

УДК 342.951(004.896)

DOI <https://doi.org/10.32844/2618-1258.2021.1.13>

КОСТЕНКО О.В.

**УПРАВЛІННЯ ІДЕНТИФІКАЦІЙНИМИ ДАНИМИ:
ПРАВОВЕ РЕГУЛЮВАННЯ АНОНІМІЗАЦІЇ ТА ПСЕВДОНІМІЗАЦІЇ****IDENTIFICATION DATA MANAGEMENT:
LEGAL REGULATION AND CLASSIFICATION**

У роботі досліджується питання розробки механізмів правового регулювання управління ідентифікаційними даними в частині їх анонімізації та псевдонімізації. Порівнюються сучасні підходи до створення дефініцій, які з юридичної точки зору описують механізми і процедури анонімізації та псевдонімізації ідентифікаційних даних суб'єктів та об'єктів в інформаційних системах та базах даних. Здійснено огляд правових позицій науковців та організацій, які акцентують увагу на дослідженні тенденцій у формуванні сучасних політик та стратегій управління ідентифікаційними даними.

Проаналізовано стан національного законодавства, що регулює правовідносини у сфері управління ідентифікаційними даними. З'ясовано, що на тепер в Україні не досить приділяється уваги проблемам анонімізації та псевдонімізації даних, а також іншим проблемним питанням у сфері управління ідентифікаційними даними, які розміщені в реєстрах, державних базах даних та інформаційно-комунікаційних системах. Це характеризується відсутністю фахівців у сфері управління ідентифікаційними даними та ситуативною, несистемною і неструктурованою модернізацією національного законодавства, насиченням його не збалансованою юридичною термінологією.

Автором запропоновано сучасне рішення, яке полягає у створенні сучасних нормативно-правових актів, стандартів, юридичних правил та норм управління ідентифікаційними даними. Є нагальна потреба розроблення сучасних дефініцій у цій сфері та формування сучасної нормативно-правової бази, яка здійснюватиме регулювання суспільних відносин у сфері управління ідентифікаційними даними, а також забезпечить необхідне правове регулювання процесами управління ідентифікаційними даними.

Наголошено на доцільності створення комплексного законодавства у сфері управління ідентифікаційними даними, яке забезпечить якісне регулювання суспільних відносин у сфері управління ідентифікаційними даними та інформації, що застосовуються для ідентифікації суб'єктів та об'єктів у державних реєстрах, базах даних та інформаційно-комунікаційних системах.

Комплексне законодавство у сфері управління ідентифікаційними даними має на меті об'єднати сукупність норм, що зосереджені у взаємопов'язаних правових інститутах і інших галузях, та забезпечити регулювання і функціонування цілої сфери життєдіяльності суспільства. Це забезпечить у сфері ідентифікаційних даних запровадження надійних заходів державного контролю та примусу, підвищить рівень відповідного фізичного, технічного, правового регулювання і захисту такого стратегічного інформаційного ресурсу держави.

Ключові слова: *анонім, псевдонім, анонімізація, псевдонімізація, управління ідентифікаційними даними, персональні дані, ідентифікація, ідентифікаційні дані.*

The paper investigates the development of mechanisms for legal regulation of identification data management in terms of their anonymization and pseudonymization. Modern approaches to the creation of definitions are compared, which from the legal point of view describe the mechanisms and procedures of anonymization and pseudonymization

of identification data of subjects and objects in information systems and databases. A review of the legal positions of scientists and organizations that focus on the study of trends in the formation of modern policies and strategies for identity management.

The state of the national legislation regulating legal relations in the field of identification data management is analyzed. It was found that today in Ukraine not enough attention is paid to the problems of anonymization and pseudonymization of data, as well as other problematic issues in the field of identity management, which are placed in registers, state databases and information and communication systems. This is characterized by the lack of specialists in the field of identification data management and situational, unsystematic and unstructured modernization of national legislation, saturation of its unbalanced legal terminology and identity management standards. There is an urgent need to develop modern definitions in this area and form a modern legal framework that will regulate public relations in the field of identity management, as well as provide the necessary legal regulation of identity management processes.

