УДК 342.378
DOI https://doi.org/10.32782/app.v73.2024.23

Н. В. Гавриленко
orcid.org/0000-0002-2043-3917
кандидат економічних наук, доцент,
доцент кафедри економіки, обліку та підприємництва
Національного університету кораблебудування імені адмірала Макарова

ПРАВОВІ ЗАСАДИ ЦИФРОВОЇ ІДЕНТИФІКАЦІЇ І РЕПРЕЗЕНТАЦІЇ ОСОБИСТОСТІ

Сучасні дослідники культури електронних носіїв інформації відмічають певний профіцит спілкування, який виник завдячуючи цифровим і електронним медіа і породжує парадоксальним чином девальвацію близькості. Тисячі друзів в Instagram і Facebook надають відчуття перебування практично в постійному потоці спілкування, але при цьому у людей не формуються прихильності та втрачається істинна близькість. Цифровий простір, віртуальна реальність, мережева свідомість, мережева комунікація створюють нове проблемне поле для вивчення феномену ідентичності особистості в умовах цифрового суспільства (Magopets, 2022; Polishchuk, 2022; Гавриленко, 2022, 2023). В праві, філософії, економіці, культурології, психології, соціології розглядаються різні аспекти ідентичності в контексті усвідомлення особою її належності до тієї або іншої соціальної групи, професійної культури; проживання в ході життєвого циклу різних его-станів: асиміляції особистісного та соціального досвіду; підтримка особистістю своєї цілісності та суб'єктності в постійно мінливому світі.

Стрімко увірвавшись в повсякденне життя загальної більшості людей технології 4 промислової революції почали висвічувати нові ракурси проблеми формування ідентичності особистості, які з точки зору науки є зовсім не вивченими, тим паче, вони вже стали повсякденною реальністю кожної людини, полем для практичних експериментів.

В зв'язку з цим, дане дослідження являє собою спробу постановки проблемних питань, які в умовах сьогодення необхідно вирішувати не лише на рівні фундаментальних гуманітарних досліджень, але й в сфері права, державного управління, фінансів, економіки, освіти, технологій, оскільки цифрова ідентичність нині здійснює неабиякий вплив на життя людини.

В процесі проведення дослідження, на основі аналізу наявних підходів щодо формування цифрової ідентичності, виявлення деякі проблеми, що характеризують відповідні процеси цифровізації суспільства. Відразу слід зазначити, що донині поняття «цифрова ідентичність» не визначене і щоб його сформулювати, необхідно ретельне дослідження сутності цього рідкісного, незвичайного явища.

В умовах цифровізації майже всіх сфер життєдіяльності в Україні, яка припускає повсюдне використання big data, як і в усьому світі гостро постала проблема контролю над формуванням цифрової ідентичності громадянина. Україна стала однією з перших в світі країн, яка запровадила електронні паспорти. Застосунок «Дія» дозволяє перевірити та завантажити копії цілої низки документів, які посвідчують особу. Наразі продовжується курс на цифровізацію повсякденного життя, що стало особливо відчутним у часи пандемії і зараз – під час війни. Життя людей майже повністю перейшло в онлайн, всі ми збільшили свою присутність в інтернеті, а одночасно з тим – збільшилася й кількість інформації, яку ми там залишаємо. Проте ми не знаємо, хто має доступ до неї, хто її збирає і яким чином використовує.

Як офіційно заявив офіс Уповноваженого Верховної ради України з прав людини – виявив в інтернеті, на одному з сайтів базу даних, що може містити персональні дані майже жителів України, яка вміщувалася майже в 53 мільйони записів. Тобто, як висновок, цифровий світ створює людству не лише можливості для кожного, але й забагато ризиків.

Що ж таке цифрова ідентичність з юридичної точки зору спробуємо наразі розібратися. Для початку варто з'ясувати, що вмішує в собі поняття «цифрової ідентичності», з чого вона побудована і що саме варто розуміти, вживаючи цей термін. Так, наприклад, медіаюристка

Оксана Максименюк трактує цифрову ідентичність як всю інформацію про людину, яка існує в інформаційному просторі. Ця інформація включає не лише ті дані, які людина особисто публікує про себе в інтернеті, а ті, які збирають про неї сайти та програми, а також дані, які ніхто не збирає, але які існують у мережі (Максименюк, 2024).

