

УДК 340.12:342.7:004.738.5

DOI <https://doi.org/10.32844/2618-1258.2026.3.14>

ДЯКОВСЬКИЙ О.С., ГАБРЕЛЯН А.Ю., ДУТОВА К.В.

ПРАВО НА ЗАБУТТЯ В ІНТЕРНЕТІ В УМОВАХ ЦИФРОВОЇ ТІНЬОВОЇ ЕКОНОМІКИ: ЗМІСТ, МЕЖІ РЕАЛІЗАЦІЇ ТА РИЗИКИ ЗЛОВЖИВАННЯ

THE RIGHT TO BE FORGOTTEN ON THE INTERNET IN THE CONTEXT OF THE DIGITAL SHADOW ECONOMY: CONTENT, LIMITS OF IMPLEMENTATION AND RISKS OF ABUSE

Стаття присвячена дослідженню змісту, меж реалізації та ризиків зловживання правом на забуття в Інтернеті в умовах цифрової тіньової економіки. Мета роботи – розкрити правову природу права на забуття, визначити підстави його застосування та обґрунтувати критерії балансування між захистом приватного життя особи, свободою вираження поглядів, доступом до інформації та суспільним інтересом. З'ясовано, що право на забуття не може розглядатися як безумовне право на видалення будь-якої небажаної інформації. Його зміст полягає у пропорційному обмеженні цифрової доступності персональних даних у випадках, коли їх подальше поширення втратило легітимну мету або непропорційно втручається у приватне життя особи.

Зазначено, що в умовах цифрової тіньової економіки право на забуття має подвійне значення. З одного боку, воно може бути засобом протидії незаконному обігу персональних даних, їх несанкціонованому агрегуванню, повторному використанню, комерційній експлуатації та репутаційному тиску. З іншого боку, це право може створювати ризики зловживання, якщо використовується для приховування відомостей про недобросовісну підприємницьку діяльність, фінансові порушення, шахрайство, корупційні ризики або інші факти, важливі для громадського контролю й економічної безпеки.

Наголошено, що чинне українське законодавство містить лише фрагментарні підстави для захисту особи від надмірної цифрової доступності персональних даних. Конституція України та Закон України «Про захист персональних даних» створюють загальну нормативну основу такого захисту, однак не формують повноцінного механізму реалізації права на забуття. Обґрунтовано доцільність закріплення процедури деіндексації, критеріїв оцінки втрати інформацією актуальності, обов'язків інтернет-посередників і пропорційних способів захисту. Найбільш збалансовано визначено модель, за якої повне видалення застосовується щодо незаконно оброблених або недостовірних даних, а щодо законно оприлюдненої, але застарілої інформації перевага надається деіндексації, знеособленню, обмеженню пошукової доступності або доповненню матеріалу актуальним контекстом.

Ключові слова: *персональні дані, деіндексація, цифрова приватність, цифровий слід, обіг персональних даних, захист приватного життя, свобода інформації, публічний інтерес, пошукові системи, незаконний обіг даних.*

© ДЯКОВСЬКИЙ О.С. – кандидат юридичних наук, старший викладач кафедри інформаційного, господарського та адміністративного права (Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського») <https://orcid.org/0000-0003-3412-9278>

© ГАБРЕЛЯН А.Ю. – доктор філософії в галузі права <https://orcid.org/0000-0001-9337-7920>

© ДУТОВА К.В. – студентка 3 курсу факультету соціології і права (Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського») <https://orcid.org/0009-0003-1184-716X>

Стаття поширюється на умовах ліцензії відкритого доступу (CC BY 4.0)



The article is devoted to the study of the content, limits of implementation, and risks of abuse of the right to be forgotten on the Internet in the context of the digital shadow economy. The purpose of the article is to reveal the legal nature of the right to be forgotten, determine the grounds for its application, and substantiate the criteria for balancing the protection of a person's private life, freedom of expression, access to information, and the public interest. It is established that the right to be forgotten cannot be regarded as an unconditional right to remove any unwanted information. Its content lies in the proportional restriction of the digital accessibility of personal data in cases where their further dissemination has lost its legitimate purpose or disproportionately interferes with a person's private life.

It is noted that in the context of the digital shadow economy, the right to be forgotten has a dual significance. On the one hand, it may serve as a means of counteracting the illegal circulation of personal data, their unauthorized aggregation, repeated use, commercial exploitation, and reputational pressure. On the other hand, this right may create risks of abuse if it is used to conceal information about unfair business practices, financial violations, fraud, corruption risks, or other facts important for public oversight and economic security.