Emphasis is placed on the feasibility of comprehensive legislation in the field of identification data management, which will ensure quality regulation of public relations in the field of identification data management and information used to identify subjects and objects in state registers, databases and information and communication systems.

Comprehensive legislation in the field of identification data management, it aims to unite a set of norms concentrated in interconnected legal institutions and other areas, and to ensure the regulation and functioning of the entire sphere of society. This will ensure the introduction of reliable measures of state control and coercion in the field of identification data, increase the level of appropriate physical, technical, legal regulation and protection of this strategic information resource of the state.

Key words: *anonymous, pseudonym, anonymization, pseudonymization, identification data management, personal data, identification, identification data.*

Вступ. Розвиток інформаційно-комунікаційних технологій та мережі Інтернет у сучасну епоху характеризується експоненціальним створенням інформаційних баз і реєстрів з персональними даними користувачів та їх численним дублюванням. Ці дані використовуються для ідентифікації фізичних та юридичних осіб в інформаційних системах. Нині все більше державних та публічних інформаційних ресурсів відмовляються від політик знеособленого доступу користувачів до інформації на користь їх реальної ідентифікації. Вимоги до ідентифікації суб'єктів є скрізь і стрімко зростають. Користувачі різних систем мають варіаційні набори ідентифікаційних даних, якими потрібно керувати та ототожнювати з конкретною фізичною або юридичною особою. Накопичення персональних та ідентифікаційних даних третіми особами збільшує ризики їх незаконного використання. Фактично ідентифікаційні дані стали стратегічним ресурсом будь-якої держави і потребують відповідного фізичного, технічного та правового регулювання, а також обов'язкового захисту.

Управління ідентифікаційними даними у цифровому світі не має чітко визначеного значення, однак технологічне управління ідентифікацією в її найширшому розумінні належить до адміністрування та характеристик ідентифікаційних атрибутів, управління процесами ідентифікації та використання ідентифікаційних даних. Правове регулювання управління ідентифікаційними даними містить досить законодавчих проблем, які лежать як у площині інформаційного права, так і стосуються інших галузей права.

Серед праць вітчизняних учених, які досліджували проблеми інформаційного права: регулювання застосування персональних даних, систем управління інформаційною безпекою, штучного інтелекту, електронних довірчих послуг, слід виділити: А. Анісімова, І. Арістову, О. Баранова, Ю. Батурина, З. Богатиренко, В. Брижка, Н. Грицяка, І. Горбенка, О. Жуковську, Є. Захарова, Р. Марутяна, А. Минькова, Є. Муньє, В. Пилипчука, О. Потія, О. Радутного, А. Семенченка, В. Цимбалюка, М. Швеця.

Дослідження правових проблем впровадження та використання цифрових технологій у сфері управління ідентифікаційними даними та їх регулювання здійснюється вченими-дослідниками різних країн, але питання юридичних проблем та шляхи їх вирішення знаходяться на початковому етапі. Зокрема, подібні дослідження у сфері регулювання управління ідентифікаційними даними здійснюють учені: Samia Bouzefrane, Ann Cavoukian, Kim Cameron, Kim Tracy,

Marit Hansen, Eleni Kosta, Simone Fischer-Hübner, Elias Pimenidis, Jonathan Kok-Keong Loo, Mahdi Aiash, Jos Dumortier, Jackson Phiri та інші.

Питанням процесів створення та функціонування нормативно-правових інститутів приділено увагу у працях С. Алексєєва, О. Кирімової, І. Казьміна, А. Колодія, Н. Левицької, Л. Луць, А. Міцкевича, С. Полєніної, В. Перевалова, І. Смоценка та інших.

Роботи вказаних та багатьох інших авторів, безперечно, мають наукове і практичне значення, але повною мірою не розкривають проблему управління ідентифікаційними даними. Серед вітчизняних наукових організацій питання анонімізації та псевдонімізації раніше не порушувалося, а українськими вченими подібних досліджень не здійснювалося.

Постановка завдання. Метою статті є дослідження правового забезпечення управління ідентифікаційними даними, а саме: правових механізмів процедури анонімізації та псевдонімізації ідентифікаційних даних, які застосовуються в реєстрах, базах даних та інформаційно-комунікаційних системах для теоретичного обґрунтування та наукової розробки пропозицій удосконалення національного законодавства.

