УДК 342.9
DOI https://doi.org/10.24144/2788-6018.2026.01.3.55

ІНФОРМАЦІЙНО-ПРАВОВІ ГАРАНТІЇ ПРАВА НА ПРИВАТНІСТЬ У ПРОЦЕСІ ЦИФРОВОЇ ІДЕНТИФІКАЦІЇ ОСОБИ

Дашо Т. Ю.,
адвокат, кандидат юридичних наук,
докторант кафедри міжнародного та кримінального права
Національного університету «Львівська політехніка»
ORCID: 0000-0003-1000-7145
e-mail: dashotaras@gmail.com

Дашо Т.Ю. Інформаційно-правові гарантії права на приватність у процесі цифрової ідентифікації особи.

У статті досліджуєтся окремі аспекти права на приватність та їх співвідношення із цифровою ідентичністю особи. Мета дослідження полягає у вивченні процесу розвитку цифровізації та ідентифікації особи в цифровому середовищі, а також, аналізі механізмів дотримання права на приватність особи при цьому. Для досягнення цієї мети у роботі використано комплекс загальнонаукових, спеціальних та спеціально-юридичних методів, зокрема системно-структурний, порівняльно-правовий та формально-логічний методи. За результатами аналізу обґрунтовано, що розвиток систем цифрової ідентифікації, водночас із розширенням можливостей доступу до публічних послуг, актуалізує проблему захисту персональних даних і загострює питання збалансування між безпекою та приватністю.

Доведено необхідність удосконалення правових механізмів захисту права на приватність за допомогою імплементації міжнародних стандартів захисту даних та розроблення ефективної системи контролю за обробкою персональної інформації.

Важливою є і цифрова грамотність населення, що є фактором самозахисту від протиправних посягань в онлайн-просторі, а також, інформування користувачів про їхні права та можливості контролю над власними даними. Окремо розглядаються технологічні методи забезпечення приватності, включаючи криптографічні засоби захисту.

Описано переваги децентралізованих систем ідентифікації, які надають користувачам більший контроль над власними персональними даними та зменшують ризики масового витоку інформації.

Сучасний етап розвитку суспільства характеризується стрімкою цифровізацією, яка істотно впливає на всі сфери суспільного життя, зокрема на форми соціальної взаємодії, комунікації та способи підтвердження особистості. Цифрові технології докорінно трансформували механізми взаємодії особи з державними інституціями та іншими суб'єктами суспільних відносин, сприяючи формуванню нових моделей реалізації прав і свобод людини. Це створює передумови для формування збалансованої моделі цифрової ідентифікації з дотриманням прав людини.

Ключові слова: права людини, право на приватність, цифровізація, цифрова ідентифікація, цифрові технології, персональні дані, захист персональних даних, електронна ідентифікація, електронні довірчі послуги.

Dasho T.Yu. Information and legal guarantees of the right to privacy in the process of digital identification of a person.

The article explores specific aspects of the right to privacy and their relationship with an individual's digital identity. The purpose of the study is to examine the development of digitalization and personal identification in the digital environment, as well as to analyze the mechanisms for ensuring an individual's right to privacy in this process. To achieve this goal, a complex of general scientific, special, and specialized legal methods was employed, including systemic-structural, comparative-legal, and formal-logical methods. Based on the results of the analysis, it is substantiated that the development of digital identification systems, while expanding access to public services, highlights the issue of personal data protection and intensifies the challenge of balancing security and privacy.

The study proves the necessity of improving legal mechanisms for protecting the right to privacy by implementing international data protection standards and developing an effective system for monitoring personal information processing. Digital literacy of the population is also highlighted as a crucial factor for self-protection against unlawful encroachments in the online space, along with informing users about their rights and options for controlling their own data. Technological methods for ensuring privacy, including cryptographic protection tools, are considered separately.

The article describes the advantages of decentralized identification systems, which provide users with greater control over their personal data and reduce the risks of mass data breaches. The current stage of societal development is characterized by rapid digitalization, which significantly impacts all spheres of social life, including forms of social interaction, communication, and methods of identity verification. Digital technologies have fundamentally transformed the mechanisms of interaction between individuals, state institutions, and other entities of social relations, contributing to the formation of new models for exercising human rights and freedoms. This creates the prerequisites for forming a balanced model of digital identification that respects human rights.