It is emphasized that current Ukrainian legislation contains only fragmentary grounds for protecting a person from excessive digital accessibility of personal data. The Constitution of Ukraine and the Law of Ukraine "On Personal Data Protection" create a general regulatory framework for such protection, but do not establish a comprehensive mechanism for implementing the right to be forgotten. The article substantiates the need to introduce de-indexing procedures, criteria for assessing the loss of relevance of information, obligations of Internet intermediaries, and proportional means of protection. The most balanced model is considered to be one under which complete removal applies to unlawfully processed or inaccurate data, while, in relation to lawfully published but outdated information, preference is given to de-indexing, anonymization, restriction of search accessibility, or supplementing the material with updated context.

Key words: *personal data, de-indexing, digital privacy, digital footprint, circulation of personal data, protection of private life, freedom of information, public interest, search engines, unlawful circulation of data.*

Вступ. Цифровізація суспільства та загальнодоступність мережі Інтернет істотно змінили характер існування інформації про людину. Відомості, які раніше поступово втрачали актуальність через обмеженість паперових архівів, локальність поширення або природне забування, сьогодні можуть зберігатися необмежено довго і залишатися доступними через пошукові системи впродовж тривалого часу. Унаслідок цього навіть достовірні й законно оприлюднені інформації здатні завдавати шкоди репутації, працевлаштуванню, соціальним зв'язкам і приватному життю особи після того, як обставини її появи втратили первісне суспільне значення.

Ця проблема не зводиться лише до конфлікту між приватністю особи та свободою інформації. У цифровому середовищі персональні дані набули самостійної економічної цінності: вони збираються, зберігаються, аналізуються, поєднуються з іншими масивами інформації та використовуються для прийняття рішень у сфері зайнятості, кредитування, страхування, реклами, довірливих відносин і ділової репутації. Поряд із легальним обігом персональних даних формуються і тіньовий сегмент такого обігу, пов'язаний із несанкціонованим копіюванням, продажем, агрегуванням, поширенням та повторним використанням інформації про людину без її згоди або поза межами первісної мети обробки [2; 4].

За таких умов право на забуття набуває особливого значення. Воно може захищати людину не тільки від надмірної влади цифрової пам'яті, а й від подальшого використання її персональних даних у тіньовому інформаційному обігу. Йдеться про ситуації, коли застарілі, надмірні або вирвані з контексту відомості використовуються для репутаційного тиску, недобросовісної конкуренції, шахрайства, маніпуляцій або комерційної експлуатації цифрового сліду особи.

Однак право на забуття не може розглядатися як безумовне право на очищення цифрової репутації. У певних випадках вимоги про видалення, деіндексацію або знеособлення інформації можуть використовуватися не для захисту приватного життя, а для приховування відомостей, що мають значення для суспільства. Насамперед йдеться про інформацію щодо недобросовісної підприємницької діяльності, фінансових зловживань, корупційних практик, шахрайства, порушення

прав споживачів або інших фактів, важливих для громадського контролю, економічної безпеки та добросовісності ринкового обігу [3].

Наявні правові механізми захисту честі, гідності, ділової репутації та персональних даних не завжди є достатніми для розв'язання цієї проблеми. Традиційні способи захисту переважно зорієнтовані на недостовірну, незаконно поширену або неправомірно оброблену інформацію. Натомість право на забуття часто стосується іншої ситуації: інформація може бути достовірною, законно оприлюдненою та суспільно допустимою на момент публікації, але з часом втратити актуальність, стати надмірною або такою, подальша доступність якої непропорційно втручається у приватне життя особи.

В Україні право на забуття залишається радше похідною правовою конструкцією, ніж окремим і процедурно врегульованим інститутом. Його окремі елементи можуть бути виведені з положень Конституції України від 28.06.1996 р. № 254к/96-ВР [8], Закону України «Про захист персональних даних» від 01.06.2010 р. № 2297-VI [9] та європейських стандартів захисту приватності. Разом із тим національне законодавство не містить спеціальної процедури деіндексації, чітких критеріїв оцінки застарілої інформації, правил звернення до пошукових систем або інших інтернет-посередників, а також усталеного механізму балансування між правом особи на приватність, свободою інформації та необхідністю недопущення зловживань у цифровому середовищі.

Питання змісту, правової природи та меж реалізації права на забуття досліджувалися у працях В.С. Батиргарєєвої, Д.М. Белова, М.В. Белової, О.Т. Горнило, О.М. Калітенко, О.В. Кіріяк, Ю.Ю. Ремінської, Д.І. Садовської, О.В. Совгирі, С.П. Телешева, В.О. Токаревої, Р.Б. Тополевського, Д.І. Фірман, О.С. Яворської та інших авторів. У науковій літературі основна увага приділяється визначенню поняття права на забуття, його співвідношенню з правом на приватність, захистом персональних даних, свободою вираження поглядів і доступом до інформації, а також аналізу практики Суду ЄС та ЄСПЛ. Разом із тим менш розробленим залишається питання реалізації права на забуття в умовах цифрової тіньової економіки, зокрема у зв'язку з незаконним обігом персональних даних, репутаційним тиском, комерційним використанням цифрового сліду особи та ризиками зловживання цим правом для приховування суспільно значущої інформації.

