

ВІРТУАЛЬНА ІДЕНТИЧНІСТЬ ТА ВІРТУАЛЬНА КОНФІДЕНЦІЙНІСТЬ ЯК ОСОБИСТЕ НЕМАЙНОВЕ ПРАВО

Булеца С.Б.,
докторка юридичних наук,
професорка, завідувачка кафедри
цивільного права та процесу
ДВНЗ «Ужгородський національний університет»
ORCID: 0000-0001-9216-0033

Булеца С.Б. Віртуальна ідентичність та віртуальна конфіденційність як особисте немайнове право.

Використовуючи Інтернет, люди створюють віртуальні особи, аватари, які відрізняються від свого реального життя. На сьогоднішній день багато людей вважають захист своєї віртуальної ідентичності цінним і гідним. Метавсесвіт змінює те, як ми сприймаємо все навколо нас і всередині нас. Це дозволяє створити нову, безпечну та надійну віртуальну ідентичність, яка є показовою для буденної ідентичності в реальному житті. Цей феномен відкриває нові можливості для самовираження та взаємодії з іншими людьми через Інтернет. Особи змінюють, використовують, припиняють свою віртуальну ідентичність із застосуванням віртуальної ідентифікації в буденному житті, тобто створення будь-якого аватара особою призводить до виникнення віртуальної ідентичності, отже, і захист віртуальної ідентичності має бути аналогічний як захист буденної ідентичності від зловживання, втрати, перевищення повноважень тощо. Такий захист може включати в себе застосування паролів, двофакторної аутентифікації та шифрування даних для запобігання несанкціонованому доступу до віртуальної ідентичності. Крім того, особлива увага повинна бути приділена збереженню конфіденційності особистої інформації при користуванні онлайн сервісами.

Якщо порівняти віртуальну спільноту з реальною спільнотою, віртуальне тіло з реальним тілом, віртуальні права на конфіденційність, свободу мови, справедливий суд і власність вони однакові, ми їх використовуємо так само у віртуальному світі як і в буденному, а хтось вже навіть більше, наприклад, віртуальні держави можуть вводити віртуальні податки та штрафи, обмежити свободу злочинних аватарів чи навіть скасувати смертну кару. Таким чином, віртуальний світ поступово наближається до реального у плані законодавства та правопорядку, викликаючи нові виклики і питання щодо цифрового суспільства. Це показує, наскільки важливо розуміти та регулювати цей аспект життя у сучасному світі.

Враховуючи всі вищезазначені моменти, ми стверджуємо, що право на віртуальну ідентичність та право на віртуальну конфіденційність нерозривно пов'язані з немайновими правами людини і можуть бути класифіковані як особисті немайнові права фізичної особи. Тому дуже важливо оцінювати ці фактори з точки зору захисту персональних даних та інтересів користувачів в Інтернеті. Це сприяє захисту прав людини в цифровій сфері. Право на віртуальну ідентичність є важливим елементом сучасного цифрового ландшафту, який потребує посиленого регулювання та захисту. Впровадження чітких норм і законів щодо використання та захисту віртуальних ідентичностей може посилити кібербезпеку та конфіденційність користувачів. Підсумовуючи, право на віртуальне приватне життя означає, що особи мають право захищати свої персональні дані та конфіденційність в Інтернеті. Це означає, що їхні дані не можуть бути використані без їхньої згоди або обізнаності. Це має вирішальне значення для захисту конфіденційності та безпеки користувачів у цифровій сфері. Це також сприяє зміцненню довіри між користувачами та інтернет-провайдером. Захист персональних даних є фундаментальним компонентом цифрової конфіденційності, що дозволяє користувачам відчувати себе в безпеці під час навігації в Інтернеті. Право на недоторканність приватного життя сприяє інноваціям і стимулює економічне зростання в цифровій сфері.

Отже, права на віртуальну ідентичність і віртуальну конфіденційність нерозривно пов'язані з немайновими правами людини, зокрема з правом на недоторканність приватного життя і свободу вираження поглядів. Ці права забезпечують особисту свободу і захищають персональні дані в цифровій сфері. Захист цих прав має вирішальне значення для збереження особистої автономії та захисту від потенційних порушень приватності в цифровій сфері. У сучасному цифровому ландшафті віртуальна ідентичність і конфіденційність набувають все більшого значення, оскільки особиста інформація стає все більш доступною і вразливою до загроз. Швидкий розвиток цифрових техно-

логій вимагає захисту персональних даних у цифровому просторі. Люди повинні керувати своєю віртуальною ідентичністю, щоб зберегти приватність і безпеку в цифровій сфері.

Ключові слова: віртуальна ідентичність, віртуальна конфіденційність, віртуальна реальність, особисті немайнові права особи, персональна дані, захист, порушення.

Buletsa S.B. Virtual identity and virtual confidentiality as a personal non-property right.

When using the Internet, people create virtual identities, avatars that differ from their real lives. Today, many people consider protecting their virtual identities valuable and worthy. The metaverse is changing the way we perceive everything around us and within us. It allows us to create a new, safe, and reliable virtual identity that indicates our everyday identity in real life. This phenomenon opens up new opportunities for self-expression and interaction with other people via the Internet. Individuals change, use, and terminate their virtual identities using virtual identification in everyday life, i.e. the creation of any avatar by a person leads to the emergence of a virtual identity, and therefore, the protection of virtual identity should be similar to the protection of everyday identity from abuse, loss, abuse of authority, etc. Such protection may include the use of passwords, two-factor authentication, and data encryption to prevent unauthorized access to the virtual identity. In addition, special attention should be paid to maintaining the confidentiality of personal information when using online services.

