Legal Regulation of Decentralized Identification Systems in the Context of Digital Sovereignty

Larysa Artyshuk-Bereziuk[1]

Published	Section	UDC
30.07.2025	Law	342.9:004.056.55:004.738.5

DOI: https://doi.org/10.5281/zenodo.18937858

Abstract. The purpose of this article is to provide a comprehensive examination of the legal regulation of decentralized digital identification models and to determine their role in strengthening the digital sovereignty of the state within the ongoing transformation of the digital legal environment. Research methods. Methods of analysis and generalization of scholarly sources, system-structural and comparative legal analysis, legal modeling, and theoretical interpretation were applied to identify patterns in the development of digital identification and to substantiate directions for improving regulatory frameworks. Results. The evolution of digital identification models was examined, and a transition from centralized registry-based approaches to distributed architectures of trust was established. Key functional characteristics of decentralized identification solutions based on the cryptographic verifiability of digital attributes and enhanced user control over personal data were identified. International and European regulatory approaches to digital identity governance were analyzed, and their influence on the transformation of interactions among the state, citizens, and digital platforms was determined. The implementation of decentralized identification mechanisms was shown to contribute to increased cyber resilience, reduced concentration of personal data risks, and the development of cross-border digital services. Conclusions. Decentralized digital identification systems were shown to constitute a new legal paradigm of digital trust and to serve as an important instrument for strengthening state digital sovereignty. The expediency of shifting legal regulation from technology-oriented approaches toward functional mechanisms that ensure trust and protection of digital rights was substantiated.

Keywords: electronic authentication, trusted digital services, personal data protection, cryptographic verification, distributed ledger technology, digital rights, e-governance, cross-border interoperability, cyber resilience, digital trust.

Правове регулювання децентралізованих систем ідентифікації в контексті цифрового суверенітету

Анотація. Актуальність дослідження зумовлена інтенсивною цифровою трансформацією публічного управління, розширенням електронних послуг та зростанням значення цифрових даних у соціально-економічних відносинах, що потребує

[1] 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, a.b.larad.0207@gmail.com, https://orcid.org/0009-0002-5505-5474

переосмислення підходів до персональної ідентифікації в цифровому середовищі. Розвиток транскордонної цифрової взаємодії, посилення кіберзагроз і необхідність забезпечення технологічної автономії держави зумовлюють формування ефективних правових механізмів сучасних моделей цифрової довіри.

Метою статті є комплексний аналіз правового регулювання децентралізованих моделей цифрової ідентифікації та визначення їх ролі в зміцненні цифрового суверенітету держави в умовах трансформації цифрового правового середовища.

Методи дослідження. Застосовано методи аналізу й узагальнення наукових джерел, системно-структурний і порівняльно-правовий аналіз, правове моделювання та теоретичну інтерпретацію для виявлення закономірностей розвитку цифрової ідентифікації та обґрунтування напрямів удосконалення нормативної бази.

Результати. Досліджено еволюцію моделей цифрової ідентифікації та встановлено перехід від централізованих реєстрових підходів до розподілених архітектур довіри. Визначено основні функціональні характеристики децентралізованих рішень, що ґрунтуються на криптографічній верифікації цифрових атрибутів і посиленому контролі користувачів над персональними даними. Проаналізовано міжнародні та європейські регуляторні підходи до управління цифровою ідентичністю та з'ясовано їх вплив на трансформацію взаємодії між державою, громадянами й цифровими платформами. Доведено, що впровадження децентралізованих механізмів ідентифікації сприяє підвищенню кіберстійкості, зменшенню ризиків концентрації персональних даних і розвитку транскордонних цифрових сервісів. Виокремлено науково-практичні проблеми, пов'язані з питаннями юрисдикції, розподілом відповідальності між учасниками цифрових екосистем та забезпеченням балансу між децентралізацією і державним контролем.

У висновках зазначено, що децентралізовані системи цифрової ідентифікації формують нову правову парадигму цифрової довіри та є важливим інструментом зміцнення цифрового суверенітету держави. Обґрунтовано доцільність переходу від технологічно орієнтованого регулювання до функціональних механізмів, спрямованих на забезпечення довіри та захисту цифрових прав. Подальші дослідження доцільно спрямувати на розроблення національної правової моделі впровадження децентралізованої цифрової ідентичності, визначення механізмів відповідальності в межах цифрових екосистем та адаптацію міжнародних стандартів до українського правового середовища.