Власну думку щодо цифрової ідентичності людини висловлює програмний директор Української Гельсінської спілки з прав людини Максим Щербатюк, який зауважує, що вона значною мірою складається з її персональних даних, які можуть бути зібрані без її відома (Щербатюк, 2024). Таким чином, цифрова ідентичність включає всю інформацію про людину, яка зберігається про неї в інтернеті та яка містить якісь дані про конкретну людину. І найближчим до цього визначення, як пояснює медіаюрист Лабораторії цифрової безпеки Максим Дворовий, є поняття «цифровий слід» (digital footprint). «Цифровий слід» – це те, що ми залишаємо в мережі, користуючись інтернетом: геомітки, фото, відео, повідомлення, пошукові запити, паролі, номери карток, пости у соціальних мережах тощо (Дворовий, 2024).

Як бачимо, цифрова ідентичність є доволі масштабним поняттям, яке включає і конфіденційну, і особисту інформацію, і персональні дані та дані про нашу взаємодію з онлайн-середовищем. Слід зауважити, що в українському законодавстві поки що відсутнє чітке визначення цього поняття, проте воно вже відіграє неабияку роль у нашому житті.

Далі зосередимося на тому, яким чином відбувається накопичення цифрового сліду, як ідентифікується особистість у цифровому середовищі та які наслідки цього процесу для реального життя та віртуального життя індивіда. Незалежно від того, подобається нам це чи не подобається, але вже зараз забагато комерційних структур схильні довіряти в більшій мірі інформації, яка є про нас в мережах, аніж тій, яку ми самі про себе розповідаємо. Так, наприклад, при поданні заявки на кредит кредитна історія буде розглядатися як більш надійний аргумент при прийнятті рішення про видачу кредиту, аніж та анкета, яку ми подаємо.

Цифровий слід, який ми залишаємо, умовно можна поділити на три рівні, які узагальнено в таблиці 1.

Таблиця 1

Структура цифрового сліду

Перший рівень	Дані (інформація), які ми розміщуємо самі про себе та можемо контролювати і управляти ними. Ці дані (інформація), які ми завантажуємо в соціальні мережі та мобільні додатки: інформація з нашого профіля в соціальних мережах (Telegram, YouTube, Facebook, Instagram, TikTok, Twitter, Viber), наші публічні та особисті повідомлення, пошукові запити, завантажені фотографії, відео, історії, тести та опитування, в яких ми прийняли участь, веб-сайти, які ми відвідали та інші результати усвідомлених взаємодій в мережі.
Другий рівень	Містять інформацію, якою людина, скоріше за все не завжди хоче з усіма ділитися, наприклад, про її місцерозташування в реальному часі (дивлячись на траєкторії місцерозташування, які показують пристрої, компанії можуть багато чого розповісти про те, з ким конкретна людина проводить свій час). Також відслідковується контент, який людина переглянула, час, який вона витратила на його читання, динаміка натискання клавіш, швидкість набору тексту і рух пальців на екрані. Це неабиякий ґрунт для аналізу людських емоцій і виявлення психологічних особливостей: характеру, темпераменту, схильностей, установок.
Третій рівень	Інтерпретація першого та другого рівнів. Людські інформаційні дані аналізуються різними алгоритмами та порівнюються з даними інших користувачів для виявлення значущих статистичних кореляцій. Тут формулюються висновки не лише про те, що людина робить, скільки про те, хто вона така. Мета цих алгоритмів – угадати те, що людина навряд чи добровільно висвітлить: це її психометричний профіль, рівень IQ, її слабкості, наміри, залежності, сімейна ситуація, хвороби, маленькі нав'язливі ідеї, (наприклад, шопінг, ігри, кредити) і серйозні зобов'язання (наприклад, інвестиції, бізнес-проекти).

Джерело: авторська розробка

Якщо проаналізувати кожен рівень, то щодо першого можна ствердити наступне:

– кожен індивід самостійно вирішує, якими світлинами він хоче поділитися, а які повинні залишатися приватними;

– кожен індивід приймає або відхиляє запрошення, теги управління і двічі подумає перед тим чи публікувати повідомлення або коментар;

– люди критичні та виборчі по відношенню контенту, який їм подобається або яким вони діляться.