Let's compare a virtual community with a real community, a virtual body with a real body, and virtual rights to privacy, freedom of speech, fair trial, and property. They are the same; we use them in the virtual world as much as in the real world, and some of us use them even more; for example, virtual states can impose virtual taxes and fines, restrict the freedom of criminal avatars, or even abolish the death penalty. Thus, the virtual world is gradually approaching the real world regarding legislation and law and order, raising new challenges and questions about the digital society. This shows the importance of understanding and regulating this aspect of life in the modern world.

Considering all the above-mentioned points, we argue that the right to virtual identity and the right to virtual privacy is inextricably linked to non-property human rights and can be classified as the personal non-property rights of an individual. Therefore, it is very important to evaluate these factors from the perspective of protecting personal data and users' interests on the Internet. This contributes to the protection of human rights in the digital sphere. The right to virtual identity is an important element of the modern digital landscape that requires enhanced regulation and protection. Introducing clear rules and laws on the use and protection of virtual identities can enhance cybersecurity and user privacy. In summary, the right to virtual privacy means that individuals have the right to protect their personal data and privacy online. Their data cannot be used without their consent or knowledge. This is crucial to protecting the privacy and security of users in the digital sphere. It also helps to build trust between users and internet service providers. Protecting personal data is a fundamental component of digital privacy, allowing users to feel secure when navigating the Internet. The right to privacy fosters innovation and stimulates economic growth in the digital sphere.

Therefore, the rights to virtual identity and privacy are inextricably linked to non-property human rights, particularly the right to privacy and freedom of expression. These rights ensure personal freedom and protect personal data in the digital sphere. Protecting these rights is crucial to preserving personal autonomy and protecting against potential privacy violations in the digital sphere. In today's digital landscape, virtual identity and privacy are becoming increasingly crucial as personal information becomes more accessible and vulnerable to threats. The rapid development of digital technologies requires protecting personal data in the digital space. People need to manage their virtual identity to maintain privacy and security in the digital sphere.

Key words: virtual identity, virtual privacy, virtual reality, personal non-property rights, personal data, protection, violation.

Постановка проблеми. Світ змінюється швидко. Розвиток особистості, який є незалежним і безперешкодним, є життєво важливим для ефективної демократичної держави, оскільки він вимагає незалежного та критичного розуміння особистих немайнових прав. Захист права на приватність людини має бути головним обов'язком демократичної держави. У сучасному світі Інтернет все більше залежить від людей, щоб бути ідентифікованими, не тільки для пошуку інформації, форумів і сайтів соціальних мереж, але й для захисту конфіденційності. Відносини, пов'язані із використанням мережі Інтернет (ІТ-відносини) визначають як *суспільні відносини, пов'язані з використанням учасниками (користувачами) телекомунікаційних і комп'ютерних технологій та інтернет-серверів, об'єднаних мережею Інтернет, що дозволяє задовольнити їх різноманітні інтереси й потреби* [1, с. 38]. Використовуючи Інтернет, люди створюють віртуальні особи, аватари, які відрізняються від свого реального життя. На сьогоднішній день багато людей вважають захист своєї віртуальної

ідентичності цінним і гідним. Зазначають, що Метавсесвіт змінює те, як ми сприймаємо все навколо нас і всередині нас. Це дозволяє створити нову, безпечну та надійну віртуальну ідентичність, яка є показовою для буденної ідентичності [2].

Мета дослідження. Метою даної статті є віртуальна ідентичність та віртуальна конфіденційність як особисте немайнове право.

Все більше і більше науковців піднімає важливі для нашого суспільства питання врегулювання особистих немайнових прав, які виникають в цифровому середовищі, та виявлення можливості захисту даних прав. Серед них можемо виділити: Бааджі, А. Долінська, А. Сліпченко, С. Сліпченко, Є. Харитонов, Р. Майданник, К. Некіт, В. Токарева та інші.

Виклад основного матеріалу. В цивільному кодексі України не передбачено права на віртуальну ідентичність та віртуальну конфіденційність. Слід розмежовувати, ідентичність на 2 види: буденну та віртуальну. Буденна ідентичність доводить наше існування в офлайн-світі. Вона включає в себе картку соціального страхування, водійські права, свідоцтво про народження, паспорт та всі фізичні нагадування про те, ким ми є у буденному нашому житті. Буденна ідентичність контролюється центральними органами державної влади, які діють як регулятори нашої інформації.

Наша віртуальна особистість є частиною інтерфейсу, який представляє користувача у віртуальному світі, в такому як чат, відеогра або віртуальний загальний простір. Віртуальні ідентичності, або онлайн-ідентичності, – це соціальні ідентичності, які приймають або представляють особи в комп'ютерно-опосередкованому спілкуванні та віртуальних спільнотах. Зазвичай вони включають текстові описи себе та аватари, які є графічно реалізованими персонажами, якими користувачі можуть керувати у грі.

