КОНСТИТУЦІЙНЕ ПРАВО; МУНІЦИПАЛЬНЕ ПРАВО

УДК 342.7: 316.4: 004.056
DOI https://doi.org/10.32782/TNU-2707-0581/2024.5/02

Горєлова В.Ю.
Таврійський національний університет імені В.І. Вернадського

ІНТЕРНЕТ РЕЧЕЙ І ЗАХИСТ ПРАВ ЛЮДИНИ: ЕТИЧНІ ТА ПРАВОВІ ВИКЛИКИ

У статті досліджується актуальне питання етики та права застосування інтернету речей (IoT), адже на сьогодні завдяки вдосконаленню сенсорних технологій, бездротового зв'язку та обробки даних, IoT еволюціонував від концепції до невід'ємного елементу сучасності, трансформуючи майже всі сфери людського буття (економіку, транспорт, охорону здоров'я та інші сфери, забезпечуючи автоматизацію процесів, оптимізацію ресурсів та розвиток «розумних» систем). У статті зазначені етичні аспекти використання IoT, зокрема, що пов'язані з прозорістю, справедливістю алгоритмів і дотриманням прав людини. Наголошено, що IoT стимулює прогрес штучного інтелекту, водночас масовий збір і зберігання даних створюють ризики порушення приватності людини, що потребує суворого правового регулювання. Актуальним питанням, таким чином, постає прблема «етики алгоритму», адже рішення на основі алгоритмів можуть бути упередженими, що потребує забезпечення прозорості та відповідальності людини за розробку технологій. Успішний розвиток IoT вимагає поєднання правового регулювання, технічних заходів, міжнародних стандартів та освітніх програм, що забезпечить безпечне та справедливе цифрове середовище. У статті наведено перелік проблем, які пов'язані із практичним застосуванням Інтернету-речей. Наголошено на необхідності розробки та впровадження етичних стандартів для Інтернету речей (IoT), що є важливим засобом забезпечення безпеки та захисту приватності людини в технологічному середовищі. У статті також розглянуті існуючі міжнародні етичні стандарти для Інтернету речей, що включають принципи захисту даних, безпеки, прозорості і відповідальності. Ці принципи сприяють інтеграції етики у процес розробки технологій, гарантуючи, що IoT не лише виконує технічні функції, а й відповідає етичним нормам, зокрема в аспектах захисту приватності людини.

Ключові слова: *Інтернет речей, права людини, етика, конфіденційність.*

Постановка проблеми. Інтернет речей (IoT) є технологічним феноменом, що відкриває широкі можливості для розвитку, проте водночас створює ризики для приватності, безпеки та прав людини. Відсутність належного регулювання й етичних стандартів загострює питання прозорості використання даних, алгоритмічної дискримінації та загроз кібербезпеки.

Аналіз останніх досліджень і публікацій. Серед сучасних досліджень, присвячених етичним і правовим аспектам IoT, слід виділити праці: А. Занелла (A. Zanella), Н. Буї (N. Bui), А. Кастеллані (A. Castellani), Л. Вангеліста (L. Vangelista), Е. Лі (E. Lee), С. Вольферт (S. Wolfert), Л. Ге (L. Ge), Дж. Вердуу (C. Verdouw), Х. Канг (H. Kang), С. Х. Кім (S. H. Kim) тощо, в яких розглядаються правові та етичні складності, що виникають при використанні IoT таких як охорона здоров'я або громадська безпека, вплив IoT на конфіденційність та етичність використання персональної інформації людини.

Розвиток IoT супроводжується стрімким впровадженням у повсякденне життя, що підвищує ризики порушення прав людини, зокрема конфіденційності та безпеки. Актуальність дослідження полягає у необхідності розробки етичних і правових підходів до врегулювання IoT та збереження прав людини у цифровому середовищі.

Постановка завдання. Метою статті є аналіз етичних і правових викликів, що виникають у контексті використання IoT, а також розробка

рекомендацій для створення безпечного та справедливого цифрового середовища.

