УДК 347.2
DOI https://doi.org/10.24144/2788-6018.2026.02.1.44

ЦИФРОВИЙ СЛІД ФІЗИЧНОЇ ОСОБИ У МЕДІАПРОСТОРІ ЯК ОБ'ЄКТ ЦИВІЛЬНИХ ПРАВ ТА ЕЛЕМЕНТ ЦИФРОВОЇ СПАДЩИНИ

Тюря Ю.І.,
доктор юридичних наук, доцент,
професор кафедри цивільного, господарського та екологічного права
Національний технічний університет «Дніпровська політехніка»,
ORCID: 0000-0001-7732-3535

Тюря Ю.І. Цифровий слід фізичної особи у медіапросторі як об'єкт цивільних прав та елемент цифрової спадщини.

У статті досліджується правова природа цифрового сліду фізичної особи у медіапросторі як об'єкта цивільно-правового регулювання у контексті захисту права на приватність та формування інституту цифрової спадщини. Актуальність дослідження зумовлена безпрецедентними викликами цифровізації суспільних відносин, за яких кожна взаємодія особи з цифровим середовищем формує стійкий цифровий слід, здатний впливати на реалізацію фундаментальних прав людини.

Проаналізовано структуру цифрового сліду через призму активної та пасивної цифрової діяльності, що в сукупності формують інтегрований цифровий портрет особи. Встановлено, що цифровий слід включає як свідомо створений контент (публікації, коментарі, профілі), так і автоматично зібрану інформацію (метадані, геолокацію, історію пошуків, файли cookie).

У роботі окрему увагу приділено дихотомії між необхідністю державного втручання задля безпеки та збереженням приватності. На прикладі системи соціального кредитування КНР розглянуто ризики тотального алгоритмічного профайлінгу та дискримінації. Водночас через призму практики Європейського суду з прав людини (справа Big Brother Watch та інші проти Сполученого Королівства) обґрунтовано тезу, що метадані потребують рівнозначного рівня правового захисту, як і зміст комунікацій, а масове перехоплення даних допустиме тільки за наявності чітко визначених законодавчих критеріїв, ефективного незалежного контролю та зовнішнього нагляду за обробкою цифрових даних.

Розглянуто проблематику цифрової спадщини та постмортальної приватності. На прикладі судової практики Німеччини обґрунтовано застосування конструкції універсального правонаступництва до цифрових активів і контенту облікових записів померлої особи, а також визначено межі балансу між правами спадкоємців і правом на повагу до приватного життя третіх осіб. Проаналізовано модель саморегулювання цифрових платформ на прикладі механізму Digital Legacy компанії Apple як можливий орієнтир для нормативного врегулювання доступу до цифрових активів після смерті власника.

У контексті рекодифікації Цивільного кодексу України доведено, що сучасні законодавчі ініціативи свідчать про поступову інтеграцію цифрового сліду та цифрових активів у систему цивільно-правових категорій. За результатами дослідження сформульовано пропозицію щодо запровадження в національному праві інституту «цифрової волі» як інструменту попереднього волевиявлення особи стосовно управління цифровими активами та даними після смерті.

Ключові слова: цифровий слід, право на приватність, цифрові активи, цифрова спадщина, постмортальна приватність, рекодифікація цивільного законодавства.

Tiuria Yu.I. The digital footprint of an individual in the media space as an object of civil rights and an element of digital inheritance.

The article examines the legal nature of an individual's digital footprint in the media space as an object of civil law regulation in the context of protecting the right to privacy and shaping the institution of digital inheritance. The study's relevance is driven by the unprecedented challenges posed by the digitalization of social relations, in which every person's interaction with the digital environment creates a persistent digital footprint capable of influencing the exercise of fundamental human rights.

The structure of the digital footprint has been analyzed through the lens of active and passive digital activity, which together form an integrated digital portrait of the individual. It has been established that the digital footprint includes both consciously created content (publications, comments, profiles) and automatically collected information (metadata, geolocation, search history, cookies).

