ЮРИДИЧНІ НАУКИ

DOI: <https://doi.org/10.32839/2304-5809/2021-3-91-21>

УДК 342.951(004.896)

Костенко О.В.

НДІ інформатики і права
Національної академії правових наук України

УПРАВЛІННЯ ІДЕНТИФІКАЦІЙНИМИ ДАНИМИ: ПРАВОВЕ РЕГУЛЮВАННЯ ТА КЛАСИФІКАЦІЯ

Анотація. Масштаби, швидкість та багатовекторність розвитку науки і техніки надзвичайно ефективно впливають на правові, економічні, політичні, духовні, професійні та інші суспільних відносин. Однією із рушійних сил нової науково-технічної революції є розвиток інформаційно-комунікаційних технологій, використання мережі Інтернет, створення, збереження, передача, обробка та управління інформацією. Це сприяє впровадженню технологій передачі та використання інформації в цифровому виді практично у всіх сферах суспільного життя, а саме текстових даних, фото-, аудіо-, відеозображень, які транслюються різноманітними способами мережею Інтернет та іншими комунікаційними засобами та системами. Одним із ключових елементів технологій та систем передачі даних є наявність інформації, за якою можливо ідентифікувати їх суб'єктів та об'єктів за притаманними ним ідентифікаційними атрибутами. В українському законодавстві, зокрема в Законі України «Про захист персональних даних», відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована визначають як персональні дані. Однак, незважаючи на сучасність даний закон все ж таки містить ряд недоліків та невизначеності, як в термінології так і в правових механізмах роботи із даними, за якими може бути ідентифікована особа, тобто ідентифікаційними даними.

Ключові слова: пристрої IoT, ідентифікаційні системи, управління ідентифікаційними даними, ідентифікація, ідентифікаційні дані, технічні стандарти, штучний інтелект, електронні довірчі послуги.

Kostenko Oleksii

Institute of Informatics and Law of the
National Academy of Legal Sciences of Ukraine

IDENTIFICATION DATA MANAGEMENT: LEGAL REGULATION AND CLASSIFICATION

Summary. The scale, speed and multi-vector development of science and technology are extremely effective in influencing legal, economic, political, spiritual, professional and other social relations. One of the driving forces of the new scientific and technological revolution is the development of information and communication technologies, the use of the Internet, the creation, storage, transmission, processing and management of information. This facilitates the introduction of technologies for the transmission and use of information in digital form in almost all spheres of public life, namely text data, photo, audio, video images, which are transmitted in various ways via the Internet and other means of communication and systems. The theoretical and methodological basis of the article began scientific developments of domestic and foreign scientists on topical problems in the information sphere and the field of law, which are mostly devoted to the problem of regulating the use of personal data, internet devices, information security systems, artificial intelligence, electronic trust services. One of the key elements of data transmission technologies and systems is the availability of information by which it is possible to identify their subjects and objects by their inherent identification attributes. In Ukrainian legislation, in particular in the Law of Ukraine «On Personal Data Protection», information or a set of information about an individual who is identified or can be specifically identified is defined as personal data. However, despite its modernity, this law still contains a number of shortcomings and uncertainties, both in terminology and in the legal mechanisms for working with data by which a person can be identified, ie identification data. The proposed solutions will contribute to the formation of the latest social relations and legal rules in the field of identity management and meet the needs of citizens, government and commercial organizations in legal instruments that will ensure the legal significance of transactions using any credentials. This will help increase trust in electronic services, secure identification of entities and objects, and ensure reliable protection of identification and personal data.

Keywords: IoT devices, identification systems, identification data management, identification, identification data, technical standards, artificial intelligence, electronic trust services.

Постановка проблеми. На даному етапі розвитку суспільних відносин більше за-
требувані питання вирішення проблеми захисту ідентифікаційних даних. В той же час питання створення об'єднаної ідентифікаційної системи із прозорими та дієвими технічними та юридичними правилами управління ідентифікаційними даними комплексно не розглядалося і наразі є вкрай актуальним.

