

УДК 342.7

DOI <https://doi.org/10.24144/2307-3322.2025.90.1.46>

ВІРТУАЛЬНА ІДЕНТИЧНІСТЬ В КОНТЕКСТІ ПРАВ ЛЮДИНИ

Чепис О.І.,
*кандидат юридичних наук, доцент,
доцент кафедри цивільного права та процесу
юридичного факультету
ДВНЗ «Ужгородський національний університет»*

Чепис О.І. Віртуальна ідентичність в контексті прав людини.

Стаття присвячена всебічному дослідженню феномену цифрової ідентичності у контексті сучасних викликів забезпечення та захисту прав людини в умовах глобальної цифрової трансформації та стрімкого розвитку віртуальних середовищ. Підкреслено, що зростання масштабів збору й обробки персональних і конфіденційних даних, зростаюча залежність від алгоритмічних систем ухвалення рішень, а також поступове витіснення безпосередньої участі людини в ідентифікаційних і контрольних процесах актуалізують необхідність переосмислення концептуальних, правових та етичних підходів до регулювання цифрової ідентичності. Визначено, що право на ідентичність досі не має уніфікованого закріплення у міжнародно-правових актах, що зумовлює існування множинних доктринальних підходів – від його розуміння як автономного суб'єктивного права до визначення як інструменту доступу до інших прав чи навіть потенційної загрози їх реалізації. Розкрито еволюцію цифрової ідентичності від базових механізмів автентифікації до багаторівневих структур, що інтегрують персональні характеристики, поведінкові патерни, біометричні дані та цифрові сліди користувачів. Виокремлено ключові ризики, зокрема дискримінацію, соціальне виключення вразливих груп, необґрунтоване профілювання, надмірний нагляд, зловживання даними та можливість використання ідентифікаційних систем як засобу політичного чи соціального тиску. Проаналізовано позиції міжнародних інституцій щодо концептуалізації цифрової ідентичності та її зв'язку з правами людини. Запропоновано перспективні технологічні рішення для збалансування безпеки та конфіденційності, зокрема децентралізовану ідентифікацію на основі блокчейну з інтеграцією смарт-контрактів, протоколи доказів з нульовим розголошенням, біометричну верифікацію та маркування перевірених облікових записів. Обґрунтовано, що оптимальна модель цифрової ідентифікації у віртуальних середовищах має поєднувати технологічну надійність, гнучкість, етичну виваженість та відповідність міжнародним стандартам, забезпечуючи баланс між правом на приватність, ефективною автентифікацією і збереженням довіри користувачів до цифрової інфраструктури.

Ключові слова: цифрова ідентичність; конфіденційність; віртуальні середовища; блокчейн; біометрична верифікація; баланс; захист прав людини.

Chepis O.I. Virtual identity in the context of human rights.

The article presents a comprehensive study of the phenomenon of digital identity in the context of contemporary challenges to the protection and safeguarding of human rights under conditions of global digital transformation and the rapid development of virtual environments. It is emphasized that the growing scale of the collection and processing of personal and confidential data, the increasing reliance on algorithmic decision-making systems, and the gradual displacement of direct human involvement in identification and control processes highlight the need to reconsider conceptual, legal, and ethical approaches to the regulation of digital identity. It is established that the right to identity still lacks unified recognition in international legal instruments, resulting in multiple doctrinal approaches—ranging from its understanding as an autonomous subjective right to its definition as a tool for accessing other rights or even as a potential threat to their realization. The evolution of digital identity is traced from basic authentication mechanisms to multi-layered structures integrating personal characteristics, behavioral patterns, biometric data, and users' digital footprints. Key risks are identified, including discrimination,

social exclusion of vulnerable groups, unjustified profiling, excessive surveillance, misuse of data, and the potential use of identification systems as tools of political or social pressure. The positions of international institutions on the conceptualization of digital identity and its relationship with human rights are analyzed. Promising technological solutions for balancing security and privacy are proposed, including decentralized blockchain-based identification with integrated smart contracts, zero-knowledge proof protocols, biometric verification, and verified account labeling. It is argued that the optimal model of digital identification in virtual environments should combine technological reliability, flexibility, ethical soundness, and compliance with international standards, ensuring a balance between the right to privacy, effective authentication, and the preservation of user trust in digital infrastructure.

