УДК 342.738
DOI https://doi.org/10.32782/TNU-2707-0581/2026.5/32

Пішта В. І.
https://orcid.org/0000-0003-2769-7189
Державний вищий навчальний заклад «Ужгородський національний університет»

Віхляєв М. Ю.
https://orcid.org/0000-0002-1906-5176
Державний вищий навчальний заклад «Ужгородський національний університет»

ПРАВО КОРИСТУВАЧА ПІДКЛЮЧЕНОГО ПРОДУКТУ НА ДОСТУП ДО ДАНИХ ІНТЕРНЕТУ РЕЧЕЙ ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ТРЕТІХ ОСІБ: ПІДХОДИ ЄС ТА ПЕРСПЕКТИВИ ДЛЯ УКРАЇНИ

У статті здійснено дослідження щодо співвідношення права користувача підключеного продукту на доступ до даних, які генеруються під час його використання, та права інших фізичних осіб на захист персональних даних. Було проаналізовано підходи, закріплені у Загальному регламенті про захист даних та Акту про дані, зокрема увагу було звернуто на ті відмінності, що існують між статусом користувача пристрою та суб'єкта персональних даних. Обґрунтовано, що право користувача на доступ до даних Інтернету речей не є абсолютним, позаяк набори даних можуть одночасно містити як технічну інформацію, так і персональні дані самого користувача чи персональні дані третіх осіб. Увагу також було приділено питанню використання службових автомобілів, систем «розумного будинку» та інших підключених пристроїв, де власник або користувач продукту не завжди є суб'єктом усіх даних, що створюються. Встановлено, що Акт про дані не містить самостійної правової підстави для здійснення розкриття персональних даних щодо третіх осіб, а натомість передбачає необхідність дотримання вимог, які встановлено Загальним регламентом про захист даних. Стверджується, що під час вирішення питання про доступ до даних необхідно окремо перевірити зв'язок заявника з продуктом, а також правовий режим даних, їх персональний або неперсональний характер, а також можливість ідентифікації інших осіб. Також було проаналізовано стан українського законодавства та виявлено відсутність комплексного механізму доступу до даних підключених продуктів. У зв'язку з цим було запропоновано розмежовувати статус користувача та суб'єкта даних, перевіряти правову підставу передачі персональних даних третіх осіб, застосовувати відокремлення або знеособлення змішаних наборів даних, забезпечувати прозорість рішень та право на оскарження. Наголошено на необхідності інформування користувачів про види даних, порядок їх отримання та обмеження доступу, що зумовлено захистом приватності. Зроблено висновок про доцільність послідовної комплексної імплементації підходів ЄС в Україні.

Ключові слова: *Інтернет речей, Акт про дані, Загальний регламент про захист даних, доступ до даних, персональні дані.*

Постановка проблеми. Підключені до мережі автомобілі, годинники, побутові прилади, системи «розумного будинку» та інші пристрої постійно генерують багато даних, які пов'язані як із їх використанням, так і з навколишнім середовищем. Частина цих даних має переважно технічний характер. Інша частина натомість прямо або опосередковано стосується людини: її місцезнаходження, режиму дня, стану здоров'я, поведінки, звичок або будь-яких дій. У зв'язку з цим право користувача отримати дані від пристрою не можна розглядати лише як питання доступу до інформації, оскільки воно може одночасно зачіпати право іншої людини на захист персональних даних.

Аналіз останніх досліджень. До недавнього часу правова дискусія щодо Інтернету речей

© Пішта В. І., Віхляєв М. Ю., 2026
Стаття поширюється на умовах ліцензії відкритого доступу CC BY 4.0

у ЄС була зосереджена переважно на застосуванні Загального регламенту про захист даних (далі – GDPR). А. Д. Кунудес та Дж. М. Капіцакі звернули увагу на те, що для Інтернету речей (далі – IoT) особливе значення мають такі базові принципи як прозорість, контроль користувача, мінімізація даних та захист даних ще на етапі створення продукту [1]. Інші науковці акцентують на іншій проблемі, а саме на тому, що у «розумному будинку» важко визначити, хто саме відповідає за обробку даних, оскільки до неї можуть бути залучені власник пристрою, виробник та постачальник цифрової послуги [2, с. 281].