Key words: human rights, right to privacy, digitalization, digital identification, digital technologies, personal data, personal data protection, electronic identification, electronic trust services.

Постановка проблеми. Цифрова ідентичність особи, з одного боку, виступає необхідною умовою функціонування сучасної цифрової держави та розвитку електронного урядування, а з іншого боку, створює потенційні ризики порушення права на приватність, зокрема через можливість неправомірного доступу до персональних даних, їх використання без згоди суб'єкта, а також формування надмірного контролю з боку держави чи приватних суб'єктів. У цьому контексті особливої ваги набуває питання встановлення балансу між потребами держави у забезпеченні безпеки та ефективності управління і необхідністю гарантування фундаментальних прав людини.

Дослідження інформаційно-правових гарантій права на приватність у процесі цифрової ідентифікації особи є актуальним як з теоретичної, так і з практичного погляду, оскільки сприяє формуванню цілісного правового підходу до регулювання цифрових ідентифікаційних систем та визначенню напрямів удосконалення національного законодавства України з урахуванням європейських стандартів захисту персональних даних.

Стан опрацювання проблеми. Проблеми інформаційно-правових гарантій права на приватність у процесі цифрової ідентифікації особи недостатньо висвітлені у вітчизняному науково-правому дискурсі. Окремі аспекти означеної проблематики фрагментарно висвітлювали у своїх працях такі науковці, як О. Баранов, Ю. Базанов, В. Брижко, В. Венедіктов, Н. Головацький, А. Колодій, В. Політанський, А. Пазюк, М. Різак, І. Сопілко, О. Старчук та інші. Проте, у наукових працях вказаних дослідників фактично відсутній аналіз інформаційно-правових гарантій права на приватність у процесі цифрової ідентифікації особи відповідно до міжнародно-правових стандартів, що зумовило цієї статті.

Мета і завдання дослідження – на основі національного законодавства, міжнародно-правових стандартів та міжнародного досвіду проаналізувати інформаційно-правові гарантії права на приватність у процесі цифрової ідентифікації особи.

Виклад основного матеріалу. Право на приватність нерозривно пов'язане із захистом персональних даних, оскільки саме персональні дані становлять інформаційну основу приватного життя особи. У зв'язку із поширенням цифровізації в сучасному суспільстві, процеси збору, обробки, зберігання та передачі інформації про особу набувають масового характеру. Відповідно, захист персональних даних виступає ключовим інструментом забезпечення права на приватність.

Право на повагу до приватного і сімейного життя передбачене у Статті 8 ЄКПЛ [1], відповідно органи державної влади не можуть втручатись у здійснення цього права, за винятком випадків, коли втручання здійснюється згідно із законом і є необхідним у демократичному суспільстві в інтересах національної та громадської безпеки чи економічного добробуту країни. Загальна декларація прав людини (1948) [2] забороняє безпідставне втручання в особисте і сімейне життя, таємницю кореспонденції, честь і репутацію.

Право на приватність в контексті цифровізації в європейському праві конкретизується в Загальному регламенті про захист даних (GDPR) [3], який встановлює принципи законності, прозорості, мінімізації даних, обмеження мети їх обробки та забезпечення прав суб'єктів персональних даних. Це основний законодавчий акт, що захищає персональні дані громадян ЄС. У регламенті наголошується, що будь-яке опрацювання персональних даних повинно бути законним та правомірним (Преамбула 39). GDPR встановлює чіткі вимоги щодо збору, обробки, зберігання та обміну персональними даними, гарантуючи, що фізичні особи зберігають контроль над своєю особистою інформацією та захищені від неправомірного використання. Важливим принципом є прозорість: особи повинні бути проінформовані про збирання, використання та поширення їхніх персональних даних, а також про те, якою мірою обробляються чи оброблятимуться ці дані. Критично важливою вимогою є отримання чіткої та недвозначної згоди від фізичних осіб перед збором, обробкою або зберіганням їхніх даних, а також надання особі вичерпної інформації про те, яким чином використовуватимуться її дані.

