УДК 341.181
DOI https://doi.org/10.24144/2307-3322.2024.83.1.27

ЕЛЕМЕНТИ ЦИФРОВОЇ ІДЕНТИЧНОСТІ

Гончарова А.В.,
кандидат юридичних наук,
доцент кафедри кримінально-правових дисциплін та судочинства
ННІП Сумського державного університету,
дослідник університету Туру (Франція)
ORCID: 0000-0002-9815-0394
e-mail: a.goncharova@yur.sumdu.edu

Гончарова А.В. Елементи цифрової ідентичності.

Стаття розкриває процес ідентифікації особи, як учасника цивільних правовідносин в сучасному цифровому світі. Наголошується, що стрімкий розвиток сучасних цифрових технологій потребує переосмислення та доопрацювання юридичної термінології. Поняття цифрової ідентичності є актуальним та складним для сучасних правових систем світу. Аналіз та адаптація вже існуючого законодавства до цифрового прогресу є неминучою. Цифрову ідентичність можливо розглядати в багатьох аспектах, акцентуючи увагу на стабільних формах, таких як соціальна та правова. Цифрова ідентичність є версією соціальної ідентичності людини. Це певна добірка інформації, отриманої в результаті онлайн-діяльності особи, яка може проявлятися у вигляді імені, публікацій, коментарів тощо.

Зазначено, що правові форми ідентичності особи в цивільно-правовому розуміння у світі цифрового права потребують розширення. Акцентується увага на класичних формах цифрової ідентичності, це – стійка ідентичність, сконструйована ідентичність та прихована ідентичність. Стійка ідентичність являє собою незмінну інформацію. Як приклад, ім'я яке дається при народженні.

Формування ідентичності, як розвиток окремої особистості цифрового індивіда, яка розглядається як стійка сутність на певному етапі цифрового життя, за допомогою якого особа позиціонує себе в цифровому світі. Цей процес визначає індивідів до інших і самих себе. Фрагменти фактичної ідентичності визначають унікальні ознаки індивіда та його приналежності до певної соціальної групи. Формування ідентичності чітко впливає на особисту ідентичність, за допомогою якої особа презентує себе як дискретну одиницю в цифровому вимірі. Це може бути через індивідуалізацію, за допомогою якої недиференційований індивід прагне стати унікальним, або проходити етапи, через які диференційовані аспекти життя людини прагнуть стати більш неподільним цілим.

Дослідження сконструйованої ідентичності надає можливість зрозуміти, що є можливість зміни інформації в даній формі ідентичності, як то, зміна прізвища при укладенні шлюбу. В мережі Інтернет, як правило, вказується тільки сконструйована ідентичність особи. Остання форма досліджуваної ідентичності, це – прихована ідентичність. Стосується інформації, яку особа без потреби не розголошує іншим учасникам цифрового простору. Як то, паспортні дані, ідентифікаційний код тощо. Дані питання потребують подальшого аналізу та дослідження. Історичний аналіз засвідчив відсутність етапів зародження цифрової ідентичності, це нова концепція, яка стосується онлайн-представлення особи та для використання в кіберпросторі.

Ключові слова: цивільне право, цифрове право, особа, дієздатність, кіберпростір, захист персональних даних.

Goncharova A.V. Elements of digital identity.

The article reveals the process of identifying an individual as a participant in civil legal affairs in the current digital world. It is agreed that the rapid development of modern digital technologies will require rethinking and updating of legal terminology. The concept of digital identity is relevant and complex for current legal systems in the world. Analysis and adaptation of existing legislation to digital progress

is inevitable. Digital identity can be seen in many aspects, focusing on stable forms, such as social and legal. Digital identity is a version of a person's social identity. Continuous collection of information obtained as a result of an individual's online activity, which can be manifested in the appearance of a name, publication, comments, etc.

It is stated that the legal forms of an individual's identity in a civil-legal sense in the light of digital law will require expansion. The emphasis is on the classic forms of digital identity, which is persistent identity, constructed identity and captured identity. Stable identity is immutable information. Like a butt, this name is given to the people.

The formation of identity, as the development of a specific feature of a digital individual, which is seen as a persistent reality at the beginning stage of digital life, in addition to which person positions himself in the digital world. This process defines individuals to others and to themselves. Fragments of factual identity represent the unique characteristics of an individual and his affiliation to a particular social group. The formation of identity clearly flows into a particular identity, in addition to which the individual presents himself as a discrete unit in the digital world. It is possible through individualization, in addition to some non-differentiation, that the individual does not become unique, but goes through stages, through some differentiated aspects of people's lives, and thus achieves more inseparable goals.