Результати дослідження. Початковий етап розвитку мережі Інтернет характеризується тим, що користувачі в більшості були анонімними або використовували псевдоніми. Ця обставина мало впливала на формування інформаційного простору в мережі. Однак зі стрімким розвитком сучасних інформаційних технологій та Інтернету питання легалізації або ідентифікації користувачів різноманітних сервісів стає нагальним для забезпечення функцій цифрової ідентичності під час персоналізації послуг та інформації. Цифрова ідентичність є версією соціальної ідентичності людини і складається із цифрових атрибутів (даних), що належать та унікально ідентифікують суб'єкта та об'єкта.

Відмінності нормативно-правових актів у різних юрисдикціях щодо використання персональних та ідентифікаційних даних становлять досить різноманітну картину правового регулювання, що ускладнює процеси створення ефективних правових норм. Це характерно для більшості конкретних дефініцій сфери управління ідентифікаційними даними. Особливу актуальність набувають процеси правового регулювання процедур анонімізації та псевдонімізації ідентифікаційних даних як родової похідної персональних даних у мережі Інтернет та різних інформаційно-телекомунікаційних системах.

У сфері управління ідентифікаційними даними регулювання анонімістю та псевдонімізацією має два напрями.

Перший напрям стосується проблематики правового та технічного регулювання процесів анонімізації та псевдонімізації в інформаційно-комунікаційних системах, які оброблюють та зберігають ідентифікаційні та персональні дані. Тобто застосування алгоритмів «камуфлювання», наявних в інформаційних системах ідентифікаційних даних з метою створення штучних перешкод для несанкціонованого доступу третіх осіб до реальної персональної інформації.

Другий напрям характеризується вивченням проблем, пов'язаних зі створенням та застосуванням анонімів та псевдонімів поза межами інформаційних систем. Тобто первинне створення нереальних ідентифікаційних даних реальними користувачами. Самостійно створені псевдоніми або заходи анонімізації можуть застосовуватися як інструментарій для сприяння кіберзлочинам, таким як фішинг, хакерство, кібершахрайство, електронні фінансові злочини, отримання або спроба отримати несанкціонований доступ до інформаційних систем та ресурсів, викрадення даних, зміна інформації або внесення змін до програмного чи апаратного забезпечення систем та пристроїв тощо.

Розглянемо проблеми законодавчого регулювання процедур анонімізації та псевдонімізації в інформаційно-комунікаційних системах.

Натепер ні в Україні, ні у більшості держав не має достатнього практичного досвіду впровадження нормативно-правових актів у сфері управління ідентифікаційними даними. Водночас у державах активно ведуться роботи з правового регулювання захисту персональних даних. Так, понад 80 країн розробили національні регуляторні акти у сфері захисту персональних даних, але практичне застосування вказаних законодавчих актів виявило низку нерегульованих нормами права суспільних відносин, пов'язаних з використанням як персональних даних загалом, так і ідентифікаційних даних зокрема.

Нині базовим документом, за яким пропонується формувати законодавство стосовно захисту персональних даних, є General Data Protection Regulation, Regulation EU 2016/679 (GDPR). Однак GDPR має правовий статус регламенту, а не директиви, тому його застосування не є безпосередньо зобов'язальним і застосовним та не примушує до прийняття законів щодо його впровадження в національні законодавства. У Регламенті 2016/679 питанню псевдонімізації приділено увагу в статтях 25 та 32 як інструментарію захисту та безпеки даних.

Разом із тим за іншими нормативними документами можна більш детально визначити або встановити загальні правила впорядкування дефініцій «анонімізація», «псевдонімізація» та інші з ними пов'язані.

Так, стандарт ISO/TS 25237:2017 визначає псевдонімізацію як конкретний тип розпізнавання, який одночасно вилучає зв'язок із суб'єктом даних і додає зв'язок між певним набором характеристик, що стосуються суб'єкта даних, та одним або кількома псевдонімами. Псевдонім також може визначатися як персональний ідентифікатор, який відрізняється від звичайно використовованого персонального ідентифікатора і використовується з псевдонімізованими даними для забезпечення узгодженості набору даних, що пов'язує всю інформацію про суб'єкта даних, не розкриваючи справжні дані особи. Цим стандартом надається визначення анонімізації як процесу, за допомогою якого персональні дані безповоротно змінюються таким чином, що суб'єкт даних більше не може бути ідентифікований прямо або опосередковано, ні самим контролером даних, ні у співпраці з будь-якою іншою стороною [1].

