as they created a risk of confusion with earlier trademarks No. 749459 Veter and No. 749644 ВЕТЕР, that belonged to Ms. V.A. Abel.

V.A. Abel challenged the registration of the Company's older trademarks on relative grounds by referring to its earlier trademarks (violation of Article 1483, Para. 6, Subpara. 2).

In return the Company has claimed early termination for lack of use of Ms Abel's trademarks Nos. 749459 and 749644 in respect of all ICGS Class 25 goods, as these trademarks were both blocking the registration of new trademark and could lead to the invalidity of its older trademarks.

Along with that claim, the Company has filed a motion for interim measures in the form of an injunction banning Rospatent from taking the following actions until a judgement took force in that case:

examining, and taking decisions on, V.A. Abel's invalidity appeal against the registration of the Company's older trademarks Nos. 792003 and 891549;

examining, and taking a decision on, the Company's appeal against the Rospatent's decision to deny trademark registration pursuant to the Company's new application.

According to the applicant, both interim measures where directly related to the subject-matter of the case on early termination of Ms. Abel's trademark.

The first instance court allowed the claim in part, as it banned Rospatent from taking a decision on the Company's appeal against the decision to deny trademark registration pursuant to the new application until a judgement was passed in that case. The remainder of the Company's motion was dismissed.

Referring to the legal position of the Plenum of the Russian Federation Supreme Court, as set out in Para. 58 of its Resolution No 15 of 01 June 2023, that a motion for interim measures should relate to the claimant's own TM applications and should not affect others' rights and lawful interests, the first instance court held that an interim measure such as an injunction suspending Rospatent's invalidity proceedings against the Company's trademarks Nos. 891549 and 792003 was unrelated to the Company's «own application» and affected Ms. Abel's rights and lawful interests in challenging the Company's trademarks.

Therefore, the first instance court found no grounds to take the abovementioned interim measure and dismissed the Company's motion in the respective part.

As the IPC Presidium examined the Company's cassation appeal, it noted that the claim for early termination of the legal protection of V.A. Abel's earlier trademarks, based on which Ms. Abel has challenged the validity of the Company's older trademarks before Rospatent, was a proper method for finding facts that are material to subsequent examination of the invalidity challenge at Rospatent.

Indeed, in Para. 162 of *its Plenary Resolution № 10 the Supreme Court* noted that one of the essential criteria to establishing the likelihood of confusion between competing trademarks, particularly to checking the junior sign for relative grounds of validity based on an earlier trademark (conformity with Article 1483, Para. 6 of the RF Civil Code), was whether the owner of the earlier trademark used it in respect of specific goods.

The IPC Presidium held that the likelihood of confusion depended not only on the degree of similarity between the signs and the goods for ordinary consumers of the relevant goods, but also on other factors, such as whether, how long and how extensively the owner has used the trademark in respect of specific goods. Consequently, where the earlier trademark is not in use, consumers of the relevant goods and service could establish no associative link to the trademark or its specific owner and were thus unlikely to confuse the trademarks compared, as the earlier trademark was less than recognizable.

The IPC Presidium thus found the interim measure sought to be related and proportionate to the subject of the dispute on early termination for lack of use and to be instrumental to the actual achievement of interim measures' purpose.

Given that Rospatent had not yet taken the respective decisions at the time of the examination of the cassation appeal, and given the urgency of considering the application for interim measures, the IPC Presidium has found it possible not to remand the Company's motion for interim measures for re-examination and to pass instead a new judicial act in that case and satisfy the above motion.

10. Trademark Gambit. Early Termination Vs. Challenge

IPC Presidium Ruling of 11 October 2023 in Case No. SIP-617/2023

The court may impose interim injunctions banning Rospatent from taking a decision on an appeal, filed by the owner of an earlier trademark (Article 1483, Para. 6, Subpara. 2 of Civil Code), where the use of that earlier trademark is disputed.

On the grounds of Article 1483, Para. 6, Subpara. 2 of Civil Code, CAROMI Company has brought a challenge before Rospatent, objecting to the provision of legal protection to the CAROMIC trademark belonging to the Caromic company, citing a likely confusion between the disputed trademark and the CAROMI's earler trademark, CAROMI.

In turn, Caromic insisted that CAROMI was not using the opposing trademark, so they had sent the latter an interested party's proposal — a mandatory pre-trial settlement proposal. If CAROMI failed to meet their stated demands, then Caromic was planning to claim early termination of the opposing trademark for lack of use before the IPC.

Also Caromic went to the court, asking to take interim measures pending the filing of their claim, as the examination of the invalidity appeal and possible cancellation of the legal protection of their own trademark, opposed to the unused trademark, would lead Rospatent to pass an illegal ruling that the company would then have to challenge in court.