Віртуальна ідентичність має бути ідентифікована певним чином, і це є віртуальною ідентифікацією – це представлення особистості у віртуальному середовищі, що складається з властивостей об'єктів, які дозволяють відрізнити ці об'єкти один від одного. Вона може існувати незалежно від контролю людини і може взаємодіяти автономно в електронній системі. Оскільки Інтернет-віртуальні ідентичності (VID) крок за кроком влітаються в (транзакції) осіб, але нехтуються в праві осіб і власності. Більшість людей не усвідомлюють, що вони використовують VID, коли заходять на ринок (наприклад, eBay, Amazon), чат або сайт знайомств. Вони сприймають як належне, що їх представляє штучна особистість. Враховуючи поширене використання веб-сайтів для проведення аукціонів і транзакцій, іноді негативна реакція громадськості на віртуальні форми не пропорційна щоденному зростанню кількості облікових записів, які використовують віртуальні особи для соціальних і комерційних транзакцій [3, с. 79]. Таким чином, особи мають, використовують, припиняють свою віртуальну ідентичність із застосуванням віртуальної ідентифікації в буденному житті, тобто створення будь-якого аватара особою призводить до виникнення віртуальної ідентичності, отже, і захист віртуальної ідентичності має бути аналогічний як захист буденної ідентичності від зловживання, втрати, перевищення повноважень тощо. Наприклад, цікавим є приклад Раміреса. У лютому 2012 року Рамірес подав до суду на TransUnion і заявив про три порушення Закону про справедливую кредитну звітність. По-перше, він стверджував, що TransUnion, використовуючи продукт Name Screen, не дотримувався розумних процедур для забезпечення точності інформації в його кредитній справі. По-друге, він стверджував, що TransUnion не надала йому всю інформацію з його кредитної справи на його запит. Зокрема, перше розсилання TransUnion не включало той факт, що ім'я Раміреса потенційно збігається з іменем у списку OFAC¹. По-третє, Рамірез стверджував, що компанія TransUnion порушила свій обов'язок надавати йому стислий опис його прав «під час кожного письмового розкриття інформації», оскільки друга розсилка TransUnion не містила короткого викладу прав Раміреса. Рамірес вимагав відшкодування збитків, передбачених законом і штрафних санкцій. У червні 2021 року Верховний суд США виніс рішення у справі TransUnion v. Рамірез, що позивачі, які постраждали від втрати особи, повинні довести «конкретну шкоду», та зазнали конкретної «інформаційної шкоди» через порушення форматування TransUnion [4]. Отже, у справі Рамірез Верховний суд США підтвердив, що завдяки цифровізації інформації особа може зазнати інформаційної шкоди та повинна отримати компенсацію. Держави не повинні використовувати інформацію, зібрану для цифрової ідентифікації, для будь-яких інших цілей, окрім тих, про які люди були поінформовані та з якими погодилися. Зокрема, держави не повинні перетворювати платформи цифрової ідентифікації на інструменти для цифрового стеження.

Віртуальні медіа-світи, такі як віртуальні спільноти та світи онлайн-ігор, також контролюються відповідними органами, такими як модератори, спеціалісти з одноліткових груп, суверени, такі як

¹ Управління з контролю за іноземними активами (OFAC) Міністерства фінансів США керує економічними й торговими санкціями та забезпечує їх виконання на основі зовнішньої політики США та цілей національної безпеки проти іноземних країн і режимів, терористів, міжнародних наркоторговців, осіб, які займаються незаконною діяльністю.

адміністратори та провайдери, а також застосовуються санкції, такі як блокування доступу до певної IP-адреси. Визначають три найважливіші теми особистого закону: 1) конфіденційність і анонімність у віртуальному світі; 2) свобода слова та думки у віртуальному світі; і 3) право власності на віртуальну особистість [3, с. 80].

Інформаційні процеси як людей, так і машин можуть бути підтримані та замінені мережами та комп'ютерами без жодних моральних заперечень. Комунікаційні інструменти використовуються як у фізичному, так і у віртуальному світах, а також між ними. Одним із прикладів цього є створення особистих паралельних мереж у обох світах, а також повний гібрид, створений досвідом. Незважаючи на те, що віртуальний світ містить недоліки та нечіткість, з'явилися нові методи встановлення контактів і нові канали зв'язку, такі як SMS. Ці (не)можливості та технічні особливості сучасної комунікаційної мережі, оскільки Інтернет дозволяє людям (анонімно) пересуватися у віртуальному суспільстві, змінюючи свої ідентичності, відносини, транзакції та звички. Завдяки таким технологіям, як Інтернет і мобільна телефонія, з'явилися нові способи спілкування, приховування та розмови, які раніше не були інтегровані в так звані віртуальні світи. Це також відбувається в стосунках один на один всередині та поза групами. Однак технології в цій галузі не досягають необхідної поведінки або функції групових комунікацій. В цьому віртуальному суспільстві розвиваються нові типи анонімності та дисоціації (ймовірно, багаторазових особистостей), що призводить до різноманітних моделей поведінки.

В 2011 році було виявлено, що конфіденційність аватару може бути порушена іншим аватаром, інструментами, такими як літаючі камери та пристрої для підслуховування, а також адміністратором платформи, який має доступ до всієї інформації, створеної та поширеної там. Справжні права на конфіденційність у всьому світі та технології захисту віртуальних платформ можуть не достатньо захистити конфіденційність віртуальної особистості. Таким чином, аватарам слід гарантувати конфіденційність свого фізичного, географічного та інформаційного життя в Інтернеті. Якщо порівняти віртуальну спільноту з реальною спільнотою, віртуальне тіло з реальним тілом, віртуальні права на приватність, свободу мови, справедливий суд і власність вони однакові, ми їх використовуємо так само у віртуальному світі як і в буденному, а хтось вже навіть більше, наприклад, віртуальні держави можуть вводити віртуальні податки та штрафи, обмежити свободу злочинних аватарів чи навіть скасувати смертну кару. Нарешті, аватари повинні мати право голосу та мати окрему судову гілку у віртуальному світі. Виконавчу владу, вважають, слід залишити в руках адміністратора платформи [5, с. 42]. права на ігрове програмне забезпечення не застосовуються до будь-якої віртуальної зовнішності. Крім того, коли гравець створює та використовує віртуальну особу, таку як аватар(и), він також не створює програмне забезпечення, відкрите для авторського права.

Права на публічність намагаються охопити зв'язок між ідентичністю та вираженнями особистості, які перегукуються зі зв'язком між аватаром та особою. Ці права інтелектуальної власності є застарілими та абсолютно чужими тому, що відбувається сьогодні у віртуальному світі та міжмедійному середовищі [3, с. 81]. Цю ідентичність слід захищати в комплексі з іншими соціальними відносинами, які створюють людину як природну, духовну, цифрову та соціальну структуру. Необхідно радикально захистити цифрову особистість людини від зловживань владою, штучного інтелекту, радикального секуляризму тощо [6, с. 103].