In the work, particular attention is paid to the dichotomy between the necessity of state intervention for security purposes and the preservation of privacy. Using the example of the PRC's social credit system, the risks

of total algorithmic profiling and discrimination are examined. At the same time, through the lens of the case law of the European Court of Human Rights (Big Brother Watch and Others v. the United Kingdom), the thesis is substantiated that metadata require an equivalent level of legal protection as the content of communications, and that mass interception of data is permissible only in the presence of clearly defined legislative criteria, effective independent oversight, and external supervision over the processing of digital data.

The issue of digital inheritance and post-mortem privacy is examined. Using the example of German judicial practice, the application of the concept of universal succession to digital assets and the content of a deceased person's accounts is substantiated, and the boundaries of the balance between the rights of heirs and the right to respect for the private life of third parties are determined. The model of self-regulation by digital platforms is analyzed using Apple's Digital Legacy mechanism as a possible reference point for the normative regulation of access to digital assets after the owner's death.

In the context of the recodification of the Civil Code of Ukraine, it has been demonstrated that current legislative initiatives indicate a gradual integration of the digital footprint and digital assets into the system of civil law categories. Based on the results of the study, a proposal has been formulated to introduce into national law the institution of «digital will» as an instrument for the prior expression of a person's will regarding the management of digital assets and data after death.

Key words: digital footprint, right to privacy, digital assets, digital inheritance, post-mortem privacy, recodification of civil legislation.

Постановка проблеми. В умовах розвитку цифрового суспільства соціальні мережі перестали виконувати виключно комунікаційну функцію, перетворившись на глобальну екосистему, де процеси збирання, поширення, обміну та зберігання персональних даних відбуваються безперервно. Будь-яка активність користувача мережі – від авторського допису до звичайного коментаря чи іншої форми онлайн-взаємодії – формує стійкий цифровий слід, що може супроводжуватися довгостроковими правовими та соціальними наслідками як для приватних осіб, так і для професійних учасників цифрового простору, зокрема лідерів думок (інфлюенсерів) та суб'єктів господарювання. Враховуючи кумулятивний характер цифрового сліду та його здатність зберігатися, відтворюватися й поширюватися незалежно від волі особи, питання забезпечення меж реалізації права на приватність у цифровому середовищі набуває особливої актуальності.

Право на приватність, закріплене у статті 12 Загальної декларації прав людини та статті 17 Міжнародного пакту про громадянські і політичні права, традиційно розглядається як одна з фундаментальних гарантій людської гідності та особистої свободи в умовах глобалізації й становлення інформаційного суспільства. Водночас стаття 8 Європейської конвенції з прав людини конкретизувала зазначені засади, закріпивши підхід до захисту приватного і сімейного життя через вимоги законності, легітимної мети та пропорційності втручання.

Проте в умовах цифрової трансформації реалізація права на приватність стикається з безпрецедентними викликами – від масового алгоритмічного спостереження та профайлінгу до втрати суб'єктом ефективного контролю над власними персональними даними, зумовивши необхідність доктринального переосмислення класичної концепції невтручання в особисте життя. Поряд з цим особливої актуальності набуває питання правового режиму доступу до інформації про особу, яка зберігається та циркулює у цифровому середовищі, зокрема після її смерті. Як наслідок у наукових дослідженнях дедалі частіше обґрунтовується концепція post-mortem privacy (постмортальної приватності), що спрямована на захист цифрового сліду померлої особи – її облікових записів, даних, метаданих й цифрового контенту – від небажаного доступу третіх осіб, у тому числі спадкоємців. Зазначене об'єктивно породжує колізію між обов'язком захисту гідності й репутації померлої особи і майновими чи інформаційними правами її правонаступників на доступ до відповідних цифрових активів.

Метою статті є дослідження правової природи цифрового сліду фізичної особи у медіапросторі як об'єкта цивільно-правового регулювання, визначення меж допустимого державного втручання у цифровий простір особи з позиції захисту права на приватність та аналіз правового режиму цифрової спадщини в контексті постмортальної приватності.

Стан опрацювання проблематики. Питання правової природи цифрового сліду, цифрової ідентичності та спадкування віртуальних об'єктів у медіапросторі останніми роками привертає дедалі більшу увагу вітчизняних цивілістів, що зумовлено необхідністю адаптації традиційних правових конструкцій до реалій цифрового середовища.

