УДК: 341.9

https://doi.org/10.32689/2617-9660-2020-6(12)-159-166

***Бабійчук Валентина Сергіївна**, бакалавр, студентка 5 курсу господарсько-правового факультету, Національний юридичний університет імені Я. Мудрого, 03186, м. Київ, Повітрофлотський пр-т, 34, тел.: 097 406 24 33, e-mail: valentynababiychuk99@gmail.com, https://orcid.org/0000-0002-6536-9939*

***Шуміло Інеса Анатоліївна**, кандидат юридичних наук, доцент кафедри міжнародного приватного права та порівняльного правознавства, Національний юридичний університет імені Я. Мудрого, 61024, м. Харків, вул. Пушкінська 77, тел.: 038 704 89 10, e-mail:i.a.shumilo@nlu.edu.ua, https//orcid.org/0000-0002-2123-7272*

ІНТЕРНЕТ РЕЧЕЙ: НОВІ НАПРЯМИ МОДЕРНІЗАЦІЇ ЗАКОНОДАВСТВА

Анотація. За умов глобальної експансії з боку інтернету речей дуже гостро постає проблема неналежного нормативно-правового регулювання даного питання. Відсутність єдиних стандартів та протоколів сертифікації для користувачів та розробників IP стає підгрунтям для здійснення правопорушень недобросовісними суб'єктами ринку інтернету речей.

У статті здійснюється аналіз правових прецедентів, досліджується зарубіжний досвід правового регулювання IP та наведені певні висновки та пропозиції щодо можливої модернізації законодавста відповідно до сучасних вимог. Зокрема досліджено проблематику конфіденційності персональних даних, балансу інтересів, обмеження правомочностей власника девайсів IP та проблеми відповідальності суб'єктів IP.

Авторами наголошено, що потенційний нормативно-правовий акт має носити міжнародний характер, спрямовувати свою дію на захист прав користувачів інтернету речей та при цьому враховувати колізійний характер норм міжнародного приватного права. Також підкреслено важливість та необхідність концентрації зусиль основних акторів ринку IP та законодавців задля створення акту, що закріплював би актуальні положення та відповідав вимогам сучасності та враховував інтереси усіх учасників ринку інтернету речей та визначав їхній правовий статус. Крім того зазначено, що владний вплив державних органів на суб'єктів IP не має бути спрямований на обмеження інновацій та гальмування розвитку технологій. Автори акцентують, що можливий нормативно-правовий акт має носити темпоральний характер і підлягати широкому тлумаченню в умовах неможливості прогнозування тенденцій розвитку технологій та оперативного реагування на них.

Зауважено, що навіть у випадку прийняття відповідного акту, все одно залишатиметься необхідним убезпечення своєчасного реагування на інноваційний елемент та постійні зрушення в галузі інформаційних технологій, які з кожним днем стають все більш масштабними. Зроблено висновок щодо сутності і форми потенційного нормативного акта.

Ключові слова. інтернет речей, права людини, персональні дані, правове регулювання, закон, прецедент, суб'єкти.

***Babiichuk Valentyna Serhiivna**, bachelor, student of the faculty of economic law, Yaroslav Mudryi National Law University, 03186, Kyiv, Poviytoflotskyi Ave, 34, tel.: 097 406 24 33, e-mail: valentynababiychuk99@gmail.com, https://orcid.org/0000-0002-6536-9939*

***Shumilo Inesa Anatoliyivna**, Candidate of Juridical Sciences, Associate Professor, Department of Internationa Private Law and Comparative Law, Yaroslav Mudryi National Law University, 61024, Kharkiv, Pushkinska Str. 77, tel.: 038 704 89 10, e-mail: i.a.shumilo@nlu.edu.ua, https//orcid.org/0000-0002-2123-7272*

INTERNET OF THINGS: NEW DIRECTIONS OF LEGISLATION MODERNIZATION

Abstract. In the context of global expansion by the Internet of Things, the problem of improper legal regulation of this issue is very acute. The lack of unified standards and certification protocols for IP users and developers becomes the basis for the perpetration of offences by dishonest actors in the Internet of Things market.

The article analyzes legal precedents, examines foreign experience in the legal regulation of IP and presents certain conclusions and proposals for possible modernization of the legislature in accordance with modern requirements. In particular, the issues of confidentiality of personal data, balance between the interests, restriction of the rights of the owner of IP devices and liability issues of IP actors were studied.

