

УДК 342.7:004.738.5

DOI <https://doi.org/10.24144/2307-3322.2024.81.1.26>

ЦИВІЛЬНО-ПРАВОВІ АСПЕКТИ ЦИФРОВОЇ КОНФІДЕНЦІЙНОСТІ

Бірюкова А.Г.,

д.ю.н., доцент,

*доцент кафедри цивільно-правової політики,
права інтелектуальної власності та інновацій*

*Національного юридичного університету
імені Ярослава Мудрого,*

ORCID: <https://orcid.org/0000-0002-2786-543X>

e-mail: a.g.biryukova@nlu.edu.ua

Колісникова Г.В.,

к.ю.н, доцент,

*доцент кафедри цивільно-правової політики,
права інтелектуальної власності та інновацій*

*Національного юридичного університету
імені Ярослава Мудрого,*

ORCID <https://orcid.org/0000-0002-9309-4282>

e-mail: g.v.kolisnykova@nlu.edu.ua

Бірюкова А.Г., Колісникова Г.В. Цивільно-правові аспекти цифрової конфіденційності.

Стаття прагне окреслити шляхи оптимізації існуючого законодавства для забезпечення балансу між правом на приватність і потребами державної безпеки, економічного розвитку та інформаційної відкритості. Мета статті – проаналізувати цивільно-правові аспекти цифрової конфіденційності в Україні, виявити основні проблеми та виклики, що виникають у зв'язку з розвитком цифрових технологій та інтернету. Особлива увага приділяється вивченню нормативно-правової бази, яка регулює захист персональних даних, а також аналізу відкритих даних та їх впливу на економіку та суспільство. У ході дослідження цивільно-правових аспектів цифрової конфіденційності в Україні було розглянуто низку ключових питань, що стосуються захисту особистої інформації індивідів у цифровому просторі. Аналіз виявив, що цифрова конфіденційність охоплює широкий спектр даних, від особистих ідентифікаторів до поведінкових патернів користувачів в Інтернеті. Особлива увага приділялася праву індивідів контролювати доступ до своїх даних та їх використання, що є критично важливим для забезпечення приватності в онлайн-середовищі. Дослідження також виявило існування конституційних протиріч між правом на свободу слова та необхідністю забезпечення державної безпеки, що впливає на обсяг та межі цифрової конфіденційності. Відсутність чіткого розмежування та визначення між «конфіденційною інформацією про особу» та «персональними даними» у законодавстві створює додаткові труднощі для правового регулювання цієї сфери. Дослідження наголошує на необхідності комплексного підходу до регулювання цифрової конфіденційності, який би включав інтеграцію різних законодавчих норм та адаптацію до сучасних викликів цифрової епохи. Крім того, висвітлено важливість адекватного регулювання збору та використання інформації через файли cookies та IP-адреси для захисту особистих даних користувачів. У підсумку, дослідження підкреслює актуальність теми цифрової конфіденційності та визначає ключові напрямки для подальшого розвитку правового регулювання в цій сфері в Україні, з огляду на забезпечення балансу між правами індивідів та інтересами держави.

Ключові слова: цивільно-правові аспекти, цифровізація, конфіденційність, цифрова ідентичність.

Biryukova A.G., Kolisnykova H.V. Civil and legal aspects of digital privacy.