Фундаментальні аспекти цифрової ідентичності як соціального та правового феномену, а також питання захисту особистих немайнових прав людини в мережі Інтернет, зокрема відшкодування моральної шкоди, завданої через соціальні мережі, досліджує С.Б. Булеца. Практичний вимір цифрового сліду – метадані, електронні комунікації, хеш-значення – як джерела доказів у цивільному судочинстві й проблеми його процесуальної верифікації розкриваються у працях М. Жушмана.

Значний масив досліджень присвячено правовому режиму облікових записів (акаунтів) як потенційних об'єктів цивільного обігу і спадкування. О.Є. Кухарєв здійснює комплексний аналіз правової природи акаунта в соціальній мережі, обґрунтовуючи необхідність розмежування самого облікового запису як юридичної конструкції та його вмісту (цифрового контенту). Ю.В. Кривенко досліджує проблематику спадкування акаунтів соціальних мереж як форми віртуальної власності та результатів інтелектуальної діяльності, наголошуючи на прогалинах договірного регулювання відносин між користувачами та платформами.

Концептуальні засади формування категорії «цифрова спадщина», її співвідношення з традиційним спадком і перспективи законодавчого закріплення цифрових речей як об'єктів спадкування ґрунтовно аналізують Л.М. Загоруй та І.С. Загоруй. Своєю чергою, М.З. Вовк вивчає специфіку спадкування цифрових активів та об'єктів інтелектуальної власності в умовах розвитку блокчейн-технологій, зокрема питання збереження доступу, передачі приватних ключів та концепції цифрового заповіту.

Проте питання цифрового сліду фізичної особи у медіапросторі як самостійного об'єкта цивільних прав та ключового елемента цифрової спадщини продовжує привертати увагу дослідників і залишається актуальним напрямом наукових пошуків у сучасній цивілістиці.

Виклад основного матеріалу. Світ дедалі більше цифровізується, і кожна дія користувача в Інтернеті – клік, пошуковий запит чи взаємодія з цифровими сервісами – залишає стійкий слід даних. Сукупність таких даних формує індивідуальну цифрову ідентичність особи, яка набуває вираженого соціально-правового значення, оскільки здатна впливати на репутацію особи, її кар'єру, доступ до фінансових послуг, освітніх можливостей та інших сфер життя. Довгострокові наслідки накопичення такої інформації стають критично помітними в умовах впровадження систем алгоритмічного прийняття рішень, коли інформація про індивіда використовується для профайлінгу, оцінки кредитоспроможності, рекрутингу або соціального скорингу.

У науковій літературі цифровий слід розглядається як масив відомостей про особу, що генерується у процесі використання цифрових технологій [1]. Він охоплює як свідомо створений контент (публікації, коментарі, профілі), так і автоматично зібрану інформацію (історія переглядів, геолокація, метадані, файли cookie тощо).

З огляду на механізм виникнення та характер збирання даних цифровий слід умовно можна поділити на активний і пасивний. Активний цифровий слід охоплює інформацію, створену особою свідомо і цілеспрямовано, зокрема публікації у соціальних мережах, коментарі, репости та лайки в соціальних мережах, заповнення онлайн-форм, реєстрація облікових записів, надсилання електронних листів, повідомлень чи створення контенту (фото, відео, блоги), завантаження контенту або участь у цифрових спільнотах [1]. Відповідно активний цифровий слід є результатом контрольованих дій користувача, який усвідомлює факт фіксації інформації та часто може частково регулювати її видимість (наприклад, через налаштування приватності). Водночас через відсутність контекстуального контролю після публікації, такі дані легко виходять за межі початкової аудиторії та зберігаються невизначений час.

Пасивний цифровий слід формується без прямої участі особи або поза межами усвідомленого контролю. До нього належать, зокрема, файли cookie та трекери, які фіксують поведінку на вебсайтах, дані про геолокацію, історія пошукових запитів, IP-адреси, метадані пристроїв, час перебування на сторінках, патерни переглядів та інші відомості, отримані шляхом автоматизованого спостереження за поведінкою користувачів. Нерідко особа не усвідомлює масштабів або змісту таких даних, що зберігаються та обробляються третіми особами [1]. Пасивний слід формується внаслідок роботи алгоритмів платформ, браузерів, мобільних додатків і мереж, часто без явної згоди користувача або з формальною згодою, прихованою в умовах використання. Він є менш контрольованим і становить значну частину масового збору даних глобальними технологічними корпораціями.