Постановка завдання. Виходячи з наведеного, метою дослідження є визначення меж права користувача підключеного продукту на доступ до даних, що виникають у процесі його використання, у випадках, коли такі дані містять персональні дані інших фізичних осіб, а також розроблення пропозицій щодо вдосконалення правового регулювання відповідних відносин в Україні з урахуванням підходів GDPR та Акту ЄС про дані (далі – Data Act).

Виклад основного матеріалу. Важливо підкреслити, що окреме значення має також право на мобільність даних, яке закріплено у статті 20 GDPR. С. Тернер та інші автори, дослідивши політики конфіденційності 160 IoT-продуктів та практику чотирьох систем, дійшли висновку, що саме по собі не забезпечує його практичної здійсненності [3, с. 2867]. Подальше дослідження С. Тернер і Л. Танцер підтвердило, що користувачі та фахівці позитивно ставляться до мобільності даних, але відсутність зрозумілих процедур суттєво зменшує практичне значення цього права [4].

Водночас право на мобільність даних за GDPR має чіткі межі, оскільки пов'язане з персональними даними конкретного суб'єкта та залежить від тих умов, які визначено у статті 20 GDPR. Разом з тим воно не створює загального права власника автомобіля, годинника чи іншого пристрою отримати всі дані, які було створено під час його використання.

Саме цю прогалину на рівні ЄС частково заповнив Data Act, який запровадив окреме поняття «користувач», під яким розуміють фізичну або юридичну особу, яка володіє підключеним продуктом або якій тимчасово передано права на використання цього підключеного продукту за договором, або яка отримує пов'язані послуги [5]. Це визначення принципово відрізняється від поняття суб'єкта даних у GDPR. Користувач отримує права у зв'язку з правомірним використанням певного продукту, тоді як статус суб'єкта даних виникає через те, що інформація стосується конкретної фізичної особи.

У цьому й полягає основна правова проблема, яку можна визначити як те, що користувач і суб'єкт даних можуть бути тією самою особою, але це не обов'язково.

Слід звернути увагу й на те, що поняття «дані пристрою» не означає автоматично «персональні дані». Data Act виходить із ширшого поняття даних і охоплює як персональні, так і неперсональні дані. Через це правовий режим конкретного набору не можна визначити, виходячи з джерела його походження. Так, дані про температуру в будинку, заряд акумулятора чи технічний стан приладу можуть не стосуватися людини безпосередньо. Але ті самі дані в поєднанні з часом, місцем, номером облікового запису або історією використання можуть дозволити зробити висновок про поведінку конкретної людини. Тому важливо оцінювати не виключно назву або тип пристрою, а зміст даних і можливість пов'язати їх з конкретною особою. Звідси можна побачити ще одну відмінність між правом на доступ, яке закріплено у Data Act та правами, які визначені у GDPR. Коли фізична особа є одночасно користувачем та суб'єктом даних, ці права можуть, по суті, діяти паралельно. При цьому Data Act прямо передбачає, що його правила доповнюють, а не замінюють права доступу та мобільності за GDPR [5]. Такий підхід може бути корисним для України, оскільки дозволяє уникнути вибору між двома моделями, а в такому разі законодавство може одночасно захищати персональні дані та надавати користувачу більш широке право на дані, які пов'язані з використанням продукту.

Очевидний приклад у цій ситуації може бути пов'язаний зі службовим автомобілем: юридична особа може бути користувачем підключеного автомобіля, однак дані про маршрут, швидкість, зупинки або час керування можуть стосуватися конкретного працівника.

Схожа ситуація виникає в «розумному будинку», оскільки власник системи є користувачем, але датчики, камери або інші пристрої можуть створювати дані про членів сім'ї, гостей чи працівників. Отже, вимога користувача надати «його» дані насправді може бути вимогою надати персональні дані інших осіб.