Постановка завдання. Метою статті є дослідження змісту права на забуття в Інтернеті, визначення підстав і меж його реалізації з урахуванням GDPR, практики Суду ЄС та ЄСПЛ, а також з'ясування його значення для захисту персональних даних в умовах цифрової тіньової економіки.

Результати дослідження. Право на забуття доцільно розглядати в контексті трансформації класичних механізмів захисту приватного життя під впливом цифрового середовища. На відміну від традиційного інформаційного обігу, Інтернет забезпечує тривале, швидке й масове відтворення персональних даних, унаслідок чого навіть правомірно оприлюднена інформація з часом може набути надмірного впливу на особу. Саме ця обставина зумовлює потребу у виокремленні права на забуття як особливого способу обмеження доступності персональної інформації. Таке право не слід отожденовати із загальним правом на спростування недостовірної інформації. Його особливість полягає в тому, що воно часто стосується даних, які на момент оприлюднення були правдивими, законними й суспільно допустимими, однак згодом втратили актуальність або стали надмірно доступними. Тому йдеться не про «знищення минулого», а про обмеження необґрунтованої цифрової доступності інформації, яка вже не виконує легітимної інформаційної функції та непропорційно впливає на приватне життя особи.

У науковій літературі право на забуття переважно аналізується не як ізольована правова вимога, а як інструмент пошуку балансу між різними інформаційними інтересами. Так, О.М. Калітенко звертає увагу на те, що це право формується на перетині двох особистих немайнових прав: з одного боку, права на інформацію, що передбачає вільний доступ до неї, її відкритість і недопустимість необґрунтованих обмежень, а з іншого – права фізичної особи на приватність, повагу до приватного й сімейного життя та захист персональних даних [6, с. 60]. Такий підхід дає змогу уникнути спрощеного розуміння права на забуття як механічного видалення небажаних відомостей. У кожному випадку необхідно з'ясувати, чи зберігається актуальний публічний інтерес до інформації та чи не буде обмеження доступу до неї непропорційним втручанням у свободу вираження поглядів.

Разом із тим сучасне цифрове середовище надає цій проблемі ще один вимір. Персональні дані стали не лише елементом приватного життя, а й економічно цінним ресурсом. Вони використовуються для профілювання, реклами, оцінки поведінки особи, формування цифрової репутації, а також прийняття рішень, що можуть мати прямі майнові або професійні наслідки.

У легальному секторі така обробка може мати правомірну мету. Проте в тіньовому інформаційному обігу вона часто здійснюється без належної правової підстави, поза контролем суб'єкта даних і без зв'язку з початковою метою їх збирання.

У цьому контексті право на забуття виконує не лише індивідуально-захисну, а й превентивну функцію. Воно дає змогу зменшити ризик подальшого використання персональних даних у незаконному або непрозорому інформаційному обігу. Деіндексація, знеособлення або обмеження пошукової доступності не завжди усувають сам матеріал, але можуть істотно зменшити можливість його автоматичного пошуку, копіювання, комерційного використання або застосування як засобу репутаційного тиску.

Важливим етапом становлення права на забуття стало рішення Суду Європейського Союзу у справі C-131/12 «Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González» від 13 травня 2014 року [12]. Справа була пов'язана з вимогою громадянина Іспанії вилучити з результатів пошуку за його іменем посилання на газетні публікації про давній аукціонний продаж нерухомості у зв'язку із заборгованістю. Матеріали не були неправдивими або незаконно опублікованими, однак заявник вважав, що після врегулювання боргу їх подальша доступність через пошукову систему втратила актуальність. Суд Європейського Союзу визнав, що оператор пошукової системи здійснює обробку персональних даних і за певних умов зобов'язаний вилучити посилання з результатів пошуку за іменем особи, навіть якщо сам матеріал залишається на первинному вебсайті законно.

Значення цієї справи полягає в тому, що було розмежовано видалення відомостей із першоджерела та деіндексацію результатів пошуку. У багатьох випадках право на забуття не потребує знищення первинного матеріалу, особливо якщо він має архівну, журналістську або суспільну цінність. Натомість може йтися про обмеження автоматичного зв'язку між іменем людини та застарілими відомостями у пошуковій видачі. Такий спосіб захисту є більш пропорційним: він не ліквідує сам матеріал, але зменшує інтенсивність його впливу на приватне життя особи.

Справа C-131/12 важлива також для розуміння економічного виміру права на забуття. Пошукова система не створювала первинний матеріал, однак саме вона забезпечувала його постійну доступність, індексацію та прив'язку до імені особи. У цифровому середовищі така індексація фактично формує публічний інформаційний профіль людини. Цей профіль може враховуватися роботодавцями, контрагентами, кредиторами, страховими компаніями, іншими учасниками ринку або недобросовісними суб'єктами. Тому деіндексація в окремих випадках може бути способом не тільки захисту приватності, а й зменшення ризику подальшого використання застарілої інформації як інструменту економічного або репутаційного тиску.

