УДК 347.5
DOI https://doi.org/10.51989/NUL.2026.1.12

ПРАВО НА ПРИВАТНІСТЬ У ЦИФРОВУ ЕПОХУ ЧЕРЕЗ ПРИЗМУ ФІДУЦІАРНИХ ОБОВ'ЯЗКІВ

Трубаков Євген Олександрович,
orcid.org/0009-0006-1005-0046
кандидат юридичних наук,
старший науковий співробітник
Інституту правотворчості та науково-правових експертиз
Національної академії наук України

У статті досліджується проблема забезпечення права на приватність у цифрову епоху через призму фідуціарних правовідносин. Автор аналізує міжнародно-правові засади охорони приватності, закріплені у Загальній декларації прав людини, Міжнародному пакті про громадянські і політичні права та Європейській конвенції з прав людини, а також простежує еволюцію доктринального розуміння приватності від класичного «права бути залишеним у спокої» до концепції контекстуальної цілісності Хелен Ніссенбаум, згідно з якою приватність є правом на відповідний потік особистої інформації в межах певного соціального контексту. Значну увагу приділено критичному аналізу домінуючої моделі інформованої згоди як основного механізму захисту персональних даних. Обґрунтовується, що ця модель є неефективною з огляду на фундаментальну нездатність користувачів оцінити всі наслідки надання згоди, значний обсяг і складність умов конфіденційності, інформаційну асиметрію на стороні контролерів даних, асиметрію влади, що проявляється у маніпулятивному дизайні інтерфейсів, а також фактичну монополію цифрових компаній, яка позбавляє користувача реальної альтернативи. На основі порівняльного аналізу ознак фідуціарних відносин та правовідносин між контролерами персональних даних і користувачами автор доводить наявність між ними значної структурної подібності, що обумовлює доцільність застосування фідуціарних обов'язків лояльності, дбайливості та конфіденційності до діяльності цифрових компаній. Розкривається зміст цих обов'язків: обов'язок лояльності передбачає заборону маніпулювання користувачами, дії в їхніх інтересах та уникнення конфлікту інтересів; обов'язки дбайливості й конфіденційності спрямовані на забезпечення безпеки персональних даних, зокрема через принцип слідування обов'язків за даними. Автор аналізує переваги фідуціарного підходу, зокрема його кореляцію з принципами обмеження мети та мінімізації даних, закріпленими у Загальному регламенті про захист даних ЄС, а також розглядає критику цієї концепції, що стосується проблеми подвійної лояльності, несумісності з рекламними бізнес-моделями та труднощів правозастосування. Водночас досліджуються альтернативні підходи до посилення приватності, включаючи антимонопольне регулювання, функціональну сумісність та екологічну аналогію надмірного збору даних. У підсумку обґрунтовується, що фідуціарна модель не є універсальним вирішенням проблеми захисту приватності, проте надає цінний додатковий правовий інструментарій, який доцільно застосовувати в українському законодавстві щодо окремих сфер, де користувач є особливо вразливим.

Ключові слова: *фідуціарні правовідносини, право на приватність, обов'язок лояльності, інформована згода, конфлікт інтересів.*

Trubakov Yevhen. The right to privacy in the digital age through the perspective of fiduciary duties

The article examines the point of ensuring the right to privacy in the digital age through the perspective of fiduciary legal relations. The author analyzes the international legal basis for the protection of privacy enshrined in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the European Convention on Human Rights, and traces the evolution of the doctrinal understanding of privacy from the classic «right to be left alone» to Helen Nissenbaum's concept of contextual integrity, according to