Key words: digital identity; privacy; virtual environments; blockchain; biometric verification; balance; human rights protection.

Постановка проблеми. Використання великих обсягів даних, зокрема персональних і конфіденційних, посилення залежності від алгоритмічних систем аналізу та ухвалення рішень, а також прогресуюча редукція людської участі й контролю в автоматизованих процесах актуалізують дискурс щодо справедливості, відповідальності та забезпечення прав людини в цифрову епоху. Коли особиста інформація постійно збирається та поширюється, важливо усвідомлювати, наскільки взаємопов'язані ідентичність та конфіденційність, адже люди повинні мати право зберігати та захищати свою особисту ідентичність, не боячись дискримінації чи стеження [1].

Метою статті є визначення місця цифрової ідентичності у системі прав людини та пошук балансу між забезпеченням безпеки і захистом конфіденційності у віртуальних середовищах.

Нині все більше науковців звертають увагу на проблеми, пов'язані із правами, що виникають у цифровому середовищі. Серед них зокрема українські вчені: Н. Бааджі, С. Булеца, А. Долінська, А. Сліпченко, С. Сліпченко, Є. Харитонов, Р. Майданник, К. Некіт, В. Токарева та інші. Серед іноземних дослідників слід згадати: Arraiza J.M., Hannah Sutor, Ghadge N., Paul De Hert, Limongelli R., Robles-Carrillo M., Sposini L. та ін.

Виклад основного матеріалу. Право на ідентичність у жодному юридично обов'язковому тексті формально та прямо не визначено. За відсутності конкретної правової основи існують різні тлумачення щодо того, чи є це правом. На думку Консультативного комітету Конвенції № 108 Ради Європи, концепція правової ідентичності була розроблена на основі статті 6 Загальної декларації прав людини, яка стверджує, що кожна людина має право на визнання її правосуб'єктності, де б вона не знаходилася [2]. Правова ідентичність розглядається як самостійне право у доповіді Генерального секретаря Організації Об'єднаних Націй «Наш спільний порядок денний» [3]. Забезпечення правової ідентичності для всіх є метою Стратегії сталого розвитку ООН на період до 2030 року [4]. Спеціальний посланник Генерального секретаря з питань технологій відносить цифрову ідентичність до цифрових прав [5]. Де Герт стверджує, що специфічне право на ідентичність слід чітко відрізнити від класичних прав або прав першого покоління, оскільки цифрову ідентичність потрібно розуміти в динамічних термінах [6, с. 12].

Еволюція цифрової ідентичності тісно пов'язана з технологічним прогресом та суспільними змінами. Спочатку вона обмежувалася такими важливими елементами, як імена користувачів та паролі, головним чином для контролю доступу. Однак, з розвитком соціальних мереж та електронної комерції, цифрова ідентичність стає складнішою та інклюзивнішою. Люди тепер беруть участь у різних онлайн-взаємодіях, залишаючи після себе слід даних, який формує детальний профіль їхнього віртуального «я» [7, с. 2]. Це не просто базова інформація, така як ім'я та вік, але й усе, що користувач робить та залишає в Інтернеті. Подібно до того, як наша реальна ідентичність має шари, цифрова ідентичність така ж багатопшарова [6, с. 1].

Зауважимо, що ще у 2007 році ОЕСР (Organisation for Economic Co-operation and Development - Організація економічного співробітництва та розвитку) визначила властивості цифрової ідентичності: соціальна, суб'єктивна, ціннісна, референційна, складна, послідовна, динамічна, контекстуальна та неоднозначна. Родрігес вважає, що вона може бути унітарною або множинною, рівною або різною, фіксованою або гнучкою, локальною або універсальною, автентичною або діяльною, володіною або власною, призначеною або передбачуваною, фрагментованою або цілісною, публічною або приватною, анонімною або псевдоанонімною, тимчасовою або постійною, видимою або невидимою [6, с. 9]. При цьому етичні міркування відіграють вирішальну роль у формуванні практики цифрової ідентичності, а такі принципи, як прозорість, згода та мінімізація

даних, керують етичною поведінкою. Крім того, дискусії щодо моральних наслідків таких технологій, як штучний інтелект та біометрія, підкреслюють необхідність постійного перегляду та коригування існуючих правових рамок для захисту цифрових ідентичностей у постійно мінливому цифровому ландшафті [8].