Право на забуття отримало нормативне закріплення у Регламенті Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (General Data Protection Regulation, GDPR) [10]. Ст. 17 GDPR має назву «Право на стирання ("право бути забутим)»». Відповідно до ст. 17(1) GDPR, суб'єкт даних повинен мати право на стирання своїх персональних даних, яке повинен здійснити контролер без будь-якої безпідставної затримки. Контролер, зі свого боку, зобов'язаний стерти персональні дані без будь-якої необгрунтованої затримки за наявності визначених у цій статті підстав: якщо немає більше потреби в персональних даних для цілей, для яких їх збирали чи іншим чином опрацьовували; якщо суб'єкт даних відкликає згоду, на якій ґрунтується опрацювання, та немає іншої законної підстави для опрацювання; якщо суб'єкт даних заперечує проти опрацювання згідно зі ст. 21(1) і немає жодних першочергових законних підстав для опрацювання; якщо персональні дані опрацьовували незаконно; якщо персональні дані необхідно стерти для дотримання встановленого законом зобов'язання; або якщо персональні дані збирали у зв'язку з пропонуванням послуг інформаційного суспільства, вказаних у ст. 8(1) GDPR.

Однак ст. 17 GDPR не встановлює абсолютного права на стирання будь-якої інформації. Відповідно до ст. 17(3), параграфи 1 та 2 не застосовують залежно від ступеня необхідності в опрацюванні, зокрема для реалізації права на свободу виразу поглядів та свободу інформації; для дотримання встановленого законом зобов'язання або виконання завдання в суспільних інтересах; на підставах суспільного інтересу у сфері охорони суспільного здоров'я; для досягнення цілей суспільних інтересів, цілей наукового чи історичного дослідження або статистичних цілей; а також для формування, здійснення або захисту правових претензій [10]. Отже, навіть у праві Європейського Союзу право на забуття має відносний характер і реалізується через балансування приватного інтересу особи та легітимних інтересів суспільства.

Ці винятки мають особливе значення для запобігання зловживанню правом на забуття. Якщо вимога про видалення або деіндексацію спрямована на усунення інформації, яка має значення для свободи вираження поглядів, громадського контролю, захисту прав інших осіб або встановлення правових вимог, вона не може задовольнятися автоматично. У контексті цифрової тіньової економіки це означає, що відомості про недобросовісну підприємницьку діяльність, фінансові порушення, шахрайські практики, корупційні ризики або систематичне порушення прав споживачів не повинні вилучатися з публічного доступу лише тому, що вони є небажаними для особи, якої стосуються.

Подальша конкретизація критеріїв деіндексації відбулася у рішенні Суду Європейського Союзу від 24 вересня 2019 року у справі C-136/17 «GC and Others v Commission nationale de l'informatique et des libertés (CNIL)». Предметом розгляду було питання деіндексації посилань, що містили особливі категорії персональних даних та інформацію про кримінальні провадження. Суд наголосив, що при розгляді таких запитів оператор пошукової системи має враховувати підвищену чутливість відповідних даних, положення статей 9 і 10 GDPR, а також баланс між правами особи на приватність і захист персональних даних та правом користувачів Інтернету на доступ до інформації [13]. Це рішення деталізувало загальну логіку, сформульовану у рішенні у справі C-131/12: чим чутливішими є дані й чим слабшим є актуальний публічний інтерес, тим вагомішими стають підстави для деіндексації.

Разом із тим відомості про кримінальне провадження, фінансові порушення чи інші правопорушення не можуть автоматично вважатися такими, що мають залишатися необмежено доступними за будь-яких умов. Вирішальним є не формальне віднесення відомостей до певної категорії, а сукупність обставин: час, що минув після події, результат відповідного провадження, статус особи, ступінь її публічності, характер правопорушення, наявність повторюваної поведінки та актуальний суспільний інтерес. Якщо подія давно втратила суспільне значення, особа не є публічною особою, а подальша доступність інформації створює непропорційне втручання у приватне життя, деіндексація може бути виправданою. Якщо ж відомості залишаються важливими для захисту прав інших осіб, запобігання шахрайству або виявлення тіньових економічних практик, приватний інтерес заявника не може безумовно переважати над публічним інтересом у доступі до такої інформації.

Юрисдикційний вимір права на забуття був конкретизований у рішенні Суду Європейського Союзу від 24 вересня 2019 року у справі C-507/17 «Google LLC v Commission nationale de l'informatique et des libertés (CNIL)». У цій справі Суд розглянув питання про територіальний обсяг обов'язку оператора пошукової системи щодо деіндексації. Суд дійшов висновку, що право Європейського Союзу не зобов'язує такого оператора вилучати посилання в усіх версіях пошукової системи у світі. Водночас оператор має забезпечити ефективне вилучення посилань у межах Європейського Союзу та застосувати заходи, які ускладнюють або стримують доступ користувачів з ЄС до відповідних результатів пошуку через інші версії пошукової системи [14]. Такий підхід засвідчує, що цифрове середовище має глобальний характер, однак юридичні механізми захисту права на забуття залишаються пов'язаними з конкретним правопорядком.

