

ЦИФРОВА ІДЕНТИЧНІСТЬ

Булеца С.Б.,

*докторка юридичних наук, професорка,
завідувачка кафедри цивільного права та процесу
юридичного факультету
ДВНЗ «Ужгородський національний університет»*

Булеца С.Б. Цифрова ідентичність.

У сучасному житті необхідно мати доступ до Інтернету та зареєструватися на веб-сайтах, щоб виконувати свої права та обов'язки, замовляти послуги, виконувати роботи та купувати товари. Користуватися державними установами, банками, медичними закладами та іншими послугами може бути складніше, якщо у вас немає доступу до Інтернету. Крім того, це може призвести до погіршення комунікації та доступу до інформації. Це змінює уявлення про людину як суб'єкта цивільних правовідносин через Інтернет, який існує як у реальному, так і в віртуальному світах. Таким чином, щоб повноцінно брати участь у житті суспільства, кожен повинен мати доступ до Інтернету. Це підкреслює важливість інфраструктури та кібербезпеки для захисту безпеки та приватності користувачів. «Цифрова ідентичність» з'являється в Інтернеті. Для того, щоб визначити свої віртуальні можливості та обмеження, цифрова ідентичність є життєво важливою для сучасного людського спілкування. Для запобігання загрозам та зловживанням цифрова ідентичність повинна бути безпечною та конфіденційною. Як соціальний феномен, інтернет-ідентичність визначає соціальну презентацію людини як онлайн, так і офлайн. Інтернет починався як інформаційно-пізнавальна платформа, але зараз він перетворився на соціальну та комунікативну платформу завдяки цифровим технологіям. Цифрова ідентичність формується через цифровий контакт і цифрову самопрезентацію. Людину постійно індивідуалізують змінні, пов'язані з інформацією та міжособистісними комунікаціями. Соціальні мережі сприяють особистій самореалізації та створюють враження, що вони залучені до важливих процесів. Це може призвести до посилення впливу цифрової ідентичності на формування особистості, а також вимагає нових стандартів етики соціальних мереж. Незважаючи на те, що в Україні існує багато законопроектів у сфері ІТ, усі вони спрямовані на покращення існуючої системи законодавства, наприклад: законопроект № 2849, який гарантує право людини на доступ до Інтернету; законопроект № 4047, який зобов'язує інтернет-магазини відповідати за неякісні товари; і законопроект № 4049, який забороняє розповсюдження інформації, яка порушує особисті немайнові права людини в Інтернеті. Діяльність людини в Інтернеті, її профілі в соціальних мережах і її рейтинг визначають її цифровий статус. Це може завдати шкоди репутації та можливостям людини в сучасному світі. Світ бореться з гендерно зумовленим кібернасильством, оскільки це загрожує безпеці та благополуччю в Інтернеті. Для вирішення цієї проблеми необхідні громадська обізнаність і профілактика. Незаконне використання персональних даних у соціальних мережах порушує честь, гідність і комерційну репутацію людей. Серед інших порушень у соціальних мережах це порушення моралі, права та етики інтернет-комунікації. Таким чином, ефективне законодавство, правова обізнаність користувачів і підтримка ІТ-сектору необхідні для захисту приватних осіб у соціальних мережах. Ці гарантії, на нашу думку, достатньо захищають користувачів соціальних мереж. Це гарантує безпеку та конфіденційність інформації, яку вносять учасники платформи.

У позасудовому порядку також можна захистити особисті немайнові права в соціальних мережах. Цифровізація означає, що моральна шкода, завдана порушенням права інтелектуальної власності, має бути відшкодована на загальних підставах, за винятком страждань і переживань, подібних до реальних душевних страждань. Переслідування в реальному житті гірше, ніж за допомогою інформаційних технологій. На нашу думку, частина 2 статті 23 Цивільного кодексу України має бути доповнена. Частина 2 – Відшкодування моральної шкоди Моральна шкода включає в себе фізичний біль і страждання, пов'язані з каліцтвом або іншим ушкодженням здоров'я, а також душевні страждання, завдані злочинним діям щодо особи, її сім'ї чи близьких родичів. 3) душевні та фізичні страждання, пов'язані з протиправною поведінкою щодо особи, її сім'ї чи близьких родичів за допомогою інформаційних технологій; 4) душевні страждання, пов'язані з втратою або пошкодженням майна; 5) приниження честі, гідності та ділової репутації особи.

Ключові слова: гендер, сім'я, дитина, рівність, члени родини, цифрова ідентичність, порушення, моральна шкода, права, інтернет, персональні дані.