Разом активний і пасивний цифрові сліди створюють інтегрований цифровий портрет індивіда. Активні дані розкривають заявлені інтереси, погляди, соціальні зв'язки та самоідентифікацію, тоді як пасивні – дозволяють реконструювати реальні звички, уподобання, маршрути пересування, споживчі патерни та навіть психоемоційний стан. Важливо враховувати, що цифровий слід не є статичним: він постійно накопичується, комбінується з даними інших джерел і може використовуватися для створення вторинних профілів (наприклад, у системах соціального кредитування чи автоматизованого рекрутингу).

Водночас процес формування цифрового портрета не обмежується виключно віртуальним середовищем, а поширюється й на фізичний простір завдяки інтеграції онлайн-даних з технологіями розпізнавання обличчя та алгоритмічного аналізу поведінки людини. Зокрема, упродовж останніх років технології розпізнавання обличчя та алгоритмічного аналізу поведінки отримали значне поширення, насамперед у великих урбанізованих просторах.

Системи відеоспостереження дедалі частіше виконують не тільки функцію фіксації подій у режимі реального часу, але й забезпечують ідентифікацію осіб, аналіз моделей їхньої поведінки з метою прогнозування потенційних загроз громадському порядку й безпеці у межах здійснення державного чи приватного контролю у публічному просторі.

Показовим прикладом використання даних цифрового сліду в поєднанні з відеофіксацією та алгоритмічним аналізом є система соціальних кредитів Китайської Народної Республіки, започаткована Планом дій щодо створення системи соціальних кредитів (2014 – 2020). Відповідна система передбачає комплексне оцінювання рівня так званої «соціальної довіри» громадян на основі агрегування різнорідних масивів даних, зокрема відомостей про фінансову дисципліну, податкову поведінку, соціальні зв'язки та цифрову активність особи, включаючи її поведінку в мережі Інтернет. Результатом такого оцінювання є формування узагальненого показника соціальної надійності, який фактично використовується як інструмент державного контролю за суспільною поведінкою індивіда та може слугувати правовою підставою для диференціації обсягу прав і свобод особи залежно від присвоєного їй рейтингу [2].

Ключовим функціональним елементом зазначеної системи є механізм диференційованого регуляторного впливу, що передбачає застосування заохочувальних і обмежувальних заходів залежно від результатів оцінювання поведінки суб'єкта. Заохочувальні заходи охоплюють, зокрема, надання пільг, пріоритетного доступу до окремих послуг або фінансових ресурсів, тоді як обмежувальні заходи включають встановлення заборон або обмежень щодо участі у державних закупівлях, отримання кредитів, пересування та реалізації інших прав. Реалізація останніх забезпечується шляхом ведення спеціальних реєстрів осіб і суб'єктів господарювання з негативною оцінкою поведінки (так званих «чорних списків») та застосування механізму спільного міжвідомчого покарання (joint punishment), що передбачає наскрізне (крос-секторальне) впровадження санкцій на підставі системної координації органів державної влади, за якої правопорушення в одній сфері (наприклад, несплата податків чи невиконання судового рішення) автоматично тягне за собою обмеження прав суб'єкта в інших, галузево чи територіально не пов'язаних сферах. На практиці функціонування системи забезпечується інтеграцією державних реєстрів, галузевих баз даних, судових рішень та інформації від приватних платформ [3].

Практика масштабного збору та обробки цифрового сліду громадян актуалізує питання щодо меж допустимого державного втручання у сферу приватного життя, а також щодо належних процесуальних гарантій захисту персональних даних у цифровому середовищі. Оскільки сьогодні цифровий слід особи набуває ознак комплексного інформаційного ресурсу, який використовується не лише для оперативних або управлінських цілей, але й здатний істотно впливати на обсяг реалізації фундаментальних прав людини, включаючи право на приватність, свободу вираження поглядів та контроль над власними цифровими активами.

