DOI 10.52468/2542-1514.2021.5(4).5-19

DIGITAL PROFILE: THE CONCEPT, REGULATORY MECHANISMS AND ENFORCEMENT PROBLEMS**

Elena V. Vinogradova[1], Tatyana A. Polyakova[1], Alexey V. Minbaleev[1,2]

[1] *Institute of State and Law of the Russian Academy of Sciences, Moscow, Russia*

[2] *Kutafin Moscow State Law University (MSAL), Moscow, Russia*

Article info

Received –
2021 August 01
Accepted –
2021 October 10
Available online –
2021 December 24

Keywords

Digital profile, identification, legal regulation, social scoring, digital transformation, digital technologies, information technologies, digital economy

The subject of the research is the legal nature of the digital profile of a citizen, as well as a set of legal norms regulating digital profiling relations in Russia.

The comparative method, the method of system analysis, as well as the method of legal modeling are used in the article.

The purpose of the article is to confirm or disprove the hypothesis that legal regulation is not the only mechanism for regulating relations in the field of digital profiling.

The main results, scope of application. The article studies the phenomenon of digital profile, the main approaches to the digital profiling as well as the circumstances that have caused the state's interest in digital profiling. The creation and operation of a digital profile should be aimed at achieving the goal set out in the legislation. The digital profile is a set of relevant, reliable information about individuals and legal entities formed in the unified identification and authentication system or other information systems of state and local government authorities. The formation of a digital profile is carried out in order to provide data to authorities, legal entities and persons who have requested access to this information through the digital profile infrastructure. The analysis of the Russian legal regulation of relations in the field of digital profiling is presented, the problems of enforcement practice are identified. The analysis revealed the main differences between the digital profile and related categories, including social scoring, the unified population register and others. The comparison of a digital profile with a digital avatar and a digital character was carried out. It is extremely important to pay close attention to the problems of digital profiling both at the level of fundamental and applied scientific research. At the state level, it is important to strategically determine what a digital profile is, as well as formulate the main directions of the digital profiling development, challenges and risks. The importance of the development of digital profiling for unified system of public authorities in the Russian Federation is outlined.

Conclusions. The analysis of the emerging practice of digital profiling in contemporary society shows that legal regulation does not always allow us to keep up with the rapidly developing relations in this area. The possibility of using other mechanisms should be considered. The use of mechanisms of regulatory experiments can also be considered as special mechanisms for regulating relations in the field of digital profiling. The goal of the research has been achieved, the legal nature of the digital profile has been revealed, approaches to regulating this phenomenon in the conditions of digital transformation have been proposed.

** The article was prepared within the framework of the state task no. 0136-2021-0042 “Legal regulation of the digital economy, artificial intelligence, information security”.

ISSN 2542-1514 (Print)

1. Introduction

Digital profiling is the process of collecting and analyzing data on individuals or legal entities, including data on the Internet. Digital profiles make a significant aspect of human life today, and this significance affects one's personalization in their social life and self-actualization in ever more aspects of personal and professional life. M. Hildebrandt notes the importance of digital profiling in today's world and mentions that "both corporate and global governance seem to demand increasingly sophisticated means for identification... citizens are screened, located, detected and their data stored, aggregated and analysed. Potential customers are profiled to detect their habits and preferences in order to provide for targeted services." [1] Generation and use of digital profiles becomes integral to digitalization and use of the ever emerging breakthrough digital technologies in the practices of public authorities [2, p. 27; 3, pp. 77-78; 4, pp. 45-46]. Thus, customer digital profiles constitute, along with the Remote ID Platform (the Unified Biometric System), the Faster Payments System, and the Marketplace Platform, a core infrastructure project based on digital technologies that the Bank of Russia imposes severe security requirements on[1].

COVID-19 has been a booster to digital profiling [5-8]. As remote services developed, digital profiling gained traction in commercial applications and public administration alike, as people had to create a multitude of accounts, digital avatars, characters, and profiles. Collection and processing of massive amounts of Internet users' personal data facilitated the creation of special digital profiling systems and other personal data collection and processing systems. Active adoption of digital tech [9] including AI [10-14] helped advance digital profiling, too.

Relations that emerge in digital profiling tend to develop chaotically, which alarms the society and gives rise to concern regarding possible violation of human rights and freedoms pertaining to personal data processing [15, p. 73-75]. Thus, some ordering needs to be applied. Today, it is crucial to define what the digital profile is, find out what regulatory mechanisms applicable to digital modeling could be used by the state and the public to effectively adopt and use digital profiling.