Buletsa S.B. Digital identity.

In modern life, you need to have access to the Internet and register on websites to exercise your rights and responsibilities, order services, perform work and buy goods. Using government offices, banks, healthcare facilities and other services can be more difficult if you do not have access to the Internet. It can also lead to poorer communication and access to information. This changes the perception of a person as a subject of civil legal relations via the Internet, who exists in both the real and virtual worlds. Thus, to fully participate in society, everyone must have access to the Internet. This underscores the importance of infrastructure and cybersecurity to protect the security and privacy of users. 'Digital identity' is emerging online. In order to define one's virtual capabilities and limitations, digital identity is vital for modern human communication. To prevent threats and abuse, digital identity must be secure and confidential. As a social phenomenon, online identity defines a person's social presentation both online and offline. The Internet started as an information and knowledge platform, but it has now evolved into a social and communication platform thanks to digital technologies. Digital identity is formed through digital contact and digital self-presentation. A person is constantly being individualised by variables related to information and interpersonal communications. Social media facilitates personal fulfilment and gives people the impression that they are involved in important processes. This can lead to an increased influence of digital identity on personality formation and requires new standards of social media ethics. Although there are many draft laws in the IT sector in Ukraine, all of them are aimed at improving the existing legal framework, for example: draft law No. 2849, which guarantees the human right to access the Internet; draft law No. 4047, which obliges online retailers to be responsible for defective goods; and draft law No. 4049, which prohibits the dissemination of information that violates personal non-property rights on the Internet. A person's online activities, social media profiles and ratings determine their digital status. This can harm a person's reputation and opportunities in the modern world. The world is struggling with gender-based cyberviolence as it threatens online safety and well-being. Public awareness and prevention are needed to address this issue. The illegal use of personal data on social media violates the honour, dignity and commercial reputation of people. Among other violations on social media, it is a violation of morality, law and ethics of online communication. Therefore, effective legislation, legal awareness of users and support from the IT sector are essential to protect individuals on social media. These safeguards, in our opinion, sufficiently protect social media users. This guarantees the security and confidentiality of the information entered by platform members.

Personal non-property rights on social media can also be protected out of court. Digitalisation means that non-pecuniary damage caused by infringement of intellectual property rights should be compensated on a general basis, with the exception of suffering and distress similar to real mental anguish. Harassment in real life is worse than through information technology. In our opinion, part 2 of Article 23 of the Civil Code of Ukraine should be supplemented. Part 2 – Compensation for non-pecuniary damage Non-pecuniary damage includes physical pain and suffering associated with injury or other damage to health, as well as mental suffering caused by criminal acts against a person, his or her family or close relatives. 3) mental and physical suffering associated with unlawful behaviour towards a person, his/her family or close relatives through information technology; 4) mental suffering associated with loss or damage to property; 5) humiliation of honour, dignity and business reputation of a person.

Key words: digital identity, breach, non-pecuniary damage, rights, Internet, personal data.

Постановка проблеми. Доступ до Інтернету, реєстрація на сайтах стали невід'ємною складовою сучасного життя, умовою успішної реалізації прав та обов'язків у суспільстві, отримання та замовлення послуг, робіт та придбання товарів. Без доступу до Інтернету може ускладнитися взаємодія з державними органами, банками, медичними установами та іншими сервісами. Також це може призвести до втрати можливості отримання актуальної інформації та спілкування з оточуючим світом. Означене, впливає на трансформацію уявлень про категорію фізична особа як суб'єкта цивільних відносин у мережі Інтернет яка одночасно співіснує у фізичному та у віртуальному світі. Таким чином, важливо забезпечити доступ до Інтернету для всіх громадян, щоб забезпечити їхню повноцінну участь у суспільстві. Це також підкреслює необхідність розвитку інфраструктури та кібербезпеки для забезпечення безпеки та конфіденційності користувачів. У цифровому просторі на перший план виходить «цифрова ідентичність». Цифрова ідентичність стає ключовим елементом взаємодії людини з сучасним світом, визначаючи її можливості та обмеження у віртуальному просторі. Важливою задачею є забезпечення безпеки та конфіденційності цифрової ідентичності для запобігання можливим загрозам та зловживанням.

Метою даної статті є дослідження поняття та захисту цифрової ідентичності і цивільному праві України. Цифрова ідентичність стає все більш актуальною в сучасному світі, де велика кількість

особистих даних зберігається в електронному вигляді. Дослідження цього питання допоможе розробити ефективні заходи для захисту конфіденційності та безпеки цифрової ідентичності громадян.