Ключові слова: електронна автентифікація, довірчі цифрові сервіси, захист персональних даних, криптографічна верифікація, розподілені реєстри, цифрові права особи, електронне врядування, транскордонна взаємодія, кіберстійкість держави, цифрова довіра.

Introduction

The contemporary digital transformation of public administration, economic relations, and social communications necessitates a reconsideration of approaches to personal identification in the information environment. The development of electronic services, cross-border interaction, and the growing volume of data exchange underscore the need for reliable identity verification mechanisms capable of combining security, human rights protection, and the technological autonomy of the state. Traditional centralized models of electronic identification increasingly reveal limitations with respect to cyber resilience, scalability, and privacy, thereby stimulating a transition toward distributed trust architectures and the strengthening of user control over personal digital data.

This issue acquires particular importance in the context of global digitalization and Russian aggression against Ukraine, where the resilience of digital infrastructure becomes an integral component of national security and the continuity of public services. The establishment

of the legal and organizational foundations for the functioning of modern digital trust models extends beyond technological solutions and is linked to the strategic objectives of e-governance development and Ukraine's European integration.

The scholarly problem lies in the necessity of reconciling the advancement of distributed technologies with the existing legal constructs oriented toward centralized data management systems. The undefined legal status of digital attributes, the distribution of responsibility among participants in digital ecosystems, and the assurance of the legal significance of electronic interactions give rise to the need for effective digital trust mechanisms capable of ensuring secure access to services while preserving the regulatory capacity of the state.

A review of current research demonstrates the formation of a comprehensive scholarly approach that integrates the issues of digital transformation of the state, human rights protection, development of decentralized technologies, and assurance of legal certainty in the use of digital data. In particular, M. Petryshyna and M. Balaban examine digital sovereignty as the capacity of the state to exercise control over digital infrastructures, information resources, and electronic identification systems, which constitutes the foundation for the realization of state functions in the digital environment [1]. H. Muliar et al. substantiate the transformation of e-governance into the concept of the digital state, in which digital identity acquires the significance of a universal legal mechanism for individual access to public services [2]. K. Tan et al., in a systematic review of digital sovereignty and digital identity, demonstrate that the development of digitalization and digital transformation alters the role of the state, which transitions from an administrator of information systems to a guarantor of trust in the digital space [3]. A. Fischer emphasizes that the legal regulation of digital governance is determined by jurisdictional rules governing data use, access regimes, and the accountability of entities managing digital platforms [4].

A substantial body of research is devoted to the human rights dimension of digital identity, encompassing issues of privacy, the legal status of the digital person, and the procedural legitimacy of electronic data. O. Chepys analyzes the phenomenon of virtual identity as a new form of socio-legal representation of the individual, which requires the adaptation of human rights protection mechanisms to the conditions of the digital environment [5]. A. Tymchyshyn and D. Tymchyshyn investigate documents as procedural sources of evidence, which is of fundamental importance for the legal recognition of electronic identification records and digital authentication confirmations in criminal proceedings [6]. A. Zwitter et al. elaborate on the concept of self-sovereign identity (SSI), according to which the user obtains control over their own identification data without the involvement of a centralized intermediary [7]. A. Giannopoulou conducts a critical analysis of digital identity infrastructures, demonstrating the necessity of creating legal mechanisms for accountability and transparent governance of decentralized systems [8].