Територіальні межі права на забуття мають практичне значення у зв'язку з транснаціональним характером тіньового обігу персональних даних. Такі дані можуть незаконно збиратися в одній державі, зберігатися на серверах в іншій, поширюватися через платформи третьої юрисдикції, а також використовуватися особами, яких складно ідентифікувати. За таких умов навіть обґрунтоване рішення про видалення або деіндексацію інформації не завжди забезпечує повне відновлення контролю особи над своїми даними. Це свідчить про необхідність поєднання матеріально-правового закріплення права на забуття з реальними процедурними та технічними механізмами його виконання.

У практиці застосування Конвенції право на забуття прямо не закріплено як самостійний інститут. Воно розглядається через призму ст. 8 Конвенції про захист прав людини і основоположних свобод від 04.11.1950 року, яка гарантує право на повагу до приватного і сімейного життя, а також у співвідношенні зі ст. 10 Конвенції, що захищає свободу вираження поглядів [7]. Така конструкція означає, що Європейський суд з прав людини не визнає автоматичного пріоритету приватності над свободою слова або навпаки. Кожна справа потребує оцінки характеру інформації, статусу особи, часу, що минув після події, ступеня поширення матеріалу, реальної шкоди для приватного життя та наявності актуального суспільного інтересу.

Для розуміння підходу ЄСПЛ важливою є справа «Węgrzynowski and Smolczewski v. Poland» від 16 липня 2013 року (заява № 33846/07). Заявники вимагали видалення з онлайн-архіву

газети статті, яка, на їхню думку, завдавала шкоди їхній репутації. Європейський суд з прав людини не поклав на державу обов'язку забезпечити видалення матеріалу з архіву, підкресливши значення електронних архівів для свободи преси та доступу суспільства до інформації [11]. Разом із тим із цієї справи випливає, що онлайн-архіви не є повністю виведеними з-під дії ст. 8 Конвенції: якщо подальше поширення матеріалу непропорційно втручається у приватне життя особи, держава має забезпечити ефективний механізм оцінки відповідного конфлікту прав.

Більш чітко критерії такого балансування були сформульовані у справі «Hurbain v. Belgium», вирішеній Великою палатою Європейського суду з прав людини 4 липня 2023 року (заява № 57292/16). Справа стосувалася власника газети «Le Soir», якого національні суди зобов'язали знеособити ім'я особи в давній статті про дорожньо-транспортну пригоду, розміщеній в електронному архіві. ЄСПЛ не встановив порушення ст. 10 Конвенції, оскільки національні суди застосували пропорційний захід: не вилучили матеріал повністю, а обмежили ідентифікацію приватної особи в онлайн-версії. Суд врахував давність події, відсутність актуального суспільного інтересу до імені особи, її непублічний статус і непропорційний вплив доступності матеріалу через пошук [15].

Практика Європейського суду з прав людини свідчить, що право на забуття в європейському правовому просторі не спрямоване на переписування історії або знищення архівів. Його мета полягає у зменшенні непропорційної шкоди, яка виникає через постійну й легку доступність застарілої інформації в цифровому середовищі. Тому перевагу часто слід надавати не радикальним заходам у вигляді повного видалення матеріалу, а більш м'яким способам захисту: деіндексації, знеособленню, обмеженню пошукової доступності, оновленню контексту або доповненню архівної публікації інформацією про подальший розвиток подій.

Пропорційність способу захисту має ключове значення і для запобігання зловживанню правом на забуття. Якщо проблема полягає лише в тому, що застаріла інформація автоматично з'являється у пошуковій видачі за іменем особи, повне видалення матеріалу може бути надмірним. Деіндексація або знеособлення здатні досягти балансу між захистом приватності та збереженням архівної чи суспільної цінності інформації. Якщо ж матеріал містить відомості, важливі для оцінки ділової репутації особи, прозорості підприємницької діяльності, захисту прав кредиторів, споживачів або інших учасників правовідносин, навіть м'які форми обмеження доступу мають застосовуватися з урахуванням публічного інтересу.

Національне законодавство України формує лише фрагментарну нормативну основу для захисту особи від надмірної або невиннованої доступності персональної інформації в цифровому середовищі. Йдеться не про спеціально врегульований інститут права на забуття, а про сукупність конституційних і галузевих положень, які можуть бути використані для захисту приватності, персональних даних та репутаційних інтересів особи. Базове значення у цьому контексті має ст. 32 Конституції України. Вона встановлює, що ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Стаття також забороняє збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. Ця ж стаття гарантує кожному громадянину право знайомитися в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе, які не є державною або іншою захищеною законом таємницею. Вона також передбачає судовий захист права спростовувати недостовірну інформацію про себе і членів своєї сім'ї та права вимагати вилучення будь-якої інформації [8]. Водночас зазначена конституційна норма не створює спеціальної процедури деіндексації, не визначає критеріїв оцінки достовірної, але застарілої інформації, і не встановлює порядку звернення до пошукових систем чи інших інтернет-посередників.