Аналіз інституційної та академічної практики показує, що існує п'ять основних підходів розуміння ідентичності: 1) цифрова ідентичність концептуалізується навколо ідеї репрезентації; 2) широкий академічний та технічний сектор розглядає цифрову ідентичність як інформацію або як суму даних, тверджень чи атрибутів. Зокрема у Керівних принципах, виданих Консультативним комітетом Конвенції 108 Ради Європи, цифрова ідентичність визначається як «обробка даних про особу таким чином, щоб вона була однозначно ідентифікована в заданих контекстах»; 3) підходи, що поєднують два попередні варіанти. До прикладу, у 2008 році ОЕСР розглядала цифрову ідентичність як «цифрове представлення набору заяв, зроблених однією стороною про себе або іншого суб'єкта даних» [6, с. 11]; 4) визначення цифрової ідентичності як «суміші індивідуальної детермінації та реляційних аспектів». На думку Херта, це «суміш ірсе-ідентичності та ідем-ідентичності. Ірсе-ідентичність – це самоідентичність. Ідем-ідентичність – це об'єктивація «я», що впливає з порівняльної категоризації [1, с. 8]; 5) підхід, згідно з яким жодне з цих визначень не відображає належним чином загальний зміст терміна «цифрова ідентичність». Зокрема Міжнародна асоціація адвокатів вважає існуючі визначення недоречними, оскільки, будучи глобальною проблемою, цифрова ідентичність потребує глобального підходу.

Слід зауважити, що на сьогодні немає консенсусу і щодо природи цифрової ідентичності: це автономне право, постачальник/провідник прав чи загроза правам? Вітчизняна цивілістка Булеца С.Б. вважає, що право на віртуальну ідентичність та право на віртуальну конфіденційність тісно пов'язані з немайновими правами людини і відносить їх до особистих немайнових прав особи. На її думку, важливо розглядати їх у контексті захисту особистих даних та інтересів користувачів в інтернеті. Це сприяє забезпеченню поваги до прав людини в цифровому просторі [10, с. 243]. Визнання ідентичності та конфіденційності правами людини дозволяє виступати за їх захист та забезпечувати дотримання гідності та автономії людей. Це передбачає сприяння прозорості у практиці збору даних, впровадження суворих законів про захист даних та поваги до конфіденційності. Підвищуючи обізнаність та розуміння ідентичності та конфіденційності як прав людини, ми можемо працювати над створенням безпечнішого та справедливішого цифрового середовища для всіх [1].

Другим підходом є розуміння цифрової ідентичності як необхідної умови для здійснення деяких прав, зокрема доступу до Інтернету, свободи інформації та вираження поглядів. Як пояснює Ханна Арентс, це «доправова передумова» або «протоправо». За даними ОЕСР, «право на ефективну цифрову особистість, можливо, буде найважливішим правом у майбутньому інформаційному суспільстві, оскільки воно визначатиме можливість людини користуватися всіма іншими правами, включаючи політичні, економічні, соціальні та культурні права» [1, с. 127].