which privacy is the right to an appropriate flow of personal information within a specific social context. Considerable attention is paid to a critical analysis of the dominant model of informed consent as the primary mechanism for protecting personal data. It is argued that this model is ineffective given the fundamental inability of users to assess all the consequences of giving consent, the significant volume and complexity of privacy policies, information asymmetry on the part of data controllers, power asymmetry manifested in manipulative interface design, and the de facto monopoly of digital companies, which deprives users of real alternatives. Based on a comparative analysis of the characteristics of fiduciary relationships and legal relationships between personal data controllers and users, the author demonstrates the existence of significant structural similarities between them, which justifies the application of fiduciary duties of loyalty, care, and confidentiality to the activities of digital companies. The content of these duties is revealed: the duty of loyalty involves prohibiting the manipulation of users, acting in their interests, and avoiding conflicts of interest; the duties of care and confidentiality are aimed at ensuring the security of personal data, in particular through the principle of data accountability. The author analyzes the advantages of the fiduciary approach, in particular its correlation with the principles of purpose limitation and data minimization enshrined in the EU General Data Protection Regulation, and also considers criticisms of this concept regarding the problem of dual loyalty, incompatibility with advertising business models, and enforcement difficulties. At the same time, alternative approaches to strengthening privacy are explored, including antitrust regulation, functional compatibility, and the environmental analogy of excessive data collection. In conclusion, it is argued that the fiduciary model is not a universal solution to the problem of privacy protection, but it provides a valuable additional legal tool that should be applied in Ukrainian legislation in specific areas where users are particularly vulnerable..

Key words: *fiduciary legal relations, right to privacy, duty of loyalty, informed consent, conflict of interest.*

Право на приватність належить до основоположних прав людини та закріплено у базових міжнародних актах з прав людини, таких як Загальна декларації прав людини [1], Міжнародний пакт про громадянські і політичні права [2] та Європейської конвенції з прав людини [3]. Зазначені акти забезпечують охорону права на приватність через заборону свавільного чи незаконного втручання в особисте і сімейне життя особи, недоторканність житла та таємницю кореспонденції, а Загальна декларація прав людини та Міжнародний пакт про громадянські і політичні права додатково надають захист честі та репутації.

Характерним є також те, що термін «приватність» не має сталого визначення: Європейський суд з прав людини зауважує, що «не вважає можливим або необхідним намагатися дати вичерпне визначення поняття «приватне життя». Однак було б занадто обмежувальним зводити це поняття до «внутрішнього кола», в якому особа може жити своїм особистим життям так, як вона вважає за потрібне, і повністю виключати з нього зовнішній світ, який не охоплюється цим колом. Повага до приватного життя повинна також певною мірою включати право встановлювати і розвивати стосунки з іншими людьми. Крім того, не існує принципових причин, чому таке розуміння поняття «приватне життя» має виключати діяльність професійного або ділового характеру, оскільки, зрештою, саме під час трудової діяльності більшість людей мають значну, якщо не найбільшу» [4].

На доктринальному рівні можна прослідкувати еволюцію розуміння приватності від класичного визначення «право бути залишеним в спокої» [5] до «претензії на контроль над особистою інформацією» [6] або реляційних підходів, де приватність, як писала професор Хелен Ніссенбаум, «не є ні правом на таємницю, ні правом на контроль, а є правом на відповідний потік особистої інформації» в межах певної контекстуальної цілісності [7, с. 127]. Ідея автора полягає в тому, що правомірність передачі інформації визначається соціальним контекстом, в якому вона виникає. Наприклад, передача інформації про пацієнта від одного лікаря іншому відповідає соціальному контексту, якщо потребується медична допомога. Водночас, передача медичної інформації, наприклад, роботодавцю порушує контекст в якому вона створювалась, тобто для лікаря [7, с. 143].

У цифрову епоху право на приватність нерозривно пов'язане з обробкою інформації про особу, зміст і характер якої можуть істотно відрізнятися: від базових ідентифікаційних відомостей (ім'я, прізвище, контактні дані) до даних про пересування, зафіксованих різноманітними GPS-пристроями та іншими трекерами, і чутливих біометричних даних таких як цифрові зображення обличчя, відбитки пальців, секвеновані зразки ДНК тощо.