The article seeks to outline the ways to optimize the existing legislation to ensure a balance between the right to privacy and the needs of state security, economic development and information transparency. The purpose of the article is to analyze the civil law aspects of digital privacy in Ukraine, to identify the main problems and challenges arising from the development of digital technologies and the Internet. Particular attention is paid to the legal framework governing the protection of personal data, as well as to the analysis of open data and its impact on the economy and society. The study of civil law aspects of digital privacy in Ukraine addressed a number of key issues related to the protection of personal information of individuals in the digital space. The analysis showed that digital privacy covers a wide range of data, from personal identifiers to behavioral patterns of users on the Internet. Particular attention was paid to the right of individuals to control access to and use of their data, which is critical to ensuring privacy in the online environment. The study also revealed the existence of constitutional tensions between the right to freedom of speech and the need to ensure state security, which affects the scope and limits of digital privacy. The absence of a clear distinction and definition between «confidential information about a person» and «personal data» in the legislation creates additional difficulties for the legal regulation of this area. The study emphasizes the need for a comprehensive approach to digital privacy regulation, which would include the integration of various legislative norms and adaptation to the current challenges of the digital age. In addition, the study highlights the importance of adequate regulation of the collection and use of information through cookies and IP addresses to protect users' personal data. In summary, the study emphasizes the relevance of the topic of digital privacy and identifies key areas for further development of legal regulation in this area in Ukraine, with a view to ensuring a balance between the rights of individuals and the interests of the State.

Key words: civil law aspects, digitalization, privacy, digital identity.

Постановка проблеми. Цифровізація сучасного світу невпинно проникає в усі сфери життя, змушуючи правову систему адаптуватися до нових викликів та можливостей. Україна, відповідаючи на ці сучасні тренди, активно працює над розвитком правових рамок, що регулюють цифрове середовище, зокрема аспекти цифрової конфіденційності. Серпень 2023 року став значущим моментом у цьому контексті, ознаменувавшись підписанням Президентом двох ключових законопроектів – № 6447 та № 6576, які вносять суттєві зміни та доповнення до існуючого законодавства [5].

Законопроект № 6447 забезпечує правову інновацію, розширюючи перелік об'єктів цивільних прав за рахунок інтеграції такої категорії, як «цифрові речі». Це поняття вводиться у Цивільний кодекс України, підкреслюючи, що цивільні права та обов'язки можуть мати своє застосування не лише у матеріальному, а й у цифровому просторі. Особлива увага приділяється диференціації між цифровими благами з майновою цінністю та тими, що цінності не мають, що відкриває дискусійний простір щодо оцінки та визнання цінності цифрових активів, зокрема криптовалют.

Законопроект № 6576, у свою чергу, встановлює комплексне регулювання цифрового контенту та цифрових послуг через введення нового Закону «Про цифровий контент та цифрові послуги». Цей закон визначає правові рамки відносин між виконавцями та споживачами, враховуючи особливості цифрової взаємодії, а також забезпечує захист персональних даних у контексті цифрових послуг.

Незважаючи на значний прогрес, зазначений у прийнятті законопроектів № 6447 та № 6576, що покликані врегулювати цивільно-правові аспекти цифрової конфіденційності в Україні, на сьогоднішній день ці ініціативи залишаються на рівні проектів. Їхнє остаточне прийняття та імплементація ще не відбулися, що залишає певну правову невизначеність у цій сфері.

Відсутність досконалого правового регулювання, специфічного для цифрової конфіденційності, спонукає до звернення до існуючих нормативних актів, таких як Закон «Про захист персональних даних» та Закон «Про інформацію». Ці закони, хоча й відіграють фундаментальну роль у захисті прав осіб у контексті обробки персональних даних та доступу до інформації, не в повній мірі відповідають викликам, що виникають у дедалі більш інтегрованому цифровому середовищі.

Сучасний цифровий ландшафт характеризується швидким розвитком технологій, що вимагає більш гнучких та адаптованих до реалій правових норм. Цифрова конфіденційність охоплює не лише захист персональних даних, а й ширший спектр питань, пов'язаних з використанням цифрового контенту, цифрових послуг, інтелектуальної власності в інтернеті та інших аспектів цифрового життя.

Таким чином, хоча існуюче законодавство закладає основу для регулювання цих питань, очевидна потреба в його розширенні та удосконаленні для адекватного відображення та вирішення специфічних проблем цифрової ери. Відсутність спеціалізованого правового регулювання в контексті цифрової конфіденційності створює правову невизначеність та може призвести до виникнення правових конфліктів та викликів, які потребують невідкладного вирішення.