Питанням цифрової ідентичності займаються наступні науковці: О. Грабовська, М. Стефанчук, В. Токарева, О. Кармаза тощо.

Виклад основного матеріалу. З поширенням ролі інтернет-ідентичності як суспільного явища власна соціальна презентація стає важливою умовою онлайн- і офлайн-життя. На початку свого розвитку мережа Інтернет слугувала, здебільшого, інформаційно-пізнавальною платформою, але з поширенням і доступністю цифрових технологій відбулось трансформування її до соціально-комунікативного простору. Явище цифрової ідентичності здійснюється шляхом міжособистісної комунікації і власної репрезентативності в цифровому середовищі. Індивідуалізація особистості набуває динамічного характеру відповідно до нових змінних, які можуть виникати як в інформаційному полі, так і в межах міжособистісної комунікації. Соціальні мережі виступають тими платформами, які надають користувачу можливість особистісної реалізації і породжують оманливе відчуття причетності до включення в масово значимі процеси [1, с. 68]. Це може призвести до збільшення впливу цифрової ідентичності на формування особистості та спричинити необхідність розробки нових етичних стандартів у використанні соціальних мереж.

Як зазначив Мічурін: «Ступень формальної індивідуалізації у мережі Інтернет може бути різною. Це залежить від мети ідентифікації, наявності відповідних юридичних прав та обов'язків суб'єктів. Індивідуалізація може бути офіційною (формальною). Тоді має вказуватися справжнє ім'я фізичної особи. У інших випадках може зазначатися вигаданий NickName. Засобами індивідуалізації фізичної особи у мережі Інтернет можуть бути її ім'я, псевдонім, зображення, URL веб-сторінки, доменне ім'я, IP-адреса, електронна поштова скринька тощо. Коло засобів індивідуалізації фізичної особи у мережі Інтернет не є вичерпним» [2, с. 94].

Частим порушенням в інтернеті є право на індивідуалізацію, слід погодитися з Стефанчуком Р.О., що цифрова індивідуалізація – це визнання за людиною конкретного, притаманного лише їй цифрового відбитка (скріну), що фактично є сукупністю основних ознак її індивідуалізації як учасника цифрових відносин. При цьому під цифрову індивідуалізацію підпадають і індивідуалізуючі ознаки, притаманні людині як учаснику ординарних правовідносин (ім'я, його замітники, їх зміна, дата народження, місце народження, фіксація актів цивільного стану, рівнів право- та дієздатності, обмежень щодо них, сімейного стану, наявності дітей, інших родичів, родинних зв'язків, смерті тощо), і індивідуалізуючі ознаки, зумовлені її безпосередньою участю у цифрових відносинах (електронна пошта, адреса веб-сайту, доменне ім'я, IP-адреса, електронний підпис, ID-паспорт, Bank ID, кредитна картка, акаунт у соціальних мережах, сканування відбитка пальця, сканування сітківки ока, Face ID, веб-гаманець). Причому окремі способи цифрової індивідуалізації на сьогодні вже активно використовуються, а з інформації щодо такої індивідуалізації формуються відповідні реєстри чи інші бази персональних даних [3, с. 40].

В Україні існує невелика кількість законопроектів у сфері ІТ, можна зробити висновок, що всі вони передусім спрямовані на удосконалення діючої системи законодавства щодо, зокрема: гарантування права на доступ фізичної особи до Інтернету (проект № 2849); встановлення відповідальності Інтернет-магазинів за неналежну якість товарів (проект № 4047); заборони поширення в мережі Інтернет інформації, якою порушуються особисті немайнові права (проект № 4401).

Стефанчук Р.О. зазначив, що слід подумати і про механізм протидії можливим негативним наслідкам від тотальної цифровізації життя людини [3, с.44], тобто повна оцифровізація, яка негативно вплине на людей. Цифровий статус людини – це сукупність її спеціальних цифрових модусів як учасника цифрових правовідносин, якими визначається обсяг і зміст наявних у людини цифрових прав, законних інтересів та обов'язків, особливості їх здійснення чи виконання, захисту й охорони. Зазвичай фіксація цифрового статусу людини може відбуватись у низці електронних реєстрів прав (їх обмежень, обтяжень чи інших особливостей здійснення), правочинів, інших юридичних фактів [3, с. 39]. Як зазначає В. Токарева у цифровому середовищі, фізична особа виступає у відносини у мережі опосередковано через свою проекцію, цифрову ідентичність, зміст якої складає сукупність всієї інформації про особу цифровому просторі, а саме: персональні дані, «цифровий слід», цифрову репутацію, дані про взаємодію із іншими суб'єктами в мережі та інформацію про будь-які вчинювані дії, навіть, якщо вони були видалені із публічного доступу в Інтернеті, тощо [4, с. 38]. Отже, цифровий статус людини визначається її активністю в інтернеті, наявністю профілів у соціальних мережах та репутацією онлайн. Це може впливати на спосіб сприйняття особи та її можливості у сучасному світі.