Проблема полягає в тому, що інформаційні дані, з якими індивіди взаємодіють усвідомлено, – це лише верхівка айсбергу, оскільки вони не бачать іншого, того, що приховане під водою дружніх інтерфейсів мобільних додатків і онлайн-сервісів. Сама цінна інформація про людину потрапляє в мережу без її контролю та згоди. Саме ці більш глибокі рівні, які людина не може усвідомлено контролювати, визначають її цифрове «Я» та впливають на прийняття рішень щодо неї.

Другий рівень містить дані (інформацію) про нашу поведінку в мережі. Це не стільки вибір людини, який вона робить усвідомлено, скільки метадані, які надають контекст для цих виборів. Результати аналізу даних третього рівня, як приклад, є дуже корисними для рекламодавців, оскільки реклама покликана створювати потреби і спонукати людей приймати рішення, які вони ще не прийняли, маркетологи будуть намагатися використовувати наші підсвідомі механізми та автоматичні реакції. Вони збирають та накопичують дані про поведінку людей і використовують алгоритми для пошуку значущих кореляції в цьому хаосі.

Вже зараз деякі важливі рішення фінансово-кредитних установ, страхових компаній, роботодавців приймаються на підставі аналізу великих масивів даних алгоритмами, а не безпосередньо людьми, і людина не в змозі вплинути, а тим більше – керувати цією інформацію про саму себе. Слід зазначити, що в рекламній індустрії існує переконання, що великі дані не брешуть – що статистичні кореляції говорять правду про людей і їх поведінку та мотивації. Але чи так це насправді? Цифровий клон людини може виглядати емоційно нестійким і таким, що не заслуговує довіри в зв'язку із застосовуваних нею пошукових запитів. Але це може зовсім не співпадати з реальним життям, проте штучний інтелект буде відноситися до кожного з нас саме так, як позиціонує себе наш цифровий клон.

Відсутність визначеного в законодавстві поняття зовсім не вказує на те, що відсутні загрози, які можуть спіткати цифрову ідентичність будь-якої людини. Це зумовлено тим, що люди довіряють значний масив особистих даних, які можуть бути використані проти них самих своїм месенджерам, соціальним мережам, застосункам та інтернету взагалі.

Єдиний спосіб, який допоможе поновити повний контроль над цифровою проекцією людини, на нашу думку – це зробити всі дані про користувача відкритими для нього. Європейське законодавство вже вимагає від компаній, які займаються відслідковуванням і профілюванням, зробити ці процеси більш прозорими для користувача. Загальний регламент по захисту даних (General Data Protection Regulation, GDPR), який вступив у силу ще в травні 2018 року, дає європейським користувачам право перевіряти свої дані, включаючи маркетингові профілі, створені брокерами даних, інтернет-платформами або on-line ЗМІ. Хоча, слід зазначити, компанії все ще можуть захищати свої коди та алгоритми як бізнес-секрети, вони більше не можуть приховувати особисті дані, які вони генерують, від своїх користувачів. (Lahlou, 2008; Yang, 2010$ Birch, 2007).

GDPR з його логікою є доволі непоганим відправним пунктом для діалогу між усіма учасниками ринку. Поки користувачі відносяться до брокерів даних і маркетологів як до ворогів, а вони відносяться до людей як до експлуатованому ресурсу, для відкритої розмови місця немає. В Україні, де ринок великих інформаційних даних лише формується, є всі шанси врахувати міжнародний досвід і почати впроваджувати моделі маркетингу даних, які засновані на довірі і прозорості, а це дає конкурентні переваги компаніям, які працюють з big data.

Вищезазначене набуває особливої актуальності в зв'язку з активною розробкою в даний час деяких напрямків цифровізації України, зокрема цифрового застосунку Дія – цифрового профілю у смартфоні, в якому здійснюються автоматичні державні послуги, відкриваються рахунки, зберігаються всі дані про громадянина України: всі види реєстрації бізнесу, ФОП,

ТОВ, документи, посвідчення, інформація про володіння нерухомістю, переміщення по країні і за кордоном та багато іншого. Задача цієї платформи – забезпечити через портал держпослуг доступ до даних про громадянина або юридичну особу, що містяться в інших державних інформаційних системах.

Інфраструктура цифрового профілю має містити сервіс, через який громадяни можуть давати або відкликати згоду на отримання тієї або іншої інформації про себе. Юридичні особи отримають можливість через «єдине вікно» обмінюватися інформацією. Вважаємо, що це позитивно вплине на ефективність бізнес-процесів, знизить витрати, пов'язані з паперовим документообігом, а також підвисить якість надання державних послуг громадянам. Цифровий профіль стане одним з основних компонентів національної системи управління даними в Україні.