Регламент також вимагає, щоб системи цифрової ідентифікації були розроблені з урахуванням конфіденційності, вимагаючи мінімізації даних та забезпечення суворого обмеження термінів

зберігання даних. До ключових вимог GDPR також належить забезпечення безпеки персональних даних за допомогою відповідних технічних та організаційних заходів. До таких належить: шифрування, контроль доступу, регулярні аудити безпеки. Також, є вимога стирання або знищення персональних даних, якщо вони більше не потрібні для цілей, для яких їх було зібрано, або за запитом суб'єкта даних. GDPR застосовується до будь-якої організації, яка обробляє персональні дані фізичних осіб у Європейському Союзі. Загалом, не має значення, чи має організація штаб-квартиру в ЄС чи за його межами. Відповідно, навіть іноземні організації, що обслуговують резидентів ЄС, повинні дотримуватися правил. GDPR встановлює певні механізми для забезпечення дотримання вимог контролерами даних. Штрафи можуть сягати 4% від світового доходу компанії.

Ще одним важливим міжнародним документом у сфері цифрової ідентифікації є Керівні принципи Організації Об'єднаних Націй щодо цифрової ідентифікації (UN Guidelines on Digital Identity) [4]. Це рекомендації з дотримання прав людини під час розробки та впровадження систем цифрової ідентифікації. Наголошується на тому, що системи цифрової ідентифікації повинні поважати право на приватність, гарантувати відсутність дискримінації та сприяти соціальній інтеграції. ООН робить наголос на принципах захисту персональних даних та прав людини і основоположних свобод, також на якості даних, безпеці обробки, та правах індивідуальних осіб. Документ містить окремі практичні рекомендації для різних категорій учасників процесу цифрової ідентифікації. Для політиків та осіб, що приймають рішення щодо розробки національних стратегій цифрової ідентифікації з урахуванням прав людини, та для контролерів даних та операторів систем, щодо забезпечення прозорості, підзвітності та технічної безпеки систем ідентифікації.

Проблема захисту прав людини на приватність у процесі цифрової ідентифікації особи не одноразово була обговорена на засіданнях Організації Об'єднаних Націй. У доповіді Верховного комісара ООН з прав людини «Право на приватність у цифрову епоху» (2018) зазначено, що право на приватність є необхідною умовою для інших прав: свобода вираження поглядів, свобода думки, свобода асоціації, право на справедливий суд. Будь-яке втручання в приватність має бути законним, необхідним і пропорційним. Держави зобов'язані захищати людей від порушень, в тому числі приватними компаніями, у контексті позитивних зобов'язань. Водночас підкреслюється необхідність знаходження балансу між інтересами національної безпеки держав та індивідуальними правами і свободами громадян [5].

Важливим кроком у цифровізації України та забезпечення безпеки особистих даних осіб є ратифікація Угоди між Україною та Європейським Союзом про участь України у програмі Європейського Союзу «Цифрова Європа» [6]. Це програма фінансування для розвитку цифрових технологій в ЄС, що підтримує кібербезпеку, штучний інтелект, цифрові навички, розвиток цифрової інфраструктури тощо. Відповідно, захист права на приватність є одним із ключових пріоритетів.

Одним із найбільших пілотних проєктів програми є Європейський цифровий гаманець ідентичності (EUDI Wallet – European Digital Identity Wallet). Це мобільний продукт, що створює безпечну, суверенну цифрову ідентичність для громадян ЄС та асоційованих країн, де особа сама контролює, які дані передавати. Після запровадження цифрового гаманця українці зможуть використовувати Дію в Європі. Програма також працює у напрямку підвищення стійкості до кібератак, фінансує AI-системи, де є обов'язковими захист персональних даних та прозорість, навчання фахівців із кібербезпеки, підтримка впровадження GDPR у країнах. Програма підтримує розвиток цифровізації в Україні та гармонізацію із цифровим ринком в ЄС, зокрема в рамках проєктів DT4UA та EU4DigitalUA. Основними компонентами є зміцнення інституцій та розвиток потенціалу, комунікація та підвищення обізнаності громадськості, розвиток електронних послуг.