Правомірність доступу держави до цифрових активів особи, включаючи її комунікації, метадані, поведінкові патерни в мережі Інтернет та інші елементи цифрового сліду, неодноразово ставала предметом судового розгляду у практиці Європейського суду з прав людини у контексті тлумачення права на повагу до приватного і сімейного життя, гарантованого статтею 8 Європейської конвенції з прав людини. Показовою у цьому аспекті є справа «Big Brother Watch та інші проти Сполученого Королівства», що виникла внаслідок оприлюднення інформації про програми масового електронного стеження, які здійснювалися розвідувальними службами США (NSA) та Великої Британії (GCHQ) [4].

Суть спору полягала у з'ясуванні того, чи може масове перехоплення інформації, що становить цифровий профіль особи, вважатися «необхідним у демократичному суспільстві» та чи існують достатні процесуальні запобіжники проти зловживань з боку державних органів при доступі до таких цифрових активів особи.

Велика Палата ЄСПЛ визнала, що в умовах сучасних транскордонних загроз національній безпеці режим масового перехоплення комунікацій сам по собі не суперечить положенням Конвенції, оскільки є необхідним і пропорційним інструментом для виявлення та протидії таким загрозам. Проте, з огляду на надзвичайно високий ризик зловживань і масштабне втручання у приватне життя людини з боку державних органів, такий режим може бути виправданим лише за умови визначених процесуальних гарантій на всіх етапах обробки даних – від надання дозволу на застосування заходів електронного спостереження, первинного збору й автоматизованого відбору інформації до подальшого її використання, визначення строків зберігання та остаточного знищення. Суд дійшов висновку, що національне законодавство не забезпечувало достатнього рівня незалежного державного контролю, відсутні чітко визначені критерії автоматизованого відбору інформації з масиву перехоплених комунікацій (на кшталт, ключові слова, електронні адреси, номери телефонів, IP-адреси, імена користувачів тощо), а також не передбачено ефективного зовнішнього нагляду за їх застосуванням, створювала надмірний ризик свавільного та непропорційного втручання держави у приватне і сімейне життя та свободу вираження поглядів [4].

Окремо Суд наголосив, що метадані, зокрема відомості про час, тривалість, учасників і місце здійснення комунікації, за своїм сукупним змістом здатні відтворювати детальну й цілісну картину приватного життя особи, тобто її цифровий профіль. Тому їх перехоплення, зберігання та аналіз потребують застосування тих самих процесуальних і матеріальних гарантій, що й доступ до змісту повідомлень. Відсутність таких гарантій у режимах масового перехоплення та доступу до інформації, що зберігається провайдерами, зумовила визнання Судом порушення статті 8 Європейської конвенції з прав людини [4].

Отже, висновки Великої Палати мають фундаментальне значення для розбудови правового режиму захисту цифрового сліду фізичної особи. По-перше, ЄСПЛ визнав, що цифровий слід особи, сформований унаслідок збору й обробки даних як державними, так і приватними суб'єктами, не може розглядатися як нейтральний або суто технічний масив інформації. Навпаки, він визнається об'єктом посиленого правового захисту, що потребує комплексного нормативного регулювання та дієвих механізмів нагляду в умовах тотальної цифровізації суспільства. По-друге, оскільки цифрові активи особи продовжують зберігатися у постачальників електронних комунікаційних послуг після її смерті, правовий режим доступу до них – чи то з боку держави, чи то з боку правонаступників – повинен відповідати аналогічним вимогам щодо законності, легітимної мети та необхідності у демократичному суспільстві, що застосовуються до втручання у приватне життя за життя особи.

Подальше дослідження правової природи цифрового сліду зумовлює необхідність аналізу його правового статусу після смерті фізичної особи. Накопичення цифрових активів – облікових записів у соціальних мережах, сервісів електронної пошти, хмарних архівів, цифрових фінансових інструментів – трансформує цифровий слід у самостійний об'єкт правового регулювання, який виходить за межі традиційного розуміння приватного життя і набуває спадкового виміру як елемент цифрової спадщини.