Вважається, що найкращою програмою, яка може вирішити цю проблему, є Metadium, екосистема ідентичності нового покоління на базі блокчейн-платформи публічних ідентифікаторів. Це пов'язано з тим, що наша особистість – це суміш онлайн-і офлайн-інформації, якою володіють різні центральні органи державної влади, і ця інформація вразлива до таких атак, як маніпуляція та крадіжка. У цій екосистемі кожен має можливість контролювати свою індивідуальну та особисту інформацію. Metadium створює екосистему, щоб досягти цієї мети. Ця екосистема складається з трьох рівнів: платформи, протоколу та сервісу. Основним компонентом проекту Metadium є блокчейн-платформа Metadium Public ID. Загальнодоступний блокчейн означає, що кожен може брати участь і ділитися даними в мережі. Metadium є «блокчейном ID», що відрізняє його від інших платформ, таких як Bitcoin та Ethereum. У блокчейні ідентифікаторів користувачі особистої інформації можуть безпосередньо створювати, керувати та керувати своїми даними. Блокчейн також зберігає всі записи про те, як використовувалися ці дані. Для побудови екосистеми Metadium ця платформа є основою, на якій будуть побудовані інші системи. Протокол – це набір правил, за допомогою яких ваш комп'ютер може зв'язуватися з іншими комп'ютерами або Інтернетом. Нарешті, сервіс забезпечує підтримку послуги командою Metadium [7]. Насамкінець, сервіс це підтримка послуги командою метадіум.

Перевизначення ідентичності вирішує два завдання. По-перше, це об'єднання різних елементів в рамках однієї незалежної, геополітично незв'язаної організації. По-друге, через децентралізацію, яку забезпечує блокчейн, контроль над ідентичністю повертається до окремих людей. Метадіум

вирішив цю проблему, створивши систему ідентифікації, яка об'єднує всі елементи особистості в один мета-ідентифікатор, який контролює користувач, а не центральний орган. Система також захищена децентралізованою інфраструктурою відкритих ключів [8].

Таким чином, національні закони, що регулюють програми цифрової ідентифікації, повинні чітко визначати їх сферу застосування та гарантії щодо зберігання, використання, знищення та доступу третіх сторін, а також захисту від свавілля та зловживань.

Два основні аспекти особливо актуальні для постачальників цифрової ідентифікації. По-перше, визначення персональних даних у Положенні про загальний захист даних – GDPR охоплює «будь-яку інформацію, що стосується ідентифікованої або ідентифікованої фізичної особи» (стаття 4-1 GDPR). По-друге, GDPR висуває перелік ключових вимог, які включають принципи законності, справедливості, прозорості, обмеження цілей, мінімізації даних, точності, обмеження зберігання, цілісності даних і конфіденційності (стаття 5 GDPR). Постачальники цифрової ідентифікації повинні розглядати ці вимоги як частину розробки технічних та організаційних заходів (стаття 25 GDPR). Розроблена конфіденційність і розроблений захист даних (стаття 25-1 GDPR) можуть допомогти уникнути поширених порушень конфіденційності та даних. Таким чином, постачальники цифрової ідентифікації можуть сприяти впровадженню найкращих практик у питаннях захисту даних, де б вони не працювали [9]. Це новий спосіб підходу до ідентичності, який дозволяє нам продовжувати розвиватися як суспільство, зберігаючи права та безпеку.

Збір і обмін особистими даними з третіми особами є важливою частиною бізнес-моделі деяких компаній. Зазвичай це соціальні мережі, пошукові системи, постачальники послуг електронної пошти та програмне забезпечення провайдерів. Компанії можуть отримати доступ до даних, які вони збирають, якщо вона активно ділиться з ними у своєму загальнодоступному профілі. Крім того, за допомогою цих даних вони можуть відстежувати електронні листи, календар, пошуки, розташування, повідомлення, сторінки та групи, які цікавлять особу, на основі ваших інтересів і переваг. Після цього вони заробляють гроші на вашу віртуальну особистість для цільової реклами. Відповідно до Положення про загальний захист даних [10] 2016 року, коли обробка персональних даних ґрунтується на згоді особи, згода особи повинна бути викладена в обґрунтованому рішенні та продемонстрована позитивними діями. Платформи питають згоду особи на обробку додаткових ваших персональних даних, яких не потрібно для надання послуги. Ця згода має бути надана без обмежень, тобто не пов'язана з наданням послуги. У будь-якому випадку особа має право в будь-який час відкликати свою згоду [11].

У епоху цифрових технологій нові технології все більше сприяють ідентифікації особи. Фактори життя, включаючи дату та місце народження, походження, етнічну приналежність, національність та біологічні особливості, такі як колір очей і волосся, все ще широко використовуються. Однак біометричні дані, такі як відбитки пальців і сканування райдужної оболонки ока, займають важливе місце в верифікації особи та ідентифікації. Наприклад, біометричні паспорти стали стандартним інструментом для багатьох держав [12, с. 134]. Іншим прикладом є індійська програма Aadhaar, яка використовує біометричні технології для запису відбитків пальців і сканування райдужної оболонки ока на додаток до особистої інформації, такої як ім'я, дата народження та місце проживання, перевірка осіб за допомогою їхньої ідентифікаційної картки Aadhaar, що містить 12-значний унікальний ідентифікаційний номер, прив'язаний до відбитків пальців особи, сканування обличчя та очей і виданий урядом Індії, є одним із способів підтвердити особу особи та відфільтрувати підроблені щоб мінімізувати ризик шахрайства особи. Перевірка картки Aadhaar проводиться як частина процесу KYC, щоб запобігти ризикам шахрайства з ідентифікаційною інформацією та відфільтрувати дублікати, підробки [13]. Перевірка Aadhaar зазвичай проводиться в різних секторах, зокрема в банківській справі, телекомунікаціях, державних послугах, електронній комерції, логістиці.