2. Digital Profile: Concept and Legal Regulation

Today's law enforcement and legal science, unfortunately, lack a single definition of digital profile. One of the more common definitions of digital profile, which is used by public authorities that handle such profiles, is presented in the bill *On Amendments to Certain Legislative Acts (Regarding Clarification of Identification and Authentication Procedures).* Digital profile is defined therein as "collection of data on individuals or legal entities contained in the data systems operated by public authorities and organizations vested with certain public powers under Federal Laws, as well as in the Unified Identification and Authentication System (ESIA)."[2]

Unfortunately, this definition fails to reflect the purpose of collecting such data or to present qualitative characteristics thereof. In fact, this definition implies that any such data on individuals or legal entities stored in such systems constitutes a digital profile. It seems that only specific systems can generate a digital profile and need to be borne in mind within the framework of defining the digital profile. Data collection and processing may only pursue a legitimate goal. Accuracy and up-to-dateness of data in the digital profile need to be mentioned as well.

Federal executive authorities use a different definition. Thus, Guidelines of the Ministry of Digital Development, Communications, and Mass Media (Mincomsvyaz) of April 2, 2021, titled Digital Profile

[1] Key Trends in Information Security in Credit and Finance in 2019-2021. Document cited as published on https://www.cbr.ru as of Sep 28, 2020 // SPS Consultant Plus.

[2] Draft Federal Law On Amendments to Certain Legislative Acts (Regarding Clarification of Identification and Authentication Procedures) (drafted by the Russian Ministry of Digital Development, Communications, and Mass Media, text cited as of March 25, 2019; bill not presented to the State Duma of the Federal Assembly of the Russian Federation). Text cited as published on http://regulation.gov.ru/ as of March 25, 2019 // SPS ConsultantPlus.

ISSN 2658-4050 (Online)

Infrastructure: Scenarios of Use. Ver. 1.2 define the digital profile as a set of digital records on a citizen as found in the information systems of public authorities and organizations[3]. A similar definition is set forth in *Digital Profile Concept and Architecture — ESIA 2.0,* a document developed by Minkomsvyaz and the Bank of Russia as part of the Information Infrastructure Plan under the program Digital Economy of the Russian Federation.

This definition is used in textbooks as well [16, p. 41]. However, it is not without flaw either, as it links the digital profile exclusively to the information systems operated by public authorities and organizations. Beside, it uses another concept, "digital record", which is not defined. In these Guidelines, the concept of digital profile does not apply to legal persons, so it would better worded as "digital profile of an individual".

Digital Profile Infrastructure: Scenarios of Use sets forth that "one of the functions of the Digital Profile is to provide an individual's data contained in the ESIA and in other public information systems connected to the ESIA by the Unified System of Interdepartmental Electronic Interaction (SMEV), upon said individual's consent and to their best interests, e.g., to a bank as part of application for a loan, and that the digital profile builds upon:

- individual's up-to-date, verified data found in the ESIA and other public information systems connected thereto;

- a distributed data structure that contains links to data generated upon queries submitted to the corresponding state registers;

- an ability to manage the individual's digital consents to the processing of their personal data retrievable from their digital profile, to which end a consent management service (the Consent Platform) must be in place[4]. It is implied that in this case, the use of the Unified Identification and Authentication System is optimal for the Russian Federation. To date, the Ministry of Digital Development has even adopted the updated ESIA Guidelines that have been amended to take into account the updated digital profiling functionality[5]. However, its definition that says that "digital profile data are generated in, and provided by, the information systems of public authorities and organizations" is apparently incomplete and inaccurate. Such data can be aggregated from any information systems operated by public authorities and local self-governments as well as by any SMEV-connected subordinate organizations thereof. It is these currently functioning information systems as well as any systems that should potentially be established under the single Public Government System enshrined in Russia's Constitution that must become the foundation for creating a digital profile institution in the Russian Federation. For instance, banks are actively joining the system today. According to the Letter of the Bank of Russia dated August 31, 2020 No. 35-3-3-2/213, "11 banks have already been connected to the Digital Profile, 8 more are preparing to join it down the line and are currently testing their respective infrastructures. The list of Digital Profile member organizations is to expand."[6]

Scientific literature does not offer a single definition of digital profile either. Thus, A.K. Zharova concludes that "a digital profile is a complex multi-tiered system created by the analysis of data found in all information systems and communication networks." [17, pp. 55-61] Some authors define the digital profile as a "person's metaprofile that contains links to legally significant records of that person in other public electronic registers." [18, pp. 22-23]

Analysis of legal regulations applicable to

[3] Guidelines of Mincomsvyaz *Digital Profile Infrastructure: Scenarios of Use. Ver.* 1.2 of April 2, 2021. URL: https://digital.gov.ru/uploaded/presentations/stsenariiispolzovaniyatspv12.pdf (retrieved July 20, 2021).

[4] Ibid.

[5] See: ESIA Guidelines. Ver. 2.84 dd. April 28, 2021. Approved by the Subcommittee for Use of IT in Provision of Public and Municipal Services, Government Committee for Digital Development and Use of IT Towards Better Quality of Life and Better Business Environment. URL: https://digital.gov.ru/uploaded/presentations/esiametodicheskierekomendatsii284_w7lEZQX.pdf (retrieved July 11, 2021).