У такому контексті виникає колізія між інтересами спадкоємців щодо доступу до цифрових активів та збереження економічної й інформаційної цінності спадщини, з одного боку, і правом на повагу до приватного життя, таємницю кореспонденції та цифровою приватністю як самої померлої особи, так і третіх осіб (кореспондентів), які брали участь у цифровій взаємодії, – з іншого. Вагоме значення для вироблення певних підходів у сфері цифрової спадщини має судова практика Німеччини, зокрема рішення Федерального суду Німеччини у справі BGH III ZR 183/17 (2018), у якому цифровий обліковий запис і пов'язаний з ним контент були віднесені до складу спадкового майна та охоплені режимом універсального правонаступництва відповідно до ч. 1 ст. 1922 Цивільного кодексу Німеччини (у разі смерті фізичної особи її майно як єдина сукупність прав і обов'язків, що становлять спадщину, переходить у порядку спадкування до однієї або кількох осіб – спадкоємців) [5].

Суд обґрунтував свою позицію тим, що цифрові комунікації за правовою природою не відрізняються від традиційних форм особистої кореспонденції – приватних листів чи щоденників, – а відтак мають успадковуватися нарівні з іншими майновими та особистими немайновими правами померлого. Федеральний верховний суд Німеччини спростував аргументи провайдера про наявність правових перешкод для доступу спадкоємців до змісту електронних комунікацій, які нібито випливають з режиму таємниці телекомунікацій, встановленого Законом про телекомунікації, а також з положень Загального регламенту про захист даних (GDPR). Зокрема, пунктом 27 преамбули GDPR визначено, що регламент не застосовується до захисту персональних даних померлих осіб, а отже його дія припиняється зі смертю суб'єкта даних [6]. Щодо таємниці телекомунікацій Суд зазначив, що хоча Закон про телекомунікації (Telekommunikationsgesetz, TKG) встановлює загальний обов'язок провайдерів забезпечувати конфіденційність комунікацій, проте цей нормативний акт не містить спеціальних положень, які б виключали або суттєво обмежували доступ спадкоємців до цифрових активів померлого користувача. Єдине положення TKG, що згадує спадкоємців (§ 91 абз. 8), стосується виключно адміністративного порядку повернення розподілених радіочастот у разі смерті користувача, якщо спадкоємець не бажає продовжувати їх використання, і не регулює доступ до змісту комунікацій [7]. Суд визнав потребу узгодження права спадкоємців на доступ до цифрових активів з правом на повагу до приватного життя третіх осіб – кореспондентів померлого, чиї повідомлення можуть міститися в обліковому записі, однак наголосив, що такий баланс не може досягатися шляхом повного позбавлення спадкоємців доступу до цифрової спадщини. Захист інтересів третіх осіб має забезпечуватися через застосування загальних цивільно-правових механізмів, зокрема норм про охорону честі, гідності, ділової репутації та конфіденційної інформації [8].

Ефективну модель унормування доступу до цифрових активів після смерті користувача запроваджено компанією Apple через функцію «Цифрова спадщина» (Digital Legacy), яка дає змогу за життя визначити до п'яти довірених осіб для доступу до даних iCloud після смерті власника. Такий доступ охоплює особистий контент (фото, повідомлення, нотатки, файли, резервні копії), водночас виключаючи платіжну інформацію, паролі, дані Keychain та придбаний контент, і надається за процедурою верифікації з використанням унікального ключа доступу та свідоцтва про смерть. Apple

створює для спадкоємця тимчасовий спеціальний обліковий запис строком до трьох років, після чого дані підлягають видаленню, зберігаючи при цьому розмежування між доступом до хмарних сервісів і фізичним доступом до пристрою [9]. Отже, такий механізм, попри його приватноправову природу, фактично виконує функцію технічного регулятора балансу між правом спадкоємців на доступ до цифрової спадщини і правом власника на посмертну приватність, демонструючи можливість поєднання договірного регулювання з технологічними засобами захисту персональних даних.

Наразі у межах рекодифікації Цивільного кодексу України, зокрема через законопроєкти № 14056 та № 14057 від 21.09.2025 змінюється підхід до розуміння цифрових активів як суто технічного чи інформаційного ресурсу.

