



<https://doi.org/10.22363/2313-2337-2024-28-3-512-527>

EDN: FTBYVW


Research Article / Научная статья

## Digital identity and digital image of an individual: Legal characteristics and the place in the system of related categories

Vladislav O. Demkin  

National Research University Higher School of Economics (HSE University),

*Moscow, Russian Federation*

 [vodemkin@hse.ru](mailto:vodemkin@hse.ru)

**Abstract.** The purpose of the work is to study the definition and content of the terms “digital personality”, “digital image of a person”, “digital profile”, “digital citizenship”, their interrelation, as well as legal problems related to these categories. The relevance of the topic is confirmed by the active discussion of regulatory legal acts in the areas of building a system of digital profiles, digital citizenship in different countries of the world. The method of research is the analysis of Russian and foreign literature and practice, identification of their fundamental provisions, study of interrelations with more “classical” legal categories, including classical human rights and personal data. The conclusion is drawn about the fundamental position of the category of “digital personality” for the study of the phenomenon of the modern digital person. It is primarily related to human rights in the modern digital world. Such a category directly affects other concepts under study, including information (data) about individuals, as well as the overall policy in the sphere of citizens' participation in state governance. In order to study the phenomenon of the digital person, it is necessary, first of all, to study the category of the digital person from the point of view of their rights in the digital world, i.e., from the point of view of human rights.

**Key words:** Digital person, digital identity, digital image of a person, digital profile, digital citizenship, personal data, human rights, identification

**Conflict of interest.** The author declares no conflict of interest.

*Received: 3rd January 2024*

*Accepted: 15th July 2024*

### For citation:

Demkin, V.O. (2024) Digital identity and digital image of an individual: Legal characteristics and the place in the system of related categories. *RUDN Journal of Law*. 28 (3), 512–527. <https://doi.org/10.22363/2313-2337-2024-28-3-512-527>

---

© Demkin V.O., 2024




This work is licensed under a Creative Commons Attribution 4.0 International License

<https://creativecommons.org/licenses/by-nc/4.0/legalcode>

## Цифровая личность и цифровой образ человека: характеристика и место понятий в системе смежных категорий

В.О. Демкин  

Национальный исследовательский университет «Высшая школа экономики»  
(НИУ ВШЭ), г. Москва, Российская Федерация  
vodemkin@hse.ru

**Аннотация.** Целью исследования – изучение определения и содержания терминов «цифровая личность», «цифровой образ человека», «цифровой профиль», «цифровое гражданство», их соотношение, а также правовые проблемы, связанные с указанными категориями. Актуальность темы подтверждается активным обсуждением нормативно-правовых актов в сферах построения системы цифровых профилей, цифрового гражданства в различных странах мира. Метод исследования составляет анализ имеющейся российской и зарубежной литературы и практики, вычленение их основополагающих положений, исследование взаимосвязей с более «классическими» правовыми категориями, в частности с классическими правами человека, с персональными данными. Сделан вывод об основополагающем положении категории «цифровая личность» для изучения феномена современного цифрового человека. Она связана в первую очередь с правами человека в современном цифровом мире. Такая категория напрямую влияет на иные изучаемые понятия, которые включают в себя, в частности, сведения (данные) об индивидах, а также в целом политику в сфере участия граждан в управлении государством. Для изучения феномена цифрового человека предлагается в первую очередь изучать категорию цифровой личности с точки зрения его прав в цифровом мире, то есть с точки зрения прав человека.

**Ключевые слова:** цифровой человек, цифровая личность, цифровой образ человека, цифровой профиль, цифровое гражданство, персональные данные, права человека, идентификация

**Конфликт интересов.** Автор заявляет об отсутствии конфликта интересов.

*Поступила в редакцию: 3 января 2024 г.*

*Принята к печати: 15 июля 2024 г.*

**Для цитирования:**

Демкин В.О. Цифровая личность и цифровой образ человека: характеристика и место понятий в системе смежных категорий // *RUDN Journal of Law*. 2024. Т. 28. № 3. С. 512–527. <https://doi.org/10.22363/2313-2337-2024-28-3-512-527>

### Introduction

In the modern world, information about individuals, as a collection on data, plays a crucial role in the global economy. Data sets are accumulated not only by the largest technology companies but also by more ordinary businesses that provide household services to the public. Additionally, a vast amount of information, often the most sensitive, is collected by various government agencies and organizations. This information is exchanged both “horizontally” (between private individuals or between state bodies), and “vertically” (between the state and private business entities and vice versa). Different entities can collaboratively process data about individuals, creating digital profiles to make automated decisions about them.

Fears about the digitalization of humanity have been expressed in various literature (both domestic and foreign) since the onset of rapid advancement in technologies for storing and processing large amounts of data. A significant portion of such publications also pertains to legal literature. Much of this literature is focused on personal data, addressing issues of confidentiality, privacy, their structure and theories of arrangement. Equally important are sociological studies on the phenomenon of digital persona, which discuss characteristics such as how individuals are perceived by others. These works are often based on the theory that each individual possesses a set of masks used in social communication.