Весь світ активно бореться з гендерною кібер-насиллю, оскільки це серйозна проблема, що впливає на безпеку та добробут людей у онлайн-середовищі. Необхідно посилювати свідомість громадськості про цю проблему та вживати заходи для її запобігання. Наприклад, 1 січня 1999

року Каліфорнія стала першим штатом у Сполучених Штатах, який запровадив кримінальну відповідальність за кіберпереслідування [5]. Однак досі не було підписано жодних багатосторонніх або регіональних договорів щодо таких типів кіберзлочинності, як кібердомогання та кіберпереслідування. Деякі країни прийняли власні закони, які безпосередньо зачіпають один або кілька видів кіберзлочинів. Наприклад, Закон Пакистану про запобігання електронним злочинам 2007 року [6] та Закон Нігерії про кіберзлочинність 2015 року [7] передбачають кримінальну відповідальність за кіберпереслідування, а Закон Сінгапуру про захист від домагань 2014 року [8] забороняє кібердомогання.

Ситуація в Україні ідентична. Тим не менш, це не означає, що законодавство України не містить жодних правил, які можна використовувати для захисту від кібернасильства. Відповідальність за кіберзлочини визначена Законом України від 15 жовтня 2017 року «Про основні засади забезпечення кібербезпеки України» [9]. У випадку погрози вбивства можна застосувати статтю 129 ККУ. Посилаючись на статтю 161 ККУ, якщо хтось зазнає будь-якого насильства за ознакою статі, гендерної ідентичності, психологічного насильства або погрози заподіяння будь-якої шкоди, він повинен негайно звертатися до поліції. Відповідно до статті 182 ККУ «Про недоторканність приватного життя», сталкінг часто є забороненим. Крім того, закон країни «Про забезпечення рівних прав і можливостей жінок і чоловіків» забороняє дискримінацію за ознакою статі. Цей закон також регулює прояви гендерної дискримінації в Інтернеті. У статті 307 Цивільного кодексу України можна заборонити використання переслідувачем ваших персональних даних, фотографій чи відео без вашого дозволу. Це незаконно використовувати ваші паспортні дані, дані про здоров'я, банківські рахунки та навіть номер телефону. Закон України «Про захист персональних даних» [9] та інші законодавчі акти гарантують захист цих персональних даних. Уповноважена Верховної Ради з прав людини, поліція чи суд – це органи, які відповідають за розповсюдження та захист персональних даних кожного [9].

Крім неправомірного використання персональних даних у соціальних мережах, права на повагу до честі, гідності фізичної особи, також порушується ділова репутація фізичних та юридичних осіб. Серед усіх інших можливих порушень в соціальних мережах, це на перетині порушень етики інтернет-спілкування, моральні норми і правова норма. Тому вирішуємо питання захисту фізичних осіб у соціальних мережах потребує не лише відповідного законодавства, але також має включати правову обізнаність користувачів і достатню підтримку ІТ сфера. На нашу думку, комплекс таких заходів забезпечує належний захист користувачів у соціальних мережах. Такий підхід дозволить забезпечити безпеку та конфіденційність даних учасників цих платформ. Також важливо посилювати контроль за вмістом, що публікується, для запобігання поширенню шкідливої інформації.

Захист немайнових прав у соціальних мережах можливий і без звернення до суду. Наприклад, Стандарти спільноти Facebook передбачають можливість звернення до адміністрації цієї соцмережі мережі зі скаргою на користувача (його обліковий запис), його публікацію або коментар, в якому є загрози громадській чи особистій безпеці, або погрози фізичної шкоди особі, переслідування чи приниження. Матеріали які можуть включати порушення прав осіб і які усуваються адміністрацією у разі скарга включає:

- 1) сторінки, які ображають окремих осіб;
- 2) зображення, відредаговані для приниження окремих осіб;
- 3) фото чи відео із зображенням фізичного насильства, розміщене з метою приниження жертви;
- 4) оприлюднення особистої інформації з метою шантажу чи переслідування;
- 5) постійне переслідування шляхом надсилання небажаних повідомлень або прохань додати в друзі [11].