Аналіз цих нововведень дозволяє глибше зрозуміти поточний стан та перспективи розвитку цивільно-правових аспектів цифрової конфіденційності в Україні. Вони свідчать про важливість правової адаптації до динамічно змінюваного цифрового середовища та висувають на перший план питання регулювання цифрових прав та обов'язків, враховуючи особливості цифрової економіки та необхідність захисту персональних даних.

Аналіз останніх досліджень і публікацій. Тема цивільно-правових аспектів цифрової конфіденційності набуває особливої актуальності у світлі стрімкого розвитку цифрових технологій та інтернету. Незважаючи на важливість цієї теми, вона залишається недостатньо дослідженою, що змушує спиратися на експертні думки та аналіз існуючого законодавства України.

Одним із піонерських досліджень у цій галузі є робота Н. Зозулі [1], яка розглядає правові аспекти використання файлів cookies та інших засобів збору інформації веб-сайтами. Авторка наголошує на необхідності забезпечення приватності користувачів та захисту їхніх персональних даних у цифровому просторі.

В.В. Маньгора та Ю.О. Михальчук розглядають використання цифрових технологій у праві, вказуючи на перспективи та виклики, пов'язані з цифровізацією правових процесів, в тому числі і з питаннями конфіденційності [3].

Публікація компанії «Правовий Альянс» [5] висвітлює новації українського законодавства щодо цифрових речей та цифрового контенту, аналізуючи договірні відносини в цифровому середовищі.

Усі ці роботи разом з міжнародними дослідженнями, такими як праця Косинські та ін. [10], яка аналізує передбачуваність особистих рис на основі цифрових записів поведінки людини, формують базу для критичного аналізу та подальшого дослідження цивільно-правових аспектів цифрової конфіденційності.

Мета статті – проаналізувати цивільно-правові аспекти цифрової конфіденційності в Україні, виявити основні проблеми та виклики, що виникають у зв'язку з розвитком цифрових технологій та інтернету. Особлива увага приділяється вивченню нормативно-правової бази, яка регулює захист персональних даних, а також аналізу відкритих даних та їх впливу на економіку та суспільство.

Вклад основного матеріалу. Для повного розуміння поняття цифрової конфіденційності необхідно спершу звернутися до концепції цифрової ідентичності. Цифрова ідентичність – це набір цифрових атрибутів та характеристик, що унікально ідентифікують особу в цифровому середовищі. Це можуть бути дані, такі як імена користувачів, електронні адреси, профілі соціальних мереж, історія браузера, фінансові дані, а також більш складні аспекти, як поведінкові патерни, відбитки пристроїв тощо. Цифрова ідентичність дозволяє індивідуумам взаємодіяти в онлайн-просторі, отримувати доступ до ресурсів, комунікувати, здійснювати транзакції та користуватися цифровими послугами [9].

На основі розуміння цифрової ідентичності, цифрова конфіденційність може бути визначена як *право особи на збереження приватності своєї цифрової ідентичності та контроль над власними персональними даними у цифровому просторі*. Це включає здатність особи обмежувати доступ до своїх даних, керувати їх використанням, розповсюдженням та зберіганням, а також право на захист від несанкціонованого доступу, зловмисного використання або розкриття. Цифрова конфіденційність охоплює широкий спектр аспектів, від комунікації в інтернеті та користування онлайн-сервісами до захисту фінансових даних та особистої інформації.

У контексті Інтернету та цифрового світу, поняття конфіденційності набуває інших вимірів порівняно з традиційним розумінням цього терміну. Конфіденційність в цифровому просторі, перш за все, пов'язана з захистом інформації, яку користувачі залишають онлайн. За словами професора права Джеррі Кана, конфіденційність охоплює три основні аспекти:

- фізичний простір, який не повинен піддаватися небажаному вторгненню;
- приватність ухвалення рішень, як це показано у відомій судовій справі Роу проти Вейда;
- захист інформації, що включає в себе обговорення щодо того, як і де збираються та зберігаються особисті дані користувачів [10].

