DIGITAL IDENTITY AS A KEY FACTOR IN THE ESTABLISHING OF THE RIGHT TO A NAME

Iryna Kononova
Ph.D., Assistant Professor, Head of Department of Social Sciences and Strategic Communications Institute of Special Communication and Information Protection, National Technical University of Ukraine "Ihor Sikorskyi Kyiv Polytechnic Institute", Ukraine
e-mail: viti21@ukr.net, orcid.org/0000-0001-6945-0323

Diana Uniegova
Student at the Department of Computer Science of the Institute of Special Communications and Information Protection,
National Technical University of Ukraine "Ihor Sikorskyi Kyiv Polytechnic Institute", Ukraine
e-mail: dianauniegova@gmail.com, orcid.org/0009-0005-5972-2344

Summary

The article explores the phenomenon of digital identity as a new form of personification of an individual in virtual space and its interrelation with the right to a name, which constitutes one of the key components of the system of personal non-property rights. The essence and structure of the concept of "digital identity" are revealed, and its main levels – legal, social, and behavioral – are identified, reflecting the multidimensional nature of modern personal identity in the digital environment. Special attention is given to the tools of self-expression in the network – nicknames, pseudonyms, accounts, avatars, and digital signatures – through which user personification in the online space is carried out.

The paper analyzes the trends in the formation of digital identity in the context of the digitalization of society, the development of social networks, and the growing influence of artificial intelligence technologies. The main threats to the realization of the right to a name in the digital space are outlined, including fake accounts, cybersquatting, identity theft, user anonymity, and the spread of deepfake technologies, which create risks of falsifying a person's digital image.

The necessity of improving national and international legal regulation in the field of digital identity protection is substantiated, in particular through the development of unified standards for user verification and authentication, as well as the introduction of ethical principles of interaction within the digital communication environment.

Key words: digital identity, right to a name, nickname, account, pseudonym, avatar, anonymity, cybersquatting, deepfake.

DOI https://doi.org/10.23856/7216

1. Introduction

The rapid development of digital technologies has led to the emergence of a new type of social and legal reality in which an individual interacts with the surrounding world not only in the physical but also in the virtual dimension. As a result, the concept of digital identity has arisen – a complex phenomenon that combines personal data, digital traces, social roles, and technological mechanisms of identity verification.

Digital identity has become a key instrument of communication, access to services, socialization, and the exercise of rights in the modern information society *(European Union, 2024)*. However, along with these advantages, new risks have emerged, related to the potential theft, falsification, or unlawful use of digital personal attributes.

One of the most important rights undergoing transformation in the context of digitalization is the right to a name. In the digital space, a name ceases to be merely a legal identifier; it acquires new forms – nicknames, domain names, accounts – which may simultaneously hold economic, social, and cultural value.

The purpose of this article is to examine the essence of digital identity, to identify its legal aspects, and to determine the main challenges arising in the realization of the right to a name under conditions of digitalization.

The objectives of the study are to:

– reveal the structure and levels of digital identity;

– analyze the role of identity elements (nickname, pseudonym, account, avatar);

– clarify the legal issues related to the use of a name in the digital space;

– formulate directions for improving legal regulation in this field.

The methodological framework is based on general scientific methods (analysis, synthesis, induction, deduction) and special legal methods (comparative-legal, formal-legal, and systemic), which make it possible to consider digital identity as a legal and social category within the dynamics of the modern digital environment.

2. The Essence and Structure of Digital Identity

The concept of digital identity encompasses a set of characteristics that allow an individual to be identified in the virtual environment. It includes not only officially verified data but also information formed through a user's interaction with digital services – such as logins, electronic signatures, profiles, search history, financial transactions, and email addresses.

Digital identity has a multilevel structure:

Legal level – officially verified personal data that carry legal significance (e.g., electronic signature, digital passport, BankID, MobileID) *(Chernenko, 2020)*;

Social level – information voluntarily disclosed by a person online (accounts, biographical details, photos, personal blogs) *(Rybalka, 2021)*;

Behavioral level – data on user actions in the digital environment (behavioral patterns, purchase history, preferences, digital traces) *(Blikhar, 2024)*.