У рішеннях Європейського Суду дані про народження та залишення особи, включаючи інформацію, необхідну для відкриття правди про важливий аспект особистості (Гаскін проти Великобританії, 1989, § 39; Мікулич проти Хорватії, 2002, §§ 54–64; Одівре проти Франції, 2003, §§ 28–29) [14].

Біометрична технологія також використовується для прикордонного контролю та управління міграцією в Європейському Союзі (Регламент Eurodac – це база даних відбитків пальців ЄС про надання притулку. Він містить відбитки пальців усіх прохачів притулку з кожної держави-члена та відбитки осіб, які отримали дозвіл на незаконний перетин кордону).

Наприклад, для цифрової ідентифікації блокчейн використовує технологію децентралізованої розподіленої книги, постачальники цифрової ідентифікації можуть отримати перевагу від того, що дані не зберігаються в одній центральній базі даних. Тим не менш, дані шифруються та зберігаються в різних блоках ланцюга, що ускладнює видалення або підробку даних. Але це також означає, що неможливо легко видалити будь-яку особисту інформацію, яка безпосередньо зберігається в

ланцюжку, що створює проблеми з безпекою даних. Подібним чином, блокчейн також стикається з проблемами безпеки; хакери можуть вкрати або втратити закриті ключі. Тим не менш, прихильники блокчейну стверджують, що технологія може допомогти створити автономну суверенну ідентичність – або цифрову ідентичність, яку може мати та контролювати користувач. Завдяки цій цифровій ідентичності користувач може вирішувати, з ким і коли ділитися даними в своєму «цифровому гаманці».

Більшість міжнародних організацій, у тому числі Світовий банк, відіграють важливу роль у просуванні та допомозі державам у впровадженні рішень цифрової ідентифікації, що охоплюють національне населення та біженців. Верховний комісар ООН у справах біженців (УВКБ ООН) забезпечує реєстрацію біженців за допомогою біометричних даних для підтвердження особи. PRIMES об'єднує всі інструменти цифрової реєстрації УВКБ ООН управління ідентифікацією та справами в одну внутрішню пов'язану та сумісну екосистему [15]. Всесвітня продовольча програма використовує технологію блокчейн для розподілу допомоги [16], а Всесвітній економічний форум підтримує фінансову доступність через технології [17]. Альянс ID2020, державно-приватна ініціатива, також фінансує рішення цифрової ідентифікації на основі блокчейну та біометричних технологій у менш розвинених країнах. З 2016 року ID2020 пропагує етичні підходи до цифрових ідентифікаторів, які захищають конфіденційність, як засіб сприяння справедливому соціальному, політичному та економічному розширенню можливостей і захисту прав людини [18].

Наразі кілька держав запровадили або розглядають рішення цифрової ідентифікації з використанням цих технологій. Окрім Індії, Естонія запровадила модель цифрового громадянства [19]. Австралія та Канада впроваджують рішення цифрової ідентифікації [20]. Гвінея та Кот-д'Івуар очолюють програму цифрової ідентифікації Західної Африки «Унікальна ідентифікація для регіональної інтеграції та залучення» [21].

Державні кампанії цифрової ідентичності можуть реалізувати свої зобов'язання згідно з Міжнародним правом прав людини, захищаючи право кожного на визнання особистості та рівне ставлення перед законом. Такі проекти можуть допомогти вирівнювати суспільну нерівність, надаючи відчуженим особам можливість підтвердити свою особистість і отримати доступ до послуг. Ці особи мають обмежений набір можливостей порівняно з рештою населення світу. Вони не мають можливості робити те, що інші сприймають як належне, наприклад, відкривати банківський рахунок чи записуватися до школи. Технології цифрової ідентифікації можуть полегшити доступ до можливостей і, таким чином, надати людям вибір. Крім того, вони можуть зробити тих осіб без юридичних документів більш помітними і, отже, менш уразливими до зловживань та експлуатації [9].

Наприклад, у звіті iProov Biometric Threat Intelligence Report¹ висвітлюються ключові моделі атак, які спостерігалися протягом 2022 року. Виокремлено три нові тренди, які виникли у 2022 році: 1) різке зростання кількості атак, розпочатих проти мобільного Інтернету, iOS і Android, свідчить про те, що зловмисники просувають атаки на різні платформи; 2) поява та зростання нових атак обміну особами вказує на те, що злочинці з низьким рівнем кваліфікації мають доступ до ресурсів для проведення складних атак; 3) автоматизовані атаки на основі руху, що запускаються одночасно через географічні кластери [22].

Слід зазначити, що нові цифрові платформи ідентифікації можуть захищати права людини лише тоді, коли вони відповідають міжнародним стандартам прав людини, достатньо зменшують ризики дискримінації та підтримують високі стандарти конфіденційності та захисту даних. Такі розрахунки повинні бути включені з самого початку в розробку платформ цифрової ідентифікації. Анна Бедуші зазначає [9], що нові платформи цифрової ідентифікації лише тоді ефективно сприятимуть захисту прав людини, якщо вони відповідатимуть вимогам міжнародного права прав людини, належним чином зменшуватимуть ризики потенційної дискримінації та сприятимуть високим стандартам конфіденційності та захисту даних. Такі міркування мають бути інтегровані в дизайн платформ цифрової ідентифікації з самого початку.