Виклад основного матеріалу. Розвиток Інтернету речей (IoT) розпочався у 1990-х роках, коли виникла ідея взаємозв'язку пристроїв через Інтернет. Завдяки вдосконаленню сенсорних технологій, бездротового зв'язку та обробки даних, IoT еволюціонував від концепції до невід'ємного елементу сучасності. Ця технологія трансформує економіку, транспорт, охорону здоров'я та інші сфери, забезпечуючи автоматизацію процесів, оптимізацію ресурсів та розвиток «розумних» систем. IoT стимулює прогрес штучного інтелекту, машинного навчання та технологій великих даних, що підвищує попит на кібербезпеку. Інтернет речей, або IoT, являє собою концепцію інтеграції фізичних об'єктів у єдину мережу, що забезпечує їх взаємодію між собою та з людиною. Ця технологія передбачає використання сенсорів, програмного забезпечення і мережевих засобів для збору, обробки і обміну даними. IoT орієнтований на створення інфраструктури, яка об'єднує речі, від побутових приладів до промислових систем, з метою підвищення ефективності, автоматизації і персоналізації процесів.

Основними елементами Інтернету речей є фізичні об'єкти, мережеві технології та аналітичні платформи. Фізичні об'єкти оснащуються датчиками і чіпами, які фіксують стан середовища або самого пристрою. Мережеві технології забезпечують передачу зібраної інформації через канали зв'язку, такі як Wi-Fi чи стільникові мережі, що сприяє синхронізації роботи пристроїв. Аналітичні системи обробляють дані, формуючи основи для прийняття рішень, адаптуючи функціонування пристроїв відповідно до умов або потреб користувачів [1].

Однак попри значний потенціал IoT, його розвиток супроводжується низкою викликів. Основні ризики пов'язані із захистом особистих даних людини, адже пристрої збирають великі обсяги інформації, яка може бути доступна стороннім особам. Кібербезпека також залишається ключовим викликом, адже вразливості пристроїв можуть стати джерелом загроз для користувачів та інфраструктури [2]. Не менш важливими є етичні аспекти використання IoT, зокрема пов'язані з прозорістю, справедливістю алгоритмів і дотриманням прав людини [3]. Таким чином, хоча Інтернет речей і є важливим інструментом трансформації суспільства, що сприяє прогресу в різних сферах, водночас його впровадження вимагає відповідального підходу, що повинно включати розробку етичних стандартів, правового регулювання та технологій захисту даних для забезпечення безпечного і справедливого використання цієї інновації [4].

Окрім того, розвиток Інтернету речей супроводжується появою численних викликів, пов'язаних із конфіденційністю, безпекою та управлінням персональними даними. У відповідь на це формуються юридичні та етичні основи, що спрямовані на захист прав користувачів, забезпечення прозорості у використанні даних і розподіл відповідальності за потенційні ризики. Міжнародні правові акти вже сьогодні прагнуть регулювати діяльність IoT у різних контекстах, намагаючись забезпечити безпечне функціонування технологій та їхню відповідність етичним принципам [5]. Одним із ключових міжнародних документів є Загальний регламент із захисту даних (надалі -GDPR), який визначає основні вимоги до збирання, зберігання та передачі персональних даних. Його застосування охоплює також IoT, вимагаючи інформованої згоди користувачів і забезпечення права на контроль над особистою інформацією. Регламент GDPR є фундаментом для впровадження політик прозорості та підзвітності у сфері IoT-технологій, стимулюючи глобальну адаптацію стандартів захисту даних. Так, міжнародна організація зі стандартизації (ISO) розробила низку рекомендацій для IoT, зокрема ISO/IEC 29182, що встановлює технічні протоколи для взаємодії пристроїв. Ці стандарти сприяють інтеграції IoT у глобальні мережі, забезпечуючи сумісність пристроїв та підвищуючи їхню безпеку. У поєднанні з іншими стандартами ISO, цей документ дозволяє розвивати IoT із дотриманням базових принципів етики і права [6].

Приналежно, варто виділити Закон «Про кібербезпеку Інтернету речей» у США, що запроваджує базові вимоги до безпеки пристроїв IoT, які використовуються урядовими установами. У Китаї діє Закон «Про захист персональних даних» (PIPL), який визначає жорсткі обмеження на обробку та передачу даних, спрямовані на посилення контролю за конфіденційністю [7].