Thus, digital identity represents a multidimensional construct that goes beyond official data and includes the broader context of human existence in virtual space.

A distinctive feature of digital identity lies in its dynamic and fragmented nature. In contrast to classical "real" identity, which is mainly embodied in official documents, digital identity is formed from numerous sources and is constantly changing. A person may possess several identities simultaneously: one for governmental services, another for professional activities, and yet another for social networks or entertainment platforms.

Scholarly literature distinguishes several approaches to the interpretation of digital identity:

Technical-legal approach – considers digital identity as a means of user verification in the network through specific technologies (electronic signature, biometric data, etc.) *(Bosak, 2021; Blikhar, 2024)*;

Sociological approach – views digital identity as a reflection of a person's social role in virtual space *(Pikulia et al., 2023)*;

Comprehensive approach – combines technical, legal, and social aspects, emphasizing that digital identity has both legal and cultural-communicative significance *(Zahorodniuk, 2022; Shyshka, 2020)*.

It is important to note that digital identity is closely connected with the right to a name, since a name has traditionally served as the main marker of a person within the legal system. In the digital era, a name may exist in the form of a nickname, domain name, email address, or another unique identifier. This necessitates a new legal approach to regulating relations concerning the protection and use of names in the digital environment.

Moreover, the increasing complexity and autonomy of artificial intelligence systems require legislative frameworks that ensure their proper regulation, particularly in the context of military technologies. Finding balanced solutions in this regard will not only preserve human dignity and rights but also contribute to the development of friendly and humane artificial intelligence, capable of exerting a positive influence on society.

3. Elements of Digital Identity

Digital identity, as a complex and multifaceted phenomenon, does not exist independently of the specific tools and manifestations through which it is realized in the virtual space. Its structural elements are various markers of individualization that allow a person to position themselves within the network and interact with other users. The most important among these are nicknames, pseudonyms, accounts, and avatars.

Nicknames are conventional names used by individuals to represent themselves in the digital environment. They may be derived from real names or entirely fictional. A nickname performs an identification function, ensuring the uniqueness of a user's presence within a community or platform. At the same time, it serves as a means of self-expression, reflecting personal preferences, creativity, or one's social role. The legal issues surrounding nicknames involve questions of copyright, unfair use of others' identifiers, and the protection of the right to a name in the online environment *(Blikhar, 2024)*.

Pseudonyms have a deeper historical tradition, having been used by artists, scholars, and public figures long before the advent of digital technologies. In the virtual space, a pseudonym performs similar functions to a nickname but usually carries greater cultural or professional significance. For example, a writer, blogger, or activist may use a pseudonym to preserve anonymity or to build a recognizable persona. From a legal standpoint, a pseudonym is protected as an element of the right to a name and may also be subject to protection in cases of plagiarism or unauthorized use *(Rybalka, 2021; Shyshka, 2020)*.

Accounts are personalized user records within a particular information system (social network, email service, banking platform, etc.) that combine various elements of digital identity. An account includes a login, password, personal data, as well as a nickname or pseudonym, avatar, and the totality of activity accumulated within it. It serves as the central tool of communication and interaction in the digital space, as access to most services is carried out through an account. In legal doctrine and practice, an account is viewed as a set of intangible personal assets, and its unauthorized use or theft is qualified as a violation of human rights *(Bosak, 2021)*.

Avatars are visual images or symbols that a user selects to represent themselves in the digital environment. They may be realistic (a photograph) or symbolic (a drawing, icon, or 3D model). An avatar performs a dual function: it acts both as a personal identifier and as a medium of artistic or cultural self-expression. In modern virtual spaces, particularly in metaverses, the avatar becomes a key element of a person's presence, through which communication,

economic activity, and even legally significant actions are conducted. This gives rise to new legal challenges, as it raises the issue of the correlation between the avatar and the real-world individual, as well as the extent of liability for actions committed under its "mask" *(Pikulia et al., 2023; Zahorodniuk, 2022)*.