Такий стандарт цікавий тим, що містить принципи та вимоги щодо захисту конфіденційності із використанням служб псевдонімізації для захисту інформації у сфері охорони здоров'я. Визначає одне базове поняття для псевдонімізації; одну основну методологію служб псевдонімізації, включаючи організаційні, а також технічні аспекти; структуру політики та мінімальні вимоги до контролюваної повторної ідентифікації; надає огляд різних випадків використання псевдонімізації, які можуть бути як оборотними, так і незворотними.

Національний інститут стандартів і технологій Сполучених Штатів Америки (NIST) визначає поняття «псевдонімізація» як конкретний тип деідентифікації, який одночасно усуває зв'язок із суб'єктом даних і додає зв'язок між певним набором характеристик, що стосуються суб'єкта даних, та одним або кількома псевдонімами. Як правило, псевдонімізація здійснюється шляхом заміни прямих ідентифікаторів псевдонімом, такими, наприклад, як випадково згенеровані значення [2].

У міжвідомчих та внутрішніх звітах NIST, пов'язаних з кібербезпекою та конфіденційністю (NISTIR), запропоновані такі визначення:

- анонімість – це умова в ідентифікації, згідно з якою суб'єкт не може бути визнаний без достатньої інформації про нього для встановлення зв'язку з відомим суб'єктом [3];
- анонімізацією є процес, який усуває зв'язок між ідентифікуючим набором даних та суб'єктом даних [4];
- анонімізованими даними вважаються дані, з яких одержувач інформації не може ідентифікувати суб'єкта [5];
- анонімізована інформація – це попередньо ідентифікована інформація, яка була деідентифікована і для якої більше не існує коду чи іншої асоціації для повторної ідентифікації [6];
- анонімним ідентифікатором особи є ідентифікатор, який не дозволяє однозначно ідентифікувати фізичну особу [7].

Звіти NISTIR також формулюють визначення терміна «псевдонім» як: ім'я особи, вибране особою, яке не підтверджується як значуще за допомогою підтвердження особи та яке використовується для захисту справжньої особистості особи [8]; ім'я, відмінне від офіційного [9]; персональний ідентифікатор, який відрізняється від персонального ідентифікатора, який зазвичай застосовується особою; всі неправдиві або неперевірені імена вважаються псевдонімами.

Псевдонімістю вважається використання псевдоніма для ідентифікації предмета. Таким чином, псевдонімізацію можна визначити як конкретний тип деідентифікації, який одночасно усуває зв'язок із суб'єктом даних і додає зв'язок між певним набором характеристик, що стосуються суб'єкта даних, та одним або кількома псевдонімами. Як правило, псевдонімізація здійснюється шляхом заміни прямих ідентифікаторів псевдонімом, таким як випадково згенероване значення [10].

Також псевдонімізація визначена у статтях 4, 5 GDPR як обробка персональних даних таким чином, що ці дані більше не можуть бути віднесені до конкретного суб'єкта без використання додаткової інформації, за умови, що така додаткова інформація зберігається окремо та підлягає технічним та організаційним заходам захисту для забезпечення того, щоб персональні дані не відповідали ідентифікованому суб'єкту.

Звертаємо увагу на те, що дані псевдонімізації не слід прирівнювати або сприймати як анонімні дані, незважаючи на те, що обидва процеси стосуються дійсних ідентифікаційних даних, які наявні в інформаційних системах. Відмінність їх полягає в тому, що псевдонімізація пов'язана із чітким наявним асоціативним зв'язком між особистими ідентифікаторами та псевдонімами.

Водночас анонімізація апіорі виключає будь-який зв'язок анонімних даних з реальними ідентифікаційними даними суб'єктів. Таким чином, анонімні дані не належать до різновиду персональних даних.