Аналіз останніх досліджень і публікацій. Теоретико-методологічним підґрунтям статті стали наукові розробки вітчизняних і зарубіжних учених з актуальних проблем у інформаційній сфері та сфері права, які здебільшого присвячені проблематиці регулювання застосування персональних даних, пристроїв Інтернет речей, систем управління інформаційною безпекою, штучного інтелекту, електронних довірчих послуг.

Так, серед вітчизняних варто виділити праці: А. Анісимова, І. Арістової, О. Баранова, Ю. Батурина, І. Бачило, К. Белякова, В. Брижка, Н. Грицяк, І. Горбенко, В. Пилипчука, О. Радутного, А. Семенченка, Ю. Тихомирова.

Дослідження правових проблем впровадження та використання цифрових технологій в сфері управління ідентифікаційними даними та їх правового регулювання здійснюються вченими дослідниками різних країн, але як і постановка юридичних проблем, так і шляхи їх вирішення все ще знаходяться на початковому етапі. Зокрема, подібні дослідження в сфері регулювання управління ідентифікаційними даними здійснюються такими вченими як: S. Bouzefrane, K. Cameron, K. Tracy, M. Hansen, E. Kosta, Simone Fischer-Hübner, Elias Pimenidis, J. Loo, M. Aiash, C. Thompson, A. Cavoukian та інші.

Виділення невирішених раніше частин загальної проблеми. Роботи вказаних та багатьох інших авторів, безумовно, мають наукове і практичне значення, але вони не дають цілісного уявлення про сучасну єдину систему управління ідентифікаційними даними. Серед вітчизняних наукових організацій питання запропонованих досліджень раніше не здійснювались, а українськими вченими результати подібних досліджень поки що не оприлюднені.

Мета статті. Розробка пропозицій та рекомендацій щодо створення єдиного класифікатора ідентифікаційних даних, критеріїв та механізмів їх застосування, формування нових дефініцій для розвитку понятійно-категоріального апарату сфери управління ідентифікаційними даними та удосконалення існуючих.

Виклад основного матеріалу. Сучасне суспільство увійшло у науково-технічну революцію 4.0, економічну глобалізацію та створення новітньої планетарної комунікаційної інфраструктури. Сьогодні мережа Інтернет як інформаційно-комунікаційне середовище кожної хвилини дає можливість створювати нові способи спілкування та створення знань, обміну даними, здійснення транзакцій між користувачами. Фактично Інтернет сприяє створенню сучасних соціальних структур та суспільних відносин, які в повсякденному житті ще не піддані правовому регулюванню.

Як відомо, Інтернет складається з мільйонів локальних і глобальних приватних, публічних, академічних, ділових і урядових мереж, пов'язаних між собою з використанням різноманітних технологій і базується на принципі відсутності централізованого управління, правил використання чи доступу. Централізовано визначаються лише правила використання адресного простору Інтернет-протоколу та Системи доменних імен.

Ідентифікація людини спочатку будувалась на форматі електронних адрес. Однак, така система не задовольнила виникаючої потреби суспільства в достовірній ідентифікації користувачів, що спричинило створенню різноманітних систем та видів ідентифікаторів, політик та схем ідентифікації. Цей набір технологій та схем ідентифікації постійно створює у суспільства правові проблеми, пов'язані із юридичною регуляцією процесів ідентифікації як на національному, так і на транснаціональному рівні.

Загальний результат цих різновекторних рішень полягає в тому, що громадяни, організації, державні установи не можуть вільно і швидко ідентифікувати своїх партнерів по спілкуванню на індивідуальному рівні [1]. Внаслідок відсутності єдиної ідентифікаційної структури суб'єктам правовідносин часто доводиться застосовувати широкий спектр персональних даних в якості ідентифікаційних даних [2].

Сьогодні ідентифікаційні дані суб'єктів є важливими інформаційним активом, який напряму впливає на суспільні відносини в багатьох сферах життєдіяльності людини. Також суспільної актуальності набувають процеси управління ідентифікаційними даними пристроїв IoT та інформаційно-технологічних продуктів із штучним інтелектом.