Following the constructed identity makes it possible to understand that it is also possible to change information in this form of identity, such as changing a name when laying a sluice. On the Internet, as a rule, only the constructed identity of an individual is indicated. The remaining form of traceable identity, which is captured identity. There is a need for information that a person needlessly does not disclose to other participants in the digital space. For example, passport data, identification code, etc. These nutritional data will require further analysis and investigation. The historical analysis reveals the multiple stages of the emergence of digital identity, and the value of the new concept of the online representation of an individual for his or her existence in the cyberspace.

Key words: civil law, digital law, person, legal capacity, cyberspace, personal data protection.

Постановка проблеми. У звичайному розумінні, ідентичність може бути визначена приблизно як постійний та фундаментальний характер особи, групи, яка створює свою індивідуальність, свою унікальність. Зустрічається поняття ідентичності в психологічному, соціальному та філософському аспектах. В юридичному аспекті поняття ідентичності розглянуто частково. Поняття цифрової ідентичності не досліджені.

Стан опрацювання. Певний вклад у вивчення окресленої проблематики внесли такі вчені як Д. Ванг, Т. Гарасимів, К. Гончаренко, В. Заїчко, О. Дольська, О. Дзьобань, Л. Морська, Н. Супрун, Т. Уварова, Л. Усанова та інші. Але все ж вказана проблематика не вивчалась зазначеними авторами цілісно.

Метою статті є дослідження впливу цифрової ідентичності на суспільство, дослідження можливостей інтеграції цифрових ідентифікаційних систем між різними платформами та країнами, забезпечення прав людини і приватності.

Виклад основного матеріалу. Щоб зрозуміти поняття цифрової ідентичності, проаналізуємо праці Ж. Рохфельд, яка стверджувала, що суть цифрової ідентичності складають елементи стабільної ідентичності, ті «соціальні координати», які вже добре відомі правовій системі, які мало змінюються протягом життя і які вказують на одну фізичну особу. Щодо стійкої ідентичності, то це сукупність елементів, які були надані особі при народженні. Подальша їх модифікація, в кращому випадку, вкрай складна, в гіршому – неможлива. Сконструйована ідентичність, з іншого боку, пропонує бачення – обов'язково часткове, перебільшене, мінливе, це подорож індивіда від народження до смерті [1].

Зазначимо, що стабільна ідентичність відіграє роль як офлайн, так і онлайн, як фундамент, навколо якого будуть створюватися всі персональні дані, що утворюють сконструйовану ідентичність. Коли особа здійснює діяльність у мережі, чи відома його стабільна особистість тим, хто робить контент і послуги доступними для нього або хто обмінюється з ним? Відповідь, в принципі, негативна: ідентичність завуальована.

Щодо прихованої ідентичності, то для неї характерна анонімність. Небезпека анонімності очевидна. Це сприяє безкарному вчиненню правопорушень, як то порушення авторських прав або численні зловживання свободою вираження поглядів. Слід, однак, зазначити, що у влади є кілька

ефективних засобів порушення анонімності, в тому числі і вже згаданий, який полягає в тому, щоб змусити інтернет-провайдера прив'язати IP-адресу порушника до його абонентського каталогу.

Таке епізодичне зняття анонімності набагато краще, ніж систематична і узагальнена ідентифікація.

Розглянемо рішення Апеляційного суду в Гаммі (Німеччина) від 2011 року, яке яскраво ілюструє ситуацію з анонімністю. Цей суд був ініційований психотерапевтом, який був незадоволений посередньою оцінкою, яку йому дав колишній пацієнт на онлайн-платформі рейтингу. Його апеляційну скаргу було відхилено, так як суд вважав, що обов'язок супроводжувати певну думку може призвести до того, що люди не висловлюватимуть свою думку, побоюючись репресій. Він додає, що цей ризик самоцензури суперечитиме фундаментальному праву на свободу вираження поглядів [2].

Європейський суд з прав людини зробив аналогічні зауваження у рішенні, винесеному його Великою палатою у 2015 році. Погрози та наклепницькі зауваження були розміщені в коментарях під статтею для преси на сайті естонської газети. Зроблені зауваження були явно незаконними, як результат, автори були притягнуті до відповідальності [3].

Користувачам інтернет за замовчуванням забезпечує анонімність для своїх. Такі соціальні взаємодії, безумовно, виявляють частково ідентифікаційні елементи, такі як зовнішність, але користувач Інтернету також виявляє фрагмент ідентифікації через свою IP-адресу. Потім ми побачимо, як ці сліди можуть бути використані, щоб виявити, яку стабільну ідентичність вони приховують.