Table 1

The Main Elements of Digital Identity and Their Functions

Element	Main Function	Legal Aspects	Examples
Nickname	Identification, self-expression	Copyright, protection of the right to a name	gamer123
Pseudonym	Creative self-expression	Protection against plagiarism	Mark Twain,
Account	Access to services, integration of identity elements	Human rights violations in case of theft	Facebook
Avatar	Visual identification, self-presentation	Correlation with the real individual	3D character model, photo

These elements complement one another and together form a comprehensive picture of digital identity. While nicknames and pseudonyms primarily perform a verbal-symbolic identification function, avatars add a visual dimension, and accounts integrate all components into a unified system. Through these elements, the right to a name is realized in the virtual space; however, it takes on a modified form that requires contemporary legal understanding and appropriate regulatory frameworks.

4. Challenges to the Right to a Name

The use of a name in the digital environment has a number of features that significantly distinguish it from traditional forms of identification in legal and social relations. While in offline reality a name primarily serves as an official identifier, online it acquires a broader spectrum of meanings and forms.

First, a name in the online space often takes on alternative forms – such as nicknames, pseudonyms, domain names, or email addresses. This creates a situation in which the same individual may have multiple representations, each performing a specific function: professional, social, creative, or communicative.

Second, an online name is frequently linked not only to a person but also to the technical parameters of the system in which it is used. For example, to access email or a social network, a user applies a unique login, which becomes analogous to a name within that specific digital space. In some cases, the login may entirely replace the real name, raising the legal question of whether it should receive the same protection as a traditional name.

Third, in the digital environment, a name may be either real or fictitious. Social networks such as Facebook strive to ensure the use of real names, whereas other platforms (Twitter/X, Instagram, online forums) allow users to choose arbitrary identifiers. This promotes freedom of self-expression but also generates risks, including fake accounts, fraud, and cyberbullying.

Fourth, the online use of a name introduces new legal categories, such as domain names. A domain name serves as an identifier on the Internet and may simultaneously be the object of intellectual property rights. Conflicts between domain names and registered trademarks are a common practical issue requiring regulation at both national and international levels.

Fifth, an online name acquires a global character, as it exists simultaneously across different jurisdictions. This complicates its legal protection, since national legislations vary in their approach to defining and safeguarding personal non-property rights.

[Nickname] ----\
\
[Pseudonym] ----> [Digital Identity] ---> [Threats: Fake Accounts, Deepfakes, and Cybersquatting]
[Account] -----/
[Avatar] ----/

Fig. 1. The Interconnection of Digital Elements and Risks to the Right to a Name

Special attention should be paid to the phenomenon of anonymity and pseudonymity on the Internet. Many users choose fictitious names to protect their privacy or for self-expression; however, this should not undermine the legal status of their real name. It is necessary to ensure a balance between the freedom to choose a mode of online self-presentation and the need for identification in cases of legal violations.

Digitalization creates new conditions in which the traditional right to a name faces a number of complex challenges. The emergence of global online platforms, anonymous services, and artificial intelligence technologies significantly complicates the control over the use of names and the protection of individual rights. The main threats in the modern digital environment include anonymity, fake accounts, cybersquatting, and deepfake technologies.

Anonymity allows users to conceal their real identity by creating pseudonyms or nicknames. While this provides privacy and personal security, it simultaneously generates risks of abuse, such as the dissemination of false information, cyberbullying, or fraud. From a legal perspective, anonymity raises questions about the possibility of holding individuals accountable for unlawful actions, complicating the realization of the right to a name as a right to protect one's identity *(Chernenko, 2020)*.

Fake accounts and fraudulent profiles are created to imitate real persons or brands. They infringe upon the right to a name because they mislead third parties and may cause reputational harm. Protection against such practices requires identity verification mechanisms and rapid platform response, which are not always adequately implemented *(Digital Security Lab Ukraine, 2023)*.

Cybersquatting involves the registration of domain names identical or similar to well-known brands or individuals' names, with the intention of reselling them or gaining profit. This practice violates the right to a name, as well as copyright and trademark law, necessitating specialized legal regulatory mechanisms such as domain name dispute resolution policies *(Murashko, 2019)*.