Вимоги до ідентифікації є скрізь і стрімко зростають [3]. Користувачі різних систем мають варіаційні набори ідентифікаційних даних, якими потрібно керувати та ототожнювати із 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, правового регулювання і захисту.

Однак відсутність уніфікованих технічних та юридичних положень щодо управління ідентифікаційними даними стримує розробку інфраструктури планетарної метасистеми ідентичності на заміну існуючого малоефективного набору із ізольованих, несумісних, вибіркового рішень.

Слід зауважити, що вірогідність запровадження єдиної планетарної цифрової метасистеми ідентифікації не слід очікувати в найближчому майбутньому. Про це свідчать результати роботи четвертої робочої групи UNCITRAL. Багато країн розцінюють створення метасистеми ідентифікації як репресивний захід, що може призвести до створення авторитарного режиму. Разом з тим функціонування окремих інтероперабельних систем ідентифікації вважається більш доцільним, що зробить Інтернет більш безпечнішим середовищем та підвищить його потенціал для прискорення електронної комерції та вирішення інших проблем цифрової ідентичності.

Управління цифровою особистістю в електронному світі не має чітко визначених правових критеріїв. Водночас технологічне та правове регулювання управління ідентифікацією в широкому сенсі можливо здійснити відносно конкретизованих атрибутів ідентифікаційних даних фізичних та юридичних осіб, пристроїв IoT та інформаційно-технологічних продуктів із штучним інтелектом [4; 5]. Однак це може лише частково мінімізувати комплекс правових питань що знаходиться під куполом загальної проблеми управління ідентифікаційними даними. Тобто правова проблема управління ідентифікаційними даними полягає в існуванні різних систем ідентифікації та різних правових підходах та рішеннях як на національному так і на транснаціональному рівнях [6]. Розвиток сучасних суспільних відносин в таких сферах як е-освіта, е-комерція, е-медицина, е-банкінг тощо фактично стримується через відсутність надійних юридичних механізмів управління ідентифікацій-

ними даними, які здатні надати онлайн та в даний момент підтвердження відповідності суб'єкта (об'єкта) пред'явленим ним атрибутам, за якими отримується доступ до інформаційних ресурсів.

Національне інформаційне законодавство містить понад 4 тис. нормативно-правових актів, які регулюють суспільні відносини в інформаційній сфері. Водночас, питання правового забезпечення суспільних відносин, що базуються на використанні цифрових технологій, в тому числі й управління ідентифікаційними даними, і мають відношення до їх впровадження, врегульовані лише частково і потребують подальшого системного опрацювання.

Як і більшість держав світу, Україна потребує масштабного реінжинірингу всіх електронних ресурсів держави, модернізації інформаційно-комунікаційних систем та адміністративно-управлінських процесів. Україною вживаються певні зусилля в напрямку технічної організації та розвитку процесів електронної ідентифікації, які спрямовані на виключно технічні способи ідентифікації. В той же час сучасна національна законодавча база не повною мірою відображає реальний стан реагування держави на суспільну трансформацію.

Склалася ситуація, коли в Україні у всі сфери суспільного життя швидкими темпами впроваджуються сучасні інформаційно-комунікаційні технології при фактичній відсутності правових інститутів управління ідентифікаційними та персональними даними, біометрією, пристроями IoT та штучним інтелектом [7].

Вирішення правових проблем у сфері управління ідентифікаційними даними пропонується здійснити в наступних напрямках

Розробити уніфіковану модель суспільних відносин в сфері управління ідентифікаційними даними в якій врахувати управління ідентифікаційними даними не тільки фізичних та юридичних осіб але й пристроїв IoT та інформаційно-технологічних продуктів із штучним інтелектом. Закласти фундамент формування правового простору довіри – національного домену довіри.

