

International law

UDC 341.1:004.056:342.7

DOI <https://doi.org/10.5281/zenodo.18900546>

International Legal Mechanisms for Protecting Digital Identity in Cross-Border Legal Relations

Larysa Artyshuk-Bereziuk,

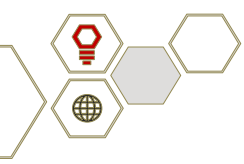
Master of Law (Jurisprudence), Founder and Scientific Director,
Project: Global Research Center for Human Identity Protection in Digital Systems,
8068 Poulson St, Citrus Heights, CA 95610, USA,
<https://orcid.org/0009-0002-5505-5474>

Accepted: 07.11.2024 | Published: 30.11.2024

Abstract. The relevance of this study is determined by the rapid digitalization of cross-border legal relations and the growing need to ensure effective international legal protection of digital identity in the context of increasing transnational data flows and technological transformations.

The purpose of this article is to substantiate the theoretical and legal foundations and to identify the distinctive features of the functioning and development of international legal mechanisms for the protection of digital identity in cross-border legal relations.

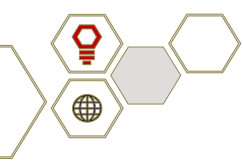
The study employed methods of scholarly literature analysis to ascertain the current state of research on the legal regulation of decentralized digital identification systems and the conceptualization of digital sovereignty, as well as methods of synthesis, generalization, and systematization to integrate doctrinal and normative approaches, structure digital identification models, identify the principal legal



challenges, and formulate substantiated conclusions regarding the improvement of the legal framework.

The study established that digital identity has acquired a complex legal nature, combining elements of personal data, electronic identification, and informational self-determination, which necessitates the formation of comprehensive international legal mechanisms for its protection. The existing international standards and principles governing the protection of personal data and digital identity were analyzed, along with the role of major international organizations, in particular the United Nations and the Council of Europe, in shaping a unified regulatory approach. The distinctive features of the European legal framework were examined, including the impact of the General Data Protection Regulation and the eIDAS Regulation on ensuring the cross-border recognition of electronic identification and trust services. It was determined that contemporary international legal mechanisms have attained a high level of normative development yet remain fragmented and insufficiently harmonized at the global level. Particular attention was devoted to the analysis of legal challenges related to jurisdiction, applicable law, and the distribution of responsibility among participants in transnational digital interactions. It was established that technological innovations, in particular artificial intelligence and decentralized digital identification models, significantly influence the transformation of legal regulation, creating both new opportunities and risks for the protection of individual rights.

The conclusions indicate that the effectiveness of international legal mechanisms for the protection of digital identity depends on the level of coordination among national legal systems, the development of interoperable standards, and the strengthening of international cooperation. It was demonstrated that the further improvement of these mechanisms requires the harmonization of legal norms, the expansion of mutual recognition instruments, and the formation of flexible, technologically neutral regulatory approaches capable of ensuring a high level of digital identity protection in the global digital space.



Keywords: electronic identification, global digital governance, international legal standards, privacy protection.

Міжнародно-правові механізми захисту цифрової ідентичності в транскордонних правовідносинах

Лариса Артищук-Березюк,

магістр права, засновник та науковий директор,

Global Research Center for Human Identity Protection in Digital Systems,

8068 Poulson St, Citrus Heights, CA 95610, USA,

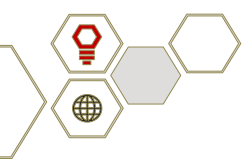
<https://orcid.org/0009-0002-5505-5474>

Анотація: Актуальність дослідження зумовлена стрімкою цифровізацією транскордонних правовідносин та зростанням потреби в забезпеченні ефективного міжнародно-правового захисту цифрової ідентичності в умовах збільшення транснаціональних потоків даних та технологічних трансформацій.

Метою статті є обґрунтування теоретико-правових засад та виявлення особливостей функціонування й розвитку міжнародно-правових механізмів захисту цифрової ідентичності в транскордонних правовідносинах.