Таким чином, діяльність програми «Цифрова Європа» спрямована на те, щоб цифровізація не створювала додаткових ризиків для приватності громадян, а, навпаки, посилювала її через впровадження сучасних технологічних та правових механізмів захисту персональних даних і надання особам реального контролю над власною цифровою ідентичністю.

За концепцією Х. Ніссенбаум, професорки кафедри інформаційних технологій Корнельського університету, приватність слід розуміти не як право на таємність чи абсолютний контроль над інформацією, а як право на контекстуальну цілісність, тобто коректний обіг персональної інформації відповідно до соціальних норм і контексту її використання [7, p. 21]. Це передбачає, що особа може самостійно оцінювати та приймати рішення щодо розкриття власних даних у цифровому просторі, залежно від конкретної ситуації та контексту. Іншими словами, людина повинна мати можливість з'ясувати, яким чином і з якою метою використовуються її персональні дані, хто є їх зберігачем і протягом якого періоду, а також коло осіб, які мають до них доступ. При цьому особа має право вимагати видалення або коригування своїх персональних даних.

Отже, варто підкреслити, що цифрова епоха не скасовує традиційних прав людини, а, навпаки, актуалізує необхідність їх ефективного захисту та адаптації до нових технологічних реалій. Забез-

печення права на приватність у контексті цифрової ідентифікації залишається одним із ключових викликів для багатьох країн світу, що потребує комплексного підходу, який поєднує правові, технологічні та організаційні механізми захисту.

В Україні право на захист персональних даних випливає з положень статті 32 Конституції України, яка гарантує кожному право на невтручання в особисте і сімейне життя, а також забороняє збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, за винятком випадків, передбачених законом і лише в інтересах національної безпеки, економічного добробуту та прав людини [8]. Реалізація цього права конкретизується в Законі України «Про захист персональних даних» [9], що регулює правові відносини, пов'язані із захистом і обробкою таких даних, і спрямований на захист основоположних прав і свобод людини та громадянина, зокрема права на невтручання в особисте життя. Цей закон визначає персональні дані, як відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Стаття 6 Закону встановлює основні принципи обробки персональних даних, а саме: законність мети, точність, адекватність, мінімальність та обмеженість у часі. Обробка даних повинна здійснюватися прозоро, за згодою особи, крім винятків, передбачених законом, та лише стільки часу, скільки це необхідно для досягнення законної мети. У статті 7 цього закону передбачені особливі вимоги до обробки персональних даних.

Головацький Н. Т. звертає увагу, що у даному законі не відокремлюються принципи обробки персональних даних. На відміну від Регламенту GDPR, де принципи обробки персональних даних чітко виокремлені в окремій статті 5, український Закон «Про захист персональних даних» не містить спеціальної норми, присвяченої виключно принципам. Натомість вони виражені у вищезгаданих статтях 6 та 7 Закону. Таке рішення обумовлене тим, що виділення окремої статті про принципи вимагало б подальшої деталізації принципів збору, обробки, захисту, зберігання, знищення та видалення персональних даних, що ускладнило б структуру Закону» [10].

Важливою гарантією права на приватність є вимога щодо наявності правових підстав для обробки персональних даних. Такі підстави передбачені в статті 11 Закону. Найважливішою умовою є згода суб'єкта персональних даних на їх обробку та поширення, що відображає принцип автономії волі особи у сфері інформаційних правовідносин. Закон також визначає систему прав суб'єкта персональних даних, що по суті відображають право на приватність. Зокрема, передбачено право особи отримувати доступ до відомостей про себе, вимагати їх коригування чи видалення, а також право на захист від неправомірної обробки своїх персональних даних [9].