However, in legal publications, the phenomenon of digital identity is mostly mentioned in passing, without delving into it in detail. In this publication, the author intends, at the very least, spark discussions on the public law characteristics of the digital persona, the digital image of a citizen, as well as provide the necessary definitions. The study is based on the provisions of personal data law, human rights law, information law, and incorporates some sociological perspectives on the phenomena under study.

The subject of this research is the study of “digital personality”, “digital image of personality” and other similar terms as legal categories. The research draws on publications by practitioners and theorists in the fields of human rights, personal data, privacy and confidentiality, and constitutional law. Special attention is given to the works of various centers for the study of digital society law, particularly those at Harvard and Stanford Universities. Legal acts and law enforcement practices of various states, including members of the European Union, the United States, and Russia, also play a significant role.

The research method involves analyzing the available theoretical and practical literature on related issues, identifying fundamental provisions related to the formation of the category of “digital personality”, and studying the relationships with more “classical” legal categories. Based on this analysis, the study aims to develop two fundamental ideas about the components of the concepts of “digital personality”, and “digital image of a person”.

### **Definition of “digital personality” in the literature**

This part of the paper will describe the ideas available in scientific publications regarding the definitions of the terms “personality”, “person”, “identity”, and other related concepts as well as their “digital” analogues.

In legal sciences, a person (as a basic concept of a biological species) is understood as “an individual who was born alive from humans, possesses legal capacity, individualizing intangible benefits, is capable to act independently, has separate property, and is characterized by biometric personal data that distinguishes them from other people, whose life ends at the moment of brain death or the onset of biological death” (Maleina, 2017).

There are many concepts of “personality”. However, as reported in specialized studies on this topic, the prevailing understanding in the Russian legal literature currently views the individual through a list of social ties and social relations in which a

person participates (Kapitonova, 2019). For example, Yu. K. Volkonsky defines personality as “a person who has an individual system of socially significant properties that manifest themselves in relations between people in their activities” (Volkonsky, 2007).

The most common definition of a digital personality (as well as similar terms such as “digital image of a person”, “digital twin”, etc.) is reduced to a set of data about the individual. For example, Daniel J. Solove, a professor of intellectual property law and technology at George Washington University and a prominent privacy scholar, defines a digital person as a digitalized entity made up of records, data fragments, and pieces of information (Solove, 2004). Additionally, doctors of law and professors of the University of Qatar, who are also employees of the Center for Law and Development, have developed a model of a digital clone of thought. They describe this as a personalized digital twin consisting of a copy of all known data and behaviors of a particular living person, including their choices, preferences, behavioral trends, and decision-making processes. Such a clone is something more than a mere “static” set of data about someone. Presented as a virtual model, it can simulate various given situations for its owner and demonstrate how the real “owner of the personality” would behave in those scenarios (Truby & Brown, 2021). This capacity can be utilized for marketing, political, or other purposes. It can be said that such a clone of thought represents the next and significantly more advanced stage in the development of digital personalities.

In sociological studies, identity is defined as a concept attributed to a person by social norms, relating to self-esteem, individuality, and self-vision (Zajmi, 2015), as well as the ability to organize one’s thoughts, feelings, and actions (Myers, 2017). Accordingly, “digital identity” can be understood as a person’s vision of themselves in the online world and their representation in such a world for others. In fact, in different social relationships, an individual presents themselves differently, depending on the impression they wish to make on a certain group of interlocutors or “observers”. This is especially noticeable when comparing the content of a person’s social media page “for friends” with their profile on job search sites.

In some sociological and legal research papers devoted to the transformation of society in the age of technology, the terms studied in this section can be understood as referring to an individual who exercises their rights and fulfills their duties using digital technologies. Publications with this understanding of the terms often address issues such as digital equality, formation of the right of every person to access technologies, and application of the principle of technological neutrality in rule-making. In our opinion, it is in such cases that it is most appropriate to use the term “digital identity”.

### **“Digital identity” as an offline person with rights in the digital world**

Based on the above provisions, it can be seen that the authors of most works (both purely legal and interdisciplinary) primarily understand “digital personality” as a set of data about an individual, expressed in a digital, virtual environment and suitable for

processing by automated means. This understanding narrows research to the area of personal data legislation.

Without detracting from the importance of this area of law, we also consider it necessary to pay attention to the sphere of human rights. There is a growing body of publications focused on studying new human rights in the digital environment (or more precisely, in the digital world), with the primary right being the right to access the Internet. E.V. Talapina and N.V. Varlamova, among others, highlight such rights and their components and examine current theories about their place in the human rights system.

The following approaches are distinguished (sometimes referred to as stages of rights evolution): a) “digital human rights” are simply classical rights applied in a digital environment; b) “digital human rights” are new human rights, but they are expressions of well-established offline rights in an online environment; c) “digital human rights” are harbingers of a completely new generation of human rights.

We believe that such indicators of personality in the modern information society, such as one’s rights in the online world, are integral attributes of a digital personality. These rights include the right to access the Internet, the right to “be forgotten”, the right to data portability, the right to “digital death”, and the right to “technological equality”. It is worth noting that some of these rights are already enshrined in the laws of various countries.