Застосувати принцип одного із трьох основних механізмів об'єктно-орієнтованого програмування – інкапсуляцію – з метою розробки та створення сучасних правових конструкцій для регулювання сфери управління ідентифікаційними даними. Тобто розробити модульні правові конструкції, які би мали уніфіковані правові норми та алгоритми їх застосування саме в сфері управління ідентифікаційними даними. Такі модульні правові конструкції призначені для регулювання суспільних відносин, що виникають під час застосування ідентифікаційних даних на різних ієрархічних рівнях правовідносин від умовно побутового до транскордонного. Застосування такої схеми дозволить кожній організації, державному органу, державі вибудувати вертикально інтегрований власний модуль, який незалежно від технологій реалізації забезпечить транзит ідентифікаційних даних, створених та юридично значимих згідно національних норм права в транскордонному середовищі довіри.

Необхідно сформулювати парадигму управління ідентифікаційними даними контексті теоретико-правових засад, а саме представити

правове регулювання процесів управління ідентифікаційними даними як саморегуляцію складних ієрархічних систем ідентифікації в умовах правової невизначеності, із послідовним створенням та забезпеченням функціонування правового простору довіри, тобто створення шляхів подолання правової нестабільності та переходу до стабільного етапу розвитку сфери управління ідентифікаційними даними.

Запропоновані підходи потребують спільної масштабної роботи фахівців у сфері інформаційних технологій, інформаційного та інших сфер права. Фактично потрібно створити новий глосарій визначень та норм в сфері управління ідентифікаційними даними шляхом трансляції та модернізації технічних норм в техніко-юридичні та юридичні. Це забезпечить логічний зв'язок між технічною та юридичною складовою нормативної бази в сфері управління ідентифікаційними даними.

Першим кроком в цьому напрямку стане розробка уніфікованого класифікатора ідентифікаційних даних. Слід враховувати, що ідентифікаційні дані це персональні дані (атрибути) фізичних та юридичних суб'єктів, які застосовуються для процесів автентифікації та ідентифікації в інформаційно-комунікаційних системах. До класу ідентифікаційних даних також слід віднести атрибути ідентифікації пристроїв IoT та інформаційно-технологічних продуктів із штучним інтелектом.

Безумовно, класифікація атрибутів ідентифікаційних даних повинна базуватися на аналізі методів ідентифікації суб'єктів та об'єктів, в тому числі пристроїв IoT і штучного інтелекту, проблем та рішень правового регулювання їх застосування. На нашу думку недоцільно застосовувати загальноприйняті градації персональних даних. Так у міжнародному законодавстві визнається умовний поділ персональних даних на дві групи: дані «загального змісту» та особливі категорії відомостей, що визначаються як дані «вразливі» або «чутливі» [8]. Проте поняття «чутливих» персональних даних, що нерідко вживається як у законодавстві Європейського Союзу, так і в багатьох рішеннях національних і міжнародних судів (зокрема, такий термін уживається у більш ніж десяти рішеннях Європейського суду з прав людини), не набуло однозначного тлумачення та вичерпного роз'яснення: чим саме і чому дані фізичної особи є «чутливими». Українською поставало питання, які категорії даних варто відносити до «чутливих», урешті, чому їм слід надавати більший рівень захисту, ніж іншим даним [9]. Зважаючи на невизначеність із конкретним змістом «вразливих», «чутливих» або «надчутливих» персональних даних та враховуючи що вони в якості ідентифікаційних даних використовуються в інформаційно-комунікаційних системах вважаємо за доцільне застосувати класифікацію їх на основі загальноприйнятого класифікатора небезпеки за кольорами.

По-перше, це дозволить чітко розмежувати дані за класами атрибутів ідентифікаційних даних та рівнями безпеки, а також рівнями загроз та наслідків у разі їх незаконного використання.

По-друге, у людини на інтуїтивному рівні у хвилини небезпеки уява працює на ототожнен-

ня кольорів із рівнем загрози життю – червоний, помаранчевий, жовтий, зелений. Відповідно пропонується розділити атрибути ідентифікаційних даних на чотири групи за важливістю даних для життєдіяльності людини, напрямку використання та цінності даного інформаційного ресурсу для держави [10].