Європейський законодавець вочевидь визнав цю небезпеку. Відповідно до статті 4(12) Data Act, якщо користувач не є суб'єктом даних, дані можуть бути надані йому лише за наявності

належної правової підстави згідно зі статтею 6 GDPR, а для спеціальних категорій даних – також з урахуванням статті 9 GDPR. Аналогічне правило містить також стаття 5(7) Data Act щодо передачі даних третій особі за запитом користувача [5]. Власне Data Act прямо не створює нової правової підстави для обробки персональних даних. Натомість у разі конфлікту перевага зберігається за правилами ЄС, що стосуються захисту персональних даних. Таке рішення є важливим, оскільки не дозволяє перетворити право доступу до даних пристрою на спосіб обходу GDPR. Ще на стадії обговорення Data Act Європейська рада із захисту даних та Європейський інспектор із захисту даних наголошували, що розширення обміну даними не повинно послаблювати гарантії для фізичних осіб [6]. Питання набуває особливого значення у тому випадку, коли дані можуть використовуватися для оцінки поведінки людини, у трудових відносинах, страхуванні або інших сферах, де неправильний доступ до даних здатний прямо впливати на її права.

У правовій доктрині зміна підходу до IoT-даних добре простежується після появи Data Act. В. Кербер розглядає нові правила як спробу послабити фактичний контроль виробників над даними, які створюють підключені пристрої, та дати користувачам реальну можливість отримувати і передавати ці дані [7, с. 120]. Г. Швайцер та А. Мецгер наголошують, що Data Act запроваджує нову категорію прав доступу до даних, яка виходить за межі традиційного режиму доступу та переносимості персональних даних, установленого GDPR [8, с. 338].

Це розмежування має принципове значення, адже GDPR відповідає передусім на питання про те, які права має людина щодо персональних даних про неї. Натомість Data Act фокусується на дещо іншому питанні: які права має користувач щодо даних, які виникли внаслідок використання окремого продукту. У першому випадку відправною точкою буде зв'язок інформації з людиною. У другому – зв'язок даних із використанням речі або послуги.

М. Екардт та В. Кербер звертають увагу, що до прийняття Data Act виробник часто мав фактичний контроль над даними IoT без окремого права власності на них [9]. Якщо здійснювати аналіз Data Act, то може йтися про перерозподіл можливостей доступу та використання таких даних. Проте дослідники переважно аналізують неперсональні дані. Саме змішані набори, у яких технічні дані поєднані з інформацією про фізичних осіб, створюють складніше правове питання. Практичність цієї проблеми підтверджують Ф. Касароза та Ф. Дженнарі на прикладі медичних IoT-пристроїв. Вони показують, що одночасне застосування GDPR, Data Act та спеціальних правил про медичні дані може створювати відмінності у поняттях, правах доступу та обов'язках учасників [10, с. 1116]. Для цього дослідження такий висновок важливий і поза медичною сферою, позаяк збільшення кількості прав на доступ до даних не завжди робить правове становище особи простішим.

Найточніше проблему доступу користувача до даних інших осіб визначили П. Т. Дж. Wolters та Й. Й. Ху, які звертають увагу на необхідність перевірити не лише те, чи має заявник статус користувача, але й те, чи має він право отримати конкретні персональні дані [11]. Від цього залежить законність усього подальшого використання інформації. Якщо особа справді є користувачем пристрою, це ще не означає, що вона має законну підставу бачити дані іншої людини.

Таким чином, доступ до IoT-даних потребує двох окремих перевірок. Перша стосується зв'язку заявника з продуктом: тобто є потреба визначити, чи є він його користувачем. Друга стосується вже самих даних: тобто, чи є в них персональні дані та кого саме вони стосуються. Змішування цих питань створює ризик неправомірного розкриття інформації.