For example, the right “to be forgotten” (“to be left alone”) originated from the right to privacy. This newly established right in Russian legislation is articulated in Article 10.3. of the Federal Law “On Information, Information Technologies and Information Protection”<sup>1</sup>. It grants individuals the ability to request the removal of outdated or inaccurate information concerning them, except for details about events involving indications of criminal offences for which the statute of limitations has not expired, and information regarding a citizen’s criminal activity that has not been expunged from their record. The right to be forgotten and the right to data portability in European practice are enshrined in the General Data Protection Regulation (hereinafter referred to as the GDPR or Regulation), providing individuals with the right to rectify or erase data processed in violation of the Regulation’s guidelines, the right to revoke consent for data processing and the right to obtain personal data in a structured, commonly used, and machine-readable format, respectively.

The significance of defining a digital person as an individual entitled to specific rights in the digital realm is paramount. N.V. Varlamova, reflecting on the seminal work of K. Vasak regarding human rights, where the concept of generations of rights was introduced, draws parallels with the ideals of the French Revolution – freedom, equality and fraternity. The rights of the first generation (inherent and inalienable rights such as freedom) embody demands for personal liberty and citizens' access to participation in State governance. These rights entail both negative obligations on the part of the State

---

<sup>1</sup> Federal Law No. 149-FZ On Information, Information Technologies and Information Protection issued 27.07.2006. Collection of Laws of the Russian Federation, 2006, No. 31, Art. 3448.

(and others) not to impede the exercise of such rights, as well as positive obligations for the State to provide protection in cases of their infringement. The rights of the second generation (equality) encompass entitlements to social services and assistance from both the state and society aimed at mitigating social disparities and ensuring a “decent standard of living” for all, as well as the redistribution of social resources in favor of vulnerable segments of the population. These rights are manifested in the State’s obligations to implement measures for providing social assistance to individuals in need, especially the impoverished. Third generation rights (brotherhood) are linked to the concept of universal solidarity and encompass entitlements such as the right to peace, disarmament, a just world order, collective ownership of humanity’s common heritage, a nation’s right to a historical homeland, and self-determination. It is worth noting that these provisions are primarily declarative, moral and political in nature (Varlamova, 2019).

When addressing a digital person and their rights in the digital domain, it is essential to categorize the measures and legal protections associated with these rights. If digital rights are not considered as a fourth generation of human rights, it becomes important to classify them within the existing three generations.

One of the most debated digital right is the right to access the Internet, with numerous publications in both Russian and foreign sources discussing its position within the human rights framework. For example, some interpret the right to access the Internet as an aspect of the right to information (to access and disseminate information). Such “well-established” right of the first generation, implies the individual’s freedom to select a specific technical means to access or distribute the information of interest. In this sense, the Internet is conventionally equated with newspapers, radio, and television. However, Internet access is also essential for obtaining various public services, participating in the political life of the country, and conducting everyday life activities familiar to most people. A defining characteristic of the Internet is the freedom it provides for individuals to create and search for content. Unlike traditional newspapers, radio and television, Internet content is generally not controlled or subject to editorial policies, except for censorship requirements in different countries. This aspect underscores the Internet’s distinctive role in creating, distributing, searching and accessing any information of interest to individuals.

Based on the literature, the prevailing opinion regarding the content of the human right to access the Internet revolves around the theory of its two aspects: technical – the right to be capable of connecting to the network and ideological – the right to access information and protection against unlawful site blocking (Khusnutdinov, 2017). The ability to connect to the Internet in many countries is already provided by States (and this approach is supported in publications). For example, the Estonian Law on Public Information (paragraph 33) provides that everyone should have free access to public information on the Internet in public libraries<sup>2</sup> without requirements regarding connection speed or the availability of information in

---

<sup>2</sup> Public Information Act. Available at: <https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/518012016001/consolide> [Accessed 06th November 2023].

general. Article 52 of the Spanish Law on Sustainable Economy establishes a broadband connection with a minimum speed of 1 Mbit per second (or higher as determined by relevant ministries) as a universal communication service. This signifies state regulation of the tariffs charged by providers for such connections with a minimum speed<sup>3</sup>. In Russia, within the framework of the “Accessible Internet” program, telematics communication service operators are obligated to provide subscribers with free access to domestically significant information resources, with the duration of access increasing from 24 hours to 7 days starting from September 1, 2024. However, access is limited to citizens with a contract with a telecom operator and is only granted to pages containing text content and is accessible solely from stationary devices. The list of such socially significant pages is established by the Government<sup>4</sup>.

Defining the right to access the Internet as the right of a digital person may lead to some interesting implications. For instance, the practice of the European Court of Human Rights acknowledges that the right to access the Internet, in its ideological aspect, may be restricted to uphold public interests and maintain State security. As an illustration, there are cases when access to certain websites is blocked. The decision to do so is permissible under the following conditions: 1) it is based on the national law; 2) the site owner is provided with genuine assurances and mechanisms to safeguard their interests, including the opportunity to participate in decision-making; 3) only information that is prohibited from dissemination is blocked to the minimum extent necessary (Talapina, 2021).

Such restriction of access to information due to its inconsistency with the law is a general practice that applies to all users in a particular territory. However, the decision to impose such a restriction can be made not by a state body “from above”, but by a private individual “from below”.