Галузеву основу такого захисту становлять положення Закону України «Про захист персональних даних». Зокрема, п. 5 ч. 2 ст. 8 надає суб'єкту персональних даних право пред'являти вмотивовану вимогу володільцю персональних даних із запереченням проти обробки своїх персональних даних. П. 6 ч. 2 цієї ж статті передбачає право пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних будь-яким володільцем та розпорядником персональних даних, якщо ці дані обробляються незаконно чи є недостовірними. Крім того, відповідно до п. 8 ч. 2 ст. 8, суб'єкт персональних даних має право звертатися із скаргами на обробку своїх персональних даних до Уповноваженого або до суду [9].

Окреме значення має ст. 15 Закону України «Про захист персональних даних», яка регулює видалення або знищення персональних даних. Відповідно до ч. 1 цієї статті, персональні

дані видаляються або знищуються в порядку, встановленому відповідно до вимог закону. Ч. 2 ст. 15 передбачає, що персональні дані підлягають видаленню або знищенню у разі: закінчення строку зберігання даних, визначеного згодою суб'єкта персональних даних на обробку цих даних або законом; припинення правовідносин між суб'єктом персональних даних та володільцем чи розпорядником, якщо інше не передбачено законом; видання відповідного припису Уповноваженого або визначених ним посадових осіб секретаріату Уповноваженого; набрання законної сили рішенням суду щодо видалення або знищення персональних даних [9]. Крім того, персональні дані, зібрані з порушенням вимог цього Закону, підлягають видаленню або знищенню у встановленому законодавством порядку.

Процедурний аспект відповідного захисту розкриває ст. 21 Закону України «Про захист персональних даних». Її ч. 3 встановлює, що про зміну, видалення чи знищення персональних даних або обмеження доступу до них володільць персональних даних протягом десяти робочих днів повідомляє суб'єкта персональних даних, а також суб'єктів відносин, пов'язаних із персональними даними, яким ці дані було передано [9]. Це положення важливе для цифрового середовища, оскільки воно допускає не лише видалення чи знищення персональних даних, а й обмеження доступу до них. Однак Закон не конкретизує механізм деіндексації результатів пошуку, не визначає статус оператора пошукової системи як адресата відповідної вимоги та не встановлює спеціальних критеріїв балансування між приватністю особи, свободою інформації та публічним інтересом.

Отже, чинне українське законодавство створює окремі правові підстави для зміни, видалення, знищення персональних даних або обмеження доступу до них, однак не відтворює зміст і процедуру ст. 17 GDPR у повному обсязі. Українська модель переважно орієнтована на випадки незаконної обробки, недостовірності даних, завершення строку їх зберігання, припинення правовідносин, припис Уповноваженого або судове рішення. Натомість менш урегульованими залишаються ситуації, коли інформація є достовірною та законно оприлюдненою, але з часом втратила актуальність і продовжує завдавати непропорційної шкоди приватному життю особи. Це свідчить про потребу подальшого розвитку українського підходу до права на забуття з урахуванням стандартів GDPR та практики європейських судових інституцій.

Одним із найбільш складних аспектів реалізації права на забуття в Україні є визначення належного відповідача та ефективного способу захисту. Залежно від характеру спірної інформації і способу її поширення відповідна вимога може бути адресована власнику вебсайту, адміністратору вебресурсу, редакції засобу масової інформації, володільцю чи розпоряднику персональних даних або оператору пошукової системи. Однак національне законодавство не встановлює спеціального порядку подання запиту на деіндексацію, строків його розгляду, критеріїв оцінки втрати інформацією актуальності, обсягу обов'язків пошукових систем та наслідків необґрунтованої відмови. За таких умов захист особи ускладнюється, оскільки заявник фактично змушений самостійно визначати суб'єкта, який має юридичну або технічну можливість припинити непропорційний вплив відповідних відомостей.

Додаткову складність зумовлює технічна природа Інтернету. Навіть якщо певний матеріал буде видалений з одного ресурсу, його копії можуть зберігатися в кеші пошукових систем, електронних архівах, соціальних мережах, на дзеркальних сайтах або в повторних публікаціях. Тому повне «забуття» у цифровому середовищі часто є технічно недосяжним. На цю проблему слушно звертають увагу Д.М. Белов, М.В. Белова та О.Т. Горнило [1, с. 61]. Саме тому ефективний захист має поєднувати юридичні засоби з технічними механізмами: деіндексацією, обмеженням пошукової доступності, знеособленням, оновленням контексту й повідомленням інших суб'єктів, які обробляють відповідні дані.