A considerable number of works are concerned with the study of technological models of decentralized identification and their legal frameworks. In particular, Š. Čučko and M. Turkanović systematize the architectures of decentralized identity and self-sovereign identity, identifying the principal challenges of standardization, trust, and interoperability of digital systems [9]. A. Boysen analyzes models of decentralized, self-sovereign, and consortium identity, demonstrating the necessity of differentiated legal regulation depending on the degree of centralization in digital infrastructure governance [10]. J. Lim substantiates the potential of distributed ledger technology (DLT) for harmonizing digital identification solutions and ensuring the cross-border recognition of digital identifiers [11]. N. Naik and P. enkins examine the Sovrin network as a practical implementation of self-sovereign identity based on distributed ledger technology, with an emphasis on issues of trust, network rule governance, and the legal status of its participants [12]. The practical dimension of digital identification in public administration is explored by H. Al-Ababneh et al., who demonstrate the potential of big data analytics for detecting economic crimes in the public procurement system, thereby

confirming the necessity of integrating analytical tools with reliable digital identification mechanisms for economic actors [13].

Despite the substantial body of scholarly work in the field of digital identity, its technological models, and legal regulation, a number of unresolved issues remain. These include the undefined legal status of digital attributes, the complexity of distributing responsibility among participants of decentralized systems, and the absence of harmonized international standards and mechanisms for the cross-border recognition of digital identifiers. The integration of technological innovations, such as distributed ledgers and self-sovereign identity, with existing legal constructs oriented toward centralized data management models remains insufficiently explored. Further analysis is also required of the interrelationship between the digital sovereignty of the state, human rights, and the security of digital services in the context of global digital transformation and cross-border interaction.

This article systematizes contemporary approaches to the development of digital identification and decentralized systems, synthesizes international and European models of their legal regulation, identifies the principal challenges of jurisdiction, liability, and the balance between user autonomy and state control, and offers recommendations for the implementation of decentralized digital systems in Ukraine from the standpoint of strengthening digital sovereignty and enhancing the security of the digital environment.

The *purpose* of this article is to determine the distinctive features of the legal regulation of decentralized digital identification systems and their role in ensuring the digital sovereignty of the state within the transformation of the digital legal environment.

To achieve this purpose, the following objectives have been defined:

1) to analyze the development of digital identification models and decentralized systems, identifying their specific features of functioning in the contemporary digital environment;

2) to examine the legal nature of digital sovereignty and its interrelationship with digital identification mechanisms, as well as to synthesize international and European approaches to the regulatory governance of such systems with due regard for security and data protection;

3) to identify the principal scientific and practical challenges in the legal framework for decentralized identification systems and to formulate recommendations for their implementation in Ukraine from the standpoint of strengthening digital sovereignty.

Results

The development of digital identification reflects the broader transformation of the digital environment, from centralized administrative models to distributed trust architectures. Whereas early systems were oriented toward the storage and verification of data within a single registry, contemporary digital ecosystems require a mobile, cross-border, and interoperable identity capable of functioning beyond the confines of an individual platform or state information system. It is precisely these requirements that have driven the formation of decentralized identification models, in which trust is ensured not through institutional centralization but through the cryptographic verifiability of digital attributes (Table 1).

Table 1

Evolution of digital identification models and their functional characteristics

Digital identification model	Data management center	Trust mechanism	User role	Areas of application
Centralized	State or corporate registry	Administrative verification	Passive entity	Banking systems, state registers

Digital identification model	Data management center	Trust mechanism	User role	Areas of application
Federated	Several trusted providers	Mutual recognition of identities	Partial control	Single Sign-On, digital platforms
Platform	Global IT companies	Account authorization	Platform dependency	Google, Apple, Meta accounts
Decentralized	Distributed network	Cryptographic verification	User control over data	SSI, DID, Web3 services

Source: compiled by the author based on [1; 2, p. 66; 3, p. 11; 4, p. 5; 5, p. 351]