The authors emphasize that a potential legal act should be of an international nature, direct its action to protect the rights of Internet of things users and take into account the conflicting nature of international private law at the same time. The importance and necessity of concentrating the efforts of the main actors of the IP market and legislators to create an act that would strengthen current situations, meet modern requirements and take into account the interests of Internet of Things users and determine their legal status. In addition, it is stated that the overbearing influence of public authorities on IP entities should not be aimed at limiting innovation and inhibiting the development of technology. The authors emphasize that a potential legal act should be temporal in nature and subject to broad interpretation under the impossibility of predicting trends in technological development and rapid response to them.

It is observed that even if the relevant act is adopted, it will still be necessary to ensure a timely response to the innovation feature and constant changes in the field of information technology, which are becoming more widespread every day. The conclusion on the nature and form of a potential legal act is made.

Keywords: Internet of Things, human rights, personal data, legal regulation, law, precedent, actors.

Постановка проблеми. Технології наразі розвиваються дуже стрімко, небачені раніше пристрої стають невід'ємною частиною нашого побуту. Одним з таких, відносно нових, явищ є впровадження технології інтернету речей або IoT (Internet of Things) мовою оригіналу. Єдиного підходу до тлумачення терміну немає, але, проаналізувавши наявні наукові праці, за допомогою порівняння, аналізу, синтезу та абстрагування, можемо детермінувати IoT наступним чином: це мережа пристроїв з доступом до інтернету, які комунікують між собою з метою збору, передання та обробки даних без зовнішнього безпосереднього втручання людини. Констатуємо, що система обміну інформацією трансформувалась з формули взаємодії людина – машина до — машина – машина (M2M) [1].

Глобальна експансія з боку IP пояснюється низькою собівартістю обчислювальних потужностей і безпосередньо передачі даних, гранично низьким показником енергозатратності, гнучкістю систем аналізу та збереження даних. Нові технології покликані спростити та урізноманітнити життя людини, проте з новими можливостями виникають і нові загрози. IoT трансформував вже існуючі проблеми та спровокував виникнення нових. Найсуттєвішим з викликів є саме правовий. Оскільки право природньо не встигає попереджувати виклики, продуковані технологіями, нормативно-праве регулювання IP є не достатньо належним.

Аналіз останніх досліджень і публікацій. Проблема правового регулювання інтернету речей в епоху стрімкого розвитку технологій є надзвичайно актуальною, проте трансформація міжнародного приватного і національного права відповідно до викликів сучасності відбувається не так оперативно, як того потребує час. Дослідженню цієї тематики присвячені роботи Баранова О. А., Пазюк А. В., Шульги М. І., Брауна Й., Брижко В. М., Рослякова А. В., Бородіна В. А., Гамелінка К. Й. та ін. Але питання безпосередньої модернізаціїї правових норм відповідно до вимог сучасності залишається недостатньо дослідженим та розробленим.

Мета статті. Проаналізувати наскільки правове регулювання IP є достатнім у сьогоднішніх реаліях і запропонувати можливі шляхи вдосконалення та модернізації чинного законодавства. Дослідити зарубіжний досвід реагування на виклики, продуковані швидкими змінами в сфері інформаційних технологій, й виокремити характерні прецеденти, які можуть стати зразковими і корисними в подальшому правозастосуванні.

Виклад основного матеріалу. Відсутність єдиних стандартів та протоколів сертифікації загалом для користувачів та розробників IoT залишає недобросовісним суб'єктам ринку інтернету речей широке поле для правопорушень. У розробників відсутнє опосередковане зобов'язання належним чином захищати виготовлений продукт, оскільки загальні нормативи з якісної оцінки безпеки відсутні. Складні та заплутані угоди користувача лише погіршують ситуацію. Певні виробники прямо зазначають, що власником інформації, яку генерує, збирає та аналізує той чи інший пристрій є не особа, яка придбала пристрій, а виробник. Так, напри-

клад, користувачі пристроїв Apple не наділені правомочністю власника, а є лише ліцензіатами копій програмного забезпечення. Більшість користувачів не читаючи приймають умови угоди та натомість не отримують ніяких гарантій щодо захисту персональних даних. Для деяких пристроїв не передбачено навіть ліцензії, що пояснюється маленьким розміром девайсу або відсутністю на ньому дисплею. Також споживачам надзвичайно складно перекласти положення угоди, яка зазвичай подається мовою виробника. Незрозумілість та складність юридичної мови на нашу думку прямо порушує право на обізнаність сторін щодо змісту угоди. Договір має бути зрозумілим для сторін.