Сенатор Кеннеді запропонував цікавий проект закону про володіння власними даними в Америці, який гарантував би, що кожна людина має право власності на всі дані, які вона створює в Інтернеті, щоб запобігти порушенням права на віртуальну конфіденційність. В проекті закону було визначено, що кожна компанія соціальних мереж повинна:

1) мати помітний і помітний значок, який кожен користувач може натиснути, щоб отримати копію даних користувача з будь-яким аналізом даних користувача, виконаним компанією соціальних мереж;

¹ iProov – єдиний постачальник біометричних засобів перевірки обличчя, здатний аналізувати дані реального світу, щоб визначити ландшафт загроз.

2) мати помітний і помітний значок, який кожен користувач може натиснути, щоб легко експортувати дані користувача з будь-яким аналізом даних користувача, виконаним компанією соціальних мереж;

3) вимагати від кожного користувача під час реєстрації облікового запису свідомо та навмисно укладати ліцензійну угоду – (i) який використовує зрозумілу мову, яку розумна особа із середнім інтелектом може зрозуміти, коли вона вперше читає або чує ліцензійну угоду; (ii) в якому користувач погоджується надати ліцензію на дані користувача компанії соціальних мереж; і (iii) що не перевищує 500 слів із використанням 6 символів у слові; і

4) мати піктограму, яку кожен користувач може натиснути, щоб негайно скасувати ліцензійну угоду [23]. Дійсно, ці вимоги до соціальних компаній спростили б роботу юристів при порушенні права на конфіденційність користувачів.

Слід зазначити, що персональна інформація, якою ми ділимося разом із використанням нашого імені, міститься в імені, яким ми ідентифікуємося як у суспільстві, так і у віртуальному світі. Наприклад, у справі Сполучених Штатів проти Міллера Верховний суд Сполучених Штатів визнав, що транзакції, які люди роблять через банк, належать до ділової документації банку. Як чітко зазначено в законі США Гремма-Ліча-Блайлі про фінансову конфіденційність, участь банку в цих записах не означає, що він має повний контроль над цією інформацією. Крім того, суди поклалися на Міллера, щоб переконатися, що особи, які мають доступ до записів ваших розмов по мобільному телефону та інших ділових записів, можуть отримати доступ до цих записів. Тим не менш, у справі «Карпентер проти Сполучених Штатів» 2018 року суд вимагав дозвіл на дані про місцезнаходження мобільних телефонів, які зберігаються постачальники послуг для використання. Суд визнав, що користувачі телефонів зберігають очікування щодо конфіденційності даних про місцезнаходження, отриманих з їхніх телефонів, незважаючи на те, що рішення Міллера не було скасовано. Пересічні інтереси також стосуються більшої частини іншої інформації, якою ми ділимося під час взаємодії з цифровими службами, такими як електронні покупки, мобільні програми, служби обміну повідомленнями та інші форми комунікації, а також зображення та інформація, якими ми ділимося в наших соціальних мережах. Крім того, все більше особистих даних зберігаються організаціями, яким ми не знайомі як споживачі, оскільки компанії передають обробку даних на аутсорсинг і використовують хмарні служби, а дистанційне зондування в різних середовищах починає розвиватися [24]. Ще в наукових статтях 2006 року зазначали, що Розділ 55 Закону Великобританії про захист даних, який передбачає кримінальну відповідальність за викрадення персональних даних у контролера даних (тобто не суб'єкта даних). Таким чином, інформацію в онлайн-світі розглядали як товар, яким можна торгувати зі знижкою у віртуальному супермаркеті або за іншу вигоду, наприклад, доступ до певної онлайн-послуги [25, с. 276].

Відповідно до міжнародних актів, кожна людина має право на визнання її як особи, на рівне ставлення до неї перед законом без будь-якої форми дискримінації. Однак на практиці рівність порушується, коли особи, які формально мають право на рівне ставлення, через матеріальні причини не можуть отримати доступ до своїх прав через відсутність реєстрації правового статусу особи. Без свідоцтва про народження діти стикаються з додатковими труднощами в доступі до освіти. Біженці без документального підтвердження своєї особи та вік у можуть зіткнутися зі значними проблемами при набутті правового статусу в країні перебування. Таким чином, підтвердити правовий статус особи є непростим завданням для тих, хто не був зареєстрований при народженні, або для тих, хто не має правових документів, втратив документи через воєнні дії в країні проживання. Щоб подолати цю серйозну проблему, Організація Об'єднаних Націй включила до 2030 року ціль сталого розвитку (ЦСР ООН) для всіх у цілях 16.9. Технологія може бути потужним інструментом для досягнення цієї мети [9].

Право на особистість не було всебічно розглянуто в одному рішенні Європейського суду з прав людини, але його різні елементи можна тлумачити на основі комбінації рішень. Перш за все, ми припускаємо, що право на ідентичність захищає такі елементи ідентичності, як ім'я, прізвище, право знати своє походження, стать або етнічну приналежність (Godelli проти Італії, 2013; Мікулич проти Хорватії, 2002; Odièvre проти Франції, 2003). Крім того, варто зазначити, що зміст права на ідентичність постійно розвивається, і таким чином нові елементи людської ідентичності інкорпуються в захист цього права, напр. свобода одягу, сексуальна ідентичність або інтернет-ідентичність.

Деякі елементи ідентифікації є об'єктивними, що дозволяють ідентифікувати конкретну особу (наприклад, ім'я, прізвище, дата народження). Однак більшість інших елементів є суб'єктивними, а це означає, що вони можуть бути сформовані нами самими. Наприклад, в ДІІ – Фізичні та юридичні особи, фізичні особи – підприємці, які звертаються до інформаційно-телекомунікаційних систем суб'єктів взаємодії та проходять електронну ідентифікацію за допомогою системи з використанням

засобів електронної ідентифікації, функціонування яких забезпечується системою, та у визначеному законодавством порядку надали згоду на обробку своїх персональних даних.