Сучасна система охорони приватності у цифровому світі концептуально тяжіє до моделі «інформованої згоди». Сучасна система охорони приватності у цифровому світі концептуально тяжіє до моделі «інформованої згоди». Це простежується вже на рівні ключових нормативних актів: згода суб'єкта персональних даних визначена як перша підстава для їх обробки відповідно до статті 11 Закону України «Про захист персональних даних» [8]; Загальний регламент про захист даних ЄС вимагає, щоб така згода «була надана шляхом чіткого ствердного акту, що встановлює вільно надану, конкретну, усвідомлену та однозначну вказівку на згоду суб'єкта даних на обробку персональних даних, що стосуються його або її» [9]; аналогічно, Керівні принципи ОЕСР щодо захисту приватності та транскордонних потоків персональних даних закріплюють знання або згоду як базові засади збирання й обробки такої інформації [10].

Така модель охорони персональних даних піддається обґрунтованій критиці, оскільки більшість користувачів не читає запропоновані умови приватності. Можна назвати декілька причин чому це відбувається: професор Ніссенбаум відзначає, у моделі обґрунтованої згоди є фундаментальний недолік, який полягає у тому, що люди не можуть розуміти всі факти, які стосуються їхнього вибору, під час укладання контрактів зі збирачами (контролерами) даних [11, с. 32], а в одному з досліджень, проведених у Сполучених Штатах Америки, виявили, що якби звичайний користувач інтернету читав кожну політику конфіденційності, з якою він стикається протягом року, то на це пішло б сімдесят шість робочих днів [12, с. 444]. Професор Джек Балкін відзначає такі фактори як: 1) асиметрію інформації на стороні контролерів даних. Вона полягає у тому, що великі цифрові компанії знають багато інформації про своїх користувачів, наприклад, уподобання, антипатії, звички, з ким, коли і скільки особа спілкується, або навіть де і коли переміщується, а натомість користувач не знає контрагентів контролера даних, не знає алгоритмів обробки отриманої інформації і як в результаті вона буде використана; 2) асиметрію влади, яка полягає у тому, що за допомогою особливостей дизайну інтерфейсів контролери даних можуть намагатися монополізувати увагу користувачів; 3) автор відзначає, що контролери даних часто не зацікавлені у тому, щоб користувачі обмежували доступ до своїх персональних даних, а тому можуть зловживати під час розробки інтерфейсів і ховати відповідні налаштування, пов'язані з обмеженням збирання даних про користувача [13, с. 11–12]. Зрештою, в більшості випадків у користувача немає іншого вибору, аніж прийняти умови приватності, запропоновані компанією, оскільки з цим пов'язана можливість користуватися необхідним користувачу сервісом, а цифрові компанії, такі як, наприклад, Apple, Microsoft або Google, є монополістами у своїх сферах надання послуг.

Вказані фактори обумовили необхідність пошуку інших способів взаємодії між збирачем (контролером) даних і користувачем. Помітивши характерну вразливість користувача у відносинах з контролером даних, яка полягає у асиметрії знань, влади та контролю на стороні контролера даних, явне запрошення до довіри (певно ви не знайдете жодного цифрового сервісу, який би не гарантував захисту персональних даних користувача), нездатність користувача, як слабшої сторони, здійснювати контроль або моніторинг за діяльністю контролера даних, деякі науковці відзначили схожість цих правовідносин із фідуціарними [13, с. 13–14]. Професор Тамар Франкель описувала фідуціарні як ті, що мають такі характерні ознаки: 1) фідуціари пропонують переважно послуги, а не товари. Такі послуги, зазвичай, є соціально бажаними і часто вимагають екс-