Процедурний компонент адміністративно-правового механізму цифрової ідентифікації охоплює сукупність адміністративних процедур, пов'язаних із встановленням особи, підтвердженням її цифрової ідентичності та наданням електронних адміністративних послуг. Закон України «Про електронну ідентифікацію та електронні довірчі послуги» визначає цифрову автентифікацію як процедуру встановлення особи в електронному середовищі за допомогою технічних і правових засобів, що дозволяє підтвердити електронну ідентифікацію. Стаття 15 Закону встановлює систему рівнів довіри до засобів електронної ідентифікації за зразком європейського регламенту eIDAS (low / substantial / high assurance levels), що передбачає низький, середній і високий рівні довіри. Вищий рівень довіри передбачає суворіші вимоги до перевірки особи та захисту від підробки, що ,відповідно, розширює перелік послуг, доступних з таким засобом ідентифікації. Високий рівень довіри означає практичну неможливість підробки без значних зусиль. Кваліфікований електронний підпис (КЕП) є прикладом високого рівня довіри та основним юридично значущим засобом цифрової ідентифікації, який забезпечує автентифікацію та підтвердження волевиявлення в електронному середовищі [11]. Система BankID також є прикладом децентралізованої моделі цифрової ідентифікації, де банки виступають посередниками між користувачами та суб'єктами електронних послуг.

У багатьох країнах, зокрема в Україні, діють електронні паспорти. За допомогою застосунку «Дія» завантажуються й перевіряються документи, що посвідчують особу, надаються державні послуги в електронній формі, здійснюються автоматичні державні послуги, відкриваються рахунки. Застосунок, по суті, є цифровим профілем особи, доступ до якого забезпечується через смартфон. Цікавим є досвід Індії та її системи Aadhaar – однієї з найбільших біометричних систем у світі, де зареєстровано понад 1,1 мільярда користувачів. Система являє собою унікальний код, що містить сканування відбитків пальців, райдужки ока, фотографію особи та персональні дані, такі, як: адреса, стать, дата народження [12].

У дослідженні, опублікованому в Довіднику Palgrave Handbook of Technological Finance, описаний 10-річний досвід Індії з Aadhaar, що показує, як працює програма, пов'язані з цією системою політичні компроміси та дебати щодо впровадження системи. Незважаючи на ефективність програми та задоволення користувачів, прийняття цієї програми викликало широке занепокоєння щодо можливості зловживання приватною інформацією людей [13]. У відповідь на численні судові позови Верхов-

ний суд Індії 26 вересня 2018 року постановив, що Aadhaar не порушує право індійців на приватне життя. Водночас суд обмежив використання системи: лише уряд, а не приватні підприємства, може вимагати номер Aadhaar для доступу до послуг. Обов'язкове прив'язування дозволено в обмежених випадках, тобто лише для державних послуг і виплат, наприклад, пенсій. Для банківських рахунків, мобільних SIM-карт, вступу до шкіл та університетів, іспитів тощо – не можна робити обов'язкове прив'язування. Також, у випадках, коли людина не має коду Aadhaar або біометрія не спрацьовує, держава зобов'язана надавати альтернативні способи ідентифікації [14].

На відміну від індійської системи Aadhaar, естонська система забезпечує високий рівень приватності та безпеки за допомогою технології блокчейн та криптографічних методів для захисту цифрових ідентифікацій. Важливим є те, що система Естонії дозволяє особам зберігати контроль над своїми даними. Користувачі можуть ділитися лише необхідною інформацією для доступу до певних послуг [12]. Кожен громадянин Естонії має цифрову ID-картку, за допомогою якої є можливість підтверджувати особу онлайн, підписувати документи електронним підписом, отримувати державні послуги та голосувати онлайн. Естонська модель цифрової ідентифікації базується на принципі децентралізації даних, що мінімізує ризики масових витоків персональної інформації. Також, в Естонії існує програма e-Residency дозволяє іноземцям отримати цифрову ідентичність без громадянства [15].

Цікавим у контексті нашої тематики є проблеми правового визначення «журналістського винятку» у законодавстві про захист персональних даних. Так, Закон України «Про медіа» встановлює межі між свободою поширення інформації та захистом приватності. Закон вказує на правове регулювання інформаційних відносин, що полягає у необхідності забезпечення балансу між свободою поширення інформації та захистом приватного життя особи [16]. Цей баланс є особливо актуальним в умовах цифрової ідентифікації, коли персональні дані стають ключовим елементом функціонування цифрових сервісів.