In the literature, with reference to the Recommendations of the Committee of Ministers of the Council of Europe, SEE/Rec(2011)8 On the Protection and Promotion of the Universality, Integrity, and Openness of the Internet, it is noted that States’ activities in regulating information on the Internet should be confined to their territorial boundaries and should not impede access to information for residents of other countries. States are encouraged to engage in communication with one another to secure

---

<sup>3</sup> Ley 2/2011, de 4 de marzo, de Economía Sostenible. Available at: <https://www.boe.es/buscar/act.php?id=BOE-A-2011-4117> [Accessed 06th November 2023].

<sup>4</sup> Resolution of the Government of the Russian Federation No. 2606 dated 31.12.2021 On Approval of the Rules for the Provision of Data Communication Services. Available at: <http://publication.pravo.gov.ru/Document/View/0001202201050010> [Accessed 15th November 2023]; Resolution of the Government of the Russian Federation No. 2607 of December 31, 2021 On Approval of the Rules for the Provision of Telematic Communication Services. Available at: <http://publication.pravo.gov.ru/Document/View/0001202201060008> [Accessed 15th November 2023]; Order of the Ministry of Communications of the Russian Federation No. 148 of March 31, 2020 (ed. of July 1, 2021) On conducting an experiment on the provision of citizens on a gratuitous basis communication services for data transmission and on providing access to the information and telecommunications network Internet in the territory of the Russian Federation for the use of socially significant information resources in the information and telecommunications network Internet. Available at: <https://digital.gov.ru/ru/documents/7146/> [Accessed 15th November 2023].

the unrestricted flow of information and preserve the integrity of the Internet (Khusnutdinov, 2017)<sup>5</sup>.

In connection with such recommendations (and in the case of recognizing the right to access the Internet as a human right), the question arises if some provisions of “economic sanctions” constitute a violation of human rights. Specifically, some sanctions may not only require blocking of access to certain websites within specific countries but also ban the import of technical components necessary for Internet operation or prohibit the provision of certain communication services related to network access. It is also important to consider whether the response to these “restrictions” would change if they are self imposed by an individual who owns websites or manufactures certain products, including under the influence of the legislation of their country of residence.

Economic sanctions serve as a political tool to address objectionable actions by a target State. While these restrictive measures are aimed at the government of the target country, they often affect its residents. Concerns have been raised by various public organizations dedicated to safeguarding the integrity of the Internet, promoting research into the impact of sanctions on the network<sup>6</sup>. These organizations highlight that the European Union authorities recognized the issue of restricting access to the Internet for citizens of the target country. On June 3, 2022, the EU adopted the “Internet-carveout” initiative. This initiative excludes funds, economic resources, and related services necessary for the operation of electronic communication services provided by telecom operators within the EU from sanctions against Russia. This exemption applies to activities both within Russia and in interactions between Russia and the European Union.

Researchers emphasize that “blocking a person’s access to the Internet is a serious interference with freedom” (Talapina, 2021). They argue that disconnecting an individual from the Internet as a sanction for repeated violations in the field of intellectual property as observed in legal practices in France and the United Kingdom), is unacceptable (Sartor, 2017). At the same time, in accordance with Article 105.1 of the Criminal Procedure Code of the Russian Federation, a suspect in the commission of a crime may be banned from Internet, as well as other communication networks, including sending and receiving mail and telegraph items. These prohibitions are seen as limitations on the traditional human rights to access and disseminate information. The question arises if such a significant restriction on a suspect’s enjoyment of human rights is justified. It seems that recognizing the right to access the Internet as a fundamental right prompts reconsideration of this issue, particularly in terms of narrowing down the extensive ban on using the network. For example, it is possible to provide limited access to specific information resources for suspects, possibly through a categorized list maintained by the Russian Government. It may include websites on municipal and state services.

---

<sup>5</sup> Recommendation CM/Rec(2011)8 of the Committee of Ministers to member states on the protection and promotion of the universality, integrity and openness of the Internet. Available at: [https://search.coe.int/cm/Pages/result\\_details.aspx?ObjectID=09000016805cc2f8](https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cc2f8) [Accessed 17th November 2023].

<sup>6</sup> Sanctions and Internet. Available at: <https://digitalmedusa.outcondev.com/wp-content/uploads/2023/11/SanctionsandtheInternet-DigitalMedusa-1.pdf> [Accessed 10th November 2023].



Thus, it is proposed to use the term “digital personality” to refer to an individual who has rights related to digital technologies and the digital world to exercise these rights guaranteed by the state.

Given this, it is difficult to imagine an opposition in the form of a “non-digital person”; however, the study of this category holds significance for legal science. Research in this area will enable a better alignment of proposed initiatives in the adoption of regulatory legal acts with the principles and objectives of human rights development on the Internet. This study may lead to the emergence of additional human rights enshrined in the law, such as the right to access the Internet. Considering the Internet’s pivotal role as the primary platform for information exchange between people and for accessing state and municipal (especially social) services, individuals could potentially be exempted from restrictions on using the network, including those stipulated in criminal procedure law.

The study of digital transformation and its impact on modern personality development also provides principles for future legal development. It emphasizes not only the importance of ensuring minimal access to the Internet for general population but also the necessity for regulatory act to adhere to specific rules. One key rule is the requirement for technological neutrality in the provisions of these laws, enabling individuals to exercise their rights and obligations both online and offline, and across diverse technological platforms and systems.