У дослідженні застосовано методи аналізу наукової літератури – для з'ясування сучасного стану розроблення проблематики правового регулювання децентралізованих систем цифрової ідентифікації та концептуалізації цифрового суверенітету; а також методи синтезу, узагальнення і систематизації – для інтеграції доктринальних і нормативних підходів, структурування моделей цифрової ідентифікації, виявлення основних правових проблем і формування обґрунтованих висновків щодо вдосконалення правового забезпечення.

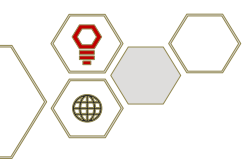
У результаті дослідження встановлено, що цифрова ідентичність набула складної правової природи, поєднуючи в собі елементи персональних даних,



електронної ідентифікації та інформаційного самовизначення, що зумовлює необхідність формування комплексних міжнародно-правових механізмів її захисту. Проаналізовано чинні міжнародні стандарти та принципи, що регулюють захист персональних даних та цифрової ідентичності, а також роль основних міжнародних організацій, зокрема Організації Об'єднаних Націй та Ради Європи, у формуванні єдиного регуляторного підходу. Розглянуто особливості європейського правового поля, зокрема вплив Загального регламенту захисту даних та Регламенту eIDAS на забезпечення транскордонного визнання електронної ідентифікації та довірчих послуг. Визначено, що сучасні міжнародно-правові механізми мають високий рівень нормативного розвитку, проте залишаються розрізненими та недостатньо гармонізованими на світовому рівні. Особливу увагу приділено аналізу правових проблем, пов'язаних з юрисдикцією, застосовним правом та розподілом відповідальності між учасниками транснаціональних цифрових взаємодій. З'ясовано, що технологічні інновації, зокрема штучний інтелект та децентралізовані цифрові моделі ідентифікації, суттєво впливають на трансформацію правового регулювання, створюючи як нові можливості, так і ризики для захисту прав особистості.

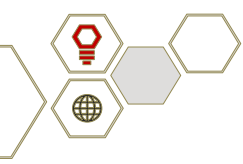
У висновках зазначено, що ефективність міжнародно-правових механізмів захисту цифрової ідентичності залежить від рівня координації між національними правовими системами, розробки сумісних стандартів та посилення міжнародного співробітництва. Доведено, що подальше вдосконалення цих механізмів потребує гармонізації правових норм, розширення інструментів взаємного визначення та формування гнучких, технологічно нейтральних регуляторних підходів, здатних забезпечити високий рівень захисту цифрової ідентичності в глобальному цифровому просторі.

Ключові слова: електронна ідентифікація, глобальне цифрове урядування, міжнародні правові стандарти, захист приватності.



Introduction. The rapid digitalization of social, economic, and administrative relations has fundamentally transformed the ways in which individuals are identified, authenticated, and represented in the global information space, thereby elevating digital identity to the status of a significant legal category within cross-border legal relations. Under conditions in which personal data circulate across multiple jurisdictions and are utilized by a broad range of public and private entities, the question of ensuring effective legal protection of digital identity acquires particular significance. The relevance of this issue is determined not only by the extensive proliferation of digital services, e-governance, and transnational platforms but also by the growing risks associated with unauthorized access to personal data, identity theft, and the misuse of digital identifiers. Existing international legal mechanisms, despite their progressive development, frequently fail to provide a sufficiently coherent and universal framework capable of addressing the complexities of cross-border data flows, resulting in a general lack of systematization in legal regulation and inconsistencies in the level of protection afforded to individuals across different jurisdictions.