Якщо розглядати цифровий профіль як частину цифрової ідентичності, гостро постає питання про можливість управління ним. Виникає низка питань, типу: Яка думка склалася про мене в мережі? Чи можу я втручатися в цю ситуацію та змінити її? Але ж держава і компанії, які мають на меті використовувати дані цифрових профілей, також несуть певні ризики, наприклад: як вони можуть бути впевнені в тому, що користувач саме той, за кого себе видає? Чи можуть вони здійснювати безпечні транзакції з таким користувачем? Як вони можуть запропонувати користувачеві сервіси, які йому дійсно необхідні? Це державна платформа? Це платформа, створена бізнесом? (наприклад, фінансово-кредитні установи створюють власні платформи). Це регіонально-розподільчі моделі платформ, які мають якісь певні загальні правила формування цифрового профілю?(наприклад, платформи Миколаївської та Одеської областей)? Чи це рішення сформоване на базі блокчейн-технологій (децентралізована мережа чи децентралізований обмін даними)?

Слід зазначити, що деякі світові компанії в умовах сьогодення успішно розвиваються в напрямку створення системи цифрових ідентифікаторів користувачів. Civic надає фізичним особам комплекс сервісів ідентифікації, в яких користувачі з допомогою мобільних пристроїв або ПК проходять ідентифікацію, отримують цифровий ідентифікатор, а вже з його допомогою можуть здійснювати покупки, отримувати послуги, укладати угоди з іншими учасниками і юридичними особами.

Некомерційний фонд Sorvin розробляє стандарти цифрової ідентифікації і підтримує мережу Sorvin Network. Для ідентифікації користувачів використовуються інститути, в яких користувачі ідентифікуються в реальному житті: державні установи, офіси, підприємства. Людина, яка пройшла процедуру ідентифікації, отримує цифровий ідентифікатор DID, з допомогою якого вона може розпоряджатися своїми даними в мережі після того, як буде пройдено блокчейн-ідентифікацію. Схожі сервіси є у IBM і Microsoft, а також у громадських організацій. Наприклад, ООН застосовує свій власний проект системи цифрової ідентичності для застосування його в програмі допомоги голодуючим. Естонія є першою в світі країною, в якій запроваджена система цифрової ідентифікації e-identity. Цифрова ідентифікація з допомогою спеціальної карти або мобільного пристрою дозволяє вирішити майже будь-які питання з державними органами. Досвід застосування цифрових профілей призводить до нових ризиків: втрати цифрового ідентифікатора, високих затрат, відсутності масовості таких проектів через відсутність загальних стандартів.

Підбиваючи підсумки наших міркувань щодо проблем цифрової ідентичності, цифрової ідентифікації і цифрового профілю, потрібно відмітити, що це теми для доволі серйозного суспільно-професійного та наукового обговорення. Цифрова ідентичність здійснює все більш зростаючий вплив на життя кожної людини і суспільства в цілому. Враховуючи наслідки цього впливу, можна із впевненістю сказати, що формування цифрової ідентичності – це питання особистої, суспільної і національної безпеки. Як раніше ми вчилися читати і писати, так само зараз ми повинні вчитися формувати свою цифрову ідентичність.

Література

Magopets, O., Havrilenko, N., Yashchyshyna, I., Kobus, O., & Kononova, D. (2022)Strategic management accounting in the conditions of digitalization of the economy. *Ad Alta: Journal of Interdisciplinary Research*. Hhe Czech republic, Vol. 12, Iss. 1. P. 92–96. Retrieved from : http://eir.nuos.edu.ua/handle/123456789/5345

Polishchuk, O., Kulinich, T., Martynovych, N., & Popova, Y.(2022) Digitalization and Sustainable Development: the New COVID-19 Challenge Requires Non-standard Solutions. *Problemy Ekorozwoju*, 17(2), 69–79. Retrieved from: https://doi.org/10.35784/pe.2022.2.08

Гавриленко, Н., & Козіцька, Н. (2022). Аналітичне забезпечення цифрових трансформацій. *Економіка та суспільство*, (38). DOI: https://doi.org/10.32782/2524-0072/2022-38-38

Гавриленко, Н., Грищенко, О., & Козіцька, Н. (2022). Вплив цифрових трансформацій на зміст фіскального адміністрування. *Економіка та суспільство,* (41). https://doi.org/10.32782/2524-0072/2022-41-38

Гавриленко, Н. В. (2023). Інформація в умовах цифровізації публічно-правового управління. Економічний простір, (187), 39-43. DOI: https://doi.org/10.32782/2224-6282/187-6

Гавриленко, Н. В. (2023). Роль цифровізації у правовому регулюванні окремих функцій органів державної влади і управління. *Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки*, 1. DOI https://doi.org/10.32782/TNU-2707-0581/2023.5/01.