[6] Letter of the Bank of Russia No. 35-3-3-2/213. dd. August 31, 2020. Question: On Credit Organizations' Access to Federal Tax Service's Data on Individuals' Income and Payments Transacted by Insurance Payers to Individuals // SPS ConsultantPlus. No. 198139.

ISSN 2542-1514 (Print)

digital profiling and of the emerging related law enforcement practices concludes that the digital profile is a set of up-to-date, accurate data and other information about individuals and legal entities found in the ESIA or other information systems of state and local government bodies, as well as organizations subordinate to them that interact with it through the SMEV in order to provide such data upon data owners' consent to subjects who have requested access to this information through the Digital Profile infrastructure.

A digital profile must always have a purpose (or several purposes), for which it is made and operated, that is, to allow actors to use the Digital Profile infrastructure to request individuals' or legal entities' consent to access their data, whereby the purposes of such data collection shall be set forth in law and by organizations or even individuals, including purpose statement by virtue of various agreements that are consistent with the applicable law. Paragraph 8, Subclause 3a of the Regulations on the Experiment Towards Better Quality and Coherence of Data in Public Information Systems as approved by the Government Decree No. 710 dd. June 3, 2019 state explicitly that the Digital Profile provides for "individuals' ability to monitor and manage organizations' access to their data contained in the ESIA and in public or municipal information systems."[7]

3. Digital Profile and Related Concepts

Digital profile is still an unstable concept in terms of how authorities, economic and social environments use it. In many ways, this is attributable to the fact that there are related concepts that individuals and the state need to deal with.

Today, digital profile is based on a particular dataset of individuals, as are some other systems. Those primarily include the Unified Population Register, the Unified Biometric System, and social scoring systems.

The digital profile mainly functions to provide an individual's data as requested by a public authority or an organization; social scoring, on the other hand, evaluates and differentiates subjects (customers, workers, passengers, etc.) involved in Internet relations on the basis of their social parameters and characteristics derived by the analysis of such persons' activity on the Internet and social media, which helps predict their behavior. This system mostly uses specialized AI-based software [19, p. 96; 20, pp. 41-44].

As social scoring is designed to evaluate a person's social characteristics, it is intended to predict their behavior by analyzing their social media presence and collecting data on what they browse on the Internet, what search queries they make, and what they buy. Social scoring uses such data as gender, age, residence, job, how long a person has work for the same company, etc. As a result, they are categorized, e.g., as whether being a potential customer, a potential buyer of goods of a specific class, etc. A customer can be assigned a rank, written as an integer and reflecting the trust and attention a business should place with them. Active use of "such source of information as a social medium helps derive an objective long-term assessment of a customer and their behavior regardless of their specific momentary intentions." [21]

Social scoring and digital profile data can even contain results of processing CCTV footage [22, 23, pp. 58-65] and further recognition [24, pp. 4-8]. Many profiles are based on digital trace that Internet users leave when visiting websites [25, pp. 37-40].

China's Social Credit System, which is designed to evaluate each citizen's credibility and trustworthiness, is one of today's most successful yet most controversial government-run scoring systems. Officially, it all started as far back as in 2007. The system is regulated by the Social Credit System Planning Outline (2014-2020) as adopted by the State Council on June 27, 2014, as well as by the State Council Guiding Opinions concerning Establishing and Perfecting Incentives for Promise-keeping and Joint Punishment Systems for Trust-

[7] Regulations on the Experiment Towards Better Quality and Coherence of Data in Government Databases, appr. by the Government Decree No. 710 dd. June 3, 2019 (rev. April 16, 2021) On the Experiment Towards Better Quality and Coherence of Data in Public Information Systems together with the Regulations on the Experiment Towards Better Quality and Coherence of Data in Government Databases. http://pravo.gov.ru, June 7, 2019.

Breaking, and Accelerating the Construction of Social Sincerity (adopted by the State Council on June 12, 2016). By the design of this System, every resident of China should by 2020 be present in the National Database that collects fiscal and governmental data including minor violations of traffic, and converts all such data into a single score, which becomes part of the person's profile; country-wide ranking is applied. China's new Civil Code entered into force on January 1, 2021 (adopted at the Third Session of the 13th National People's Congress on May 28, 2020), which officially and legally enshrines the new "social credit system".

China has implemented and continues to operate its Social Credit System https://www.creditchina.gov.cn/, which in fact serves as the official government database for credit scoring of individuals and organizations. "Scoring is based on four key criteria: integrity in public affairs, good business practices, social behavior, and judicial history. AAA corresponds to a score of 1050 and constitutes the highest possible rating, followed by AA at 1000 points, B, C, and then D, the lowest possible rating at 599 points. D-rated persons have limited opportunities and even rights, as they may no longer move freely across the country, have difficulties with employment, and can even compromise the scores of their better-credited fellow citizens simply by virtue of communication. Thus, low-score people experience social isolation [26, p. 314]. A similar system is in place for legal entities: companies are rated for their environmental and legal compliance. Working conditions and occupational safety as well as financial accounts are subject to evaluation as well.