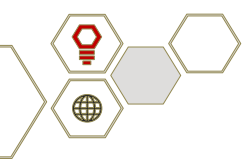
At the same time, the relevance of strengthening international legal mechanisms for the protection of digital identity is increasing due to the growing interdependence of states and the need to ensure trust in global digital interaction. The absence of harmonized standards and effective enforcement instruments complicates cooperation among states, particularly in the context of the mutual recognition of electronic identification means and the protection of fundamental human rights in the digital space. This creates a situation in which the legal status of an individual's digital identity may differ significantly depending on the applicable jurisdiction, thereby undermining legal certainty and the principle of equal protection. Furthermore, the dynamic development of new technologies and digital infrastructures outpaces the evolution of legal regulation, creating regulatory gaps and new forms of legal risk. In this context, the scholarly and practical significance of the problem lies in the necessity of developing comprehensive, adaptive, and



internationally coordinated legal approaches that would ensure a high level of protection for digital identity while facilitating the secure and effective functioning of cross-border legal relations.

Literature review. In contemporary scholarly discourse, the problem of international legal protection of digital identity in cross-border legal relations is examined through the lens of the digital transformation of society, the development of information technologies, and the increasing role of legal mechanisms in ensuring security and human rights. In particular, S. Stender, O. Frother, and Yu. Snitko substantiate the interrelationship between digital integration processes and the need to improve legal mechanisms for the cyber protection of economic systems, which directly affects the formation of effective instruments for the protection of digital identity [1]. V. Tokareva focuses on the evolution of virtual identity from multiple forms to unified authentication models, reflecting trends toward the centralization and standardization of identification processes in the digital environment [2]. Yu. Anistratenko, O. Bodunova, and I. Hrytsiuk examine the administrative and legal foundations of e-governance, emphasizing the significance of international experience in creating effective systems of electronic identification and data management [3]. An important research direction is also the analysis of emerging digital environments. O. Kostenko and O. Holovko address the problems of electronic jurisdiction in virtual spaces, focusing on the risks of legal uncertainty and the complexity of applying traditional norms in metaverse environments [4].

A substantial contribution to the development of scholarly approaches to the issue of human rights in the context of digitalization is made by M. Khaustova, who substantiates the necessity of adapting state policy to the new challenges of the digital era, including the protection of digital identity as a component of information rights [5]. O. Dzioban examines the phenomenon of the “digital human” as a philosophical and legal category that transforms traditional conceptions of the legal subject and requires a reconceptualization of legal protection mechanisms [6]. In the context of international standards, L. Chulinda and N. Bem analyze the specifics of

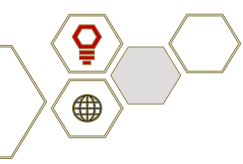


personal data use in accordance with ICAO requirements, emphasizing the significance of unified approaches to personal identification in the global space [7]. O. Radutnyi investigates the mutability of the concept of the subject of legal relations under the influence of artificial intelligence, which has a direct impact on the transformation of approaches to the definition and protection of digital identity [8]. V. Tokareva elucidates the process of forming the category of virtual identity, enabling a deeper understanding of its legal nature and place within the system of contemporary legal relations [9].

A synthesis of the scholarly approaches presented demonstrates the interdisciplinary character of the problem under investigation and confirms the necessity of further developing comprehensive international legal mechanisms for the protection of digital identity in the context of the globalization of the digital space.

Identification of previously unresolved aspects of the general problem.

Despite the substantial body of scholarly work in the field of digital identity and its legal regulation, a number of unresolved aspects remain in contemporary research that require further theoretical and legal analysis. In particular, the question of forming comprehensive international legal mechanisms for the protection of digital identity specifically in the context of cross-border legal relations, where different jurisdictions and legal regimes converge, remains insufficiently explored. Existing scholarly approaches are predominantly focused on individual elements, such as personal data, electronic identification, or digital human rights, yet do not provide a comprehensive vision of their integration into a global system of legal protection. The challenges of aligning international standards with national legal systems and the mechanisms for their effective implementation in the domain of digital identity are also addressed only fragmentarily. The impact of emerging technologies on the transformation of the legal status of the individual and the corresponding challenges for international law requires separate attention. The scholarly contribution of this article lies in the formation of a comprehensive theoretical and legal approach to



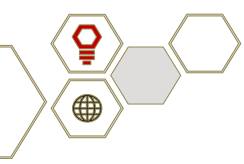
understanding international legal mechanisms for the protection of digital identity specifically within the dimension of cross-border legal relations.