З огляду на це право на забуття в Україні доцільно розглядати не як можливість повного вилучення будь-яких небажаних відомостей, а як механізм пропорційного обмеження цифрової доступності персональних даних. Якщо такі дані обробляються незаконно, є недостовірними або підлягають знищенню відповідно до закону, належним способом захисту може бути їх видалення. Якщо ж відомості були законно оприлюднені, але з часом втратили актуальність і непропорційно впливають на приватне життя особи, більш обґрунтованими є деіндексація, знеособлення або доповнення матеріалу актуальним контекстом. У випадках, коли відповідні дані мають суспільне чи економічне значення, зокрема для громадського контролю, захисту прав споживачів, прозорості підприємницької діяльності або виявлення тіньових економічних практик, вимога про їх видалення чи обмеження доступу до них має оцінюватися з підвищеною обережністю.

Таким чином, у сфері цифрового інформаційного обігу межі права на забуття мають визначатися за двома взаємопов'язаними критеріями. Перший полягає в оцінці того, чи створює подальша доступність інформації непропорційне втручання у приватне життя особи. Другий передбачає з'ясування, чи зберігає відповідна інформація актуальне суспільне або економічне значення, зокрема для запобігання тіньовим практикам, захисту економічної безпеки та прав учасників майнового обігу. Лише поєднання цих критеріїв дає змогу уникнути як надмірної цифрової стигматизації особи, так і необґрунтованого приховування суспільно значущої інформації.

Український підхід має ґрунтуватися не на механічному відтворенні моделі GDPR, а на її адаптації до національної системи захисту приватності, свободи вираження поглядів, доступу до інформації та протидії тіньовому обігу персональних даних. Доцільним є нормативне визначення права на забуття як права на пропорційне обмеження цифрової доступності персональних даних. Поряд із цим мають бути закріплені критерії оцінки відповідних вимог: достовірність і характер інформації, час, що минув після події, статус особи, наявність актуального суспільного інтересу, ступінь шкоди для приватного життя, пропорційність обраного способу захисту та значення таких відомостей для запобігання тіньовим економічним практикам. Окремого врегулювання потребує розмежування правових наслідків для первинного поширювача інформації, власника архіву, адміністратора вебресурсу та оператора пошукової системи.

Найбільш збалансовано видається модель, за якої повне видалення інформації застосовується лише тоді, коли її подальше зберігання або поширення не має правової підстави, або коли дані є незаконно обробленими, недостовірними чи такими, що підлягають знищенню відповідно до закону. Якщо ж інформація була законно оприлюднена і зберігає архівну, журналістську або суспільну цінність, але її поширення через пошукові системи непропорційно впливає на приватне життя особи, перевагу слід надавати менш інтенсивним заходам: деіндексації, знеособленню, обмеженню пошукової доступності або доповненню матеріалу актуальним контекстом.

У випадках, коли інформація стосується суспільно значущої економічної поведінки особи, повне видалення або деіндексація мають застосовуватися лише після особливо ретельної перевірки. Для цього доцільно враховувати, чи пов'язана відповідна інформація з підприємницькою діяльністю, виконанням публічних функцій, управлінням чужими коштами, захистом прав споживачів, фінансовими ризиками, судовими справами, банкрутством, корупційними діями або іншими обставинами, що можуть мати значення для інших учасників правовідносин. У таких випадках приватний інтерес особи у зменшенні негативного впливу інформації має співвідноситися з правом суспільства знати факти, важливі для економічної безпеки та доброчесності ринкового обігу.

Висновки. Право на забуття в Інтернеті слід розглядати не як безумовне право на видалення будь-якої небажаної інформації, а як механізм пропорційного обмеження цифрової доступності персональних даних. Його зміст полягає у зменшенні непропорційного впливу застарілих, надмірно доступних або вивраних із контексту відомостей на приватне життя особи. Європейські стандарти свідчать, що реалізація цього права завжди потребує балансування між приватністю, захистом персональних даних, свободою вираження поглядів, доступом до інформації та актуальним суспільним інтересом.

В умовах цифрової тіньової економіки право на забуття має подвійне значення. Воно може бути засобом протидії незаконному обігу персональних даних, їх несанкціонованому агрегуванню, повторному використанню, комерційній експлуатації та репутаційному тиску. Разом із тим це право не повинно перетворюватися на інструмент приховування відомостей про недобросовісну підприємницьку діяльність, фінансові порушення, шахрайство, корупційні ризики або інші факти, важливі для громадського контролю й економічної безпеки.

Українське законодавство містить окремі положення, які можуть застосовуватися для захисту особи у цифровому середовищі, зокрема норми Конституції України та Закону України «Про захист персональних даних». Проте ці положення не утворюють повноцінного механізму реалізації права на забуття. Найменш урегульованими залишаються ситуації, коли інформація є достовірною та законно оприлюдненою, але з часом втратила актуальність і продовжує непропорційно впливати на приватне життя особи.