Decentralized identification systems under contemporary conditions operate on the principle of "verifiability without centralized data storage": digital attributes of a person are formalized as verifiable credentials signed by the issuer and stored in the user's wallet, while the external infrastructure is primarily needed for publishing and verifying cryptographic identifiers and keys. The technological foundation consists of decentralized identifiers (DIDs), which provide the ability to uniquely reference a subject and the associated DID document (public keys, services, update methods) without dependence on a single registry or provider [14]. At the level of application scenarios, this means that when a service is accessed, the system does not "pull" the profile from a centralized database but rather verifies the cryptographic proof that the user possesses a valid attribute (e.g., age, status, access rights), and only the minimum required set of data is transferred. In regulatory and applied terms, such approaches are already being incorporated into the European digital identity infrastructure through the digital wallet model, in which the user controls the presentation of documents and attributes for public and private services, and interoperability is ensured through common requirements and technical "building blocks" of the ecosystem [15]. The practical value of decentralization is evident in three effects directly experienced by service operators: the concentration of risks is reduced (fewer "single points of failure" involving personal data arrays), the volume of data that must be stored and protected by the service itself is diminished, and the portability of identity across different trust domains (government services, fintech, education, mobility) is enhanced. At the same time, in real-world operation, it is the legal framework that determines whether such an architecture will be not only technically viable but also legally significant – specifically, who is recognized as the issuer of attributes, how liability for false certification is established, and how the revocation or suspension of credentials and the audit of evidence are ensured without excessive surveillance. Accordingly, the distinctive character of decentralized models in the contemporary digital space is manifested not so much in the use of a distributed ledger as in the strategic redistribution of roles and legal risks among the ledger administrator, attribute issuers, wallet providers, and verifiers, while simultaneously strengthening user control over the data presentation process.

Digital sovereignty in contemporary legal discourse is understood as the ability of a state to ensure the autonomous functioning of the digital environment by establishing regulatory rules for data circulation, trust services, and electronic identification procedures. Its significance extends beyond traditional control over infrastructure and is primarily linked to the legal definition of digital identity as the bearer of a person's rights and obligations in the online space. It is identification mechanisms that constitute the practical dimension of digital sovereignty, as it is through them that the state ensures access to public services, the legitimacy of electronic transactions, and the legal certainty of digital interaction among entities (Table 2).

Table 2

Components of digital sovereignty and their connection to digital identification mechanisms

Component of digital sovereignty	Legal content	Role of digital identification	Practical outcome
Data jurisdiction	Determination of the legal regime for information processing	Identity verification for lawful access	Control of data use
Regulatory autonomy	Formulation of national digital rules	Legal recognition of electronic identity	Legitimacy of online transactions
Infrastructure independence	Reduced dependence on global platforms	Own trusted authentication mechanisms	Resilience of digital services
Digital rights of individuals	Exercise of rights in the digital environment	Identification as a condition of access	Electronic services and contracts
Cross-border integration	Mutual recognition of identities	Interoperable means of identification	Single digital market

Source: compiled by the author

In practical terms, digital sovereignty is realized through the legal establishment of a framework for trusted identification rather than through the centralization of digital control. A notable example is the introduction of the EU Digital Identity Wallet, enshrined in the updated Regulation on Electronic Identification, Authentication and Trust Services (eIDAS 2.0), which establishes a unified legal model for digital identity across all EU member states. The regulation stipulates that digital identities continue to be issued by member states but must be mutually recognized within the Union, ensuring that citizens and businesses can access public and private services in different jurisdictions without the need to re-identify themselves [16]. This structure demonstrates a new logic of sovereignty: the state retains regulatory control over the legal force of identity while permitting its use in a supranational digital space.

In practice, this means that digital identification functions as a legal “gateway” between national jurisdictions and global digital services. For example, a user can open a bank account, sign a contract, or obtain a public service in another EU country using a national digital identity recognized under a single legal standard of trust. As a result, digital sovereignty is realized not as the isolation of the digital space but as the ability of the state to establish legally binding rules for the functioning of digital identity, ensuring a balance among intergovernmental integration, personal data protection, and control over the digital rights of citizens.

A synthesis of international and European approaches to the regulatory framework for decentralized digital identification indicates the formation of a multilevel system of legal guarantees within which the technological architecture is subject to security requirements, legal certainty, and personal data protection. European Union law establishes the legal validity of electronic identification and trust services through Regulation (EU) № 910/2014, while the General Data Protection Regulation (GDPR) [18] defines the boundaries of lawful processing of identification information and enshrines the principles of data minimization and individual control over one’s own attributes. At the international level, the recommendations of the Financial Action Task Force (FATF) [19] and the standards of the US National Institute of Standards and Technology (NIST) [20] constitute a risk-oriented model for assessing the reliability of digital identification, which enables the integration of decentralized solutions into the financial and public sectors without compromising security requirements (Table 3).