Formulation of the article's objectives. The purpose of this article is to substantiate the theoretical and legal foundations and to identify the distinctive features of the functioning and development of international legal mechanisms for the protection of digital identity in cross-border legal relations.

In accordance with this purpose, the following objectives have been defined:

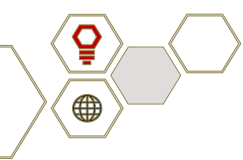
- 1) to conduct a theoretical and legal analysis of the essence and structure of digital identity in contemporary international law;
- 2) to examine the international standards and institutional mechanisms for its legal protection, as well as to analyze the distinctive features of the functioning of such mechanisms in cross-border legal relations;
- 3) to identify the principal challenges and prospects for their further development in the context of the digitalization of the global environment.

Results. The conceptualization of digital identity in legal scholarship occurs at the intersection of information law and international law, integrating human rights protection standards and underscoring the fundamental role of digital identification in the globalized space. In the most general terms, digital identity is understood as a set of data that uniquely identifies an individual within information systems and enables their verification during digital interaction [9, p. 64]. At the international level, the concept of digital identity is interpreted through a range of regulatory approaches: from rights-oriented models focused on the protection of personal data and privacy, as enshrined in the General Data Protection Regulation (GDPR) [10], to technologically and administratively oriented models aimed at ensuring secure electronic identification and trust services, as provided for in the eIDAS Regulation [11]. Within these approaches, digital identity encompasses both static identifiers – such as name, date of birth, or national identification number – and dynamic attributes – including behavioral data, biometric characteristics, and digital footprints – which collectively form a complex multilevel legal structure [10–11].



Accordingly, the classification of digital identity types may be conducted according to several criteria: by the degree of centralization – centralized, federated, and decentralized systems; by the nature of identifiers – biometric, alphanumeric, and behavioral; and by the level of assurance or trust in identity verification mechanisms. Such classification approaches are of considerable significance for determining the scope of legal regulation and the application of corresponding legal regimes across different jurisdictions, particularly in the context of the rapid development of autonomous identification models and blockchain infrastructures [10–11].

At the same time, digital identity is increasingly being integrated into cross-border legal relations characterized by the participation of entities from different jurisdictions, the use of transnational digital platforms, and the application of numerous, often mutually incompatible legal regimes. Such relations give rise to a range of legal challenges, particularly with regard to jurisdiction, applicable law, the mutual recognition of electronic identification means, and the assurance of compliance with legitimate rights in a transnational context. The absence of harmonized international standards complicates the effective protection of digital identity, especially in cases of data transfer between states with differing levels of information protection, with additional risks arising in connection with the use of artificial intelligence technologies [12, p. 9]. In this context, the risks associated with the protection of digital identity acquire a systemic character and encompass unauthorized access to personal data, identity theft, surveillance, profiling, and the misuse of biometric information. Simultaneously, the growing reliance on private entities involved in the management of digital identification systems raises concerns regarding accountability, transparency, and the maintenance of a balance between security and fundamental human rights. Accordingly, the development of effective international legal mechanisms for the protection of digital identity requires not only the harmonization of legal standards but also the formation of interoperable, human rights-oriented frameworks capable of ensuring a high level of protection in a dynamic digital environment.



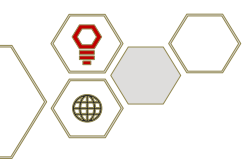
The formation of international legal mechanisms for the protection of digital identity is grounded in a system of universally recognized standards and principles that define the permissible boundaries of data processing and establish guarantees for the protection of individual rights in the digital environment [13]. Among these principles, particular significance attaches to the lawfulness, fairness, and transparency of data processing, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, as well as the accountability of data controllers. These principles are enshrined in such international instruments as the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and its modernized version, and are also reflected in the legal standards developed by the Organisation for Economic Co-operation and Development [14]. These principles constitute the normative foundation for the development of digital identity protection mechanisms, ensuring a balance between technological innovation and compliance with fundamental human rights.