### **The concept of “Digital image” as a system of information about an individual. Related legal categories**

The most common method of defining a “digital personality” in Russian and foreign literature is through the “data approach”. This approach is characterized by the terminology of personal data legislation and refers to a binary representation of a person's interests, behavior, and history. This “avatar of an individual” can be used for political and marketing purposes to predict an individual’s voting preferences for a particular candidate, the probability of ordering a specific product, conducting scoring, as well as developing a behavioral model to influence actions that are of interest to the “avatar” owner. These capabilities have emerged in the era of “Big Data” technology, which can be understood as “a set of tools and methods for processing structured and unstructured data of vast volumes from various sources, constantly updated to enhance the quality of management decision-making, create new products and improve competitiveness” (Saveliev, 2015).

It appears that due to the creation of such representation of an individual’s personality and its transfer to the digital realm for the purpose of constructing algorithmic processes and distinguishing it from the term “digital personality”, it may be more appropriate to use the term “digital image of a person” in such cases.

In foreign literature, the term “digital identity” is frequently used to denote data about a person involved in specific transactions. For example, Clare Sullivan, an expert in the legal regulation of the digital persona, categorized “digital identity” into identifying information, token identity, and other details about an individual (Sullivan, 2009). According to this approach, the establishment of digital identity occurs at the time

of individual's registration in the system and provision of identifying information, which may include items like photo, signature sample, biometric data, and PIN-codes. This process allows establishing a connection between a specific individual and their associated information. When an individual, seeks to conduct a transaction or engage with state or municipal authorities, they present the requisite information anew, which is then automatically compared with the data stored in the verified database. Based on this, Claire Sullivan arrives at a rather controversial conclusion that in such a relationship, a token acts as the subject of rights, rather than the person themselves, a legal person.

The author highlights that a similar scheme of relations involving digital identity was implemented in the UK from 2006 to 2011, coinciding with the existence of a national register of identity cards. During this period, British citizens, individuals from the European Economic Area and immigrants were issued electronic cards instead of passports, and certain information about them was recorded in the national database of cardholders. However, in 2011, this undertaking was discontinued, and the information was subsequently removed from the national register.

The term “digital profile (of a citizen)” is also often used in Russian regulatory and scientific literature to denote a unified platform for citizens to interact with various state authorities, local self-government bodies, and credit organizations, as well as to manage the consent provided for the processing of personal data, including biometric data. Additionally, from 2019 to 2022, the State Duma of the Russian Federation deliberated on a draft law related to the introduction of the concept of “digital profile” and certain other provisions concerning identification and authentication through specialized information systems of a digital profile and electronic identity cards in information legislation.<sup>7</sup> Following deliberations, the draft law was returned for revision with certain comments.

The term “digital profile”, which pertains to an individual, is encompassed by the definition of “digital image of a person”. In literature, a digital profile is understood as a collection of current, reliable data and other information about individuals and legal entities generated within the Unified Identification and Authentication System or other information systems of public and local governments, as well as organizations subordinate to them that interact with this system through a Unified Interdepartmental Electronic Interaction System. Its purpose is to secure the consent of relevant citizens or legal entities to subjects who have sought access to this information through the appropriate infrastructure (Vinogradova, Polyakova & Minbaleev, 2021). Thus, the digital profile system involves personal data, including their special categories, biometric data, and other sensitive data, such as health, religion, financial status, military service, employment and place of residence. The digital image of a person extends beyond information relevant solely to the implementation of state public policy and encompasses data contained in pertinent state information systems.

---

<sup>7</sup> Bill No. 747513-7. Available at: <https://sozd.duma.gov.ru/bill/747513-7> [Accessed 31st December 2023].

The development of a digital profile system aligns with the Russian government's objective to establish a Single Population register. In accordance with the adopted Federal Law on the Unified Federal Information Register containing information on the population of the Russian Federation, the transition period is set for the period until 31.12.2025. The unified information system will include a variety of information about Russian citizens, foreigners, and stateless persons to facilitate the exercise of State powers.

The establishment of a digital citizenship system represents a natural progression from the advancement of digital profile infrastructure. Researchers in the field of constitutional and state law perceive digital citizenship not merely as a public law category defining an individual's relationship to a specific state and their subordination to its legal system, but rather as the next phase in the evolution of a democratic society and its institutions. It can be characterized, for example, as an opportunity for online participation in social affairs (Mossberger, Tolbert & McNeal, 2008); as a public law procedure for interaction between the state and individuals in the digital and information space; as a means of engaging in the public sphere, discussing and contributing to decisions of public significance; and as a digital platform facilitating communication to address both public and private interests (Kravets, 2023). In this sense, digital citizenship is closely associated with the expression of the rights of a digital person on the Internet. To truly advance democracy and public participation in governance, it is crucial to enhance systems of public and expert oversight of the proposed laws under discussion. This can be achieved by establishing a platform for such discussion, enabling the proposal of amendments and comments on individual provisions (thereby avoiding batch approval or disapproval of the entire draft law).