Table 3

Regulatory approaches to decentralized digital identity

Regulatory act/standard	Level of regulation	Subject of legal influence	Significance for decentralized models
Regulation (EU) No. 910/2014 (eIDAS)	European Union	Legal recognition of electronic identification and trust services	Possibility of cross-border use of digital attributes
Regulation (EU) 2016/679 (GDPR)	European Union	Protection of personal data	Restrictions on centralized data storage, minimization of data transfer
FATF Digital Identity Guidance	International	Requirements for remote customer identification	Recognition of digital evidence subject to audit and verifiability
NIST Digital Identity Guidelines (SP 800-63)	National (US), internationally applicable	Levels of identification and authentication reliability	Technology neutrality and measurable security criteria

Source: compiled by the author based on [4, p. 8; 6, p. 973; 7; 11, p. 106; 12, p. 4; 13, p. 8866]

The Regulation on Electronic Identification, Authentication, and Trust Services (eIDAS) [17] establishes the obligation of member states to recognize the electronic means of identification of other countries, provided that they meet specified levels of assurance, thereby forming the legal basis for the cross-border use of digital attributes without re-establishing identity. The General Data Protection Regulation [18] directly affects the architecture of modern identification systems, as it enshrines the principles of data minimization, proportionality of processing, and accountability of controllers, which effectively encourages the transition from the transfer of complete sets of personal information to the confirmation of individual legally significant attributes of a person. The recommendations of the Financial Action Task Force (FATF) [19] extend these approaches to the financial sector, permitting remote digital identification provided that there is an adequate level of identity verification, auditable procedures, and risk management. The guidelines of the US National Institute of Standards and Technology (NIST) [20] detail the criteria for assessing the reliability of identification and authentication, enabling various technological solutions, including decentralized ones, to be evaluated through the lens of security rather than their organizational model.

These approaches are of direct practical importance for Ukraine, as national legislation already implements the European logic of legal regulation of electronic identification through the Law of Ukraine “On Electronic Trust Services” [21], harmonized with the provisions of eIDAS [17], and the Law of Ukraine “On Personal Data Protection” [22], which establishes fundamental principles comparable to the requirements of the GDPR. The practice of using digital documents and electronic identification within the state platform “Diia” [23] demonstrates a transition from a registry-based model of identity verification to a service-oriented model of digital trust, in which access to services is provided through the verification of digital attributes without the physical exchange of documents. At the same time, Ukraine’s current legal framework remains focused primarily on a centralized registry infrastructure, creating a regulatory gap between international trends in the development of decentralized

identification and national legal control mechanisms. Accordingly, international and European instruments not only shape universal security and data protection requirements but also set the direction for the further transformation of Ukrainian legislation – from the regulation of electronic documents to the regulation of digital identity as an independent object of legal protection. It is the adaptation of these approaches that will determine the feasibility of integrating decentralized identification systems into the Ukrainian model of e-governance without forfeiting state control and while preserving digital sovereignty.

The development of decentralized digital identification systems raises a number of scientific and practical issues related to the incompatibility of traditional legal mechanisms of territorial jurisdiction with the networked nature of digital interactions. In decentralized models, the creation, storage, and verification of identification attributes can be carried out by different entities under different legal regimes, which complicates the determination of the applicable law, the competent regulator, and the procedures for protecting individual rights [13, p. 8866]. The legal force of digital identity in cross-border legal relations remains dependent on national recognition, while the infrastructure itself operates outside a single control center, creating risks of legal fragmentation.

A significant challenge is the distribution of responsibility among participants of the decentralized ecosystem. Unlike centralized registry-based models, where the system operator bears primary obligations for data protection and identification reliability, in a decentralized environment responsibility is distributed among attribute issuers, software solution developers, wallet providers, and verification entities [6, p. 973]. This complicates the determination of liability for identification errors, key compromise, loss of access to digital identity, or the use of invalid credentials, thereby constraining the full-scale application of such systems in the domains of public administration and financial services.