Подальший розвиток українського підходу до права на забуття має передбачати визначення процедур деіндексації, критеріїв оцінки втрати інформацією актуальності, обов'язків інтернет-посередників і належних способів захисту. До таких критеріїв доцільно віднести достовірність і характер інформації, час, що минув після події, статус особи, ступінь шкоди для приватного життя та наявність актуального суспільного чи економічного інтересу.

Найбільш збалансованою для України є модель, за якої повне видалення застосовується переважно щодо персональних даних, які є незаконно обробленими, недостовірними або такими, що підлягають знищенню. Щодо законно оприлюдненої, але застарілої інформації доцільно надавати перевагу менш інтенсивним заходам: деіндексації, знеособленню, обмеженню пошукової доступності або доповненню матеріалу актуальним контекстом. Такий підхід дає змогу захищати особу від надмірної цифрової стигматизації, не допускаючи при цьому цензури, репутаційного очищення або необґрунтованого приховування суспільно значущої інформації.

Список використаних джерел:

1. Белов Д. М., Белова М. В., Горнило О. Т. Право людини на забуття. *Науковий вісник Ужгородського національного університету. Серія: Право*, 2024. Т. 2. № 81. С. 57–62. URL: <https://doi.org/10.24144/2307-3322.2024.81.2.9> (дата звернення: 15.06.2026).
2. Габрелян А. Ю. Тіньова економіка: сутність, ознаки, структура та форми прояву. *Успіхи і досягнення у науці*, 2026. № 5(27). С. 2944–2960. URL: [https://doi.org/10.52058/3041-1254-2026-5\(27\)-2944-2960](https://doi.org/10.52058/3041-1254-2026-5(27)-2944-2960) (дата звернення: 15.06.2026).
3. Габрелян А. Ю. Зарубіжний досвід державного регулювання детінізації економіки в контексті економічної безпеки. *Наука і техніка сьогодні (Серія «Право»)*, 2026. № 5(59). С. 685–702. URL: [https://doi.org/10.52058/2786-6025-2026-5\(59\)-685-702](https://doi.org/10.52058/2786-6025-2026-5(59)-685-702) (дата звернення: 15.06.2026).
4. Габрелян А. Ю. Цифрові активи як новий чинник трансформації тіньової економіки. Sectoral research XXI: characteristics and features : Collection of Scientific Papers «SCIENTIA» with Proceedings of the XII International Scientific and Theoretical Conference (June 12, 2026). Chicago, USA: International Center of Scientific Research, 2026. С. 55–61.
5. Дяковський О. С., Габрелян А. Ю. Основні засади та принципи протидії дезінформації. *Юридичний вісник*, 2024. № 4. С. 30–36.
6. Калітенко О. М. Право на забуття: здобуток європейський чи глобальний? *Часопис цивільстики*, 2019. Вип. 35. С. 60–64. URL: <https://doi.org/10.32837/chc.v0i35.189> (дата звернення: 15.06.2026).
7. Конвенція про захист прав людини і основоположних свобод від 04.11.1950 р. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text (дата звернення: 15.06.2026).
8. Конституція України від 28.06.1996 р. № 254к/96-ВР. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text> (дата звернення: 15.06.2026).
9. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (дата звернення: 15.06.2026).
10. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27.04.2016 р. про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (General Data Protection Regulation, GDPR; Загальний регламент про захист даних). URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 15.06.2026).
11. Judgment of the European Court of Human Rights of 16.07.2013 in the case of Węgrzynowski and Smolczewski v. Poland, application no. 33846/07. URL: <https://hudoc.echr.coe.int/eng?i=001-122365> (дата звернення: 15.06.2026).
12. Judgment of the Court of Justice of the European Union of 13.05.2014 in Case C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, ECLI:EU:C:2014:317. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0131> (дата звернення: 15.06.2026).
13. Judgment of the Court of Justice of the European Union of 24.09.2019 in Case C-136/17, GC and Others v Commission nationale de l'informatique et des libertés (CNIL), ECLI:EU:C:2019:773. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62017CJ0136> (дата звернення: 15.06.2026).
14. Judgment of the Court of Justice of the European Union of 24.09.2019 in Case C-507/17, Google LLC v Commission nationale de l'informatique et des libertés (CNIL), ECLI:EU:C:2019:772. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62017CJ0507> (дата звернення: 15.06.2026).
15. Judgment of the European Court of Human Rights of 04.07.2023 in the case of Hurbain v. Belgium, application no. 57292/16. URL: <https://hudoc.echr.coe.int/eng?i=001-225814> (дата звернення: 15.06.2026).

Дата першого надходження статті до видання: 08.05.2026

Дата прийняття статті до друку після рецензування: 29.05.2026

Дата публікації (оприлюднення) статті: 15.06.2026