Слід назначити, що етичні стандарти, які на сьогодні розробляються в рамках міжнародних організацій, таких як OECP, що пропонує принципи прозорості, довіри та відповідальності для IoT спрямовані на стимулювання виробників і розробників дотримуватись високих стандартів у створенні безпечних і надійних пристроїв. Зокрема, рекомендації включають забезпечення прав користувачів на інформованість і контроль

над своїми даними. Важливість правових і етичних аспектів використання IoT підкреслюється їхньою роллю у створенні довіри до технологій. Незважаючи на різноманітність підходів у різних країнах, усі вони спрямовані на мінімізацію ризиків і забезпечення справедливих умов для використання Інтернету речей у суспільстві [8].

Інтернет речей інтегрується у повсякденне життя, створюючи екосистему пристроїв, які взаємодіють між собою для підвищення ефективності, комфорту та безпеки. Ця технологія дозволяє автоматизувати рутинні процеси, зменшити витрати та оптимізувати використання ресурсів, що робить IoT ключовим елементом цифрової трансформації у багатьох галузях[9]. Наприклад: у медицині IoT сприяє вдосконаленню діагностики та моніторингу здоров'я (розумні сенсори та носимі пристрої дозволяють лікарям отримувати дані про стан пацієнтів у режимі реального часу, що підвищує якість лікування, а також варто зазначити пристрої автоматизованого введення ліків та дистанційного моніторингу мінімізують людський фактор, знижуючи ризики для пацієнтів і забезпечуючи їхню безпеку) [10]; у транспорті IoT трансформує інфраструктуру в «розумну» систему, що підвищує ефективність і знижує аварійність, адже автомобілі з вбудованими датчиками можуть прогнозувати технічні несправності та оптимізувати витрати пального. Окрім того, у міських умовах «розумні» світлофори та системи управління рухом дозволяють зменшити затори, сприяючи більш раціональному використанню доріг [11]; у сфері розумного дому IoT автоматизує управління освітленням, опаленням і безпекою, забезпечуючи комфорт і знижуючи енергоспоживання. Розумні холодильники та системи дистанційного управління побутовими приладами оптимізують домашні процеси, надаючи користувачам більше часу для важливих справ [12]; у сільському господарстві IoT впроваджує сенсорні системи для моніторингу умов вирощування культур. Завдяки даним про вологість ґрунту, температуру та якість повітря фермери можуть покращувати врожайність і знижувати витрати. Аналогічні технології застосовуються у тваринництві для моніторингу здоров'я тварин і контролю умов їхнього утриманняр [13]; у промисловості використовується IoT для моніторингу стану обладнання, що мінімізує ризик аварій та забезпечує безперервність виробництва. Ці технології дозволяють прогнозувати зношування деталей, оптимізувати енергоспоживання та скорочувати витрати, підвищуючи загальну ефективність підприємств [14]; у торгівлі IoT змінює традиційні бізнес-моделі завдяки використанню розумних полиць, датчиків і систем аналізу поведінки покупців. Ці інструменти дозволяють оптимізувати управління запасами, покращувати маркетингові стратегії та підвищувати зручність обслуговування споживачів [15], тощо. Таким чином, розвиток IoT забезпечує значні переваги, проте також створює виклики, пов'язані із забезпеченням конфіденційності та кібербезпеки. Тобто впровадження цих технологій потребує ретельного технічного та правового регулювання та етичного підходу для забезпечення безпеки користувачів і довіри до технологій.

Інтернет речей генерує значні обсяги даних, які часто включають чутливу інформацію про користувачів, їхні звички та середовище перебування. Ці дані стають вразливими до витоків, несанкціонованого доступу та використання третіми сторонами. Прикладом є витік даних у додатках для фітнесу, коли зібрані дані дозволяли ідентифікувати місця розташування військових об'єктів, ставлячи під загрозу безпеку. Таким чином, для мінімізації таких ризиків необхідно впроваджувати строгі заходи захисту даних та інформувати користувачів про можливі загрози [16].