A separate set of challenges relates to the need to maintain a balance between decentralization and state control. Transferring data management to the user strengthens individual privacy and autonomy; however, it simultaneously complicates the state's exercise of supervisory functions, cybersecurity assurance, financial monitoring, and enforcement of judicial decisions [12, p. 4]. Persistent difficulties remain with regard to the mechanisms for revoking digital attributes, confirming their validity, conducting audits without accumulating personal data, and ensuring the evidentiary value of electronic actions in law enforcement practice. Additional risks are associated with technological dependence on foreign digital platforms, the absence of unified certification standards for software solutions, and the complexity of integrating decentralized models with existing state registries.

Under these circumstances, the improvement of the legal framework for implementing decentralized digital identification systems in Ukraine should be pursued through a reorientation of regulation from technological solutions toward the functions of digital trust. It is necessary to establish a normative definition of the legal status of decentralized digital identity, to codify the roles of the issuer, holder, and verifier of digital attributes, to introduce procedures for their verification and revocation, and to develop a model of state oversight compatible with the principle of data minimization. Strategically, such changes should be regarded as an element of strengthening digital sovereignty, entailing the development of a national infrastructure for trusted digital services, integration with European electronic identification mechanisms, and the assurance of citizen control over their own digital identity without the state forfeiting its regulatory capacity.

Conclusions

The transformation of the digital legal environment drives a natural transition from centralized registry-based models of electronic identification to decentralized systems in which trust is ensured through the cryptographic verifiability of attributes and the redistribution of control in favor of the individual. Decentralized digital identity acquires not only technological

but also independent legal significance, as it defines the means of confirming a subject's legal status, the legitimacy of electronic transactions, and the mechanisms of access to public and private services. Such systems can serve as instruments for realizing the digital sovereignty of the state, provided that their legal force, recognition procedures, revocation mechanisms, and oversight frameworks are properly established in regulation.

A synthesis of international and European approaches has revealed the emergence of a multilevel regulatory model that integrates requirements for security, data processing minimization, accountability of participants, and technological neutrality. At the same time, a number of systemic challenges have been identified, including the undefined legal status of digital attributes in decentralized environments, the complexity of delineating responsibility among issuers, wallet providers, and verifiers, the existence of cross-border jurisdictional conflicts, and the limited interoperability of decentralized models with existing centralized registries. A further challenge concerns the need to maintain a balance between user autonomy and the state's exercise of supervisory, financial monitoring, and cybersecurity functions.

The expediency of transitioning to a functionally oriented model of legal regulation for digital identification has been substantiated. Within this model, regulatory focus shifts from technological solutions as such to the functions of digital trust, the legal consequences of attribute use, and the mechanisms for their verification.

Prospects for further research are associated with developing a national model for implementing decentralized digital identity, elaborating standardized procedures for the verification and revocation of digital attributes, and assessing their impact on the resilience of digital infrastructure, the effectiveness of e-governance, and the protection of individual rights in the digital space.

References

1. Петришина М. О., Балабан М. М. Підходи ЄС до формування цифрового суверенітету: досвід Естонії для України. *Український політико-правовий дискурс*. 2025. № 10. DOI: https://doi.org/10.5281/zenodo.15306095

2. Муляр Г. В., Фур'яка Я. А., Галка Д. І. Концепція «цифрової держави» в сучасній теорії держави і права: від електронного врядування до цифрового суверенітету. *Вісник ОНДІСЕ*. 2025. № 17. С. 63–70. DOI: https://doi.org/10.32782/2522-9656/2025-17-7

3. Tan K. L., Chi C. H., Lam K. Y. Survey on digital sovereignty and identity: From digitization to digitalization. *ACM Computing Surveys*. 2023. Vol. 56, № 3. P. 1–36. DOI: https://doi.org/10.1145/3616400

4. Fischer A. Data sovereignty and e-governance: The legal implications of national laws on digital government systems. *Legal Studies in Digital Age*. 2023. Vol. 2, № 4. P. 1–12. URL: https://www.jlsda.com/index.php/lsda/article/view/39/41 (дата звернення: 25.06.2025).

5. Чепис О. І. Віртуальна ідентичність в контексті прав людини. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2025. Т. 1, № 90. С. 349–353. DOI: https://doi.org/10.24144/2307-3322.2025.90.1.46.