In any case, the most significant protection for individuals when using their digital images and profiles is provided by legislation on personal data. Its key components include: 1) defining information as personal data and extending relevant legislative provisions to it; 2) determining the lawful grounds, duration, and purposes for processing of personal data and the extent of control by the data subject; 3) imposing requirements on data controllers to safeguard personal data during processing, and consequently outlining actions that data subjects can demand to be undertaken under the threat of applying liability measures to the data controller. Consideration of constructing a "digital image" when using "Big Data" technologies, introduces a contradiction between the objectives of personal data legislation, practical application of its provisions, and the extent of protection for personal data subjects. Moreover, the amalgamation of diverse personal data into a single database (register or registry) entails the risks of potential hacking and unauthorized disclosure by external parties. This risk is particularly significant when the state is establishing a single population database.

Across most legal systems globally, the term "personal data" is elucidated through a broad definition encompassing any information related to a specific or identifiable individual. Elaborations of this definition can be found in various documents of state bodies and judicial practice. In the Opinion 4/2007 on the Concept of Personal Data, issued by the Article 29 Working Party, the European Union's data protection and privacy

advisory body, the concept of personal data is divided into its constituent elements. Through practical examples, general recommendations are provided on how to identify specific information as personal data<sup>8</sup>. Meanwhile, in the United States, the Supreme Court's rulings on defining the scope of privacy protection for citizens under the Constitution play a significant role. Thus, the safeguarding of privacy and personal data (including utilization of various technologies) is conducted considering reasonable expectations of consumers. It is crucial for individuals to establish a reasonable expectation regarding privacy protection, and this expectation should be deemed reasonable by society as a whole (Talapina, 2021).

One practical method for an information processor to evade compliance with personal data laws is through anonymization, where data is rendered non-personal. It is important to note that the definition of a similar term, "depersonalization", as outlined in the Russian Federal Law on Personal Data, does not entirely remove such data from the realm of personal data. In contrast, the GDPR employs the term "pseudonymization". This distinction exists because by eliminating certain data and replacing it with more general information (like a digital identifier), an individual can still be potentially identifiable through other seemingly non-personal information. This blending of databases is at the core of Big Data technology. It is recognized that in the era of "Big Data", information can either be valuable for processing or anonymous, but never both (Ohm, 2010). Consequently, this approach is unlikely to serve as a viable strategy for data controllers seeking to circumvent the obligations stipulated in personal data legislation.

The conventional approach to legitimizing the process of personal data through the consent of the data subject faces significant challenges in the era of creating digital profiles of citizens using "Big Data" technologies. The universal requirements for consent, including awareness, specificity, and voluntariness, pose inherent limitations in the context of "Big Data" technologies. Securing consent for processing for specific purposes within the optimal timeframe becomes unfeasible due to the inherent unpredictability of which individuals will be implicated through the results of data processing. Consequently, obtaining advance consent for such actions becomes impractical. This underscores the complexity of ensuring meaningful consent in the context of rapidly evolving data processing methods.

Considering the reasonableness of using the subject's consent as the main legitimizing basis for processing personal data in modern times is a prevailing issue in the literature on privacy protection<sup>9</sup>. When exploring the historical aspects of the emergence of such a system in the world's legal systems, researchers conclude that it currently does not function with a sufficient degree of efficiency. Individuals often do not read privacy policies or descriptions outlining the purposes and conditions of their data processing, generally written in language that is challenging for the average consumer. Furthermore, users are frequently in a dependent position and may not

---

<sup>8</sup> Opinion 4/2007 on the Concept of Personal Data. Available at: [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index\\_en.htm](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm) 7 [Accessed 01st December 2023].

<sup>9</sup> Burt A. Nowhere to Hide: Data, Cyberspace, and the Dangers of the Digital World. Digital future whitepaper series. Available at: [https://law.yale.edu/sites/default/files/area/center/isp/documents/white\\_paper\\_2020\\_nowhere\\_to\\_hide\\_burt\\_yls\\_isp\\_digital\\_future.pdf](https://law.yale.edu/sites/default/files/area/center/isp/documents/white_paper_2020_nowhere_to_hide_burt_yls_isp_digital_future.pdf) 7 [Accessed 03rd December 2023].

accurately weigh the value of their data against the digital service they receive when granting consent, as refusal to provide personal data may result in the risk of losing out on the desired service. Understanding the additional, secondary purposes for processing personal data on behalf of the primary data controller presents even greater challenge.

The establishment of a citizen digital profile system of is not founded on consent as the legitimizing basis for processing personal data and consolidating them into a unified database, but rather on processing to fulfill objectives provided for by law. In this scenario, individuals effectively lose the ability to exert control over their data; they cannot make decisions regarding their inclusion in the integrated register, their retrieval and utilization by third parties (such as in the case of obtaining banking services), or other forms of processing. Their only available action is to update information in the information systems of data controllers that are mandated to process it.

The concept of a “digital image” seems more appropriate term considering the definition of a digital persona through the data associated with it, since the primary focus of this type of activity is to capture a representation of the individual’s personality to accomplish specific objectives. However, it is important to explicitly emphasize that the use of a person’s digital image (their digital profile) is inherently intertwined with the rights of a digital person.