Штучний інтелект в журналістиці: юридичний аспект та ризики використання. https://rayon.in.ua/topics/667586-shtuchniy-intelekt-v-zhurnalistitsi-yuridichniy-aspekt-ta-riziki-vikoristannya.

Цифрова ідентичність людини : як її захистити. Укрінформ. https://www.ukrinform.ua/rubric-society/3316842-cifrova-identicnist-ludini-ak-ii-zahistiti.html.

Lahlou S. (2008) Identity, Social Status, Privacy and Face-Keeping in Digital Society. *Social Sciences Information*. 2008. Vol. 47. No 3. Pp. 299–330.

Yang Y., Lewis E., Newmarch J.(2010) Profi le-Based Digital Identity Management – a Better Way to Combat Fraud. *Proceedings of 2010 IEEE International Symposium on Technology and Society*. Wollongong, NSW, Australia. Pp. 260–267. doi: 10.1109/ISTAS.2010.5514629

David Birch (2007). Digital Identity Management: Perspectives On The Technological, Business and Social Implications. Aldershot, Hants.

References

Magopets, O., Havrilenko, N., Yashchyshyna, I., Kobus, O., & Kononova, D. (2022)Strategic management accounting in the conditions of digitalization of the economy. *Ad Alta: Journal of Interdisciplinary Research* . HhеCzech republic, Vol. 12, Iss. 1 .P. 92–96. Retrieved from : http://eir.nuos.edu.ua/handle/123456789/5345

Polishchuk, O., Kulinich, T., Martynovych, N., & Popova, Y.(2022) Digitalization and Sustainable Development: the New COVID-19 Challenge Requires Non-standard Solutions. *Problemy Ekorozwoju*, 17(2), 69–79. Retrieved from: https://doi.org/10.35784/pe.2022.2.08.

Havrylenko, N., & Kozitska, N. (2022). Analitychne zabezpechennia tsyfrovykh transformatsii. Ekonomika ta suspilstvo, (38).[Analytical support of digital transformations]. DOI: https://doi.org/10.32782/2524-0072/2022-38-38. [in Ukrainian].

Havrylenko, N., Hryshchenko, O., & Kozitska, N. (2022). Vplyv tsyfrovykh transformatsii na zmist fiskalnoho administruvannia. [The influence of digital transformations on the content of fiscal administration]. Ekonomika ta suspilstvo, (41) https://doi.org/10.32782/2524-0072/2022-41-38. [in Ukrainian].

Havrylenko, N. V. (2023). Informatsiia v umovakh tsyfrovizatsii publichno-pravovoho upravlinnia [Information in the conditions of digitization of public and legal administration] Ekonomichnyi prostir, (187), 39-43. DOI: https://doi.org/10.32782/2224-6282/187-6 [in Ukrainian].

Havrylenko, N. V. (2023). Rol tsyfrovizatsii u pravovomu rehuliuvanni okremykh funktsii orhaniv derzhavnoi vlady i upravlinnia.[The role of digitalization in legal regulation of certain functions of state authority and management bodies].Vcheni zapysky TNU imeni V.I. Vernadskoho. Seriia: yurydychni nauky, 1 DOI https://doi.org/10.32782/TNU-2707-0581/2023.5/01. [in Ukrainian].

Shtuchnyi intelekt v zhurnalistytsi: yurydychnyi aspekt ta ryzyky vykorystannia. [Artificial intelligence in journalism: legal aspect and risks of use]. https://rayon.in.ua/topics/667586-shtuchniy-intelekt-v-zhurnalistitsi-yuridichniy-aspekt-ta-riziki-vikoristannya.