Так, до атрибутів ідентифікаційних даних «червоної» групи, на нашу думку, доцільно віднести:

Ідентифікаційні біометричні атрибути фізичної особи:

– Статичні атрибути: ДНК, форма скелету, 2D-3D зображення та термограма обличчя, група крові, візерунки сітківки та райдужної оболонки ока, капілярні візерунки долоні, відбитки пальців, вушні раковини, характеристики окремих органів, тощо.

– Динамічні атрибути: голосові характеристики, біомеханічні характеристики рухів, фізіологічні особливості моторики, просторові елементи (пози, положення, прості суглобові рухи, групи одночасних, ряди послідовних і послідовних рухів), інформаційна структура рухів (сенсорні, психологічні, рефлексорні, поведінкові).

Ідентифікаційні атрибути інформаційно-технологічних продуктів із штучним інтелектом, кіберфізичних систем, роботів-андроїд ASI класу III, супер III: квантовий цифровий підпис, коди керування та блокування, інші технології ідентифікації, що будуть застосовані для ідентифікації III.

Ідентифікаційні атрибути пристроїв IoT, що застосовуються в пристроях нейро/кардіо-медицини, військовій техніці та зброї, на об'єктах критичної інфраструктури, виведення з ладу або порушення функціонування яких може становити критичну (фатальну) загрозу для життя і здоров'я людей: Object Identifier (OID), електронний код продукту (EPC), універсально унікальний ідентифікатор Identifier (UUID), міжнародний ідентифікатор мобільного обладнання Identity (IMEI), ID-ключ, кваліфікований цифровий ключ, квантовий ключ.

До атрибутів ідентифікаційних даних «помаранчевої» групи доцільно віднести:

Документальні атрибути фізичної особи: П.І.Б., ПН, паспорт громадянина України, паспорт громадянина України для виїзду за кордон, дипломатичний паспорт України, службовий паспорт України, ID-картка, посвідчення особи моряка, посвідчення члена екіпажу, посвідчення особи на повернення в Україну, тимчасове посвідчення громадянина України, посвідчення водія, посвідчення особи без громадянства для виїзду за кордон, посвідка на постійне проживання, посвідка на тимчасове проживання, картка мігранта, посвідчення біженця, проїзний до-

кумент біженця, посвідчення особи, яка потребує додаткового захисту, проїзний документ особи, який надано додатковий захист.

Ідентифікаційні атрибути юридичної особи, що здійснює діяльність в сфері медицини, оборони, захисту держави та на об'єктах критичної інфраструктури: найменування юридичної особи згідно з Єдиним державним реєстром підприємств та організацій України, ідентифікаційний код юридичної особи згідно з Єдиним державним реєстром, реєстраційний номер облікової картки платника податків або серія (за наявності) та номер паспорта.

Ідентифікаційні атрибути інформаційно-технологічних продуктів із штучним інтелектом, роботів та роботів-андроїдів класу AAI, AAIІ: програмні коди, коди зовнішнього керування та блокування, інші технології ідентифікації.

Ідентифікаційні атрибути пристроїв IoT, що застосовуються в пристроях нейро/кардіо-медицини, військовій техніці та зброї, на об'єктах критичної інфраструктури, виведення з ладу або порушення функціонування яких може становити потенційну загрозу для життя і здоров'я людей: Object Identifier (OID), електронний код продукту (EPC), універсально унікальний ідентифікатор Identifier (UUID), міжнародний ідентифікатор мобільного обладнання Identity (IMEI), ID-ключ, кваліфікований цифровий ключ, квантовий ключ.

До групи «жовті» та «зелені» пропонується включити атрибути ідентифікаційних даних: сертифікати та ідентифікаційні документи, видані неурядовими організаціями, будь-яка інформація, яку за власним бажанням розповсюджує особа, також або третя сторона за згодою в межах своєї професійної компетенції (за винятком даних секторів «червоного» та «помаранчевого»). Перелік атрибутів «Жовтої» та «зеленої» груп можуть мати досить великий список ідентифікаційних даних, що використовуються в недержавних цифрових ресурсах.