Активні дослідження в напрямі процедур та методів анонімізації та псевдонімізації здійснюються робочою групою Департаменту юстиції захисту прав споживачів та гендерної рівності Європейської комісії (ENISA) та британським національним постачальником інформації, даних та ІТ-систем для уповноважених, аналітиків та клініцистів у галузі охорони здоров'я, соціальної допомоги обслуговування (NHS).

Цими організаціями розглядаються такі методи анонімізації та псевдонімізації ідентифікаційних даних, що перебувають у відносно статичному стані, тобто, які зберігаються у файлах або базах даних [11; 12; 13]:

- додавання шуму, тобто внесення умисної похибки чи неточності до вихідних даних;
- заміна, під час якої інформаційні значення вихідних даних замінюються іншими параметрами;
- агрегація або об'єднання в групах даних за найбільш поширеними для групи даними;
- К-анонімність як форма агрегування, що перешкоджає повторній ідентифікації, видаляючи окрему інформацію, але залишаючи цілі цілими для подальшого використання;
- L-різноманітність захищає анонімність, надаючи кожному атрибуту, принаймні L, різних значень;
- диференційована конфіденційність, яка формує анонімний набір даних для забезпечення зовнішнього доступу до інформації третій стороні, водночас залишає оригінальні ідентифікаційні дані під захистом;
- хеш-функції для зіставлення даних будь-якого розміру з кодами фіксованого розміру;
- токенизація, за допомогою якої певні компоненти даних замінюються нечутливим еквівалентом (лексемою). Маскування або приховування частини ідентифікатора особи випадковими символами або іншими даними;
- скремблювання даних шляхом застосування загальних прийомів змішування або затуманення персонажів;
- розмиття даних шляхом використання наближених значень даних для зменшення точності реальних даних та можливості ідентифікації;
- класифікація довідкової інформації або маркування штрих-кодами, QR-кодами тощо;
- видалення прихованих метаданих з файлів.

В Україні також вживаються певні заходи щодо технічної організації та розвитку процесів електронної ідентифікації, які спрямовані на виключно технічні способи ідентифікації. Національне законодавство безперервно модернізується та поповнюється новими нормативно-правовими актами та дефініціями, однак сучасна національна законодавча база неповною мірою відображає реальний стан реагування держави на суспільну трансформацію.

Натепер в Україні задекларовано 22 схеми електронної ідентифікації надавачів електронних довірчих послуг, 32 схеми електронної ідентифікації банків-ідентифікаторів системи BankID Національного банку України, 3 схеми електронної ідентифікації надавачів послуг MobileID, 4 схеми електронної ідентифікації на основі хмарного підпису та 1 схема електронної ідентифікації на основі ID-картки. Законодавча регуляція окремих процесів ідентифікації здійснюється Законом України «Про електронні довірчі послуги», Постановою правління Національного банку України від 30.08.2016 № 378 «Про затвердження Положення про Систему BankID Національного банку України» та Постановою Кабінету Міністрів України від 19.07.2019 № 546 «Про затвердження Положення про інтегровану систему електронної ідентифікації».

Зважаючи на викладене вище, з'ясовано, що питання анонімізації та псевдонімізації ідентифікаційних даних у національному законодавстві в повному обсязі не вивчалося, відсутні норми та дефініції, які повинні стати основою нормативно-правових актів у сфері управління ідентифікаційними даними. Це характерно загалом для законодавства України.

Нині в Україні склалася ситуація, коли у всі сфери суспільного життя стрімкими темпами впроваджуються сучасні інформаційно-комунікаційні технології за фактичної відсутності правових інститутів управління ідентифікаційними та персональними даними, біометрією, пристроями IoT та штучним інтелектом. Водночас наявна нормативно-правова база України застаріла та фактично недостатньо відповідає стану суспільних відносин [14]. Прийняті регуляторні акти носять загальний характер або є суто технічними, що оминають правові проблеми у сфері управління ідентифікаційними даними, незважаючи на очевидну необхідність впровадження масштабованих методологій та найкращих практик управління даними, які впроваджено в інших країнах світу.