6. Тимчишин А., Тимчишин Д. Документи як процесуальні джерела доказів у кримінальному судочинстві. *Наука і техніка сьогодні*. 2024. Вип. 2, №30. С. 970–980. DOI: https://doi.org/10.52058/2786-6025-2024-2(30)-970-980

7. Zwitter A. J., Gstrein O. J., Yap E. Digital identity and the blockchain: Universal identity management and the concept of the "self-sovereign" individual. *Frontiers in Blockchain*. 2020. Vol. 3. Article 26. DOI: https://doi.org/10.3389/fbloc.2020.00026

8. Giannopoulou A. Digital identity infrastructures: A critical approach of self-sovereign identity. *Digital Society*. 2023. Vol. 2, № 2. Article 18. DOI: https://doi.org/10.1007/s44206-023-00049-z

9. Čučko Š., Turkanović M. Decentralized and self-sovereign identity: Systematic mapping study. *IEEE Access*. 2021. Vol. 9. P. 139009–139027. DOI: https://doi.org/10.1109/ACCESS.2021.3117588

10. Boysen A. Decentralized, self-sovereign, consortium: The future of digital identity in Canada. *Frontiers in Blockchain*. 2021. Vol. 4. Article 624258. DOI: https://doi.org/10.3389/fbloc.2021.624258

11. Lim J. Self-sovereign identity: The harmonising of digital identity solutions through distributed ledger technology. *ANU Journal of Law and Technology*. 2020. Vol. 1, № 2. P. 97–119. URL: https://search.informit.org/doi/epdf/10.3316/informit.20220516066965 (дата звернення: 25.06.2025).

12. Naik N., Jenkins P. Sovrin network for decentralized digital identity: Analysing a self-sovereign identity system based on distributed ledger technology. *2021 IEEE International Symposium on Systems Engineering (ISSE)*. IEEE, 2021. P. 1–7. DOI: https://doi.org/10.1109/ISSE51541.2021.9582551

13. Al-Ababneh H. A., Fedorchuk Y., Tymchyshyn A., Pishchenko G., Hrytsai S. The use of big data in the detection of economic crimes in public procurements. *Journal of Theoretical and Applied Information Technology*. 2024. Vol. 102, № 24. P. 8860–8871. URL: https://www.jatit.org/volumes/Vol102No24/3Vol102No24.pdf (дата звернення: 25.05.2025).

14. Decentralized Identifiers (DIDs) v1.0. *W3C: вебсайт*. 2022. https://www.w3.org/TR/did-core/ (дата звернення: 25.05.2025).

15. EU Digital Identity Wallet Home. *European Commission (Digital Building Blocks): вебсайт.* 2024. URL: https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/694487738/EU%2BDigital%2BIdentity%2BWallet%2BHome (дата звернення: 25.05.2025).

16. European Digital Identity Regulation. *European Commission: вебсайт*. 2024. URL: https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/915931811/The%2BEuropean%2BDigital%2BIdentity%2BRegulation (дата звернення: 25.06.2025).

17. Regulation (EU) № 910/2014 on electronic identification and trust services for electronic transactions in the internal market. *EUR-Lex: вебсайт*. 2014. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0910 (дата звернення: 25.05.2025).

18. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). *EUR-Lex: вебсайт.* 2016. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (дата звернення: 25.05.2025).

19. Guidance on Digital Identity. Financial Action Task Force (FATF). 2020. URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-on-Digital-Identity.pdf (дата звернення: 25.05.2025).

20. Digital Identity Guidelines (Special Publication 800-63). *National Institute of Standards and Technology (NIST): вебсайт.* 2023. URL: https://pages.nist.gov/800-63-3/ (дата звернення: 25.05.2025).

21. Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 05.10.2017 № 2155-VIII. URL: https://zakon.rada.gov.ua/go/2155-19 (дата звернення: 25.05.2025).

22. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/go/2297-17 (дата звернення: 25.06.2025).

23. Єдиний державний вебпортал електронних послуг «Дія». *Міністерство цифрової трансформації України: вебсайт*. URL: https://diia.gov.ua (дата звернення: 25.05.2025).