Зрозуміло, що регулювання питань, пов'язаних з захистом персональних даних, має відбуватися через призму забезпечення права на приватність, що є фундаментальним принципом в сучасному правовому полі України. З цією метою було прийнято Закон України «Про захист персональних даних» (Документ 2297-VI), який станом на 27 жовтня 2022 року має останню редакцію, затверджену на підставі Закону 2438-IX. Цей нормативний акт є важливим кроком на шляху до вдосконалення правового поля у сфері захисту персональних даних, адаптуючи його до вимог сучасних міжнародних стандартів [7].

У контексті Національної стратегії [4] у сфері прав людини, прийнятої у 2021 році, особлива увага приділяється розробці та впровадженню ефективних механізмів захисту права на приватне життя громадян. Це передбачає не лише законодавче регулювання, а й створення відповідних інституційних рамок, здатних забезпечити реалізацію та захист зазначеного права у всіх сферах життєдіяльності, включаючи медичну, соціальну сфери, а також у контексті проведення оперативного-розшукових та негласних слідчих дій.

Захист персональних даних є також невід'ємною складовою процесу європейської інтеграції України, де вимоги до рівня захисту даних постійно зростають у відповідності до європейських норм та стандартів. Це, в свою чергу, потребує постійного оновлення та адаптації українського законодавства, зокрема, шляхом імплементації положень Загального регламенту про захист даних (GDPR), що замінив Директиву 95/46/ЄС.

Однак, як було зазначено, в Україні досі існує правова невизначеність щодо цифрової конфіденційності через відсутність спеціалізованого законодавства, яке б враховувало всі нюанси сучасного цифрового простору. Поточне законодавство, зокрема Закони «Про захист персональних даних» та «Про інформацію», не повною мірою відповідає викликам, пов'язаним з цифровою ідентичністю та конфіденційністю. Однак необхідність розгляду питання конфіденційності в Інтернеті в українському правовому полі відбувається крізь призму захисту інформації.

Складові конфіденційної інформації. Конфіденційна інформація про фізичну особу, відповідно до ЗУ «Про інформацію» [8] охоплює різноманітні аспекти особистого життя, які визначаються як захищені від небажаного розголошення. Ця інформація включає, але не обмежується, даними про:

- національність – відноситься до етнічної приналежності особи;
- освіту – охоплює відомості про освітній рівень, навчальні заклади, спеціальності;
- сімейний стан – інформація про шлюбний статус, наявність дітей, сімейні відносини;
- релігійні переконання – дані про релігійну приналежність або вірування особи;
- стан здоров'я – медична інформація, включаючи історію хвороб, медичні діагнози, лікування;
- адреса, дата і місце народження – точні відомості про місце та час народження, а також постійне місце проживання.

Також до цього переліку можна віднести інші категорії даних, які можуть розглядатися як конфіденційні, залежно від бажання особи їх розкривати, включно з:

- хобі та інтереси – особисті захоплення, уподобання, відпочинкові активності;
- особливості сімейних стосунків – інформація про внутрішньосімейні відносини, включаючи конфлікти, угоди тощо;
- майновий стан – інформація про доходи, власність, фінансові зобов'язання та активи.

У Законі України «Про захист персональних даних» персональні дані визначаються як інформація або зібрані відомості, які дозволяють ідентифікувати фізичну особу. Це може включати інформацію про расове або етнічне походження особи, політичні, релігійні переконання, членство в організаціях, кримінальне минуле, а також відомості, що стосуються здоров'я, сексуального життя, біометричні та генетичні дані. Законодавство наголошує, що обробка таких чутливих даних дозволена тільки в окремих, чітко визначених випадках, щоб забезпечити високий рівень захисту цих інформацій.