Відповідно до третього підходу системи та процедури цифрової ідентифікації можуть не тільки впливати, а навіть завдавати шкоди правам людини. У своїх Керівних принципах щодо національної цифрової ідентичності Консультативний комітет Конвенції Ради Європи вже попереджав про негативні наслідки цифрової ідентифікації для прав людини. Окрім ризиків для конфіденційності, ці наслідки можуть «варіювати від дискримінації та виключення до маргіналізації, необґрунтованого профілювання та спостереження, втрати людиною контролю над своєю особистістю або навіть зловживання власною особистістю» [6, с. 14]. Фактично, національні схеми цифрової ідентифікації «можуть не враховувати, не передбачати або не захищати від ризиків для основних прав і свобод осіб». Більш конкретно, основна проблема виникає через використання цифрової ідентичності як засобу контролю та спостереження. Адже якщо у фізичному світі це засіб ідентифікації, то у цифровому світі вона виконує три основні функції – ідентифікацію, автентифікацію та авторизацію – і є фактичною точкою входу до цієї екосистеми [6, с. 18]. Тож впровадження цифрової ідентифікації є територією високого ризику для прав людини. Шкода, якої завдають системи цифрової ідентифікації, полягає в наступному: 1) через неадекватні процедури реєстрації, неадекватні закони, надмірні вимоги, ігнорування контекстів із цифровим розривом, технічні збої та випадки цифрового адміністративного насильства, цифрова ідентифікація увічнює структурну ізоляцію вразливих груп. У цьому сенсі суспільство погоджується з тим, що державні установи не повинні вимагати обов'язкової реєстрації в системах цифрової ідентифікації або вимагати використання цифрової ідентифікації для доступу до

державних послуг; 2) масова цифрова ідентифікація, що впроваджується без надійного захисту, призводить до зловживань у зборі та використанні даних і легко порушує конфіденційність; 3) проектування, розгортання, впровадження та управління цими системами часто зумовлені потужними фінансовими та приватними інтересами, за умови малого обсягу громадських консультацій; 5) цифрові посвідчення особи, особливо ті, що інтегрують біометричні дані, можуть використовуватися для відстеження переміщень, покупок та онлайн-активності осіб без їхнього відома чи згоди. Уряди також можуть неправомірно переслідувати певних осіб, використовуючи блокування цифрового посвідчення особи або інші методи як зброю проти політичних опонентів або вразливих груп, таких як мігранти [12].

Очевидно, що фундаментальною проблемою у сфері віртуальних світів є те, що розробка та впровадження процесів ідентифікації та верифікації повинні враховувати два конкуруючі фактори: конфіденційність та безпеку [13, с. 12]. Встановлення балансу між перевагами віртуальної анонімності та обов'язками ідентифікованої присутності є ключовим для навігації в правовому та технологічному ландшафті віртуальних середовищ, що розвиваються [14, с. 18]. До перспективних рішень проблеми збалансування вимог конфіденційності та безпеки належать:

Система ідентифікації на основі блокчейну може забезпечити децентралізований, безпечний та захищений від несанкціонованого доступу метод зберігання та перевірки ідентичності користувачів. Кожному користувачеві може бути призначена унікальна цифрова ідентифікація, криптографічно пов'язана з його реальною ідентичністю. Системи перевірки особи на основі блокчейну також можуть інтегрувати смарт-контракти, що дозволяє автоматично забезпечувати виконання дозволів на доступ, ліцензійних угод та інших договірних умов на основі перевірених ідентичностей. Крім того, притаманна блокчейну прозорість сприяє відстеженню дій, підвищуючи підзвітність у віртуальних світах. При цьому системи на основі блокчейну повинні бути продумано розроблені з урахуванням норм конфіденційності користувачів та захисту даних [13, с. 12].

Незважаючи на анонімність, якою користуються користувачі у віртуальних середовищах, платформи зазвичай можуть ідентифікувати людей, які стоять за аватарами, за допомогою зібраних реєстраційних даних, включаючи IP-адреси. У випадках серйозних неправомірних дій платформам пропонується розкрити особу користувача-порушника. Таке розкриття має обмежуватися серйозними випадками, щоб зберегти цілісність системи та довіру користувачів, збалансовуючи потребу у підзвітності та право на конфіденційність [14, с. 19].

Методи, що забезпечують надійну безпеку без шкоди для конфіденційності чи користувацького досвіду, такі як протоколи доказів з нульовим розголошенням, можуть бути особливо цінними. Ці протоколи можуть довести правдивість заяв, не розкриваючи жодної додаткової інформації, забезпечуючи баланс між безпекою та конфіденційністю [15].

Ключову роль у підвищенні безпеки та надійності у сфері цифрової ідентичності відіграє інтеграція систем біометричної верифікації. Зі зростанням попиту на безпечний контроль доступу в таких галузях, як охорона здоров'я, фінанси та адміністрування, впровадження біометричних методів забезпечує зручні рішення [7, с. 4].