According to the new requirements valid since 2021, China's "new Code sets forth scoring points for participation in charitable activities, caring for elderly family members, good relations with neighbors, aiding the poor, blood donations, posting on social media in support of the government, a good credit history, any heroic deeds, etc. Score can be reduced for traffic violations, protesting against the government or anti-government post on social media, unsatisfactory assistance to elderly parents, spreading rumors and fakes on the Internet, insincere apologies for offences, participation in sectarian activities, cheating in online games, etc." Social crediting criteria are subject to change. For instance, in March 2020, citizens infected with the novel coronavirus and hiding the fact of such infection were fined by lowering their socials core[8].

Provinces also develop their social credit frameworks on top of the national one. Thus, Shandong has recently adopted its *Foundations for the Construction of Social Credit System in Shandong Province in 2021*[9]. Tianjin, Guangdong, and Gansu have adopted similar documents.

Unlike social scoring, the Unified Population Register and the Unified Biometric System are more similar to digital profiling. Pursuant to Art. 2 of the Federal Law No. 168-FZ dd. June 8, 2020 On the Unified Federal Information Register of the Russian Federation's Residents, the Federal Register is a "set of data on the Russian Federation's residents collected under this Federal Law from data on Russian citizens, aliens, and stateless persons listed in Cl. 6.2 of the Federal Law On the Unified Federal Information Register of the Russian Federation's Residents, which data is found in state information systems operated by the public authorities and administrations of public non-budgetary funds of the Russian Federation[10].

The purpose of creating and maintaining this Federal Register is to have a system of up-to-date and accurate data on the Russian Federation's demographic [27, pp. 28-31]. Thus, unlike digital profiling that collects data on individuals and legal entities to provide such data to other parties, including (and mainly) for commercial purposes, data in the Federal Register is processed mainly for the purposes of e-government. Within the

[8] Hiding Coronavirus-Infected Chinese to Lose Social Credit. URL: https://www.tadviser.ru/index.php/ (retrieved: July 17, 2021).

[9] Notice on the release of *Foundations for the Construction of Social Credit System in Shandong Province in 2021*. URL: https://www.creditchina.gov.cn/zhengcefagui/zhengcefagui/difangzhengcefagui1/202105/t20210514_234678.html (retrieved July 17, 2021).

[10] Federal Law No. 168-FZ dd. June 8, 2020 On the Unified Federal Information Register of the Russian Federation's Residents. http://www.pravo.gov.ru, June 8, 2020.

ISSN 2542-1514 (Print)

framework of the Unified State Cloud Platform, potential merger of all citizen identification and data systems into one is becoming subject to ever more active discussion [3, p. 183; 28, pp. 26-30].

Russia operates its special Unified Biometric System that processes biometric personal data. Federal Law on Information, Information Technology, and Information Security defines this system as a single personal data system that processes, collects, and stores biometric personal data, verifies such data, and reports on whether and to which degree such data matches the provided personal biometric data of individuals. Unlike the ESIA, which serves as the foundation of the digital profile, the UBS generates people's biometric profiles. Thus, it can be seen as a special system that generates, among other things, a special biometric digital profile.

With respect to the personalization of this or that subject, the concept of digital profile is often compared to such concepts as digital twin, digital character, or digital avatar. These concepts are, to a certain extent, synonymous with the digital profile in the sense of their common purpose, which is to create a digital copy of a real natural or legal person or an object, e.g., a settlement, an island, or a river, as they function in a digital environment. This is why it is crucial to distinguish between these concepts today.

Digital twin is most often considered an umbrella term for digital character and digital profile. Digital profile is always an exact copy (a visual copy, in the sense that it fully matches personal data and displays actual actions and deeds of a person). A digital character is a visual "reincarnation" of a natural or legal person that takes form of an image created to serve a specific purpose. Digital character is gradually becoming synonymous with digital avatar. The latter was originally considered as a graphical illustration of a user or group of users, including individuals and/or legal entities. An avatar often has a 2D format, that of a personal symbol on a forum or a web service; it can also have a 3D format when used in games, virtual states, or specially created miscellaneous virtual spaces (worlds, metaverses, etc.). Today, a digital avatar mainly pertains to a personality bound to a nickname on the screen or a user descriptor on the Internet. Digital avatars are much closer to digital profiles than digital characters, as they often imply non-anonymous functioning of the avatar-represented users. A character always implies abandonment of one's own image or real data, and making it a policy to exaggerate one's abilities. Like profiles, avatars of today mainly exist to enable their users to use the opportunities and benefits of the digital environment, including property-related benefits; for instance, digital avatars and profiles often get access to discounts, and some companies are founded to work exclusively with digital avatars.