The first instance court has rejected the application for interim measures.

In turn, the IPC Presidium has pointed out that the examination of an appeal filed under Article 1483, Para. 6, Subpara. 2 of Civil Code required Rospatent to assess the likelihood of confusion between the competing trademarks, which, in turn, involved finding out whether the owner used the earlier trademark in respect of specific goods.

The IPC Presidium has stated that if the eventual claim for early termination of the legal protection of the earlier trademark were to be satisfied, that would mean that the non-use of the opposing trademark would have to be taken into account in assessing the likelihood of confusion between the competing trademarks.

The IPC Presidium stressed that non-use of the earlier trademark by its owner might be taken into account as a factor suggesting that confusion between the disputed trademark and the unused earlier trademark was unlikely (as consumers were not aware of the earlier trademark).

In view of the foregoing, the IPC Presidium held that under the said circumstances the first instance court had no grounds to dismiss the application for interim measures.

On the other hand, the IPC Presidium has noted that, at the time of the examination of their cassation appeal, Caromic had already filed a claim against CAROMI for early termination of the legal protection of the CAROMI trademark.

Because of it, the IPC Presidium has found it impossible to satisfy the claim for interim measures where Caromic would thereafter file their claim, for Caromic had already fulfilled that requirement.

The IPC has concluded that Caromic was thus entitled to apply to the first instance court for taking measures to secure the claim.

B. Procedure at Rospatent

11. The Limits of Independence

IPC Presidium Decision of 21 November 2023 in Case No. SIP-3/2023

When considering an invalidity claim against a registered trademark, Rospatent may not identify and evaluate any new grounds that are not disclosed in the applicant's appeal.

Upon considering an administrative appeal to trademark registration, Rospatent has decided to partially invalidate it. However, it was not on the grounds contained in the invalidity application (Para. 1, Subpara. 1, and Para. 8 of Article 1483 of the Civil Code), but on the grounds identified on its on by Rospatent (Para. 1, Subpara. 3 and Para. 3, Subpara. 1 of Article 1483). In doing so, Rospatent followed the provision of Para. 45 of the Rules for Assessment and Resolution of Administrative Disputes by Rospatent, approved by Order of the Ministry of Science and Higher Education and the Ministry of Economic Development No. 644/261 of 30 April 2020 ("Patent Dispute Regulations"). This Paragraph provides that "the grounds for invalidating the granting of legal protection to an intellectual property object or the grounds preventing the granting of legal protection shall be recorded in the minutes of the panel meeting and shall be taken into account when forming the panel's conclusion on the results of the consideration of the dispute."

The company that filed the appeal and the trademark rightholder challenged the Rospatent's decision in the Intellectual Property Court, but the first instance court dismissed the claims.

The IPC Presidium has cancelled the decision of the first instance court and passed a new judgement invalidating Rospatent's decision.

The IPC Court has reminded that the Patent Dispute Regulations have less legal force and should be applied subject to the norms of the Civil Code, and pointed out that Para. 45 of the Patent Dispute Regulations is applied differently based on whether the refusal to grant legal protection to a trademark is being challenged or Rospatent is considering an appeal against an already registered trademark.

In the former case, since legal protection has not been granted to the trademark, the provisions of the Civil Code governing the procedure for granting the right shall apply. Rospatent may analyse the issue of an object's validity within the limits established by the Civil Code.

In the latter case, the legal protection of the trade mark has been granted, which means that the presumption of validity arising from the registration of the right to the trademark can be defeated only through the procedure established by the legislator. In this case, the IPC Presidium relies on the position of the Russian Federation Constitutional Court in its Ruling of 03 July 2018 No. 28-P, which states that registration of the exclusive right to a trademark contributes to legal certainty in commerce that allows the parties to the legal relations to reasonably foresee the consequences of their behaviour and to be sure that their officially recognised status, acquired rights and obligations would remain unchanged.

Taking into account the provisions of Article 1512, Paras 1-3 of the Civil Code, the IPC Presidium has clarified that civil law does not give Rospatent any other possibility to verify the validity of the registered trademark outside the appeal filed by the interested party. Rospatent has no right to identify and evaluate any new grounds that have not been disclosed in the interested party's appeal. The court cannot use Para. 45 of the Patent Dispute Regulation because it does not comply with the provisions of Articles 1512 and 1513 of the Civil Code that have a greater legal force (Article 12 of the Civil Code, Article 13 of the Code of Commercial Procedure).