пертизи та знань. Наприклад, лікування, юридичні послуги, викладання, управління активами, корпоративне управління та релігійні послуги; 2) надання фідуціарних послуг вимагає передачі майна або повноважень; 3) передача майна або повноважень створює для довірителів ризик того, що фідуціари будуть зловживати довірою. Наприклад, фідуціар може привласнити передане йому майно або зловживати наділеною владою, або ж не надавати обіцяних послуг належним чином; 4) існує ймовірність того, що (а) довіритель самостійно не зможе захистити себе від ризиків, пов'язаних з фідуціарними відносинами; (б) ринки можуть бути не в змозі захистити довірителів від зазначених ризиків; і що (в) витрати за здійсненням моніторингу або контролю за діяльністю фідуціаріїв можуть бути для бенефіціарів вищими, ніж вигоди від цих відносин [14, с. 6]. Із вказаного опису ознак фідуціарних відносин можна дійти висновку, що цифрові компанії не є класичними фідуціарами, насамперед, тому, що це не спеціалісти у певній галузі (наприклад, лікарі або юристи), однак і спільних ознак достатньо: цифрові компанії здебільшого надають послуги, користувач наділяє їх правом збирати інформацію про себе як необхідну умову для надання послуг або покращення їх якості. Через описані вище вразливості користувача у контролера даних є можливість зловживати довірою, і відповідні персональні дані можуть використовуватися не за призначенням[1] або не в інтересах користувача (наприклад, таргетування незаконної реклами, зокрема онлайн казино). Таким чином, цифрові компанії – контролери даних дійсно мають більшість ознак фідуціаріїв.

Поширення на контролерів даних режиму фідуціарних відносин обумовлює застосування фідуціарних обов'язків, серед яких виокремлюють обов'язки лояльності, дбайливості і конфіденційності. Професор Джек Балкін зауважує, що обов'язки дбайливості і конфіденційності покликані забезпечити конфіденційність і безпеку персональних даних користувачів, а особливість полягає у тому, що ці фідуціарні обов'язки повинні слідувати за даними («run with the data»): контролери даних повинні перевіряти своїх партнерів, яким вони передають зібрані персональні дані, щоб переконатися в їх етичності та надійності, а також піддавати їх регулярним перевіркам, і у випадку виявлення порушень – вжити заході для повернення даних. Обов'язок лояльності, на думку автора, означає, що контролери даних не повинні «маніпулювати кінцевими користувачами або зраджувати їхню довіру». Вони повинні діяти в інтересах користувачів, чиї дані вони збирають, і розробляти інформаційні платформи таким чином, щоб уникнути конфлікту інтересів зі своїми кінцевими користувачами. Як приклад наводиться обов'язок уникати практик заохочення до адиктивної поведінки [13, с. 14], а також експеримент Facebook з емоційного зараження (Facebook emotional contagion experiment), який полягав у тому, що дослідники маніпулювали стрічкою новин Facebook, показуючи менше позитивних постів деяким категоріям користувачів, щоб перевірити, чи призведе це до більшого вираження смутку [12, с. 470]. Ще одним прикладом порушення обов'язку лояльності є показ сервісом для бронювання готелів Orbitz більш дорогих номерів користувачам, які заходять на сайт через комп'ютери компанії Apple, через припущення про їх більшу платоспроможність [12, с. 470].

Фідуціарний підхід до регулювання приватності у цифрову епоху має низку як переваг, так і недоліків. До переваг можна віднести більш адекватне регулювання з огляду на те, що наявність нерівних за статусом учасників є однією із характерних рис фідуціарних відносин. За допомогою цього підходу можливо подолати «ілюзію» «інформованої згоди», оскільки користувачі або не читають відповідні умови приватності, або не можуть їх зрозуміти через склад-

[1] У статті 2 Закону України «Про захист персональних даних» [8] зазначається, що персональні дані збираються відповідно до сформульованої мети їх обробки, а у статті 5 Загального регламенту про захист даних ЄС [9] визначено, що одним із принципів обробки персональних даних є обмеження за метою, яке полягає у тому, що дані, зібрані для визначених, чітких і законних цілей (мети), не повинні обробляються в подальшому у спосіб, несумісний з такими цілями.