A person's digital avatar or character on social media or other platforms and the actual person behind it are often two different entities or hypostases. And yet, a digital profile needs to be associated with a specific person to avoid confusion among others. The image a digital character projects tends to drastically differ from the actual state of affairs, and other users need to be informed immediately that such difference could exist. We believe law should clearly require to inform other persons of such discrepancies so that they be aware of the fictional nature of the character, except, of course, cases of special anonymized systems, where users are informed by virtue of signing the end-user agreement that the data provided by system users is a matter of fiction. We also believe a digital profile should always be clearly linked to a specific person.

4. Digital Profiling and Regulatory Mechanisms

Analysis of the emerging practices of digital profiling today shows that legal regulations tend to lag behind the rapid advancements in the area. Other mechanisms need to be considered. Regulatory experiments could be considered in application to digital profiling and its associated relations [29, 30]. In this case, we can speak of legal regulation of experiments and on the possible experimental legal frameworks applicable to digital innovation and adoptable under the special Federal Law No. 258-FZ dd. July 31, 2020 On Experimental Legal Frameworks Applicable to Digital Innovations in the Russian Federation[11].

[11] Federal Law No. 258-FZ dd. July 31, 2020 On Experimental Legal Frameworks Applicable to Digital

ISSN 2658-4050 (Online)

Thus, pursuant to the Government Decree No. 710 dd. June 3, 2019, an experiment for better quality and coherence of data in government databases is taking place from July 1, 2019 till December 31, 2021. The purpose of the experiment is to "ensure the quality and coherence of data contained in government databases involved in the experiment, in the scope defined for such experiment, by creating and testing an infrastructure as part of the Unified System for Identification and Authentication in the Infrastructure for Communication of E-Government Systems (ESIA); this newly created infrastructure shall provide citizens with access to data and documents accessible to public authorities and local self-governments and used to provide e-government services, perform public and municipal functions, as well as to data generated by the rendition of such services and contained in public and municipal information systems; it shall also provide organizations with access to individuals' data they might need, including access initiated and consented by such individuals ('Digital Profile infrastructure')[12]."

The objectives are first and foremost "to develop Digital Profile infrastructure with multiple functions such as storage of individuals' data in the ESIA, access to required personal data as consented by their owners, and testing the functionality of this infrastructure."[13]

This experiment will help find out whether Russian law needs amendment to develop and implement such infrastructure. With this in mind, we can also assume this experiment constitutes a regulatory mechanism that affects such infrastructure and may influence, among other things, further development of the legislation. In fact, experimental testing of the system involves multiple methods, techniques, and means for optimizing the advancement of legal and other regulators applicable to digital profiling.

We believe that this mechanism is what will enable further regulation of the mechanisms of digital profiling and its social functions. Thus, April 2, 2021 Russia's Ministry of Digital Development, Communications, and Mass Media has adopted its Guidelines *Digital Profile Infrastructure: Scenarios of Use*. Ver. 1.2 pursuant to the Government Decree No. 710 dd. June 3, 2019 On the Experiment Towards Better Quality and Coherence of Data in Government Databases. This document outlines the basic scenarios of use for the Digital Profile infrastructure: requesting users' consent to access their data; retrieval of Digital Profile-stored register data by the information systems of the experiment participants; notifying such participants on changes in the Digital Profile-stored registers[14].

Experimental and other special legal frameworks do indeed help test the effectiveness of this or that novel institute, as showcased by international practices [31, pp. 10-36].institution However, according to special studies into their functional effectiveness, "the existing special and distinct legal frameworks existing in Russia today do not focus on evaluating the risks of using advanced technology, identifying and addressing the existing legal constraints the hinder the advancement of such technology, or creating novel legal regulations regarding such advancement." [32, p. 74]. This should be borne in mind when designing digital profile experiments.

Ethics, including the issues of the possibility and limits of ethical regulation, remains subject to much discussion in the context of regulaturing digital profiling. Many believe that technological sectors are more likely to recognize and understand ethical rather than legal standards. Data ethics is a key aspect of digital transformation ethics. "Setting the boundaries of ethical access to data is a complex issue that affects various stakeholders: individuals,

Innovations in the Russian Federation // Codes of the Russian Federation. 2020. No. 31 (Part I). Art. 5017.

[12] Cl. 121 of the Regulations on the Experiment Towards Better Quality and Coherence of Data in Government Databases, appr. by the Government Decree No. 710 dd. June 3, 2019 (rev. April 16, 2021) On the Experiment Towards Better Quality and Coherence of Data in Government Databases together with the Regulations on the Experiment Towards Better Quality and Coherence of Data in Government Databases // http://pravo.gov.ru, June 7, 2019.

[13] Ibid.

[14] Guidelines of Mincomsvyaz *Digital Profile Infrastructure: Scenarios of Use. Ver.* 1.2 of April 2, 2021. URL: https://digital.gov.ru/uploaded/presentations/stsenariiispolzovaniyatspv12.pdf (retrieved April 20, 2021).