Додатково, інші закони України, такі як «Основи законодавства України про охорону здоров'я», «Про нотаріат» та «Про психіатричну допомогу», розширюють поняття конфіденційності, включаючи таємницю стосовно здоров'я, нотаріальні відомості та психічний стан особи. Наприклад, вказано, що пацієнти мають право на таємницю щодо свого здоров'я, а медичні працівники не можуть розкривати інформацію про хворобу, медичне обстеження та особисте життя пацієнтів. Нотаріуси також мають зберігати в таємниці отриману інформацію під час надання своїх послуг,

а інформація про психічний стан особи вважається конфіденційною, і її розкриття допускається лише за письмовою згодою особи або її законного представника.

Існує ряд законів в Україні, які можуть сприяти кращому регулюванню цифрової конфіденційності, зокрема Закон України «Про захист інформації в інформаційно-комунікаційних системах». Цей закон забезпечує захист даних в автоматизованих системах, встановлюючи правила для збереження, обробки та передачі інформації в цифровому вигляді [6]. Крім того, Закон України «Про оперативно-розшукову діяльність» встановлює, що інформація, отримана в результаті оперативно-розшукових дій і стосується особистого життя, честі та гідності особи, якщо вона не містить доказів злочинної діяльності, не підлягає зберіганню і має бути знищена. Також, Закон України «Про розвідку» гарантує, що конфіденційна інформація про особу, яка стала відома розвідувальним органам під час виконання їхніх завдань, захищена від розголошення, окрім випадків, передбачених законодавством.

Проблеми законодавчого регулювання. Загальні проблеми законодавчого регулювання в сфері правового захисту часто виникають через різні цілі та інтереси, які необхідно збалансувати. На рівні конституції можуть виникати протиріччя між правом громадян на свободу слова та необхідністю забезпечення державної безпеки. З одного боку, Конституція України гарантує кожному право на свободу думки і слова, включаючи право на вільне вираження поглядів, збір та розповсюдження інформації. З іншого боку, ті ж самі конституційні норми дозволяють обмеження цих прав для захисту національної безпеки та громадського порядку [2]. Наприклад, публікація відкритих даних має значний вплив на боротьбу з корупцією, забезпечення відкритості урядових дій та стимулює економічний розвиток. У 2017 році відкриті дані додали до української економіки понад 700 мільйонів доларів, що становить 0,67% від загального внутрішнього продукту країни. Очікується, що за умови збереження поточного рівня розвитку, до 2025 року економічний внесок відкритих даних подвоїться, досягнувши понад 1,4 мільярда доларів, або 0,92% ВВП [3].

Проблеми законодавчого регулювання поширення індивідуальної інформації виникають і в розрізі застосування різних правових документів. Зокрема виникає питання щодо визначення відносин між поняттями «конфіденційна інформація про особу» та «персональні дані», оскільки вони часто використовуються як синоніми. З'ясування цих відносин є важливим аспектом для уточнення предмету кримінального правопорушення, передбаченого статтею 182 Кримінального кодексу України, що стосується порушення конфіденційності.

Таким чином, для ефективного регулювання цифрової конфіденційності необхідний комплексний підхід, який включає застосування та координацію норм різних законів, а також чітке визначення ключових понять і принципів захисту інформації в цифровому середовищі.

Конституційний Суд України вказує, що такий перелік конфіденційної інформації не може бути вичерпним, оскільки особисті та сімейні права включають необмежене коло поведінкових аспектів у приватному житті особи. Це означає, що будь-яка інформація, що стосується особистого життя особи та її сім'ї, може розглядатися як конфіденційна, якщо її розкриття не бажане самою особою. І в даному випадку необхідне чітке розмежування між відкритими даними, персональними даними і відомостями про особисте життя.

Зрозуміло, що ці поняття мають спільні характеристики, адже певні відомості можуть одночасно виступати в різних ролях: як персональні дані, так і як інформація, що характеризує особисте життя індивіда. Ключовим критерієм для визначення статусу цих відомостей є *факт їх обробки*. Тобто, відомості стають персональними даними, коли їх починають збирати, реєструвати, зберігати, адаптувати, змінювати чи знищувати, використовуючи при цьому інформаційні системи.