In particular, this is especially noticeable in the provision of public services. As part of the research conducted by the Harvard Center for the Study of Digital Society Law, several works were published on the necessary structure of any system, including the state system, which involves reflecting real personalities within it and classifying them according to certain characteristics<sup>10</sup>. It is noted that one of the principles of building such systems should be the desire to match the real and digital personalities of each individual, which also implies the possibility of changing the digital personality after the real one. A simple example is given: any registration form involves classifying the user according to certain criteria. Often, the system developer assumes a choice from a certain closed list of options, which, in general, is understandable, since this allows for the processing of results obtained with greater convenience and the division of individuals into groups. However, such a list does not always align with a person’s own self-perception (which is not always stable), and some traits may evolve and change during the course of life. This can include occupation type, profession, social status, wealth, political preferences, gender, age, race and nationality.

Big Data technologies proved to be effective in situations such as the case of the large retail chain “Target” in 2012 where employees accurately predicted a customer’s due date and sent targeted advertisements, even before the customer’s family were aware of the pregnancy<sup>11</sup>.

---

<sup>10</sup> For example: Digital Identity & Discretion. Available at: <https://cyber.harvard.edu/projects/digital-identity> [Accessed 02nd December 2023]; Cortesi S., Gasser U., Hasse A. Transforming State-of-the-Art Offline Approaches for the Digital World. Available at: <https://cyber.harvard.edu/publication/2022/transforming-state-art-offline-approaches-digital-world> [Accessed 02nd December 2023].

<sup>11</sup> Hill K. How target figured out a teen girl was pregnant before her father did. Available at: <https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/?sh=3f2acbd66668> [Accessed 02nd December 2023].

However, this scenario presents not only a risk or threat to privacy as we understand or prefer it, but also a technological perspective for the development of information systems. It is no coincidence that the GDPR not only aims to protect personal data and regulate its processing, but also advocated for free flow of such data.

Thus, the “digital image” of a person can be understood as a set of reliable, accurate, up-to-date information about a person expressed in digital form and can be used to make automatic decisions about them based on algorithmic analysis of such information.

### **Conclusion**

The category of “digital person” should be primarily examined within the scope of human rights, encompassing their rights in the digital realm, new opportunities for interaction with other individuals, legal entities, and the state. While understanding the digital person as a collection of personal data is not inherently incorrect, its validity is contingent upon the interpretations drawn from a human rights perspective. Consequently, defining a “digital person” as an individual endowed with new rights or as a novel manifestation of existing rights in the online sphere is a pivotal and unifying focus of research in the realm of digital humanity. An expert well-versed in discerning the digital persona through the lens of human rights may not have the capacity to concurrently address intricate issues in criminal, information, procedural, civil law, and data protection law. However, they can pinpoint and present pertinent challenges in these domains and gradually steer their specialized counterparts in their investigations. This underscores the intrinsic value of exploring the digital person within the current landscape of legal scholarship. Similar terms are used in the legal literature and regulatory activities: “digital personality”, “digital image of a person”, “digital profile”, and “digital citizen”. The term “digital identity” should primarily refer to all individuals, regardless of their national origin, citizenship, or place of residence as it pertains to human rights in the digital world and the guarantees for their implementation. The “digital image of a person” refers to a set of personal data that collectively represents an individual. “Digital profile” is used to describe data about a citizen within state and municipal information systems, which is utilized for identification, provision of state and municipal services, and decision-making in public policy. “Digital citizenship” is essential for developing state policies related to the implementation of citizens’ rights on the Internet.

All these terms are interrelated, and research on them is complementary. This paper will be useful for future research at more clearly distinguishing these terms and categorizing them by branches of law. Additionally, it will aid in developing methods for such research and for regulating relevant public relations.

### **References / Список литературы**

- Kapitonova, E.A. (2019) On understanding of the term “person” in modern legal science. *Law and Right*. (9), 50–53. <https://doi.org/10.24411/2073-3313-2019-10395> (in Russian).  
*Капитонова Е.А. О понимании термина «личность» в современной правовой науке // Закон и право. 2019. № 9. С. 50–53. <https://doi.org/10.24411/2073-3313-2019-10395>*