ISSN 2542-1514 (Print)

governments, corporations, public institutions, etc.; as such, it calls for a comprehensive solution. Novel technologies and methods for the collection, storage, analysis, and use of data are ever more likely to leave developers, researchers, and managers puzzled over whether use of data in this or that situation is allowable or not, legal or risky, effective or not." [33, p. 9]

Indeed, ethical standards are adopted, implemented, and come into use faster in data industries. However, in this case the government is losing its organizational role in control over relations pertaining to the use of citizens' data, something it should not be allowed to lose. One possible resolution would consist in governmental initiation of ethical regulation as well as in delimitating the regulated aspects. Some issues, e.g., AI-related ones, should be government-controlled [5, 6, 13].

Governments of states and non-governmental organizations as well as international organizations have already proposed certain principles, frameworks, and recommendations regarding ethics and data management. They first of all concern the wording of recommendatory principles for parties using or processing big data. These principles conventionally include the legality and respect for the interests of all parties; respect for values and culture; risk management; well-being and security; accountability; transparency; ethical use of data. Analysis of these principles highlights the fact that the world uses standard approaches to systematizing them. They rather differ from application to application within frameworks of digital profiling and social scoring.

Challenges of ethical regulation of data collection and processing give rises to many more issues facing today's societies and governments: unconsented collection of data, confidentiality of personal data, inherent bias, risk of profiling and discrimination, and non-transparency of some AI-made decisions resulting from data processing. Another important concern is that of reputational risks associated with the society's fear that corporations use consumer data in bad faith to gain insight into consumer profiles as well as unfair competitive digital advantage.

Notably, digital profiling relies on artificial intelligence [6, pp. 81-90], which is not necessarily concerned with today's democratic values in the process of data collection and processing.

Today, most researchers studying the regulation of digital relations note a need to use a comprehensive framework of regulators including legal, ethical, technical, and self-regulation [3]. We believe digital profiling should prioritize legal regulations today. Yet, legal frameworks including Acts of the Government of the Russian Federation may indeed enshrine the ethical principles and standards derived from documents of international organizations as well as from recommendations of industrial experts. Rules may also contain recommendations on their use by non-governmental legal entities, sole entrepreneurs, or individuals that create or use digital profiles. We believe this approach will help prevent the emergence of multiple ethical codes and regulations in public and private sector whilst not being redundant.

Ethical standards have traditionally been an important foundation and precursor for future self-regulation in this or that sector. Self-regulation can potentially serve as a mechanism for regulation of data collection and processing as part of digital profiling. We can see it emerge in Russia. Thus, the Institute of Internet Development (IID) and the Big Data Association (BDA) adopted their Data Ethics Code in 2019; the Code builds upon the principles and provisions found in Russian and international law[15]. It is a set of principles of professional ethics applicable to digital data, industrial standards of professional and ethical conduct that the Code participants, acting reasonably and in good faith, recognize voluntarily and undertake to comply with. "The Code is intended to lay the foundations for self-regulation of market actors and their relations with individuals, legal entities, the government, and each other. Self-regulation of data processing and use represents the market actors' social responsibility founded upon the standards of business ethics." [3, p. 132] The White Paper, which generalizes examples of local regulations, resolutions, and actions of the Code-recognizing parties, constitutes a

[15] Code of Data Ethics URL: https://ac.gov.ru/files/content/25949/kodeks-etiki-pdf.pdf (retrieved July 15, 2021).

ISSN 2658-4050 (Online)

crucial part of the document. The Code seems to be an important component of the development of self-regulation in digital profiling. In many ways, it might one day lay the foundations for associations in the use of digital data, and will be cited or referred to in other ethical codes and legal regulations [3, p. 132].

5. Conclusions

A digital profile may contain personal data, personal and family secrets including information on personal traits, behavior, activities and actions, memberships and social status, connections and interactions. The scope of digital profiling keeps expanding. Whilst it initially served marketing and advertising purposes, it is now used in security measures at all levels, in public administration and justice, in employment and in the work of e-government. In the context of coronavirus and social distancing, digital profiling has become integral to most information relations at distance, which imply individualization of subject space and the need to identify and authenticate persons, which is why digital profiling keeps developing and is reaching a whole new level today.

In this regard, it becomes critical to duly focus on the challenges of digital profiling in basic and applied research alike. For the government, it is important to strategically determine what constitutes a digital profile, the focus areas of the development of digital profiling, challenges and risks, as well as the importance of the development of profiling within the framework of the emerging unified system of public authorities.

REFERENCES

1. Hildebrandt M. Profiling and the rule of law. *Identity in the Information Society*, 2008, vol. 1, pp. 55–70. DOI: 10.1007/s12394-008-0003-1.

2. Blazheyev V.V., Egorova M.A. (eds.) *Digital law*, Textbook. Moscow, Prospekt Publ., 2020. 640 p. (In Russ.).

3. *Mechanisms and models of regulation of digital technologies*, Monograph. Moscow, Prospekt Publ., 2020. 224 p. (In Russ.).