Поєднання технічних і культурних засобів, пропонованих Інтернетом для використання анонімності та псевдонімності, створює потужний психологічний ефект. Це можливість для індивіда, поводитися так, ніби він на кілька годин позбувся своєї стійкої ідентичності.

Потреба в онлайн-ідентифікації є неодмінним елементом при укладенні цивільно-правових договорів. Право на доступ до певної інформації та послуг не надається жодному відвідувачу без підтвердження стабільної ідентичності. Тільки вони мають право проконсультуватися з конкретним банківським рахунком або видати розпорядження щодо переказу; ознайомитися з документом, на який поширюється податкова таємниця; ознайомтеся з інформацією, призначеною для співробітників компанії або студентів ВНЗ. З іншого боку, укладення договору не завжди вимагає глибокої ідентифікації, як офлайн (наприклад, купівля газети в місцевому газетному кіоску), так і онлайн. Але поряд з дрібними договорами повсякденного життя існують угоди, що мають істотне значення, які неможливо уявити собі укладення без знання здатності до укладення договору або навіть повної цивільної ідентичності свого партнера.

Крім того, потреба в ідентифікації на деяких онлайн-платформах є обов'язковою, так як надавач послуг повинен знати хто є користувачем. Але користувач також повинен переконатися, що він має справу з автентичною платформою. На жаль, є багато сайтів, які видають себе за продавців або кредитні установи з метою викрадення особистих даних – насамперед платіжних.

Аутентифікація користувачів є необхідним етапом для укладення цивільно-правових договорів. Як перевірити особу відвідувача? У світі відсутня глобальна система «офлайн» ідентифікації з подальшим наданням індивідуального цифрового сертифіката. Визначальне значення простої декларативної форми, яке повсюдно зустрічається в інтернеті, практично дорівнює нулю. Такої односторонньої декларації недостатньо, якщо ідентифікація є обов'язковою умовою для обміну конфіденційною інформацією або для укладення угод із серйозними правовими наслідками. Існує три набори зчитування інформації: 1) ім'я користувача, пароль, підпис тощо; 2) смарт-карта, магнітна картка, телефон, на який надходить SMS тощо; 3) біометрична характеристика, наприклад, відбиток пальця або розпізнавання сітківки. Слід зазначити, що жоден з цих процесів не забезпечує ідеальну безпеку [4, с. 218]. Однак вибір ідентифікаційного фактора, а особливо використання ізольованого фактора або комбінації декількох факторів, дуже істотно змінює достовірність результату. Таким чином, офлайн, що вимагає лише підпису з автографом, пропонує дуже мало безпеки, оскільки ноу-хау, необхідне для імітації, не дуже важко отримати.

Розглянемо етапи захисту інформації та ідентифікації користувача в договірному праві в цифрову епоху. Надавач послуг, зазвичай задовольняється одностороннім визнанням особи, яке може бути вигаданим. Якщо мова йде про доставку фізичного товару, він може певною мірою покластися на необхідність надати фактичну поштову адресу. Перш за все, у всіх випадках, коли корис-

тувачеві доводиться платити, спосіб оплати, швидше за все, створить зв'язок з його стабільною особистістю. Однак ми побачимо, що цей зв'язок є хитким: оплата ціни могла бути запропонована користувачеві третьою стороною, яка надасть свої платіжні дані, але, строго кажучи, не буде контрагентом. Перш за все, платіжні дані могли бути викрадені. Таким чином, ідентичність погано розкривається тим, як працює електронна комерція [5, с. 345].

Нарешті, слід пам'ятати, що більшість безкоштовних сервісів в мережі не встановлюють ніякого серйозного зв'язку між передбачуваною особистістю і реальною стабільною особистістю інтернет-користувача. Верифікуються лише облікові записи, прив'язані до установ або організацій, за допомогою «офлайнових» процесів: вони позначаються маленькою білою галочкою на синьому тлі. Інші вільно дозволяють використовувати псевдоніми, але також становлять ризик узурпації особистості іншої особи [6].

Щодо кримінального захисту цифрової ідентичності, слід зазначити, що крадіжка особистих даних часто супроводжується іншим правопорушенням: у першому випадку – наклепом; у другому – впровадження в автоматизовану систему обробки даних. Що стосується крадіжки цифрової ідентифікації, яка мала б на меті, наприклад, взяти під контроль банківський інтерфейс з метою здійснення переказу на нього, то це буде відповідно Кримінального кодексу України визначено як шахрайство [7, с. 83].