Користувачі ICEI можуть отримати доступ до електронних послуг і послуг за допомогою процедур електронної ідентифікації на сайті ID.GOV.UA. Він також взаємодіє та сумісний з інформаційно-телекомунікаційними системами та схемами електронної ідентифікації.

- дотримання законних вимог щодо захисту інформації та персональних даних;
- Розвиток систем електронної ідентифікації (ICEI) у напрямку інтеграції до ІТС для транскордонної електронної ідентифікації;
- Включення ICEI в інформаційно-телекомунікаційні системи суб'єктів взаємодії.

За допомогою Mobile ID – це технологія, яка дозволяє фізичним особам дистанційно ідентифікуватися, автентифікуватися та використовувати електронний підпис у інформаційно-телекомунікаційних системах. Технологія дозволяє передавати дані через SMS і зберігати особисті ключі електронного підпису на SIM-карті. Використання цієї технології можливо на старих мобільних телефонах, які не є смартфонами. Безпека ваших особистих даних є основною перевагою Mobile ID, окрім його зручності та мобільності.

До недавнього часу створення власної ідентичності, що складається з суб'єктивних елементів, відбувалося в реальному світі завдяки тому, як ми представляємо себе іншим людям і як люди навколо нас сприймають нас. Однак наразі можливість створювати власну ідентичність також перемістилася в Інтернет, а тлумачення статті 8 ЄКПЛ є стандартом для інших законів у системі європейського законодавства, яке регулює ці питання [26].

Виділяють найпоширеніші проблеми, які не мають законодавчого регулювання. По-перше, це відсутність єдиних принципів правового регулювання відносин у соціальних мережах. По-друге, немає чітко встановлених принципів захисту та відповідальності за порушення прав інтелектуальної власності в соціальних мережах. По-третє, не вирішено правове регулювання реклами, електронної комерції та використання торгових марок у соціальних мережах. По-четверте, залишаються проблемними питання інформаційної безпеки та захисту персональних даних користувачів соціальних мереж [27, с. 114]. По-п'яте, юридично не врегульовано поняття віртуальної ідентичності та віртуальної конфіденційності. По-шосте, відсутній порядок та способи захисту віртуальної ідентичності та віртуальної конфіденційності в нормативно-правових актах. По сьоме, необхідне правове визначення суб'єктів, об'єкти та зміст права на віртуальну ідентичність та віртуальну конфіденційність.

Враховуючи, що втрата або компрометація нашої онлайн-ідентичності може мати різноманітні наслідки, включаючи фінансові втрати, емоційний стрес і репутаційну шкоду [28, с. 478]. Слід зазначити, що діяльність кіберполіції відіграє важливу роль у захисті особистості в соц мережі в Україні. Наприклад, співробітники Київського управління Департаменту кіберполіції Національна Поліція України спільно зі слідчим управлінням поліції Київської області викрила 40-річного мешканець Київщини, який за гроші продавав персональні дані українців в Інтернеті. Такого роду порушення досить характерні для України. Найбільше стає саме персональних даних користувачів соцмереж вразливий. У зв'язку з цим, аналізуючи одну з найпопулярніших соціальних мереж Facebook, варто відзначити деякі правила, використовуючи які користувач соціальної мережі, може запобігти порушенню своїх прав.

Дослідники відзначають, що для того, щоб знайти надійні засоби захисту в соцмережах, необхідно знати засоби порушення прав осіб у соціальних мережах, у тому числі:

- 1) захоплення пошти для перехоплення пароля від сторінки в соціальній мережі;
- 2) фейкові листи нібито від технічної підтримки, оскільки, відповідаючи на них, користувач розкриває свою особисті дані;
- 3) фішинг, який використовується для створення схожого на оригінальний сайт соціальної мережі, але з іншою адресою у відповідному полі, тому користувач, не звертаючи на це уваги і заповнюючи всі дані своєї сторінки, передає їх на шахраї;
- 4) використання файлів cookie, які сайт передає на комп'ютер користувача під час входу, які зберігаються на комп'ютері користувача, оскільки якщо хакер отримає файл cookie, він зможе читати особисте листування та надсилати повідомлення далі від імені користувача [29, с. 200-201].

Висновки. Таким чином, враховуючи все вищезазначене можемо стверджувати, що право на віртуальну ідентичність та право на віртуальну конфіденційність тісно пов'язані з немайновими правами людини і ми можемо їх віднести до особистих немайнових прав особи. Отже, важливо розглядати ці аспекти у контексті захисту особистих даних та інтересів користувачів в інтернеті. Це сприяє забезпеченню поваги до прав людини в цифровому просторі. Право на віртуальну ідентичність є необхідним аспектом в сучасному цифровому світі, який потребує додаткового регулювання та захисту. Встановлення чітких правил та норм щодо використання та захисту віртуальної

ідентичності може сприяти покращенню кібербезпеки та конфіденційності користувачів. Таким чином, право на віртуальну конфіденційність означає, що користувачі мають право на захист своїх персональних даних та конфіденційності у мережі Інтернет. Це означає, що їхні дані не можуть бути використані без їхнього дозволу або знання. Це важливо для забезпечення приватності та безпеки користувачів у цифровому середовищі. Також, це сприяє побудові довіри між користувачами та провайдерами послуг в Інтернеті. Захист персональних даних є ключовим аспектом віртуальної конфіденційності, оскільки це дозволяє користувачам відчувати себе безпечними під час використання Інтернету. Право на конфіденційність також сприяє розвитку інновацій та стимулює економічний розвиток у цифровому світі.