Деякі традиційні соціальні мережі, такі як Twitter та Facebook, зазвичай надають «значок» для облікових записів, особи власників яких перевірені, і користувачі, як правило, більше довіряють цим «перевіреним обліковим записам». Подібний механізм може бути адаптований до спільнот соціальної віртуальної реальності, що надає статус ідентичності автентифікованим користувачам [8].

Висновки. Відсутність уніфікованого визначення права на ідентичність у міжнародно-правових актах зумовлює наявність численних підходів до його розуміння – від концептуалізації як автономного суб'єктивного права до трактування як інструменту доступу до інших прав або потенційної загрози їх реалізації. Нині цифрова ідентичність має багатовимірний характер, поєднуючи правові, технологічні та етичні аспекти. Для віртуальних середовищ особливо актуальною є розробка гнучких моделей ідентифікації, які поєднують захист приватності з ефективною верифікацією, зберігаючи при цьому користувацький досвід і довіру до цифрової інфраструктури. Хоча суворіші процеси ідентифікації та перевірки можуть підвищити безпеку у віртуальних світах, вони повинні бути ретельно збалансовані з урахуванням конфіденційності користувачів та взаємодії з ними. Надмірно нав'язливі методи ідентифікації можуть порушувати конфіденційність користувачів та перешкоджати участі у віртуальних середовищах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Hannah Sutor. Safeguarding Identity and Privacy: Fundamental Human Rights in the Digital Age. Available at: <https://idpro.org/safeguarding-identity-and-privacy-fundamental-human-rights-in-the-digital-age>.
2. Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data of the Council of Europe (n 25) 6.
3. <https://www.un.org/en/un75/common-agenda>.
4. <https://sdgs.un.org/2030agenda>.
5. <https://www.un.org/techenvoy/es/content/digital-human-rights>.
6. Robles-Carrillo, Margarita. Digital identity: an approach to its nature, concept, and functionalities. *International Journal of Law and Information Technology*, 2024, vol. 32, eaac019. Available at: <https://doi.org/10.1093/ijlit/eaac019>.
7. Ghadge, Nikhil. Digital Identity in the Age of Cybersecurity: Challenges and Solutions. *London Journal of Research in Computer Science and Technology*, 2024, vol. 24, issue 1, compilation 1.0. Available at: https://www.researchgate.net/publication/381852443_Digital_Identity_in_the_Age_of_Cybersecurity_Challenges_and_Solutions.
8. Lin J and Latoschik ME, Digital body, identity and privacy in social virtual reality: A systematic review, 2022. *Front. Virtual Real.* 3:974652. doi: 10.3389/frvir.2022.974652.
9. Paul De Hert, *A Right to Identity to Face the Internet of things* (2007) 15–16, available at <https://researchportal.vub.be/en/publications/a-right-to-identity-to-face-the-internet-of-things-2>.
10. Булеца С.Б. Віртуальна ідентичність та віртуальна конфіденційність як особисте немайнове право. Випуск № 2, 2025. С. 243–252. DOI <https://doi.org/10.24144/2788-6018.2025.02.33>.
11. Arendt, Hanna *e Origins of Totalitarianism*. Meridian Books, 1967.
12. José María Arraiza. Between Progress and Exclusion: The Human Rights Challenges of Digital ID. Available at: <https://www.salzburgglobal.org/news/topics/article/between-progress-and-exclusion-the-human-rights-challenges-of-digital-id>.
13. Limongelli R, Sposini L. The (virtual) battle for intellectual property rights in the metaverse: The case of copyright, trademarks and the NFT technology. *Metaverse*. 2025; 6(1): 3056. Available at: <https://doi.org/10.54517/m3056>.
14. Chawki, M., Basu, S., & Choi, K.-S. Redefining Boundaries in the Metaverse: Navigating the Challenges of Virtual Harm and User Safety. *Laws*, 2024, 13(3), 33. Available at: <https://doi.org/10.3390/laws13030033>.
15. Balis J. How brands can enter the metaverse. HBR Online. 2022; 1–6. Available online: <https://hbr.org/2022/01/how-brands-can-enter-the-metaverse>.