Слід зазначити, що насамперед правове регулювання суспільних відносин у сфері управління ідентифікаційними даними носить комплексний характер – поєднує норми інформаційного, адміністративного, цивільного, кримінального, трудового та інших галузей і інститутів права, а також інститутів забезпечення безпеки держави, інформаційної та кібербезпеки. Отже, правовий режим регулювання та методи цих галузей та інститутів відрізняються, однак з метою забезпечення єдиного і комплексного правового регулювання таких відносин необхідно здійснити специфічне поєднання цих методів і режимів, що і має забезпечуватися комплексним інститутом права управління ідентифікаційними даними.

Висновки. Україна потребує найскорішого впровадження масштабного реінжинірингу всіх електронних ресурсів держави, модернізації інформаційно-комунікаційних систем та адміністративно-управлінських процесів. При цьому правовий режим регулювання та методи цих галузей та інститутів відрізняються, однак з метою забезпечення єдиного і комплексного правового регулювання таких відносин необхідно здійснити специфічне поєднання цих методів і режимів.

Таким чином, необхідно доповнити основні положення окремих галузей права, в тому числі у сфері кібербезпеки та національної інформаційної безпеки, новими нормами права з урахуванням розвитку сфери управління ідентифікаційними даними, що підвищить рівень відповідного фізичного, технічного, правового регулювання і захисту стратегічного інформаційного ресурсу держави.

Питання, що пов'язані з управлінням ідентифікаційними даними, в тому числі юридичні механізми забезпечення процедур анонімізації та псевдонімізації ідентифікаційних даних у національному законодавстві, необхідно вирішувати комплексною розробкою сучасних нормативно-правових актів у сфері управління ідентифікаційними даними.

Список використаних джерел:

1. ISO 25237:2017 Health informatics – Pseudonymization. URL: <https://www.iso.org/standard/63553.html>
2. Information Technology Laboratory Computer Security Resource Center. Pseudonymization. URL: <https://csrc.nist.gov/glossary/term/pseudonymization>.
3. ISO / IEC 24760-1: 2011 Information technology – Security techniques – A framework for identity management. Part 1: Terminology and concepts. Anonymity. URL: <https://csrc.nist.gov/glossary/term/anonymity>.
4. ISO / TS 25237: 2008 Information Technology Laboratory Computer Security Resource Center pseudonymization. Anonymization. URL: <https://csrc.nist.gov/glossary/term/anonymization>.
5. ISO / TS 25237: 2008 Information Technology Laboratory Computer Security Resource Center pseudonymization. Anonymized data. URL: https://csrc.nist.gov/glossary/term/anonymized_data.
6. NIST SP 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII). Anonymized Information. URL: https://csrc.nist.gov/glossary/term/Anonymized_Information.
7. NISTIR 8053 ISO/TS 25237: 2008. URL: https://csrc.nist.gov/glossary/term/anonymous_identifier.
8. CNSSI 4009-2015 Committee on National Security Systems (CNSS) Glossary. April 2015. URL: <https://www.cnss.gov/CNSS/openDoc.cfm?uaq+Vxc4+Ff0fLwbRuhSVw==>.
9. NIST Special Publication 800-63-3 Digital Identity Guidelines. June 2017. URL: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf>.
10. NISTIR 8053 De-Identification of Personal Information. October 2015. URL: <https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf>.
11. European Commission, Justice and Consumers, Newsroom, Article 29 Working Party, Opinion No. 05/2014 on Anonymization Techniques. URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.
12. Cédric Burton, Sára Hoffman. Personal Data, Anonymization, and Pseudonymization in the EU. September 2015. URL: https://www.wsgrdataadvisor.com/2015/09/personal-data-anonymization-and-pseudonymization-in-the-eu/#_ftnref1.
13. National Health Service. Pseudonymisation and anonymisation of data policy. NHS Business Services – Pseudonymisation and anonymisation of data policy. NHSBSAPA001. April 2015. URL: <https://www.nhs.uk/sites/default/files/2017-05/anonymisation-of-data-policy.pdf>.
14. Kostenko O.V. Identification data management (identification): problem of the conceptual and categorical apparatus. Collective monograph. Cuiavian University in Wloclawek. Wloclawek, Poland. 2021. P. 317–324.