Moreover, the IPC Presidium notes that if in such a situation part of the appeal is considered to be filed by Rospatent, then its constitutional function as a body considering an administrative dispute is violated: Rospatent has its own interest, evaluates this interest, and then considers its own opposition on the merits.

The Presidium of the IPC has satisfied the cassation appeal of the initial trademark right holder, invalidated the decision of Rospatent and ordered it to restore legal protection to the disputed trademark.

Later in 2024, Para. 45 of the Patent Dispute Regulations was partially invalidated by the IPC Presidium in separate judicial proceedings (IPC Presidium Ruling of 16.08.2024 № SIP-1302/2023).

Information about the authors:

M.A. Kolzdorf — LLM, Senior Lecturer.

N.I. Kapyrina — Candidate of Sciences (Law), Associate Professor.

N.E. Goloyad — Master of Sciences.

Contribution of the authors:

M.A. Kolzdorf — Para 3.

N.I. Kapyrina — Para 1, 4–7, 11.

N.E. Goloyad — Para 2, 8–10.

The article was submitted to editorial office 14.08.2024; approved after reviewing 30.09.2024; accepted for publication 15.10.2024.

Legal Issues in the **DIGITAL AGE**

AUTHORS GUIDELINES

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

Article Length

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

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

Article Title

The title should be concise and informative.

Author Details

The details about the authors include:

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

Abstract

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

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

Keywords

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

References

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

A reference list should be attached to the article.

Footnotes

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

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

ARTICLES

D.I. Tekutyev
Key and Issues of Private Law Transformation under Influence of Behavioural Economics and Data Science 4

L.M. Pakhomova
Acceptance of Goods and Services under the Contractual System: Regulation and Digitization Issues 19

A. Duflot
Artificial Intelligence in the French Law of 2024 37

G.I. Uvarkin
Copyright Protection for Characters in Transmedia Environment 57

COMMENTS

M.A. Kolzdorf, N.I. Kapyrina, N.E. Goloiad
Key Issues in the Intellectual Property Court's Presidium Rulings 78

REVIEWS

M.S. Sitnikov
The Russian Legal Researches on Metaverses: a Scholar Review 98

MD. Mahmud Hasan
Regulating Artificial Intelligence: A Study in the Comparison between South Asia and Other Countries 122

ARTIFICIAL INTELLIGENCE AND LAW

A.A. Kartskhiya
Legal Horizons of the New Artificial Intelligence Paradigm 4

I.G. Ilyin
Progress in Natural Language Processing Technologies:
Regulating Quality and Accessibility of Training Data 36

IT, INDUSTRIES, LAW: TELEMEDICINE

B.A. Edidin, A.V. Bunkov, K.V. Kochetkova
The Use of AI in Medicine: Health Data, Privacy Risks and More 57

G. Rousset
The French Telemedicine System: Challenges, Procedures
and Difficulties. 80

IT, INDUSTRIES, LAW: MEDIA

Reeta Sony A.L., Shruti Chopra
Regulating Digital Era: A Comparative Analysis of Policy Perspectives
on Media Entertainment 97

E- GOVERNMENT

E.V. Burdina, V.N. Kornev
Technologies Versus Justice: Challenges of AI Regulation
in the Judicial System 113

A.A. Doschatov
Digitizing Law-Making at Federal Executive Agencies 127

REVIEW

L.K. Tereschenko, O.E. Starodubova, N.A. Nazarov
Digital Platforms in the Focus of National Law 148

DIGITAL AGE: CIVIL LAW

R.N. Adelshin
Obligations in the Digital Environment: Legal Doctrine. 4

DIGITAL AGE: LABOUR LAW

M.O. Buyanova, E.S. Batusova
Legal Regulating Electronic Employment Contracts
as a Modern Factor of Integration at International Regional Bodies
(Exemplified by EEU, CIS and BRICS States Legislation). 31

IT, INDUSTRIES, LAW

Li Yao
Legal Regulation of Smart Wearable Devices in China 49

E-GOVERNMENT

A.V. Belyakova
Artificial Intelligence in the Judiciary: Issues and Outlooks 68

L.V. Saenko, P.A. Nepomnyaschiy
Child Neglect and Juvenile Delinquency Prevention Bodies:
Priorities and Prospects in Context of Digitization 88

INTERNATIONAL LAW AND CYBERSECURITY

E.A. Martynova
Collective Countermeasures in Response to Cyber Operations
under International Law 103

LEGAL INFORMATICS

S. Sharma, R. Shandilya, D. Dwivedi, M. Pant
eLegalls-as-a-Service: Towards Developing Cloud-based
Legal Tech System to Aid Lawyering in the Digital Age. 129