Законодавство, зокрема Закон України «Про захист персональних даних», детально визначає персональні дані як будь-яку інформацію, пов'язану з ідентифікованою або ідентифікованою особою. Це включає широкий спектр даних, від інформації про особистість до чутливих даних, таких як здоров'я, біометричні та генетичні відомості. Ідентифікація особи може бути здійснена за допомогою різних ознак і властивостей, зокрема за ім'ям, прізвищем, індивідуальним податковим номером або навіть за даними паспорта.

В контексті цифрової ідентифікації, Закон «Про електронні довірчі послуги» вводить поняття «електронної ідентифікації», яка базується на ідентифікаційних даних особи в електронній формі. Це дозволяє однозначно визначати особу при наданні або отриманні електронних послуг. Процес ідентифікації може здійснюватися різними способами, зокрема віддалено, за допомогою

засобів електронної ідентифікації високого рівня довіри або за даними, що містяться в кваліфікованому сертифікаті електронного підпису.

Окрім відкритих даних цифрової конфіденційності, існують інформаційні елементи, які не є доступними для звичайного користувача, зокрема, дані, зібрані через файли cookies та IP-адреси. Ці елементи часто вважаються персональними даними особи, особливо в контексті сучасних норм і регуляцій, таких як GDPR, які визначають широкий спектр інформації як персональні дані. Інформація, отримана за допомогою файлів cookies, майже завжди розглядається як персональні дані, оскільки може містити відомості про поведінкові звички користувачів, їх переваги та інтернет-активність. Що стосується IP-адрес, то як статичні, так і динамічні IP-адреси в руках провайдерів інтернет-послуг зазвичай вважаються персональними даними. Для контролерів, які не є інтернет-провайдерами, статичні IP-адреси вважаються персональними даними у більшості випадків, а динамічні IP-адреси можуть вважатися такими, якщо контролер має можливість ідентифікувати власника IP-адреси.

Збір інформації про користувачів в інтернеті відбувається в багатьох контекстах, починаючи з моменту придбання комп'ютерної техніки та укладання договорів з інтернет-провайдерами, закінчуючи повсякденним використанням інтернет-ресурсів. Специфічні ситуації, такі як реєстрація на сайтах, використання геолокаційних сервісів, відвідування веб-сайтів, які зберігають дані у браузерній історії, а також активність в соціальних мережах, включаючи публікації, повідомлення та використання пошукових систем, є потенційними джерелами збору даних. Важливим є також використання функцій «автозаповнення» та зберігання інформації через файли cookies, які відіграють значну роль у процесі збору даних.

Враховуючи викладене, можна сформулювати наступні важливі висновки для користувачів інтернету, особливо тих, хто перебуває на території України:

- коли cookies завантажуються на пристрій користувача в Україні, це вимагає застосування відповідного українського законодавства про обробку даних користувача. Важливим є розуміння, чи потрібно користувачу давати згоду на таку обробку.
- у випадках, коли для ідентифікації особи відвідувача веб-сайту, з інформації отриманої через cookies, потрібно витратити значні зусилля та час, і якщо така інформація технічно може вважатися конфіденційною, але ідентифікація особи є непрактичною, то ця інформація не вважається персональною. Таким чином, вона не підпадає під дію закону «Про захист персональних даних» України, включно з вимогою про отримання згоди на її обробку чи розповсюдження.

Окрему увагу слід звернути на судову практику, яка підтверджує фактичний збір та використання інформації ресурсами в інтернеті. Наприклад, спір між компанією, що надає рекрутингові послуги, та користувачем, який заперечував використання сервісу, ілюструє, як аналіз системних файлів веб-ресурсу може виявити детальну інформацію про активність користувача, включаючи тривалість сесій та перегляди резюме. Цей випадок підкреслює, що дії користувачів в інтернеті, навіть ті, що здаються незначними, можуть бути зафіксовані та аналізовані власниками веб-сайтів, надаючи їм можливість ідентифікувати користувачів та їхню поведінку в мережі [1].