Захист персональних даних у сфері медіа містить спеціальні винятки щодо застосування законодавства про персональні дані. Так, згідно із частиною 2 статті 26 Закону України «Про захист персональних даних», дозволяється обробка персональних даних без застосування положень цього Закону, якщо така обробка здійснюється виключно для журналістських та творчих цілей, за умови забезпечення балансу між правом на повагу до особистого життя та правом на свободу вираження поглядів [9]. Цей підхід закріплено і в європейському праві, а саме у статті 85 GDPR. Стаття зобов'язує законодавчо узгодити право на захист персональних даних з правом на свободу вираження поглядів та інформації, включаючи обробку для журналістських цілей та цілей академічного, художнього чи літературного вираження [3].

У деяких країнах які прийняли національне законодавство, що містить виняток для журналістів, присутні певні неточності у формуванні такого законодавства. До прикладу, Закон Словацької Республіки Про захист даних передбачає «виняток з винятку», тобто, персональні дані можуть оброблятися для журналістських цілей без згоди суб'єкта даних, за винятком випадків, коли це порушує захист його особистості або конфіденційності. Закон Іспанії про захист даних, своєю чергою, зовсім не дає жодних вказівок на те, як вимоги GDPR слід узгоджувати із журналістикою та свободою слова.

Відповідно, «журналістський виняток» у GDPR залишено на розсуд держав та межі допустимого втручання у приватне життя особи з боку медіа залишаються недостатньо визначеними. Це створює можливість використовувати закони про захист даних для перешкоджання журналістським розслідуванням.

У практиці Європейського суду з прав людини співвідношення права на приватність та свободи вираження поглядів є одною із важливих проблем. Суд наголошує, що жодне з цих прав не має абсолютного характеру, а їх балансування здійснюється з урахуванням принципу пропорційності та суспільного інтересу. ЄСПЛ у своїх рішеннях формує критерії оцінки допустимості втручання у приватне життя, зокрема статус особи, внесок інформації в суспільну дискусію та наслідки її поширення.

У справі Von Hannover v. Germany (2004, 2012) Кароліна, принцеса Ганноверська, протягом деякого часу намагалася запобігти публікації її фотографій у німецькій пресі. Німецькі суди постановили, що вона була «фігурою сучасного суспільства par excellence» , яка мусила зазнавати певного рівня пильної уваги преси, коли перебувала на публіці. Після того рішення принцеса подала нові позови щодо схожих фотографій, сподіваючись на кращий захист. ЄСПЛ не встановив порушення статті 8 ЄКПЛ та встановив критерії зважування, такі, як: внесок до обговорення громадського інтересу , як головний критерій; наскільки відома особа і яка тема публікації; попередня поведінка особи; зміст, форма та наслідки публікації; обставини фотографування [17].

Інша справа, Axel Springer AG v. Germany (2012) стосувалася публікації інформації про кримінальну справу проти відомої особи. Суд зробив висновок, що ЗМІ можуть повідомляти про кримі-

нальні провадження, а також, розкривати особу обвинуваченого, якщо він є публічною особою та є суспільний інтерес. Важливою є також правдивість інформації. Однак, ЗМІ не можуть порушувати презумпцію невинуватості та розкривати інтимні деталі приватного життя [18].

Висновки. Отже, правові основи для функціонування системи цифрової ідентифікації в Україні визначене національним законодавством через положення Закону України «Про захист персональних даних» та Закону України «Про електронні довірчі послуги». Процедурний компонент механізму, що охоплює різні рівні довіри до засобів електронної ідентифікації, такі, як: низький, середній, високий, забезпечує диференційований підхід до автентифікації залежно від характеру послуг. Впровадження системи «Дія» демонструє практичну реалізацію принципів цифрової трансформації публічного адміністрування в Україні.

Порівняльний аналіз міжнародного досвіду дозволив виокремити два основні підходи до побудови систем цифрової ідентифікації: централізований (як у випадку індійської Aadhaar) та децентралізований (естонська модель). Рішення Верховного суду Індії у справі Aadhaar ілюструє важливість збалансування ефективності системи з гарантіями права на приватність, обмежуючи обов'язкове використання ідентифікатора лише державним сектором. Естонський досвід, натомість, демонструє переваги децентралізованого зберігання даних та надання користувачам контролю над власною інформацією.