The institutional dimension of international regulation is shaped by the activities of major organizations, in particular the United Nations [15, p. 147], the Council of Europe, and the European Union [16, p. 13–14]. Each of these organizations influences the development of binding and non-binding legal instruments, policy guidelines, and supervisory practices. Their impact is manifested not only in the establishment of standards but also in the promotion of interoperability among digital identity systems and the dissemination of best practices in cross-border data governance (Table 1).

Table 1

International organizations and their role in shaping legal mechanisms for the protection of digital identity

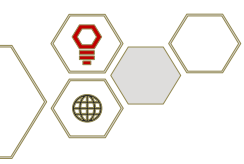
International organization	Principal legal instruments and initiatives	Role in the protection of digital identity
United Nations	Resolutions on the right to privacy in the digital age	Establishes universal human rights standards and facilitates global dialogue



International organization	Principal legal instruments and initiatives	Role in the protection of digital identity
Council of Europe	Convention 108 and its modernization (Convention 108+)	Develops binding regional standards for data and identity protection
European Union	GDPR, eIDAS Regulation	Provides a high-level regulatory framework and mechanisms for cross-border interaction
OECD	Privacy Guidelines	Ensures adherence to legal principles that influence national legislation
World Bank	ID4D Initiative	Supports the development of inclusive and secure digital identification systems

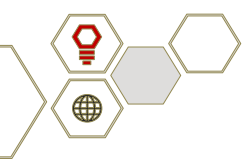
Source: compiled by the author based on [10–16]

At the same time, the development of international mechanisms for the protection of digital identity demonstrates a complex interaction between state sovereignty and international legal obligations. States seek to maintain control over national identification systems while simultaneously participating in transnational regulatory structures. This dualism generates tension, particularly with regard to data localization, national security exceptions, and the extraterritorial application of legal norms, which may conflict with the principle of sovereign equality of states. The implementation of international standards at the national level frequently encounters significant complications due to differences in legal traditions, levels of technological development, and political priorities, resulting in the fragmentation of digital identity regulation. This necessitates the development of flexible legal instruments capable of accommodating such differences while simultaneously ensuring a consistent level of protection. Particular attention in this context is devoted to mutual recognition mechanisms, adequacy assessments, and international cooperation frameworks aimed at eliminating regulatory gaps and ensuring the secure cross-border functioning of digital identification systems while preserving fundamental human rights and freedoms in the digital space.



The current stage of development of international legal mechanisms for the protection of digital identity is characterized by the strengthening of regulatory approaches, particularly within the European legal space, where a comprehensive and multilevel system has been established [17]. This system is distinguished by the interaction of binding regulations, directives, and judicial decisions that collectively set high standards for the protection of personal data and digital identity. A pivotal role is played by the General Data Protection Regulation (GDPR) [10], which not only harmonizes data protection rules among member states but also introduces extraterritorial effect, extending its influence beyond the European Union. The system is complemented by the eIDAS Regulation [11], which establishes legal certainty for electronic identification and trust services, ensuring the cross-border recognition of electronic signatures and authentication mechanisms. The case law of the Court of Justice of the European Union further reinforces the system by developing doctrines concerning data transfers, the principle of proportionality, and the protection of fundamental rights in the digital domain [18]. The normative influence of the Council of Europe also extends beyond the EU, notably through human rights instruments such as the Framework Convention for the Protection of National Minorities, which, although not specialized in digital regulation, contributes to the protection of identity-related rights, including linguistic and cultural aspects that are increasingly manifested in the digital environment [19].