Чи буде електронне посвідчення особи найкращим доказом? Юридична практика вважає, що так. У такому контексті, деякі країни впроваджують рішення, які повинні забезпечувати як високий рівень надійності, так і дуже широкий спектр використання в Інтернеті. Особливо це стосується електронних посвідчень особи, які були впроваджені в таких країнах, як Бельгія, Іспанія, Португалія, Італія, Швеція, Фінляндія, Естонія, Литва та Монако [8]. Щодо бельгійського посвідчення особи, який можна використовувати як «офлайн», так і «онлайн». Громадяни Бельгії, наприклад, вставляють цю картку в зчитувач, підключений до комп'ютера, щоб отримати доступ до свого податкового місця в Інтернеті або до своєї медичної картки [9, с. 109]. Держава відіграє роль органу сертифікації та надає третім особам, які мають справу з громадянином Бельгії в мережі, надійні докази його особи завдяки шифруванню. Ці сертифікати також можна використовувати для накладення електронного підпису на документ.

Звичайно, недостатньо просто вставити карту в зчитувач, щоб користуватися нею. Потрібен другий фактор аутентифікації, щоб вкрадена картка не могла бути використана. Влада Бельгії обрала PIN-код з максимальною довжиною 16 цифр, при цьому картка блокується, якщо поспіль вводяться три неправильні коди. Система протидії в разі втрати або крадіжки доповнює систему, за загальною моделлю, яку ми зрозуміємо, змодельована на банківських картах. Вибір PIN-коду здається розумним, в той час, коли біометрична аутентифікація, і зокрема за відбитком пальця, розвивається швидкими темпами, особливо для розблокування смартфонів. Аналогічним чином, рішення бельгійської влади зберігати конфіденційну інформацію на кожній картці, яка розглядається окремо, замість того, щоб створювати централізовану базу даних, яка б запитувалася дистанційно щоразу, коли громадянин просить ідентифікувати його, має бути схвалено. Дійсно, така база даних була б головною мішенню для хакерів.

Користувачі смартфонів зараз звикли до все більш досконалої системи «дозволів». Це дозволяє їм надавати або забороняти доступ до певної програми до своєї контактної книги, геолокації тощо. Ідея надання онлайн-співрозмовникам чіткого і більш-менш глибокого доступу до шарів стабільної ідентичності є привабливою. Звичайно, технічних викликів, які потрібно вирішити, не бракує. Наприклад, громадяни повинні мати можливість перевірити, що програмне забезпечення, яке отримує доступ до ідентифікаційної інформації та передає її, діє відповідно до того, що воно заявляє. Це, зокрема, означає, що його вихідний код має бути публічним, щоб його могли оцінити члени громадянського суспільства з необхідними навичками. Якщо припустити, що ці виклики будуть подолані, результат відкриє величезні можливості для регулювання.

Висновки. Розглядаючи взаємозв'язок між цифровими технологіями і системами ідентичності, припускаємо, що нові технології дозволяють агломерувати навколо стабільної ідентичності інформацію, яка взята ізольовано та є менш ідентифікованою. Процес коректної ідентифікації особи в сучасному цифровому світі, як учасника цивільних правовідносин є принциповою, так як стрімкий розвиток сучасних цифрових технологій потребує розуміння поняття цифрової ідентичності для вироблення концепції захисту персональних даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Judith Rochfeld. Le patrimoine affecté de l'EIRL. URL: https://theses.fr/2015MONTD008 (дата звернення: 10.05.2024).
2. Arrêt I-3 U 196/10 du 3 août 201. URL: http://www.justiz.nrw.de. (дата звернення: 18.05.2024).
3. CEDH, 16 June 2015, Delfi AS c. Estonia, 64569/09. URL: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22002-10776%22] (дата звернення: 18.05.2024).
4. Хижняк Є.С. (2017). Ідентифікація особистості злочинця за віртуальними слідами в мережі інтернет. *Підприємство, господарство і право*, № 11, С. 217–221.
5. Одарченко А.М., Сподар К.В. (2015). Особливості електронної комерції та перспективи її розвитку в Україні. *Бізнес Інформ*, № 1, С. 342–346.
6. Smith A.D. Nationalism and modernism. A critical survey of recent theories of nations and nationalism. A.D. Smith. New York; London; Routledge, 1998. P. 30.
7. Бишевець О.В., Романенко Т.В. (2016). Особа злочинця як елемент криміналістичної характеристики шахрайств, що вчиняються в мережі Інтернет. *Вісник кримінального судочинства*, № 1, С. 81–87.
8. У яких країнах є практика використання КЕП на ID? URL: https://dmsu.gov.ua/faq/u-yakix-krajnax-e-praktika-vikoristannya-kep-na-id.html (дата звернення: 27.05.2024).
9. Потій О.В., Брошеван Є.В. (2015). Методи формування унікального електронного ідентифікатора і процес видачі електронних посвідчень: досвід Євросоюзу. *Прикладная радиоэлектроника*. 370 с.