Основою етичного використання IoT є прозорість у зборі та обробці даних і отримання інформованої згоди користувачів. Багато користувачів не усвідомлюють обсяг зібраної інформації та її можливе використання. Інформована згода потребує чіткого і доступного пояснення щодо збору, зберігання та використання даних людини. Наприклад, користувачі часто погоджуються з політиками конфіденційності, не читаючи їх, через складність та обсяг документів. Втім, на думку іноземних дослідників, необхідність у забезпеченні прозорості зміцнює довіру між користувачами та компаніями [17].

Автоматизація процесів, що забезпечується IoT, іноді призводить до втрати контролю користувачів над рішеннями. Розумні системи, як-от холодильники, можуть приймати рішення про покупки, аналізуючи наявність продуктів, але це може обмежувати автономію користувачів. Більше того, хакерські атаки на медичні пристрої, як-от кардіостимулятори, створюють загрозу для життя, демонструючи необхідність посилення безпеки в IoT [18]. Тобто, розвиток IoT потребує чітких правових рамок, які визначають відповідальність розробників, виробників та користувачів за безпеку пристроїв, своєчасне оновлення програмного забезпечення та захист даних. Правова визначеність тут буде сприяти зменшенню

етичних ризиків і підвищенню довіри до технологій [19].

Інтернет речей створює загрозу приватному життю через автоматизований збір, зберігання та аналіз особистих даних користувачів. Розумні пристрої, такі як фітнес-трекери, голосові помічники чи системи відеоспостереження, часто фіксують більше даних, ніж користувачі можуть усвідомлювати. Ці дані використовуються для створення профілів, аналізу поведінки чи комерційної реклами, часто без згоди користувачів. Захист права на приватність вимагає впровадження суворих регламентів, таких як GDPR, що зобов'язує компанії забезпечувати прозорість у зборі даних та отримувати інформовану згоду від користувачів [20]. Вразливість IoT-пристроїв до кібератак створює загрозу як для фізичної, так і для інформаційної безпеки користувачів. Злам «розумних» будинків, автомобілів або медичних пристроїв може поставити під загрозу життя та здоров'я людей. Для забезпечення безпеки необхідно запроваджувати сучасні протоколи кіберзахисту, обов'язкове шифрування даних та регулярні оновлення програмного забезпечення. Правове регулювання має стимулювати виробників дотримуватися високих стандартів захисту даних людини [21]. Забезпечення прозорості у використанні IoT вимагає відкритого інформування користувачів про цілі збору даних, методи їх зберігання та обробки. Компанії мають розробляти доступні й зрозумілі політики конфіденційності, надавати користувачам право переглядати, редагувати або видаляти власні дані. Це сприяє довірі між користувачами та розробниками IoT-технологій.

Окрім того, освітні програми та інформаційні кампанії можуть допомогти користувачам краще розуміти свої права в умовах цифрової епохи [22]. Діти, літні люди та особи з інвалідністю є особливо вразливими до ризиків IoT. Для дітей важливо створювати пристрої з обмеженим збором даних, захищати їх від маніпуляцій та формування залежності. Літні люди можуть бути мішенню для кіберзлочинців через недостатню обізнаність про ризики. Пристрої для осіб з обмеженими можливостями мають враховувати специфічні потреби й гарантувати безперебійність роботи. Розробка етичних стандартів для IoT, орієнтованих на ці групи, є важливим напрямом розвитку технологій [23]. Захист прав людини в умовах впровадження IoT потребує системного підходу, що поєднує технологічні рішення, правові регламенти та етичні принципи. Забезпечення приватності, безпеки та прозорості має стати пріоритетом у розробці IoT-пристроїв, аби технології сприяли покращенню якості життя без загроз для прав і свобод користувачів.