Особливої уваги потребує питання балансу між правом на захист персональних даних та свободою вираження поглядів у контексті «журналістського винятку». Аналіз статті 26 Закону України «Про захист персональних даних» та статті 85 GDPR виявляє недостатню визначеність меж допустимого втручання медіа у приватне життя. Практика Європейського суду з прав людини, зокрема рішення у справах Von Hannover v. Germany та Axel Springer AG v. Germany, формує систему критеріїв для оцінки пропорційності такого втручання, однак національне законодавство окремих держав-членів ЄС демонструє непослідовність у врегулюванні цього питання.

Перспективами подальших досліджень є вироблення чітких критеріїв застосування «журналістського винятку» в українському законодавстві, вдосконалення механізмів контролю за обробкою персональних даних у цифровому середовищі, а також імплементація принципу децентралізації даних за естонським зразком для мінімізації ризиків масових витоків інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Конвенція про захист прав людини і основоположних свобод. *База даних «Законодавство України» / ВР України.* URL: https://zakon.rada.gov.ua/laws/show/995_004#Text.
2. Загальна декларація прав людини. *База даних «Законодавство України» / ВР України.* URL: https://zakon.rada.gov.ua/laws/show/995_015#Text.
3. Загальний регламент про захист даних (GDPR). URL: https://gdpr-text.com/uk.
4. Guidelines on National Digital Identity (2023). URL: https://edoc.coe.int/en/data-protection/11578-guidelines-on-national-digital-identity.html.
5. The right to privacy in the digital age: report of the United Nations High Commissioner for Human Rights (A/HRC/39/29). (2018, August). URL: https://docs.un.org/en/a/hrc/39/29.
6. Закон України «Про ратифікацію Угоди між Україною та Європейським Союзом про участь України у програмі Європейського Союзу «Цифрова Європа» (2021-2027)». *База даних «Законодавство України» / ВР України.* URL: https://zakon.rada.gov.ua/laws/show/2926-20#Text.
7. Nissenbaum, H. Protecting Privacy in an Information Age: The Problem of Privacy in Public (2000, September). URL: https://nissenbaum.tech.cornell.edu/papers/privacy.pdf.
8. Конституція України. *База даних «Законодавство України» / ВР України.* URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.
9. Закон України «Про захист персональних даних». *База даних «Законодавство України» / ВР України.* URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.
10. Головацький Н. Т. Прозорість та згода як основні принципи захисту персональних даних в Україні. *Науковий вісник Ужгородського Національного Університету*. Серія ПРАВО. 2024. Випуск 83. Частина 2. С. 178–184. DOI: https://doi.org/10.24144/2307-3322.2024.83.2.25.
11. Закон України «Про електронну ідентифікацію та електронні довірчі послуги». *База даних «Законодавство України» / ВР України.* URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text.
12. Mehrdad Amini, Laleh Javidnejad. Legal Frameworks for Digital Identity Systems in E-Governance: Privacy, Security, and Inclusion. *Legal Studies in Digital Age.* URL: https://jlsda.com/index.php/lsda/article/view/21.
13. Bhagwan Chowdhry, Amit Goyal, and Syed Anas Ahmed. Digital Identity in India. URL: https://anderson-review.ucla.edu/wp-content/uploads/2022/04/Digital-Identity-in-India-Palgrave-Handbook-of-Technological-Finance.pdf.

14. Supreme Court of India Justice K.S.Puttaswamy(Retd) vs Union Of India on 26 September, 2018. URL: https://indiankanoon.org/doc/127517806.
15. Republic of Estonia e-residency. URL: https://www.e-resident.gov.ee.
16. Закон України «Про медіа». *База даних «Законодавство України» / ВР України.* URL: https://zakon.rada.gov.ua/laws/show/2849-20.
17. Справа VON HANNOVER проти Німеччини (№ 2). Переклад було здійснено за підтримки Фундації з прав людини Ради Європи. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-126822%22]}.
18. (1 DE 1) CASE OF AXEL SPRINGER AG v. GERMANY. URL: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-109034%22]}.

Дата першого надходження рукопису до видання: 20.12.2025
Дата прийняття до друку рукопису після рецензування: 26.01.2026
Дата публікації: 2.02.2026