The global dimension of digital identity protection is shaped by the standard-setting activities of the United Nations, which has developed a series of principles and resolutions concerning the right to privacy in the digital age, underscoring the universality of human rights regardless of the technological context. Although these standards are predominantly recommendatory in nature, they influence national legal systems and contribute to the formation of a global consensus on minimum guarantees in the processing of personal data [16, p. 13]. At the same time, international agreements and regional arrangements on the mutual recognition of electronic identification and trust services, which facilitate cross-border digital

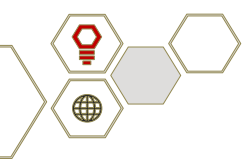


transactions and administrative cooperation, are acquiring increasing significance. In particular, such mechanisms are manifested in bilateral and multilateral agreements aligned with the eIDAS framework [11], which guarantee functional interoperability among national digital identification systems. The system of international oversight encompasses institutional actors such as the European Court of Human Rights and the Council of Europe Commissioner for Human Rights, whose activities are directed toward monitoring compliance with human rights standards and countering violations related to digital identity. Case law, particularly in the areas of surveillance, data retention, and cross-border data transfers, plays a pivotal role in the interpretation of legal norms and their adaptation to technological realities (Table 2).

Table 2

Comparative characteristics of international legal mechanisms for the protection of digital identity and their effectiveness

Mechanism / instrument	Scope of application	Achievements	Limitations
GDPR (EU)	EU and extraterritorial application	High level of data protection, unified standards	Complexity of compliance, conflicts with third-country legislation
eIDAS Regulation	Cross-border electronic identification within the EU	Legal recognition of electronic signatures and trust services	Limited global interoperability
Council of Europe instruments	Regional (Europe and beyond)	Robust human rights protection system	Indirect regulation of digital identity issues
UN standards	Global	Universal principles of privacy and data protection	Absence of binding force



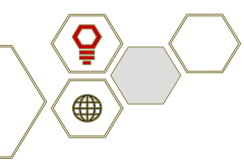
International recognition agreements	Bilateral and multilateral	Facilitation of cross-border digital interaction	Fragmentation and uneven implementation
--------------------------------------	----------------------------	--	---

Source: compiled by the author based on [10–11; 16–18]

An overall assessment of the effectiveness of existing international legal mechanisms reveals their dual nature, combining significant achievements with persistent structural limitations. On the one hand, the consolidation of legal standards, the expansion of cross-border mutual recognition mechanisms, and the growing role of judicial and quasi-judicial bodies have contributed to the strengthening of digital identity protection in the context of a globalized digital environment. On the other hand, the fragmentation of legal regimes, the absence of universally binding global instruments, disparities in enforcement capabilities, and the rapid pace of technological change continue to call into question the adequacy and coherence of the existing legal frameworks. These limitations underscore the need for the development of coordinated international approaches that would ensure legal certainty, effective protection of individual rights, and the fostering of trust in digital identification systems across different jurisdictions.

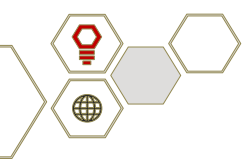
The further evolution of international legal mechanisms for the protection of digital identity is driven by a complex of systemic challenges that arise in the context of cross-border digital interactions and reveal the limitations of existing regulatory approaches. One of the key problematic aspects is the legal uncertainty associated with the determination of jurisdiction and applicable law in cases where digital identity data are processed simultaneously in several states, often through distributed infrastructures and transnational platforms. The situation is compounded by the inconsistency of national legislation, differing data protection standards, and the absence of universally recognized criteria for the distribution of responsibility among the numerous entities involved in the identity data management ecosystem.

Furthermore, the growing asymmetry between technologically advanced states and countries with limited regulatory and infrastructural capacity results in



uneven levels of digital identity protection, undermining the principle of legal certainty and predictability in international legal relations. The increasing role of private entities as principal operators of digital identification systems further complicates the regulatory landscape, as it raises questions of accountability, transparency, and the effective fulfillment of international obligations in the absence of direct state control [20, p. 438].