Tsyfrova identychnist liudyny : yak yii zakhystyty. Ukrinform. [A person's digital identity: how to protect it. Ukrinform]. https://www.ukrinform.ua/rubric-society/3316842-cifrova-identicnist-ludini-ak-ii-zahistiti.html.

Lahlou S. (2008) Identity, Social Status, Privacy and Face-Keeping in Digital Society. *Social Sciences Information*. 2008. Vol. 47. No 3. Pp. 299–330.

Yang Y., Lewis E., Newmarch J.(2010) Profi le-Based Digital Identity Management – a Better Way to Combat Fraud. *Proceedings of 2010 IEEE International Symposium on Technology and Society*. Wollongong, NSW, Australia. Pp. 260–267. doi: 10.1109/ISTAS.2010.5514629

David Birch (2007). Digital Identity Management: Perspectives On The Technological, Business and Social Implications. Aldershot, Hants.

Анотація

Гавриленко Н. В. **Правові засади цифрової ідентифікації і репрезентації особистості. –** Стаття.

Стаття присвячена дослідженню деяких проблемних питань, які стосуються цифрової ідентичності, цифрової самоідентифікації особи та цифрового профілю. Пошуком відповідей на ці питання займаються не лише вчені гуманітарного спрямування, але й спеціалісти в сфері державного управління, фінансів, економіки, освіти, філософії і етики, високотехнологічних секторів економіки, оскільки формування цифрової ідентичності – це сфера особистої, корпоративної і національної безпеки. Завданнями дослідження, описаного в статті є визначення на підставі аналізу підходів до цифровізації суспільства, які склалися, можливих проблем в сфері формування цифрової ідентичності особи та виявлення основних шляхів вирішення таких проблем. Зауважено, що в українському законодавстві поки що відсутнє чітке визначення цього поняття, проте воно вже відіграє неабияку роль у всіх сферах життєдіяльності.

Проведене аналітичне дослідження по виявленню питань, які характеризують процеси цифровізації суспільства. В ході дослідження аргументовано, що в умовах цифрової економіки, яка припускає повсюдне використання великих масивів даних, особливого значення набуває рішення проблеми контролю над формуванням цифрової ідентичності громадянина. Вважаємо, що єдиний спосіб відновити повний контроль над цифровою проекцією людини – це зробити всі дані про користувача відкритими для нього. Досвід застосування відповідних цифрових профілей породжує нові ризики, які перераховані в представленій статті: втрати цифрового ідентифікатора, високих затрат, відсутності масовості таких проектів через відсутність загальних стандартів.

Проблеми цифрової ідентичності, цифрової ідентифікації і цифрового профілю є темами для подальшого серйозного суспільно-правового, професійного та наукового обговорення. Цифрова ідентичність здійснює все більший вплив на життя людини і суспільства. Формування цифрової ідентичності є питанням особистої, суспільної і національної безпеки.

Ключові слова: інформаційне право, цифровізація, цифровий профіль, ідентифікація, правове регулювання, закон.

Summary

Havrilenko N. V. **Legal principles of digital identification and representation of personality. –** Article.

The article is devoted to the study of some problematic issues related to digital identity, digital self-identification of a person and digital profile. The search for answers to these questions is not only conducted by humanitarian scientists, but also by specialists in the field of public administration, finance, economics, education, philosophy and ethics, high-tech sectors of the economy, since the formation of digital identity is a sphere of personal, corporate and national security. The tasks of the research described in the article are to determine, based on the analysis of existing approaches to digitalization of society, possible problems in the field of forming a person's digital identity and to identify the main ways to solve such problems. It is noted that the Ukrainian legislation does not yet have a clear definition of this concept, but it already plays a significant role in all spheres of life.

Analytical research was conducted to identify issues that characterize the processes of digitalization of society. In the course of the study, it is argued that in the conditions of the digital economy, which assumes the widespread use of large data sets, the solution to the problem of control over the formation of a citizen's digital identity is of particular importance. We believe that the only way to regain full control over the digital projection of a person is to make all data about the user open to him. The experience of using the appropriate digital profiles gives rise to new risks, which are listed in the presented article: loss of a digital identifier, high costs, lack of mass of such projects due to the lack of common standards. The problems of digital identity, digital identification and digital profile are topics for further serious socio-legal, professional and scientific discussion. Digital identity exerts an increasing influence on the life of a person and society. The formation of a digital identity is a matter of personal, public and national security.

Key words: information law, digitization, digital profile, identification, legal regulation, law.