Висновки і пропозиції. Запропоновані рішення сприятимуть формуванню новітніх суспільних відносин формування і права в сфері управління ідентифікаційними даними та задоволення потреб громадян, державних й комерційних організацій в правових інструментах, які забезпечать юридичну значимість транзакцій із застосуванням будь-яких ідентифікаційних даних. Це сприятиме зростанню довіри до електронних сервісів, надійній ідентифікації суб'єктів та об'єктів, забезпеченню надійного захисту ідентифікаційних та персональних даних, за умов термінової модернізації та узгодження положень вітчизняного законодавства з положеннями міжнародних стандартів.

Список літератури:

1. Elias Pimenidis Digital Identity Management 2014. URL: <https://www.researchgate.net/publication/259972539>
2. Cavoukian A. (2006) Laws of identity the case for privacy-embedded laws of identity in the digital age. URL: http://www.ipc.on.ca/images/Resources/up-7laws_whitepaper.pdf
3. Kim Cameron. The Laws of Identity Architect of Identity and Access Microsoft Corporation. URL: <http://www.identityblog.com>
4. Kim Tracy Identity management systems 2008. URL: <https://www.researchgate.net/publication/260492739>
5. Marit Hansen Privacy and identity management // Curity & Priva Cymar ChaPril. 2008. P. 38–45.
6. Samia Bouzebrane, Khaled Garri, Pascal Thoniell. A user-centric PKI based-protocol to manage FC2 digital identities Le Centre pour la Communication Scientifique Directe 2011. URL: <https://hal.archives-ouvertes.fr/hal-00628633>

7. Романов В., Галелюка І., Галелюка О. На часі – біометрична ідентифікація особи в Україні. *Світогляд*. 2010. № 6. С. 42–45.
8. Різак М.В. Класифікація персональних даних як необхідний елемент введення ефективної комунікації в суспільстві. *Науковий вісник Міжнародного гуманітарного університету. Сер. Юриспруденція*. 2013. № 6-3. Том 1. С. 91–95.
9. Литвиненко А.А. До питання визначення та нормативного змісту «чутливих персональних даних». *Науковий вісник публічного та приватного права*. 2020. С. 160–172.
10. Kostenko O.V. Identification data: legal mechanisms development of classifiers. *Social and Economic Aspects of Education in Modern Society*. 2021. P. 22.

References:

1. Elias Pimenidis. Digital Identity Management 2014. URL: <https://www.researchgate.net/publication/259972539>
2. Cavoukian A. (2006) Laws of identity the case for privacy-embedded laws of identity in the digital age. URL: http://www.ipc.on.ca/images/Resources/up-7laws_whitepaper.pdf
3. Kim Cameron. The Laws of Identity Architect of Identity and Access Microsoft Corporation. URL: <http://www.identityblog.com>
4. Kim Tracy. Identity management systems 2008. URL: <https://www.researchgate.net/publication/260492739>
5. Marit Hansen (2008) Privacy and identity management. *Curity&Privacy*, pp. 38–45.
6. Samia Bouzebrane, Khaled Garri, Pascal Thoniell. A user-centric PKI based-protocol to manage FC2 digital identities Le Centre pour la Communication Scientifique Directe 2011. URL: <https://hal.archives-ouvertes.fr/hal-00628633>
7. Romanov V., Galeuka I. (2010) On time – biometric identification of a person in Ukraine *Worldview*, no. 6, pp. 42–45.
8. Rizak M. (2013) Classification of personal data as a necessary element of the introduction of effective communication in society. *Scientific Bulletin of the International Humanities University. Ser. Jurisprudence*, no. 6-3, vol. 1, pp. 91–95.
9. Lytvynenko A. (2020) On the issue of definition and normative content of "sensitive personal data". *Scientific Bulletin of Public and Private Law*, issue 2, pp. 160–172. DOI: <https://doi.org/10.32844/2618-1258.2020.2.27>
10. Kostenko O. (2021) Identification data: legal mechanisms development of classifiers. *Social and Economic Aspects of Education in Modern Society*, p. 22.