Станом на сьогодні в Україні ця проблема є наразі не врегульованою. Зокрема, чинний Закон України «Про захист персональних даних» визначає загальні правила обробки персональних даних, права суб'єкта та обов'язки володільців і розпорядників [12]. Водночас він не встановлює загального права користувача підключеного продукту вимагати всі дані, які виникли під час використання такого продукту. Закон України «Про цифровий контент та цифрові послуги» також не вирішує це питання, оскільки його предметом є насамперед відносини щодо надання цифрового контенту і цифрових послуг споживачеві [13]. Не зважаючи на це, на сьогодні є спроби приведення українського законодавства до цифрового acquis ЄС. Так, проєкт Закону № 8153 був прийнятий за основу 20 листопада 2024 року і станом на серпень 2026 року готується до другого читання [14]. Проте навіть оновлення загального закону про захист персональних даних саме по собі не вирішить питання доступу до даних підключених продуктів. Для цього необхідно визначити окремий правовий режим доступу до таких даних та одразу погодити його з правилами захисту персональних даних.

Для українського законодавства доцільно використати підхід, за якого право користувача на доступ до IoT-даних не є абсолютним. Воно має діяти в межах, які не порушують права суб'єктів персональних даних. Право власності на пристрій також не повинно тлумачитися як право на всі персональні дані, які цей пристрій здатний зібрати.

Насамперед необхідно здійснити розмежування таких категорій як «користувач підключеного продукту» і «суб'єкт персональних даних». Користувачем може бути фізична або юридична особа. Суб'єктом персональних даних може бути лише фізична особа, якої стосується відповідна інформація. Якщо ці статуси збігаються, то доступ не має суттєво обтяжуватися. Якщо не збігаються, то доцільно здійснити додаткову перевірку. При цьому наявність належної правової підстави, що дає можливість користування пристроєм не повинні визнаватися достатньою підставою для отримання персональних даних третіх осіб. Інакше може виникнути ситуація, коли цивільно-правовий зв'язок особи з річчю фактично визначатиме обсяг її прав щодо інформації про інших людей, що, на нашу думку, суперечить самій логіці захисту персональних даних.

Щодо змішаних наборів даних, то на практиці один масив може містити технічну інформацію, персональні дані користувача та персональні дані третіх осіб. Відмова у доступі до всіх даних лише через наявність у ньому персональних даних була б надмірною. Однак і передача даних без перевірки створювала б загрозу приватності. Тому очевидно, що закон має дозволяти відокремлення даних, а коли у разі, коли це можливо – знеособлення тієї частини інформації, яка стосується інших осіб.

Важливо також, хто саме перевіряє наявність правової підстави для передачі. У моделі Data Act ключова роль часто належить особі, яка фактично має дані і повинна надати їх на запит. Для України варто прямо встановити, що особа, яка надає персональні дані користувачу або визначеній ним третій особі, повинна до передачі перевірити правову підставу такого розкриття. Самого посилання заявника на право користування пристроєм для цього недостатньо. Водночас така перевірка не повинна перетворюватися на зручний спосіб постійно відмовляти користувачам у доступі. Тому закон має вимагати дотримання юридичної визначеності, щоб відмова була обґрунтованою та містила вказівку на конкретну причину, через яку передача відповідних даних порушувала б права іншої особи.

Законодавцю також слід буде чітко визначити питання щодо мети використання, оскільки навіть законно отримані дані не повинні автоматично ставати доступними для будь-якої подальшої мети. Це особливо важливо, якщо йдеться про трудові правовідносини. Наприклад, право роботодавця користуватися службовим автомобілем та отримувати певні технічні дані не повинно саме по собі створювати необмежене право контролювати пересування працівника. Подальша обробка персональних даних повинна обов'язково мати визначену законну мету та відповідати загальним принципам захисту даних. Те саме буде стосуватися і страхових компаній, орендодавців, власників житла чи інших осіб, які формально можуть бути користувачами пристрою, але не є суб'єктами всіх даних, що створюються під час його роботи.

Крім цього суб'єкт персональних даних повинен мати можливість дізнатися, кому і на якій підставі були передані його дані, а також вимагати припинення незаконної обробки. Водночас користувач пристрою має отримати можливість оскаржити необґрунтовану відмову у доступі до тих даних, які він має право отримати.