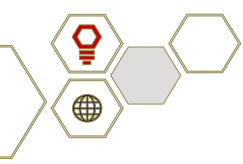
At the same time, technological innovations are substantially transforming both the nature of digital identity and the means of its legal protection, creating new opportunities and challenges. The use of artificial intelligence, particularly in automated identification and profiling systems, enhances the efficiency of identity verification but simultaneously gives rise to risks of algorithmic bias, opacity in decision-making, and potential violations of fundamental rights, which are increasingly discussed within United Nations programs. Blockchain technologies and decentralized identity models open prospects for greater user control over personal data and the realization of the concept of self-sovereign identity, yet they simultaneously call into question traditional legal concepts of liability and jurisdiction due to their distributed and often anonymous nature. The proliferation of cloud services for data storage provides scalability and flexible information management while simultaneously raising complex issues of data localization, access by foreign authorities, and the protection of digital identity in transnational data flows. In response to these challenges, the improvement of international legal mechanisms requires the development of adaptive and technologically neutral regulatory approaches that integrate binding and non-binding instruments, strengthen international cooperation, and ensure interoperability among different legal systems. A promising direction is also the development of unified digital identity standards at the global level with the participation of leading international organizations, in particular the International Telecommunication Union, which would contribute to the formation of a coherent regulatory environment.



Thus, the harmonization of international norms entails the gradual convergence of legal standards, the expansion of mutual recognition mechanisms, and the institutionalization of global governance mechanisms capable of ensuring a high and consistent level of digital identity protection in a dynamically evolving digital society.

Conclusions. The study has substantiated that digital identity in contemporary international legal discourse constitutes a complex legal category that combines elements of personal data, electronic identification means, and mechanisms of informational self-determination, forming a new dimension of the legal status of the individual in the digital environment. It has been demonstrated that international legal mechanisms for its protection are grounded in a system of universal and regional standards developed with the participation of such institutions as the United Nations, the Council of Europe, and the European Union, and are directed toward ensuring a balance between the innovative development of digital technologies and guarantees of fundamental human rights. It has been established that the functioning of these mechanisms in cross-border legal relations is characterized by the complexity of jurisdictional links, the necessity of mutual recognition of electronic identification, and the existence of conflicts among national legal regimes, which results in the fragmentation of legal regulation and uneven levels of digital identity protection on a global scale.

At the same time, it has been established that the further development of international legal mechanisms for the protection of digital identity is determined by the influence of emerging technologies, in particular artificial intelligence, decentralized identification systems, and cloud services, which simultaneously expand identification capabilities and intensify the risks of human rights violations. The necessity of improving international legal regulation through the harmonization of norms, the expansion of international cooperation instruments, and the introduction of technologically neutral approaches to the legal framework for digital identity has been substantiated. It has been determined that the effectiveness of such

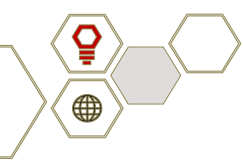


mechanisms depends on the ability of the international community to develop coordinated standards, ensure their proper implementation, and establish effective mechanisms of oversight and accountability.

Prospects for further scholarly research lie in the in-depth analysis of global digital identity governance models, the development of universal legal standards for its protection, and the investigation of the impact of emerging digital technologies on the transformation of international legal mechanisms in this domain.

References

1. Стендер С. В., Фротер О. С., Снітко Ю. М. Цифрова інтеграція та кіберзахист економіки України: правові аспекти та інноваційні стратегії. *Академічні візії*. 2023. № 26. DOI: <http://dx.doi.org/10.5281/zenodo.10389831>
2. Токарева В. О. Трансформація віртуальної ідентичності: від множинності до єдиної автентичності в мережі Інтернет. *Актуальні проблеми вітчизняної юриспруденції*. 2022. № 3. С. 47–52. DOI: <https://doi.org/10.32782/392295>
3. Аністратенко Ю. І., Бодунова О. М., Грицюк І. В. Адміністративно-правові засади регулювання електронного урядування: світовий досвід. *Юридичний науковий електронний журнал*. 2021. № 8. С. 400–404. DOI: <https://doi.org/10.32782/2524-0374/2021-8/94>
4. Костенко О. В., Головка О. М. Електронна юрисдикція Metaverse: виклики та ризики правового регулювання віртуальної реальності. *Інформація і право*. 2023. № 1 (44). С. 105–115. DOI: [https://doi.org/10.37750/2616-6798.2023.1\(44\).287729](https://doi.org/10.37750/2616-6798.2023.1(44).287729)
5. Хаустова М. Державна політика в сфері прав людини в епоху цифрових трансформацій. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2022. № 69. С. 328–333. DOI: <https://doi.org/10.24144/2307-3322.2021.69.55>