- Khusnutdinov, A.I. (2017) The right to access the Internet – a new human right? *Comparative Constitutional Review*. 4(119), 109–123. <https://doi.org/10.21128/1812-7126-2017-4-109-123> (in Russian).  
*Хуснутдинов А.И.* Право на доступ в Интернет – новое право человека? // Сравнительное конституционное обозрение. 2017 № 4(119). С. 109–123. <https://doi.org/10.21128/1812-7126-2017-4-109-123>
- Kravets, I.A. (2023) Digital citizenship and constitutional challenges in the information and algorithmic society. *Comparative Constitutional Review*. (2), 93–123. <https://doi.org/10.21128/1812-7126-2023-2-93-123> (in Russian).  
*Кравец И.А.* Цифровое гражданство и конституционные вызовы в информационном и алгоритмическом обществе // Сравнительное конституционное обозрение. 2023. № 2. С. 93–123. <https://doi.org/10.21128/1812-7126-2023-2-93-123>
- Maleina, M.N. (2017) Formation of the concept of “human being” in Russian law. *State and Law*. (1), 16–23. (in Russian).  
*Малеина М.Н.* Формирование понятия «человек» в российском праве // Государство и право. 2017. № 1. С. 16–23.
- Mossberger, K., Tolbert, C.J. & McNeal, R.S. (2008) *Digital Citizenship: The Internet, Society, and Participation*. Cambridge, MA: The MIT Press.
- Myers, D.G. (2017) *Exploring Social Psychology*. 8th edition. New York, McGraw Hill.
- Ohm, P. (2010) Broken promises of privacy: responding to the surprising failure of anonymization. *UCLA Law Review*. (57), 1701–1777.
- Sartor, G. (2017) Human Rights and Information Technologies. *The Oxford Handbook of Law, Regulation and Technology*. 424–450. <https://doi.org/10.1093/oxfordhb/9780199680832.013.79>
- Saveliev, A.I. (2015) The issues of implementing legislation on personal data in the era of Big Data. *Law. Journal of the Higher School of Economics*. (1), 43–66. (in Russian).  
*Савельев А.И.* Проблемы применения законодательства о персональных данных в эпоху «Больших данных» (Big Data) // Право. Журнал Высшей школы экономики. 2015. № 1. С. 43–66.
- Solove, D.J. (2004) *The Digital person. Technology and privacy in the information age*. New York, New York University Press.
- Sullivan, C. (2009) Digital identity – The legal person? *Computer Law & Security Review*. (25), 227–236. <https://doi.org/10.1016/j.clsr.2009.03.009>
- Talapina, E.V. (2021) Comparative digital law: formation and prospects. *Journal of Russian Law*. 25(9), 18–32. <https://doi.org/10.12737/jrl.2021.108> (in Russian).  
*Талапина Э.В.* Сравнительное цифровое право: становление и перспективы // Журнал российского права. 2021. Т. 25. № 9. С. 18–32. <https://doi.org/10.12737/jrl.2021.108>
- Talapina, E.V., Antopolsky, A.A. & Monakhov, V.N. (2021) *Human Rights in the Era of the Internet: public-law aspect: monograph*. Talapina, E.V. (ed.). Moscow, Prospect Publ. (in Russian).  
Права человека в эпоху интернета. Публично-правовой аспект: монография / Э.В. Талапина, А.А. Антопольский, В.Н. Монахов; отв. ред. Э.В. Талапина. М.: Проспект, 2021. 143 с.
- Truby, J. & Brown, R. (2021) Human digital thought clones: the Holy Grail of artificial intelligence for big data. *Information & Communications Technology Law*. 30 (2), 140–186. <https://doi.org/10.1080/13600834.2020.1850174>
- Varlamova, N.V. (2019) Digital rights – a new generation of human rights? *Proceedings of the Institute of State and Law of the Russian Academy of Sciences*. 14(4), 9–46. <https://doi.org/10.35427/2073-4522-2019-14-4-varlamova> (in Russian).

- Варламова Н.В.* Цифровые права – новое поколение прав человека? // Труды Института государства и права РАН. 2019. Т. 14. № 4. С. 9–46. <https://doi.org/10.35427/2073-4522-2019-14-4-varlamova>
- Vinogradova, E.B., Polyakova, T.A. & Minbaleev, A.V. (2021) Digital profile: concept, mechanisms of regulation and problems of implementation. *Law Enforcement*. 5(4), 5–19. [https://doi.org/10.52468/2542-1514.2021.5\(4\).5-19](https://doi.org/10.52468/2542-1514.2021.5(4).5-19) (in Russian).
- Виноградова Е.В., Полякова Т.А., Минбалеев А.В.* Цифровой профиль: понятие, механизмы регулирования и проблемы реализации // Правоприменение. 2021. Т. 5, № 4. С. 5–19. [https://doi.org/10.52468/2542-1514.2021.5\(4\).5-19](https://doi.org/10.52468/2542-1514.2021.5(4).5-19)
- Volkonsky, Y.K. (2007) *Modern political and legal relations of the individual and the state in the Russian Federation: Candidate of Legal Sciences dissertation*. Vladimir, Vladimir State Pedagogical University. (in Russian).
- Волконский Ю.К.* Современные политико-правовые связи личности и государства в Российской Федерации: дис. ... канд. юрид. наук. Владимир: Владимирский государственный педагогический университет, 2007. 189 с.
- Zajmi, I. (2015) Online Identity. In: *Global Information and national cultures*. Pristina, Kosovo. pp. 331–341.

**About the author:**

*Vladislav O. Demkin* – graduate student of the Doctoral School of Law, National Research University “Higher School of Economics”; 3 Bolshoy Trekhsvyatitsky Pereulok, Moscow, 109028, Russian Federation

**ORCID: 0000-0002-1079-425X; SPIN-код: 1755-2053**

*e-mail: vodemkin@hse.ru*

**Об авторе:**

*Демкин Владислав Олегович* – аспирант Аспирантской школы по праву, Национальный исследовательский университет «Высшая школа экономики»; 109028, Российская Федерация, г. Москва, Большой Трёхсвятительский переулок, д. 3

**ORCID: 0000-0002-1079-425X; SPIN-код: 1755-2053**

*e-mail: vodemkin@hse.ru*