4. Kovaleva N.N. Trends in the development of legal regulation of digital transformations. *Informatsionnoe pravo = Information Law*, 2019, no. 4, pp. 45–46. (In Russ.).

5. Egorova M.A., Minbaleev A.V., Kozhevina O.V., Duflo A. The main directions of legal regulation of the use of artificial intelligence in the conditions of a pandemic. *Vestnik Sankt-Peterburgskogo universiteta. Pravo = Bulletin of the St. Petersburg University. Pravo*, 2021, vol. 12, no. 2, pp. 250–262. DOI: 10.21638/spbu14.2021.201. (In Russ.).

6. Blazheev V. V., Egorova M. A. (eds.) *Legal regulation of artificial intelligence in the conditions of a pandemic and infodemia*. Moscow, Prospekt Publ., 2020. 240 p. (In Russ.).

7. Lungu E.V. COVID-19 pandemic. New challenge for constitutional relations. *Pravoprimenenie = Law Enforcement Review*, 2020, vol. 4, no. 3, pp. 69–75. DOI: 10.24147/2542-1514.2020.4(3).69-75. (In Russ.).

8. Williams C.C., Kayaoglu A. The coronavirus pandemic and europe's undeclared economy: impacts and a policy proposal. *South East European Journal of Economics and Business*, 2020, no. 15(1), pp. 80–92. DOI: 10.2478/jeb-2020-0007.

9. Barocas S., Selbst A.D. Big Data's Disparate Impact. *California Law Review*, 2016, vol. 104, no. 3, pp. 671–732. DOI: 10.15779/Z38BG31.

10. Neznamov A.V., Naumov V.B. Questions of the development of legislation on robotics in Russia and in the world. *Yuridicheskie issledovaniya = Legal Studies*, 2017, no. 8, pp. 14–25. (In Russ.).

11. Nikolskaia K., Naumov V. Artificial Intelligence in Law, in: *2020 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon)*, Vladivostok, Russia, 2020, pp. 1–4. DOI: 10.1109/ FarEastCon50210.2020.9271095.

12. Nikolskaia K., Naumov V. Ethical and Legal Principles of Publishing Open Source Dual-Purpose Machine Learning Algorithms, in: *2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)*, Yaroslavl, Russia, 2020, pp. 56–58. DOI: 10.1109/ITQMIS51053.2020. 9322897.

13. Naumov V.B. (ed.) *Legal and ethical aspects related to the development and application of artificial intelligence and robotics systems: history, current state and prospects of development*, Monograph. St. Petersburg, NP-Print Publ, 2020. 258 p. (In Russ.).

14. Gabov A.V., Khavanova I.A. Evolution of Robots and the 21st-Century Law. *Vestnik Tomskogo gosudarstvennogo universiteta = Tomsk State University Journal*, 2018, no. 435, pp. 215–233. (In Russ.).

15. Kaftannikov I., Zhernova V., Minbaleev A. Problems of structuring risks and ensuring legal relations in IoT. *Advances in Economics Business and Management Research*, 2019, vol. 81: Proceedings of the 1st International Scientific Conference on Modern Management Trends and the Digital Economy – From Regional Development to Global Economic Growth (MTDE),Yekaterinburg, apr 14-15, 2019, pp. 73–79. DOI: 10.2991/mtde-19.2019.14.

16. Kargina L.A. (ed.) *Digital Economy*, Textbook. Moscow, Prometei Publ., 2020. 222 p. (In Russ.).

17. Zharova A.K. Issues of ensuring the security of the digital profile of a person. *Yurist = Lawyer*, 2020, no. 3, pp. 55–61. (In Russ.).

18. Treshcheva O.Yu., Balayan E.Yu. Municipal power in the conditions of modernization of society and the state. *Gosudarstvennaya vlast' i mestnoe samoupravlenie = State Power and Local Self-government*, 2020, no. 9, pp. 22–25. (In Russ.).

19. Minbaleev A.V. Problems of social efficiency and protection of human rights when using artificial intelligence in the framework of social scoring. *Vestnik Yuzhno-Ural'skogo gosudarstvennogo universiyeta. Seria: Pravo = Bulletin of the South Ural State University. Series: Pravo*, 2020, vol. 20, no. 2, pp. 96–102. (In Russ.).

20. Lazarov A. A. Legal regulation of social scoring in the field of public service: Russian and foreign experience. *Informatsionnoe pravo = Information Law*, 2020, no. 4, pp. 41–44. (In Russ.).

21. Skiba S.A., Loiko V.I. Social scoring. *Nauchnyi zhurnal KubGAU = Scientific Journal of the Kuban State Agrarian University*, 2013, no. 91 (07), available at: http://ej.kubagro.ru/2013/07/pdf/89.pdf (In Russ.).