Deepfake technologies allow for the creation of audio and video content in which a person appears or sounds as if performing specific actions or expressing particular opinions. The use of deepfakes can lead to the unauthorized dissemination of personal images, reputational damage, and deception, directly infringing upon the right to a name and associated non-property rights *(Blikhar, 2024; Digital Security Lab Ukraine, 2023)*.

5. Prospects for Improving Legal Regulation

Digitalization complicates jurisdictional protection. Since online actions are often carried out on a global scale, the legal mechanisms of a single country may be insufficient for effective response. This necessitates international cooperation and the harmonization of norms regulating the protection of names and addressing digital violations.

For the effective protection of digital identity, a systematic legal modernization is required, encompassing the following directions:

- the creation of a unified legislative framework for regulating digital personal data;
- the implementation of international standards for the protection of digital privacy;
- the development of mechanisms for verifying digital authenticity;
- the ethical regulation of artificial intelligence technologies in the creation of digital representations.

In the future, the right to a name may acquire an expanded interpretation – as the right to control one's digital identity, encompassing not only the name itself but the entire set of personal digital attributes.

6. Conclusions

Digital identity is an integral element of modern life, combining legal, social, and technological aspects and determining the ways in which individuals present themselves in the virtual space. It is directly linked to the right to a name, but assumes new forms and functions in the digital environment.

In the digital context, a name serves not only as an official identifier but also as a means of self-expression, communication, and economic activity. At the same time, digitalization generates new risks – from fake accounts to deepfake technologies – requiring a comprehensive legal response.

Further research should focus on developing the concept of the right to digital identity as a distinct legal category, which would ensure a balance between freedom of online self-expression, user security, and the protection of personal non-property rights.

References

1. Blikhar, M. (2024). Legal regulation of personal data protection. Bulletin of Lviv Polytechnic National University. Series: Legal Sciences, 11(1(41)), 26–33. https://science.lpnu.ua/law/all-volumes-and-issues/volume-11-number-1-41-2024/leg al-regulation-personal-data-protection.
2. Bosak, V. V. (2021). Pravove zabezpechennia zakhystu tsyfrovoi identychnosti osoby [Legal support for the protection of a person's digital identity]. Yurydychnyi Visnyk Ukrainy, 3(101), 45–52. [in Ukrainian].
3. Chernenko, S. (2020). Tsyfrova identychnist u mizhnarodnomu pravi: problemy pravovoho rehuliuvannia [Digital identity in international law: Legal regulation issues]. Pidpryiemnytstvo, hospodarstvo i pravo, 6, 56–60. [in Ukrainian].
4. European Union. (2024). Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. https://better-internet-for-kids.europa.eu/en/rules-guidelines/european-digital-identi ty-regulation-eu-20241183-european-parliament-and-council.

5. Murashko, V. (2019). Problemy pravovoho rehuliuvannia tsyfrovykh prav osoby v umovakh informatsiinoho suspilstva [Problems of legal regulation of digital human rights in the information society]. Derzhava i Pravo, 84, 75–80. [in Ukrainian]
6. Oliinyk, O. (2025). Legal regulation of artificial intelligence in Ukraine: Challenges and prospects. Social Development: Economic and Legal Issues, 6. https://www.eu-scientists.com/index.php/sdel/article/view/268.
7. Pikulia, T., & Shornikova, S. (2023). Artificial intelligence: Problems and prospects of legal regulation in Ukraine. SWorld-Ger Conference Proceedings. https://www.proconference.org/index.php/gec/article/view/gec30-00-005.
8. Rybalka, I. V. (2021). Internet-identychnist yak nova forma samoprezentatsii osobystosti [Internet identity as a new form of self-presentation]. Psykholohichnyi Zhurnal, 7(2), 113–120. [in Ukrainian].
9. Shyshka, R. B. (2020). Poniattia i sutnist tsyfrovoi osobystosti v tsyvilnomu pravi [The concept and essence of digital personality in civil law]. Pravo Ukrainy, 4, 45–49. [in Ukrainian].
10. Zahorodniuk, S. O. (2022). Tsyfrova osobystist: problemy formuvannia ta zakhystu v pravovomu poli [Digital personality: Issues of formation and protection in the legal field]. Informatsiine Pravo Ukrainy, 1(33), 24–30. [in Ukrainian].