Зокрема законопроєктом № 14056 вводиться у цивільно-правовий обіг категорія «цифрової речі» (стаття 177^5 ЦК України у запропонованій редакції) як нематеріального блага, що створюється, існує та обертається виключно у цифровому середовищі та має майнову цінність. До таких об'єктів віднесено, зокрема, облікові записи в цифрових системах, цифровий контент і бази даних, віртуальні активи, а також доменні імена. Унаслідок цього цифровий слід особи перестає розглядатися виключно як сукупність розрізнених даних і набуває ознак самостійного об'єкта цивільних прав, здатного входити до складу майнової маси, бути предметом правочинів та спадкування [10].

Паралельно законопроєкт № 14057 спрямований на оновлення регулювання особистих немайнових прав та формування комплексної концепції цифрової приватності. Уперше на законодавчому рівні пропонується закріплення поняття «цифрового сліду» як складової права на приватність у цифровому середовищі (стаття 306^3 у запропонованій редакції). Зміст такого права охоплює, зокрема, метадані, історію пошукових запитів, дані геолокації та інші відомості, що виникають у процесі цифрової активності особи. Важливою новелою є також виокремлення права на цифровий образ – обліковий запис, профіль або інший елемент цифрової ідентичності, що має на меті запобігання крадіжці ідентичності, створенню підроблених облікових записів та несанкціонованому використанню персоналізованих цифрових репрезентацій (стаття 294^6 у запропонованій редакції). Важливим є те, що відповідні гарантії поширюються не лише на фізичних, а й на юридичних осіб, що відповідає реаліям сучасного цифрового обігу та практиці використання цифрових інструментів у господарській діяльності [11].

Для забезпечення ефективності зазначених прав законопроєкти передбачають низку інструментів правового захисту цифрового сліду, які корелюють із європейськими стандартами захисту персональних даних. Серед них – право на забуття як можливість вимагати вилучення неактуальної, недостовірної або неправомірно поширеної інформації; заборона використання штучно згенерованих зображень або голосу особи без її згоди як відповідь на загрозу поширення діпфейків; право на інформаційний спокій, спрямоване на захист приватного життя в умовах постійної цифрової комунікації; а також гнучкі моделі ідентифікації, що допускають використання цифрового коду або псевдоніма поряд із традиційним ім'ям [12].

Підсумовуючи, можна констатувати, що цифрова активність особи формує стійкий цифровий слід, який безпосередньо впливає на реалізацію фундаментальних прав і свобод людини та потребує не тільки технічних засобів захисту, а й певних правових механізмів регулювання, контролю та відповідальності. У цьому сенсі рекодифікація Цивільного кодексу України демонструє поступову інтеграцію цифрового сліду до системи цивільно-правових категорій та закладає нормативні передумови для комплексного захисту цифрових активів, права на приватності та інституту цифрової спадщини на рівні національного законодавства.

Висновки. Отже, чи залишається право на приватність реальною гарантією людської гідності в умовах тотальної цифровізації, коли кожна взаємодія особи з цифровим середовищем фіксується, аналізується та зберігається невизначений час, водночас формуючи стійкий цифровий слід, здатний впливати на реалізацію фундаментальних прав? Результати дослідження дозволяють дати обережно оптимістичну відповідь: захист приватності можливий, однак лише за певних умов.

По-перше, необхідно переосмислити класичні цивілістичні конструкції (майнові та немайнові права, універсальне правонаступництво, об'єкти цивільних прав, спадкова маса) з урахуванням специфіки цифрових активів як нематеріальних благ, що існують виключно у цифровому середовищі, мають майнову цінність і водночас тісно пов'язані з особистими немайновими правами (таємниця кореспонденції, право на ім'я, честь, гідність, ділова репутація).

По-друге, цифровий слід фізичної особи формується як результат поєднання активної та пасивної цифрової діяльності, становить цілісний цифровий портрет, здатний суттєво впливати на реалізацію фундаментальних прав і свобод людини, зокрема права на приватність, свободу вираження поглядів і доступ до соціально значущих благ. Практика Європейського суду з прав людини підтверджує, що як зміст електронних комунікацій, так і метадані здатні відтворювати детальну картину приватного життя особи, а отже доступ до них, збирання та обробка мають відповідати критеріям законності, легітимної мети та пропорційності незалежно від суб'єкта втручання. Після

смерті фізичної особи її цифровий слід трансформується у складову цифрової спадщини, слугуючи основою для визначення складу цифрових активів та передачі прав доступу до них спадкоємцям у порядку універсального правонаступництва.