6. Дзьобань О. П. Цифрова людина як філософська проблема. *Інформація і право*. 2021. № 2 (37). С. 9–19. DOI: [https://doi.org/10.37750/2616-6798.2021.2\(37\).238330](https://doi.org/10.37750/2616-6798.2021.2(37).238330)

7. Чулінда Л., Бем Н. Використання персональних даних відповідно до міжнародних стандартів ІСАО. *International Science Journal of Jurisprudence & Philosophy*. 2022. № 1 (2). С. 64–73. DOI: <https://doi.org/10.46299/j.isjpp.20220102.6>

8. Радутний О. Мінливість концепту суб'єкта правовідносин у мінливому світі штучного інтелекту та цифрової людини. *Філософія права і загальна теорія права*. 2019. № 1. С. 146–167. DOI: <https://doi.org/10.21564/2227-7153.2019.1.186467>

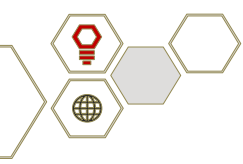
9. Токарева В. О. Формування категорії «віртуальна ідентичність» у мережі інтернет. *Часопис цивілістики*. 2022. № 45. С. 63–68. DOI: <https://doi.org/10.32837/chc.v0i45.468>

10. Загальний регламент про захист даних (GDPR). *GDPR Text: вебсайт*. URL: <https://gdpr-text.com/uk/> (дата звернення: 05.09.2024).

11. Regulation (EU) № 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. *EUR-Lex: вебсайт*. 2014. URL: <http://data.europa.eu/eli/reg/2014/910/oj> (дата звернення: 05.09.2024).

12. Пряникова П., Пряников В. Перша у світовій історії Конституція Штучного Інтелекту, Організація Об'єднаних Націй, Нью-Йорк, 2023–2025. *International Science Journal of Jurisprudence & Philosophy*. 2023. № 2 (3). С. 1–29. DOI: <https://doi.org/10.46299/j.isjpp.20230203.01>

13. Beduschi A. Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights. *Big Data & Society*. 2019. Vol. 6 № 2. DOI: <https://doi.org/10.1177/2053951719855091>



14. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних. Документ 994_326, редакція – Ратифікація від 06.07.2010. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text (дата звернення: 05.09.2024).

15. Hamad A. M., Jannial J., Indriyani R. Mechanisms of the legal protection of human rights in global regulation. *Human Rights in the Global South (HRGS)*. 2022. Vol. 1. № 2. P. 143–155. DOI: <https://doi.org/10.56784/hrgs.v1i2.31>

16. Polakiewicz J. A Council of Europe perspective on the European Union: Crucial and complex cooperation. *Europe and the World: A law review*. 2021. Vol. 5. № 1. P. 1–19. DOI: <https://doi.org/10.14324/111.444.ewlj.2021.30>

17. Beduschi A. Rethinking digital identity for post-COVID-19 societies: Data privacy and human rights considerations. *Data & Policy*. 2021. № 3. DOI: <https://doi.org/10.1017/dap.2021.15>

18. Mooij A. M. Reconciling transparency and privacy through the European Digital Identity. *Computer law & Security review*. 2023. № 48. DOI: <https://doi.org/10.1016/j.clsr.2023.105796>

19. Рамкова конвенція про захист національних меншин. Документ 995_055, редакція – Ратифікація від 09.12.1997. URL: https://zakon.rada.gov.ua/laws/show/995_055#Text (дата звернення: 25.08.2024)

20. Sullivan C., Tyson S. A global digital identity for all: the next evolution. *Policy Design and Practice*. 2023. Vol. 6. №4. P. 433–445. DOI: <https://doi.org/10.1080/25741292.2023.2267867>