Однак у Заяві про права та обов'язки у Facebook зазначено, що адміністрація не несе відповідальності за будь-які дії користувача, а також будь-які претензії, підстави позову, суперечки з адміністрацією мережі. Все претензії користувачі повинні звертатися виключно до федерального окружного суду Північного округу Каліфорнії або в суд штату Каліфорнія [12, с. 52].

Науковці стверджують, що чітке та обґрунтоване розмежування між правами на захист даних, конфіденційність та ідентичність є надзвичайно важливими. І це не лише заради узгодженості і дієвості правової системи, але особливо заради досягнення всеохоплюючої та надійного захисту усіх аспектів, пов'язаних з особистістю людини [13, с. 1051].

Висновки. Таким чином, компенсація моральної шкоди при порушенні ОНП в умовах цифровізації має місце, компенсація має відбуватися на загальних підставах, крім винятку, що особа може зазнати тільки психічних страждань та переживань, які нічим не будуть відрізнятися від страждань чи переживань в реальному світі. Переслідування особи за допомогою інформаційних технологій завдає ще більше страждань ніж переслідування в реальному житті. На нашу думку необхідно внести зміни в статтю 23 ч. 2 ЦК України Відшкодування моральної шкоди: ч. 2. Моральна шкода по-

лягає: 1) у фізичному болю та стражданнях, яких фізична особа зазнала у зв'язку з каліцтвом або іншим ушкодженням здоров'я; 2) у душевних стражданнях, яких фізична особа зазнала у зв'язку з протиправною поведінкою щодо неї самої, членів її сім'ї чи близьких родичів; 3) у душевних та психічних стражданнях, яких фізична особа зазнала у зв'язку з протиправною поведінкою щодо неї самої, членів її сім'ї чи близьких родичів за допомогою інформаційних технологій; 4) у душевних стражданнях, яких фізична особа зазнала у зв'язку із знищенням чи пошкодженням її майна; 5) у приниженні честі та гідності фізичної особи, а також ділової репутації фізичної або юридичної особи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Усанова Л.А. Цифрова ідентичність як відображення інформаційного суспільства. Актуальні проблеми філософії та соціології : Науково-практичний журнал / Голов. ред. С.Г. Секундант, відпов. ред. Д.В. Яковлев; Міністерство освіти і науки України; Національний університет «Одеська юридична академія». Одеса, 2021. Вип. 30. С. 67–70.
2. Мічурін Є. Ідентифікація і індивідуалізація фізичної особи у комп'ютерній мережі інтернет: правові аспекти. *Вісник Харківського національного університету імені В.Н. Каразіна. Серія «Право»*, 2022. (34), 91–96. URL: <https://doi.org/10.26565/2075-1834-2022-34-10>.
3. Стефанчук Р.О. Інформаційні технології та право: Quo Vadis? *Право України*, 2018. № 1. С. 30–50.
4. Токарева В.О. Щодо питання цифрової ідентичності у мережі інтернет. *Приватне і публічне право*. 2022. № 4. С. 35–40. URL: http://pp-law.in.ua/archive/4_2022/6.pdf.
5. Penal Code California 1872. URL: https://leginfo.ca.gov/faces/codes_displaySection.xhtml?sectionNum=646.9&lawCode=PEN.
6. BILL lo mqkr proviions for prevenlion of eletronic crimes. URL: https://www.na.gov.pk/uploads/documents/1470910659_707.pdf.
7. Cybercrimes (Prohibition, Prevention, Etc) Act, 2015. URL: <https://www.nfiu.gov.ng/images/Downloads/downloads/cybercrime.pdf>.
8. Protection from Harassment Act 2014. URL: <https://sso.agc.gov.sg/Act/PHA2014>.
9. Про основні засади забезпечення кібербезпеки України: закон України від 28.06.2024, підстава – 3783-IX URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>.
10. Про захист персональних даних. Закон України. *Відомості Верховної Ради України (ВВР)*, 2010, № 34, ст. 481.
11. Facebook. Community Standards. [online]. (2020). URL: https://www.facebook.com/communitystandards/recentupdates/violence_criminal_behavior.
12. Milash V. Legal aspects of the emergence and implementation of contractual relations on the Internet. Legal regulation of relations on the Internet. Kharkiv: "Law", 2016, p. 52–91.
13. Mark A. Lemley & Eugene Volokh. Law, Virtual Reality, And Augmented Reality. *University Of Pennsylvania. Law Review*. Vol. 166. April 2018. No. 5. Pp. 1051–1138.