По-третє, доцільним є впровадження в національне цивільне законодавство інституту «цифрової волі» як спеціального правового механізму розпорядження цифровими активами та цифровим слідом на випадок смерті особи. За аналогією з моделлю Digital Legacy компанії Apple цифрова воля має надавати власнику можливість за життя визначити коло осіб, уповноважених на доступ до його цифрових активів після смерті, обсяг такого доступу (повний або обмежений), а також порядок подальшої обробки, збереження чи видалення відповідних цифрових даних.

По-четверте, приватність у цифровому середовищі еволюціонує від традиційного права на невтручання в особисте життя в комплексне право на контроль над власним цифровим слідом, що включає право на цифровий образ, право на забуття, право на інформаційний спокій, захист від несанкціонованого використання персоналізованих цифрових репрезентацій (діпфейків, deepfake), а також право на посмертний захист гідності та репутації (post-mortem privacy).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Що таке цифровий слід і як його мінімізувати: ProIT. URL: https://proit.ua/shcho-takie-tsifrovii-slid-i-iak-iogho-minimizuvati/.
2. Planning Outline for the Construction of a Social Credit System (2014-2020): China Copyright and Media. URL: https://chinacopyrightandmedia.wordpress.com/2014/06/14/ planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/.
3. Китайське попередження – як працює соціальний рейтинг на основі Big Data: Blog Imena.UA. URL: https://www.imena.ua/blog/big-data-big-brother-china/.
4. CASE OF BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOMURL: HUDOC – European Court of Human Rights. URL: https://hudoc.echr.coe.int/fre?i=001-210077.
5. German Civil Code (BGB) on January 1, 1900: Das Bundesministerium der Justiz und für Verbraucherschutz und das Bundesamt für Justiz. URL: https://www.gesetze-im-internet.de/englisch_bgb/.
6. General Data Protection Regulation (27 April 2016): EUR-Lex. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.
7. Telekommunikationsgesetz (TKG) 23.06.2021: Das Bundesministerium der Justiz und für Verbraucherschutz und das Bundesamt für Justiz. URL: https://www.gesetze-im-internet.de/tkg_2021/BJNR185810021.html.
8. German Federal Court of Justice: Facebook must grant heirs full access to a deceased person's account (Update 2020): Ihde & Partner. URL: https://ihde.de/en/german-federal-court-of-justice-facebook-must-grant-heirs-full-access-to-a-deceased-persons-account-update-2020/.
9. «Цифрова спадщина» Apple – нова функція, яка дозволяє заповідати свої дані на iPhone близьким людям: iSpace. URL: https://ispace.ua/blog/tsifrova-spadshhina-apple-nova-funktsiya-yaka-dozvolyaye-zapovidati-svoyi-dani-na-iphone-blizkim-lyudyam/.
10. Проект Закону про внесення змін до Цивільного кодексу України у зв'язку із оновленням (рекодифікацією) положень книги першої № 14056 від 21.09.2025: Верховна Рада України. URL: https://itd.rada.gov.ua/billinfo/Bills/CardByRn?regNum=14056&conv=9.
11. Проект Закону про внесення змін до Цивільного кодексу України у зв'язку із оновленням (рекодифікацією) положень книги другої № 14057 від 21.09.2025: Верховна Рада України. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/57355.
12. В Україні оновлять Цивільний кодекс: деталі законопроєктів: ЮРЛІГА. URL: https://jurliga.ligazakon.net/news/239213_v-ukran-onovlyat-tsivlniy-kodeks-detal-zakonoproktv?&_ga=2.167108606.175481634.1768062894-1104389210.1644165567#_gl=1*1xo3m7n*_gcl_au*Mjk0NjUxMzY0LjE3Njc4MDY1NjA.

Дата першого надходження рукопису до видання: 2.03.2026
Дата прийняття до друку рукопису після рецензування: 20.03.2026
Дата публікації: 3.04.2026