22. Fedorov A., Nikolskaia K., Ivanov S., Shepelev V., Minbaleev A. Traffic flow estimation with data from a video surveillance camera. *Journal of Big Data*, 2019, vol. 6, no. 1, p. 73. DOI: 10.1186/s40537-019-0234-z.

23. Himchenko A.I., Bulanova V.S. Features of development and legal regulation of technological innovations on the example of facial recognition technology and biometrics. *Vestnik Moskovskogo universiteta. Seriya 26: Gosudarstvennyi audit = Bulletin of the Moscow University. Series 26: State Audit*, 2019, no. 4, pp. 58–65. (In Russ.).

24. Naumov V.B. Theoretical information and legal issues of identification in the digital sphere. *Information Law*, 2020, no. 4, pp. 4–8. (In Russ.).

25. Knyshoid M.Z. Digital footprint and its legal regulation. *Informatsionnoe pravo = Information Law*, 2020, no. 4, pp. 37–40. (In Russ.).

26. Troshchinsky P.V., Molotnikov A.E. Features of the regulatory and legal regulation of the digital economy and digital technologies in China. *Pravovedenie = Jurisprudence*, 2019, vol. 63, no. 2, pp. 309–326. (In Russ.).

27. Himchenko A.I. On the creation of a unified state information resource about the population. *Informatsionnoe pravo = Information Law*, 2020, no. 3, pp. 28–31. (In Russ.).

28. Kamalova G.G. State Unified cloud platform: prospects and risks. *Informatsionnoe pravo = Information Law*, 2020, no. 2, pp. 26–30. (In Russ.).

29. Polyakova T.A., Minbaleev A.V., Krotkova N.V. New vectors of information law development in the conditions of the civilizational crisis and digital transformation. *Gosudarstvo i pravo = State and law*, 2020, no. 5, pp. 75–87. (In Russ.).

30. Efremov A.A. Special legal regimes for conducting experiments in public administration. *Konstitutsionalism i gosudarstvovedenie = Constitutionalism and State Studies*, 2019, no. 2, pp. 29–34. (In Russ.).

31. Gromova E., Ivanc T. Regulatory Sandboxes (Experimental Legal Regimes) for Digital Innovations in BRICS. *BRICS Law Journal*, 2020, vol. 7, no. 2, pp. 10–36. DOI: 10.21684/2412-2343-2020-7-2-10-36.

32. Yuzhakov V.N. (ed.) *Experimental legal regimes: foreign experience and Russian start*. Moscow, Delo Publ., 2020. 126 p. (In Russ.).

33. *Ethics and the "figure" – briefly about the main thing. Robot doctor, robot teacher, robot policeman: social risks and industry ethical challenges*, analytical note to Volume 2 of the report “Ethics and "Digital": ethical problems of digital technologies”. Moscow, RANEPA Publ., 2020, 124 p. (In Russ.).

34. Winfield A. Ethical standards in robotics and AI. Nat Electron. *Nature Electronics*, 2019, vol. 2, pp. 46–48. DOI: 10.1038/s41928-019-0213-6.

INFORMATION ABOUT AUTHORS

Elena V. Vinogradova – Doctor of Law, Professor, Acting First Deputy Director
Institute of State and Law of the Russian Academy of Sciences
10, Znamenka ul., Moscow, 119019, Russia E-mail: evigpran@igpran.ru
ORCID: 0000-0002-3568-9042
RSCI SPIN-code: 8022-0021

Tatyana A. Polyakova – Doctor of Law, Professor, Chief Research Fellow, Acting Head of the Information Law and International Information Security sector
Institute of State and Law of the Russian Academy of Sciences
10, Znamenka ul., Moscow, 119019, Russia E-mail: polyakova_ta@ mail.ru
ORCID: 0000-0003-3791-2903
RSCI SPIN-code: 4224-3174

ISSN 2542-1514 (Print)

Alexey V. Minbaleev – Doctor of Law; [1] Chief Research Fellow, Information Law and International Information Security sector; [2] Associate Professor, Head, Department of Information Law and Digital Technologies
[1] *Institute of State and Law of the Russian Academy of Sciences*
[2] *Kutafin Moscow State Law University (MSAL)*
[1] 10, Znamenka ul., Moscow, 119019, Russia
[2] 9, Sadovaya-Kudrinskaya ul., Moscow, 125993, Russia
E-mail: alexmin@bk.ru
ORCID: 0000-0001-5995-1802
RSCI SPIN-code: 7148-1527

BIBLIOGRAPHIC DESCRIPTION
Vinogradova E.V., Polyakova T.A., Minbaleev A.V. Digital profile: the concept, regulatory mechanisms and enforcement problems. *Pravoprimenenie = Law Enforcement Review*, 2021, vol. 5, no. 4, pp. 5–19. DOI: 10.52468/2542-1514.2021.5(4).5-19. (In Russ.).

ISSN 2658-4050 (Online)