Існуючі міжнародні етичні стандарти для Інтернету речей (IoT) спрямовані на забезпечення безпеки, конфіденційності та соціальної відповідальності при використанні цієї технології. Важливими ініціативами є стандарт IEEE «Ethically Aligned Design», який включає принципи захисту даних, безпеки, прозорості і соціальної відповідальності. Ці принципи сприяють інтеграції етики у процес розробки технологій, гарантуючи, що IoT не лише виконує технічні функції, а й відповідає етичним нормам, зокрема в аспектах захисту приватності та забезпечення справедливості [24]. Також стандарти ISO/IEC 27001 та ISO/IEC 27018 визначають вимоги до безпеки інформації та захисту персональних даних у хмарних середовищах, що має пряме відношення до IoT. Вони сприяють інтеграції кібербезпеки та конфіденційності в проекти, пов'язані з IoT, гарантуючи, що дані користувачів обробляються відповідно до міжнародних стандартів захисту. Регламент GDPR, в свою чергу, встановлює правила для збору, зберігання та обробки персональних даних, зокрема для IoT-пристроїв, підкреслюючи важливість мінімізації даних та забезпечення доступу до них лише для уповноважених осіб [25]. Міжнародні організації, такі як Організація Об'єднаних Націй (ООН), ОЕСР, ЄС і IEEE, активно працюють над розробкою етичних стандартів для IoT. Їхні ініціативи включають створення принципів прозорості, захисту даних, безпеки та соціальної відповідальності, що сприяє етичному розвитку IoT. Наприклад, ЄС розробив «Етичні керівництва для штучного інтелекту та IoT», а IEEE запроваджує стандарти для етики в дизайні IoT-пристроїв, що забезпечують безпеку та конфіденційність даних [26].

Державне регулювання відіграє ключову роль у формуванні етичних норм щодо IoT, забезпечуючи відповідність технологій соціальним, правовим та етичним вимогам. Зокрема, в Україні були ухвалені закони щодо захисту персональних даних і кібербезпеки, що мають опосередковане відношення до застосування IoT. Етичні підходи до регулювання IoT вимагають інтеграції міжнародних стандартів, правових норм та технічних заходів, які гарантують безпеку та конфіденційність. Розробка і впровадження чітких етичних стандартів сприятиме зниженню ризиків і забезпечить довіру користувачів до IoT. Технології повинні бути орієнтовані на покращення якості

життя, зберігаючи при цьому високі стандарти безпеки та приватності.

Висновки. Етичні виклики IoT вимагають комплексного підходу, включаючи вдосконалення кібербезпеки, розробку зрозумілих політик конфіденційності та посилення правової регуляції. Лише гармонійне поєднання технологічних, етичних і правових аспектів може забезпечити безпечне і відповідальне використання IoT у сучасному суспільстві.

Етичні стандарти для Інтернету речей (IoT) є важливим засобом забезпечення безпеки та захисту приватності людини в технологічному середовищі. Вони сприяють інтеграції принципів захисту даних, прозорості та відповідальності в процес розробки IoT-пристроїв. Оскільки розвиток IoT підвищує ризики порушень приватності людини та безпеки користувачів, гостро стоїть питання впровадження ефективних механізмів захисту прав людини, зокрема через забезпечення прозорості збору даних та інформованої згоди користувачів. З метою покращення захисту прав користувачів та розвитку етичних норм у сфері IoT необхідно удосконалити чинне законодавство України, забезпечити високі стандарти прозорості та кібербезпеки, а також підвищити обізнаність користувачів щодо ризиків, пов'язаних із технологіями IoT.

Список літератури:

1. Atzori L., Iera A., Morabito G. The Internet of Things: a survey. *Computer Networks*. 2010. Vol. 54, No. 15. P. 2787–2805.

2. Gubbi J., Buyya R., Marusic S., Palaniswami M. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*. 2013. Vol. 29, No. 7. P. 1645–1660.

3. Weber R. H., Studer E. Cybersecurity in the Internet of Things: Legal aspects. *Computer Law & Security Review*. 2016. Vol. 32, No. 5. P. 715–728.

4. Floridi L., Taddeo M. What is data ethics? Philosophical Transactions of the Royal Society A: *Mathematical, Physical and Engineering Sciences*. 2016. Vol. 374.

5. Voigt P., Von dem Bussche A. The EU General Data Protection Regulation (GDPR): *A* Practical Guide. *Springer,* 2017. 125 p.

6. ISO/IEC 29182: Framework for Sensor Networks. International Organization for Standardization. URL: https:.standards.iteh.ai/catalog/standards/iec/d363bdb-162c-451a-8d32-c9611be99b2c/iso-iec-19637-2016 (дата звернення: 04.12.2024).

7. U.S. Congress. IoT Cybersecurity Improvement Act. 2020. URL: https:.www.congress.gov/bill/116th-congress/house-bill/1668 (дата звернення: 04.12.2024).