Отже, право на віртуальну ідентичність та право на віртуальну конфіденційність тісно пов'язані з немайновими правами людини, такими як право на приватне життя та свободу вираження. Ці права гарантують індивідуальну свободу та захист особистих даних у цифровому середовищі. Забезпечення цих прав є важливим для збереження особистої автономії та захисту від можливих порушень приватності в онлайн просторі. Віртуальна ідентичність та конфіденційність стають все більш актуальними у сучасному цифровому світі, де особиста інформація стає все доступнішою та вразливою.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Долінська А.М. Охорона прав користувачів у мережі інтернет. Дисертація на здобуття наукового ступеня доктора філософії з галузі знань право. Хмельницький. 2021. С. 38.
2. Virtual Identity: What is it and its role in the Metaverse? 2022. URL: <https://designhubz.com/virtual-identity-what-is-it-and-its-role-in-the-metaverse/>.
3. J. Van Kokswijk. Legal aspects of virtual identity, *International conference on cyberworlds (CW'07)*. Hannover. Germany. 2007. Pp. 77–82, DOI: 10.1109/CW.2007.66. URL: <https://xyuan.myweb.cs.uwindsor.ca/references/virtualidentity07.pdf>.
4. Supreme Court of the United States Syllabus Transunion Llc V. Ramirez Certiorari to the United States Court Of Appeals For The Ninth Circuit No. 20–297. Argued March 30, 2021—Decided June 25, 2021. URL: https://www.supremecourt.gov/opinions/20pdf/20-297_4g25.pdf.
5. Bart Van Der Sloot. Virtual identity and virtual privacy: towards a concept of regulation by analogy. «Egov Präsenz» 1. 2011. P. 41–43 URL: https://www.ivir.nl/publicaties/download/egov_prasenz_2011_1.pdf.
6. Tuliakov V.O. Virtual identity and echr jurisprudence. Jour. 2019. P. 103 URL: <http://dspace.onua.edu.ua/bitstream/handle/11300/20742/tuliakov%20v.%20o.%20virtual%20identity%20and%20jurisprudence.pdf?sequence=1>.
7. So, What Exactly Is Metadium? 2023. URL: <https://medium.com/metadium/so-what-exactly-is-metadium-af2c47d2c37c>.
8. Mundane vs Virtual Identity – What's the difference? 2018. URL: <https://medium.com/metadium/mundane-vs-virtual-identity-whats-the-difference-c492abf468a6>.
9. Beduschi A. Digital Identity: Contemporary Challenges For Data Protection, Privacy And Non-Discrimination Rights. Big Data & Society. 2019. 6(2). URL: <https://doi.org/10.1177/2053951719855091>.
10. Regulation (Eu) 2016/679 of the European parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC (General Data Protection Regulation). URL: <https://eur-lex.europa.eu/legal-content/en/txt/pdf/?uri=celex:32016r0679>.
11. Take control of your virtual identity. 2019. European commission. URL: https://commission.europa.eu/system/files/2019-10/virtual_identity_en.pdf.
12. John Torpey. *The invention of the passport. surveillance, citizenship and the state*, Cambridge University Press, Cambridge, New York 2000, 211 pages.
13. All you need to know about aadhaar verification API. 2023. URL: <https://authbridge.com/blog/all-you-need-to-know-about-aadhaar-verification-api/>.
14. Guide to the case-law of the of the European Court Of Human Rights. Data Protection. Updated On 31 August 2022. P. 8. URL: https://www.echr.coe.int/documents/d/echr/guide_data_protection_eng
15. Registration and identity management. URL: <https://www.unhcr.org/what-we-do/protect-human-rights/protection/registration-and-identity-management>.
16. Innovation and digital transformation. 2023. URL: <https://www.wfp.org/innovation>.
17. How new technologies create a pathway to financial inclusion. 2022. URL: <https://www.weforum.org/agenda/2022/05/new-technologies-improve-financial-inclusion/>.

18. The need for a good digital ID is universal. 2023. URL: <https://id2020.org/>.
19. Estonia is the world's first country to also function as a digital service. 2023. URL: <https://estonia.ee/enter/>.
20. Katya Pivcevic. Governments in Australia and Canada are investing in digital ID. 2021. URL: <https://www.biometricupdate.com/202102/governments-in-australia-and-canada-investing-in-digital-id>.
21. An individual consultant should be engaged to develop a communication strategy for the West Africa unique Identification for Regional Integration and Inclusion (WURI) Project. 2023. URL: <https://projects.worldbank.org/en/projects-operations/procurement-detail/op00229088>.
22. Iproov Biometric Threat Intelligence Report 2023. URL: <https://www.biometricupdate.com/202305/iproov-biometric-threat-intelligence-report-2023>.
23. A Bill S. 806 (116th): Own your own data Act. March 14, 2019. To prohibit the collection of data or information generated on the Internet. URL: <https://www.govtrack.us/congress/bills/116/s806/text/is>.
24. Cameron F. Kerry, John B. Morris. Why data ownership Is the wrong approach to protecting privacy. 2019. URL: <https://www.brookings.edu/blog/techtank/2019/06/26/why-data-ownership-is-the-wrong-approach-to-protecting-privacy/>.
25. Corien Prins. When personal data, behavior and virtual identities become a commodity: would a property rights approach matter? Volume 3, Issue 4, June 2006. DOI: 10.2966/Scrip.030406.270 P.270-303
26. Michalkiewicz-Kadziela, Ewa And Ewa Milczarek. Legal boundaries of digital identity creation. *Internet Policy Review* 11.1. 2022. Web. 15 Mar. 2023. URL: <https://policyreview.info/articles/analysis/legal-boundaries-digital-identity-creation>
27. Baadzhi N. Legal Nature Of Legal Relations On The Internet. *Journal Of Civil Law*, 2017. 22, P. 112-116.
28. Clare Sullivan. Digital Citizenship And The Right To Digital Identity Under International Law. *Computer Law & Security Review*. Volume 32, Issue 3, June 2016, P. 474-481
29. Pfo O. Protection In Social Networks. Current Issues And Achievements In The Field Of Cybersecurity. 2016. 3. P. 200-201.