ність або значний обсяг, або не мають можливості не надати згоду, оскільки постачальник послуг є монополістом. Крім того, фідуціарна модель переносить відповідальність з ex ante (контролеру потрібно отримати згоду користувача до початку обробки персональних даних) на ex post (обов'язок контролера даних діяти в інтересах користувача не залежить від згоди на обробку персональних даних). Обов'язок лояльності має два аспекти: заборону діяти в умовах конфлікту інтересів, а також збагачуватися за рахунок бенефіціара, якщо на це відсутня безпосередня згода. Збір більшої кількості інформації контролером даних, ніж йому потрібно для цілей надання послуг, з метою подальшої агрегації та продажу третім особам (наприклад, для цілей таргетування реклами або профілювання інтересів особи) вже буде означати, що контролер даних діє в умовах конфлікту інтересів. В цьому сенсі фідуціарна лояльність корелює із закріпленими у статті 5 Загального регламенту про захист даних ЄС [9] принципами «обмеження мети» (зібрані для певної мети персональні дані не підлягають обробці для інших цілей) та «мінімізації даних» (обробка персональних даних має бути адекватною, релевантною та обмеженою лише тим, що є необхідним для мети, для яких вони обробляються). Продаж «надлишкових» персональних даних контролером даних також втратив би сенс, оскільки обов'язок лояльності передбачає заборону на збагачення контролера даних за рахунок користувача, якщо останній не надав прямої згоди на інше. Фідуціарне право дозволить формувати поведінкові стандарти для цифрових компаній: наприклад, логічним наслідком заборони конфлікту інтересів є унеможливлення надмірного витрачання коштів користувачами онлайн казино за певний період часу, оскільки надмірні витрати також перебуватимуть в конфлікті з інтересами користувача.

Слід відзначити, що фідуціарна концепція приватності піддається критиці: відзначається проблема «подвійної» лояльності, оскільки директора вже мають обов'язки лояльності перед акціонерами цифрових компаній, фідуціарна модель приватності не є сумісною із бізнес-моделями компаній, які заробляють на таргетованій рекламі (наприклад, Facebook), проблеми правозастосування, пов'язані з великою чисельністю користувачів, яким потенційно можуть надати право на позов [15, с. 503, 521, 524–525]. Крім того, автори критики пропонують альтернативні способи посилення приватності, а саме: розглядати великі цифрові компанії як платформи суспільної телекомунікаційної інфраструктури та впливати на них безпосередньо, активно застосовувати антимонопольні заходи, створення конкуренції та альтернативи цифровим гігантам через запровадження функціональної сумісності, що дозволить користувач змінити надавача послуг, введення прямих заборон на певні джерела прибутку, також пропонується відійти від приватних механізмів захисту приватності і розглядати надмірний збір та обробку персональних даних за аналогією як екологічне забруднення, а відтак необхідним є запровадження відповідальності за масові «витоки» інформації з цифрових компаній, введення податку Пігу (коригувальний податок на діяльність, яка створює негативні зовнішні ефекти) за збирання персональних даних, пряма заборона примусової агрегації даних за прикладом німецького Федерального антимонопольного відомства, яке постановило, що «Facebook більше не буде дозволено змушувати своїх користувачів погоджуватися на практично необмежений збір і присвоєння даних, що не належать Facebook [отриманих із сторонніх джерел], їхнім обліковим записам у Facebook» [15, с. 538–540].

Отже, гострота дискусії та різноманіття підходів, починаючи від приватноправових і закінчуючи публічно-правовими (податки, заборони, антимонопольне законодавство), свідчить про те, що забезпечення права на приватність у цифрову епоху є комплексною задачею. Застосування юридичної конструкції фідуціарних правовідносин до права на приватність не є однозначним вирішенням цієї проблеми. Натомість це надає додатковий правовий інструментарій, який враховує характерну нерівність правового положення та інфор-