Людина також має розуміти, які види даних створює пристрій, який вона використовує, хто їх зберігає, які дані можна отримати безпосередньо, а які – лише через окремий запит. Таке інформування не слід змішувати з повідомленням про обробку персональних даних. Вочевидь, що це різні за метою юридичні обов'язки, де один стосується доступу до даних продукту, а інший – безпосередньо захисту персональних даних. Водночас для користувача вони мають бути узгодженими та не суперечити один одному. Доцільним було б також прямо передбачити обов'язок повідомляти користувача про те, що частина даних може бути недоступною або надаватися в обмеженому вигляді через необхідність захисту персональних даних інших осіб. Це дозволить уникнути ситуації, коли обмеження доступу стає для користувача несподіваним уже після придбання продукту.

Зрештою для України важливо обрати комплексний варіант імплементації положень acquis ЄС, а не фрагментарним. Якщо законодавець запровадить лише право користувача вимагати дані, але не визначить співвідношення цього права із законодавством про персональні дані, виникне нова невизначеність. Якщо ж обмежитися лише оновленням закону про персональні дані, проблема фактичного контролю виробника над неперсональними IoT-даними залишиться поза регулюванням.

Висновки. Розвиток права ЄС показує перехід від підходу, за якого IoT-дані розглядалися переважно через захист персональних даних, до ширшого регулювання доступу та використання даних підключених продуктів. Data Act надав користувачу окремі права щодо даних, але не скасував вимоги GDPR. Ключовим тут є правило відповідно до якого статус користувача продукту та статус суб'єкта персональних даних мають різну правову природу.

Для України це означає, що майбутнє регулювання IoT не слід зводити до простого права власника пристрою «отримати всі свої дані». Тут важливо розуміти, що дані пристрою не завжди є даними його власника. У них може міститися інформація про інших фізичних осіб. Тому доцільно закріпити послідовний правовий механізм, який включатиме: (1) встановлення статусу заявника як користувача; (2) визначення складу запитуваних даних; (3) визначення того, чи стосуються персональні дані самого користувача або третіх осіб; (4) за наявності даних третіх осіб перевірити окрему правову підставу їх передачі; (5) за можливості відокремити або знеособити такі дані; (6) забезпечення права на оскарження рішення. При цьому зв'язок особи з пристроєм та зв'язок інформації з конкретною фізичною особою мають оцінюватися окремо.

Вважаємо, що такий підхід дозволить поєднати дві законні потреби. По-перше, користувач не залишатиметься повністю залежним від виробника або постачальника послуги у питанні доступу до даних, які створює його пристрій. По-друге, право на доступ не перетвориться на підставу для отримання чужих персональних даних. Саме це розмежування варто покласти в основу майбутнього українського регулювання даних, що створюються підключеними продуктами.

Список літератури:

1. Kounoudes A. D., Kapitsaki G. M. A mapping of IoT user-centric privacy preserving approaches to the GDPR. *Internet of Things*. 2020. Vol. 11. Art. 100179. DOI: https://doi.org/10.1016/j.iot.2020.100179

2. Chen J., Edwards L., Urquhart L., McAuley D. Who is responsible for data processing in smart homes? Reconsidering joint controllership and the household exemption. *International Data Privacy Law*. 2020. Vol. 10. Is. 4. P. 279–293. DOI: https://doi.org/10.1093/idpl/ipaa011

3. Turner S., Galindo Quintero J., Turner S., Lis J., Tanczer L. M. The exercisability of the right to data portability in the emerging Internet of Things (IoT) environment. *New Media & Society*. 2021. Vol. 23. Is. 10. P. 2861–2881. DOI: https://doi.org/10.1177/1461444820934033

4. Turner S., Tanczer L. M. *In principle* vs *in practice*: User, expert and policymaker attitudes towards the right to data portability in the internet of things. *Computer Law & Security Review*. 2024. Vol. 52. Art. 105912. DOI: https://doi.org/10.1016/j.clsr.2023.105912

5. Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (Text with EEA relevance). URL: https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng

6. EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act). URL: https://www.edpb.europa.eu/documents/legislative-opinion/edpb-edps-joint-opinion-22022-on-the-proposal-of-the-european_en

7. Kerber W. Governance of IoT Data: Governance of IoT Data: Why the EU Data Act Will not Fulfill Its Objectives. *GRUR International*. 2023. Vol. 72. Is. 2. P. 120–135. DOI: https://doi.org/10.1093/grurint/ikac107

8. Schweitzer H., Metzger A. Data Access under the Draft Data Act, Competition Law and the DMA: Opening the Data Treasures for Cowmpetition and Innovation? *GRUR International*. 2023. Vol. 72. Is. 4. P. 337–356. DOI: https://doi.org/10.1093/grurint/ikad012

9. Eckardt M., Kerber W. Property rights theory, bundles of rights on IoT data, and the EU Data Act. *European Journal of Law and Economics*. 2024. Vol. 57. P. 113–143. DOI: https://doi.org/10.1007/s10657-023-09791-8

10. Casarosa F., Gennari F. Data Sharing in the Internet of Medical Things: Between the Data Act and the EHDS. *European Journal of Risk Regulation*. 2025. Vol. 16. Spec. Is. 3. P. 1115–1137. DOI: https://doi.org/10.1017/err.2025.18

11. Wolters P. T. J., Hu Y. Y. Authentication and authorisation and the access of the user in the Data Act. *Computer Law & Security Review*. 2026. Vol. 61. Art. 106292. DOI: https://doi.org/10.1016/j.clsr.2026.106292

12. Про захист персональних даних: Закон України від 01 червня 2010 року № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

13. Про цифровий контент та цифрові послуги: Закон України від 10 серпня 2023 року № 3321-IX. URL: https://zakon.rada.gov.ua/laws/show/3321-20#Text

14. Проєкт Закону про захист персональних даних: № 8153 від 25 жовтня 2022 року. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/40707

Pihta V. I., Vikhliaiev M. Yu. THE RIGHT OF THE USER OF A CONNECTED PRODUCT TO ACCESS DATA FROM THE INTERNET OF THINGS AND THE PROTECTION OF PERSONAL DATA OF THIRD PARTIES: EU APPROACHES AND PROSPECTS FOR UKRAINE

The article studies the relationship between the right of a user of a connected product to access data generated during its use and the right of other individuals to the protection of personal data. The approaches enshrined in the General Data Protection Regulation and the Data Act were analyzed, in particular, attention was paid to the differences that exist between the status of a device user and a personal data subject. It is argued that the user's right to access Internet of Things data is not absolute, since data sets can simultaneously contain both technical information and the user's personal data or the personal data of third parties. Attention was also paid to the issue of the use of company cars, smart home systems and other connected devices, where the owner or user of the product is not always the subject of all the data created. It is established that the Data Act does not contain an independent legal basis for the disclosure of personal data to third parties, but instead provides for the need to comply with the requirements established by the General Data Protection Regulation. It is argued that when deciding on data access, it is necessary to separately verify the applicant's relationship with the product, as well as the legal regime of the data, their personal or non-personal nature, and the possibility of identifying other persons. The state of Ukrainian legislation was also analyzed and the absence of a comprehensive mechanism for accessing data from connected products was revealed. In this regard, it was proposed to distinguish between the status of the user and the data subject, verify the legal basis for the transfer of personal data of third parties, apply separation or depersonalization of mixed data sets, and ensure transparency of decisions and the right to appeal. The need to inform users about the types of data, the procedure for obtaining them and restricting access, which is due to the protection of privacy, was emphasized. The conclusion was made on the feasibility of consistent comprehensive implementation of EU approaches in Ukraine.

Keywords: *Internet of Things, Data Act, General Data Protection Regulation, data access, personal data.*

Дата першого надходження статті до видання: 07.09.2026
Дата прийняття статті до друку після рецензування: 21.09.2026
Дата публікації (оприлюднення) статті: 18.11.2026