Законодавство України також визначає певні категорії інформації, які не підпадають під визначення конфіденційної інформації. Згідно з Законом «Про захист персональних даних», не вважаються конфіденційною інформацією відомості, що стосуються здійснення особою офіційних функцій, а також інші дані, які не містять персональних відомостей про приватне життя. Це включає інформацію про виконання особою державних або місцевих обов'язків, дані, зазначені у деклараціях згідно із законом «Про запобігання корупції», інформацію про отримання державних коштів та іншу подібну інформацію. Таке регулювання вказує на необхідність чіткого розмежування між конфіденційною та неконфіденційною інформацією, особливо в контексті забезпечення захисту персональних даних в цифровому середовищі.

Висновок. Цифрова конфіденційність охоплює захист особистої інформації та ідентичності індивідів в онлайн-просторі, включаючи дані, що ідентифікують особу через різноманітні цифрові атрибути та поведінку в інтернеті, як-от профілі в соціальних мережах, історію браузера, фінансову інформацію та інше. Вона забезпечує право індивіда контролювати власні дані, обмежувати їх доступність і використання третіми сторонами, та захищати їх від несанкціонованого доступу або зловмисного використання. Українське законодавство, включаючи Конституцію та спеціалізовані закони, намагається врегулювати цю сферу, враховуючи потребу забезпечення прав на приватність, але також і необхідність захисту державної безпеки, що може призводити

до певних обмежень у використанні особистих даних. Основні проблеми цивільно-правових аспектів цифрової конфіденційності в Україні включають конституційне протиріччя між свободою слова і державною безпекою, відсутність чіткого визначення та розмежування між «конфіденційною інформацією про особу» та «персональними даними», необхідність комплексного підходу до регулювання цифрової конфіденційності через інтеграцію різних законодавчих норм, неможливість створення вичерпного переліку конфіденційної інформації, зважаючи на широкий спектр особистих та сімейних прав, та виклики, пов'язані зі збором та використанням інформації через файли cookies та IP-адреси, що вимагають адекватного правового регулювання для захисту особистих даних та приватного життя користувачів в цифровому середовищі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Зозуля Н. Правовий погляд на cookies або як веб-сайти збирають інформацію про користувачів. Українське право, 2018. URL: https://ukrainepravo.com/scientific-thought/legal_analyst/pravovyy-poglyad-na-cookies-abo-yak-veb-sayty-zbyrayut-informatsiyu-pro-korystuvachiv/.
2. Конституція України. Верховна Рада України; Закон від 28.06.1996 № 254к/96-ВР: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>.
3. Маньгора В.В., Михальчук Ю.О. Використання цифрових технологій у праві: перспективи та виклики. Інформація і право, 2023, 4, 47. URL: <http://il.ippi.org.ua/article/view/291618>.
4. Національна стратегія у сфері прав людини, затверджена Указом Президента України від 24 березня 2021 року №119/2021. URL: <https://zakon.rada.gov.ua/laws/show/119/2021#Text>.
5. Правовий Альянс. Цифрові речі та цифровий контент: новації законодавства, договірні відносини. Лігазакон, 2023. URL: https://biz.ligazakon.net/analytics/223070_tsifrov-rech-ta-tsifroviy-kontent-novats-zakonodavstva-dogovrn-vdnosini.
6. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 5 липня 1994 року № 80/94-ВР. URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>.
7. Про захист персональних даних. Закон України від 01.06.2010 № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>.
8. Про інформацію. Закон України від 02.10.1992 № 2657-XII. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>.
9. Цифрова ідентичність людини. Як її захистити? Укрінформ, 2023. URL: <https://www.ukrinform.ua/rubric-society/3316842-cifrova-identichnist-ludini-ak-ii-zahistiti.html>.
10. Kosinski, M. Stillwell, D.; Graepel, T. Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences*, 2013, 110 (15): 5802–5805. Bibcode:2013PNAS.110.5802K. PMC 3625324. PMID 23479631. doi:10.1073/pnas.1218772110.