8. OECD. Recommendation of the Council on Artificial Intelligence. 2019. URL: https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449 (дата звернення: 04.12.2024).

9. Zanella A., Bui N., Castellani A., Vangelista L., Zorzi M. Internet of Things for smart cities. *IEEE Internet of Things Journal*. 2014. Vol. 1, No. 1. P. 22–32.

10. Lee E. A., Seshia S. A. Introduction to Embedded Systems: A Cyber-Physical Systems Approach. *MIT Press*, 2017. 210 p.

11. Wolfert S., Ge L., Verdouw C., Bogaardt M. J. Big data in smart farming: A review. *Agricultural Systems*. 2017. Vol. 153. P. 69–80.

12. Kang H. S., Lee J. Y., Choi S., Kim H., Park J. H., Noh S. D. Smart manufacturing: Past research, present findings, and future directions. *International Journal of Precision Engineering and Manufacturing-Green Technology*. 2016. Vol. 3, No. 1. P. 111–128.

13. Grewal D., Roggeveen A. L., Nordfält J. The future of retailing. *Journal of Retailing.* 2017. Vol. 93, No. 1. P. 1–6.

14. Weber R. H. Internet of Things: Privacy issues revisited. *Computer Law & Security Review*. 2015. Vol. 31, No. 5. P. 618–627.

15. Nissenbaum H. A contextual approach to privacy online. *Daedalus*. 2011. Vol. 140, No. 4. P. 32–48.

16. Ziegeldorf J. H., Morchon O. G., Wehrle K. Privacy in the Internet of Things: Threats and challenges. *Security and Communication Networks*. 2014. Vol. 7, No. 12. P. 2728–2742.

17. Cavoukian A. Privacy by design: Leadership, methods, and results. *Information and Privacy Commissioner of Ontario*, 2012. P. 175–202.

18. Tene O., Polonetsky J. Big data for all: Privacy and user control in the age of analytics. *Northwestern Journal of Technology and Intellectual Property*. 2013. Vol. 11, No. 5. P. 239–273.

19. Roman R., Zhou J., Lopez J. On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*. 2013. Vol. 57, No. 10. P. 2266–2279.

20. Cavoukian A. Privacy by design: The 7 foundational principles. Information and Privacy Commissioner of Ontario. URL: https:.privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf (дата звернення: 04.12.2024).

21. Zuboff S. Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*. 2015. Vol. 30, No. 1. P. 75–89.

22. Borenstein J., Herkert J. R., Herkert L. The ethics of autonomous cars. *The Atlantic*. 2017. 110 p.

Horielova V.Yu. INTERNET OF THINGS AND HUMAN RIGHTS PROTECTION: ETHICAL AND LEGAL CHALLENGES

The article examines the topical issue of ethics and law of the Internet of Things (IoT), since today, thanks to the improvement of sensor technologies, wireless communication and data processing, IoT has evolved from a concept to an integral element of modernity, transforming almost all spheres of human existence (economy, transport, healthcare and other areas, ensuring process automation, resource optimisation and development of smart systems). The article outlines the ethical aspects of using IoT, in particular, those related to transparency, fairness of algorithms and respect for human rights. It is noted that IoT stimulates the progress of artificial intelligence, while massive data collection and storage create risks of violation of human privacy, which requires strict legal regulation. Thus, the issue of 'algorithm ethics' becomes an urgent one, as algorithm-based solutions can be biased, which requires transparency and human responsibility for technology development. The successful development of IoT requires a combination of legal regulation, technical measures, international standards and educational programmes to ensure a safe and fair digital environment. The article presents a list of problems associated with the practical application of the Internet of Things. The author emphasises the need to develop and implement ethical standards for the Internet of Things (IoT), which is an important means of ensuring security and protecting human privacy in the technological environment. The article also discusses existing international ethical standards for the Internet of Things, including the principles of data protection, security, transparency and responsibility. These principles promote the integration of ethics into the technology development process, ensuring that IoT not only performs technical functions but also complies with ethical standards, in particular in terms of protecting human privacy.

Key words: *Internet of Things, human rights, ethics, privacy.*