маційну асиметрію контролера даних та користувача, яка також характерна для фідуціарних відносин. Більш того, використання цього інструментарію вже має місце у принципах Загального регламенту про захист даних ЄС, і до положень якого буде адаптуватися українське законодавство у сфері захисту персональних даних. Це дискусійне питання чи потрібна імплементація фідуціарних відносин в регулювання права на приватність в українське законодавство, оскільки цей правовий механізм більше притаманний країнам загального права, хоча в останні декілька років знайшов значне поширення і в корпоративному праві. Проте видається, що існують окремі сфери суспільного життя, такі як, наприклад, онлайн гемблінг або соціальні мережі з агресивними маркетинговими політиками, в яких доцільно було б запровадити обов'язок лояльності по відношенню до користувача. Це дало б можливість застосовувати правило про відсутність конфлікту інтересів і на підставі цього виробити якісно нові політики (наприклад, заборона алгоритмів, які відстежують поведінку та розклад гравця та направляють повідомлення, що спонукають його більше грати) по відношенню до застосунків та цифрових платформ у тих випадках, коли користувач є особливо вразливим.

ЛІТЕРАТУРА:

1. Загальна декларація прав людини: прийнята і проголошена резолюцією 217 А (III) Генеральної Асамблеї ООН від 10.12.1948. URL: https://zakon.rada.gov.ua/laws/show/995_015#Text (дата звернення: 24.02.2026).

2. Міжнародний пакт про громадянські і політичні права: прийнято резолюцією 2200 А (XXI) Генеральної Асамблеї ООН від 16.12.1966. URL: https://zakon.rada.gov.ua/laws/show/995_043 (дата звернення: 24.02.2026).

3. Конвенція про захист прав людини і основоположних свобод: прийнята в Римі 04.11.1950. URL: https://zakon.rada.gov.ua/laws/show/995_004 (дата звернення: 24.02.2026).

4. Рішення Європейського суду з прав людини у справі «NIEMIETZ v. GERMANY» (заява № 13710/88) від 16.12.1992. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57887%22]} (дата звернення: 24.02.2026).

5. Warren S. D., Brandeis L. D. The Right to Privacy. *Harvard Law Review*. 1890. Vol. 4, No. 5. C. 193–220. URL: https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html (дата звернення: 24.02.2026).

6. Austin L. M. Rereading Westin. *Theoretical Inquiries in Law*. 2019. Vol. 20. No. 1. P. 53–81. DOI: https://doi.org/10.1515/til-2019-0003. URL: https://ssrn.com/abstract=3290887 (дата звернення: 24.02.2026).

7. Nissenbaum H. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford : Stanford University Press, 2010. 304 с.

8. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 24.02.2026).

9. 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/eli/reg/2016/679/oj/eng (дата звернення: 24.02.2026).

10. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Paris: OECD Publishing, 2002. URL: https://doi.org/10.1787/9789264196391-en (дата звернення: 24.02.2026).

11. Nissenbaum H. A Contextual Approach to Privacy Online. *Daedalus*. 2011. Vol. 140, No. 4. P. 32–48. URL: https://doi.org/10.1162/DAED_a_00113 (дата звернення: 25.02.2026).

12. Richards N. M., Hartzog W. Taking Trust Seriously in Privacy Law. *Stanford Technology Law Review*. 2016. Vol. 19. C. 431–472. URL: https://ssrn.com/abstract=2655719 (дата звернення: 25.02.2026).

13. Balkin J. M. The Fiduciary Model of Privacy. *Harvard Law Review Forum*. 2020. Vol. 134. C. 11–33. URL: https://harvardlawreview.org/wp-content/uploads/2020/10/134-Harv.-L.-Rev.-F.-11.pdf (дата звернення: 25.02.2026).

14. Frankel T. Fiduciary law. New York: Oxford University Press, 2011. 332 c.

15. Khan L. M., Pozen D. A skeptical view of information fiduciaries. *Harvard Law Review*. 2019. Vol. 133. C. 497–541

Дата першого надходження статті до видання: 26.02.2026
Дата прийняття статті до друку після рецензування: 23.03.2026
Дата публікації (оприлюднення) статті: 08.05.2026