Звуження обсягу правомочностей власника є дуже поширеною практикою серед великих транснаціональних компаній. Deere & Company випускає транспортні засоби — трактори John Deere, у котрі вбудовано програмне забезпечення та іншого роду системні компоненти, які не дозволяють користувачу ремонтувати машини, ліцензійним договором передебачено лише звернення до авторизованих сервісів або дилерів. Якщо особа наважиться власноруч модифікувати пристрій — подібні діїї будуть кваліфіковані як несанкціоноване втручання та спровокують дистанційну деактивацію пристрою компанією-власником. Як і у випадку з Apple, трактори перебувають у власності John Deere, а користувачі мають лише ліцензію на есплуатацію [2]. Такі діїї з боку компаній можна характеризувати як намагання самостійно заповнити правові прогалини у сфері IP та певною мірою убезпечити себе від позовів з боку споживачів.

Як вже зазначалось, основним призначенням IoT пристроїв є збір даних. Превалюча більшість інформації, зібраної пристроєм Інтернету Речей (далі IP), схильна використовуватись не за призначенням. Користувачі опиняються у зоні ризику перед несанкціонованим доступом до персональних даних.

Інтернет речей вже є нашою буденністю, а тому необхідно встановити певні стандарти та гарантії щодо забезпечення схоронності персональних даних. Оскільки право не встигає вчасно трансформуватись до кожного технологічного виклику, в законодавчих актах нового покоління мають бути прописані такі вимоги та принципи, певні етичні норми, які б діяли незалежно від того, чи існує наразі технологія чи буде доступна лише через певний проміжок часу. Це можуть бути не якісь конкретні постулати, а щось загальне, здатне до широкого тлумачення та темпоральної дії. Даний акт має бути обов'язково міжнародного характеру, адже виробник і споживач зазвичай громадяни різних держав, враховувати колізійність міжнародного приватного права та повною мірою обумовлювати захист прав людини у сфері IT в умовах транснаціональної взаємодії. Та обов'язково не бути спрямованим на жорстке законодавче обмеження. Важливе також оперативне прийняття заходів і чітка взаємодія виробників, розробників та законодавців, адже недостатня врегульованість взаємодії між споживачами та виробниками пристроїв IoT може загальмувати подальший технологічний прогрес.

Суперечлива світова судова практика, невизначеність статусу споживача (власник чи ліцензіат) можуть

спричинити відтік чи призупинення інвестицій та як наслідок поставити ринок IoT у нестабільне становище. Оскільки повну безпеку пристроїв наразі забезпечити неможливо, необхідно ухвалити акт, який принаймні мінімізував ризики та зобов'язував зберігати приватну інформацію у рамках компанії чи іншого органу без передавання її невизначеним третім особам.

Певні зрушення простежуються у законодавчих актах зарубіжних країн, де питання врегулювання взаємодії IoT та людини виникло набагато раніше. Але зауважимо, більшість з них, хоч і регулюють приватність, головним чином є лише дотичними до IoT, і не спеціалізуються безпосередньо на пристроях інтернету речей. Такими законами є Закон про захист конфіденційності дітей в Інтернеті (Children's Online Privacy Protection Act), яикй забороняє збирати та зберігати інформацію про дітей, молодше 13 років без згоди їхніх батьків (опікунів). Відомий правовий прецедент з GOOGLE та YouTube, котрі звинувачені у зборі персональної інформації про дітей-користувачів відеохостингом, та мають виплатити великий штраф [3].

Також, приватність даних захищає галузеве законодавство: Закон про медичне страхування, доступність та підзвітнітсь медичних послуг, про охорону та відповідальність за інформацію, отриману в результаті медичного страхування — Health Insurance Portability and Accountability Act of 1996 (HIPPA), що стосується захисту конфіденційної інформації про фізичне та психічне здоров'я пацієнтів на федеральному рівні та Закон про недоторканість приватного життя в засобах електронної комунікації Electronic Communication Privacy Act of 1986 (ECPA), що покликаний захистити телеграфні, усні і електронні повідомлення, що перебувають у процесі пересилання та безпосередньо тих, що вже зберігаються на ПК, закон також поширює свою дію на електронну пошту, телефонні розмови та інші електронні дані [4].

Так само рівновіддаленими від проблематики інтернету речей є національні акти: Закон України «Про захист персональних даних» від 01.06.2010 р. № 2297-VI, Закон України «Про інформацію» від 02.10.1992 р. № 2657-XII, Розпорядження КМУ «Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації» від 17.01.2018 р. № 67-р. Акти містять загальні положення щодо конфіденційності та недоторканості інформації, приватного життя, але перелічені закони дуже важко застосувати до сучасних реалій інтернету речей.

Каліфорнія стала першим штатом із Законом, що прямо регулює кібербезпеку при використанні IoT пристроїв (№SB-327). Проект отримав шквал критики через загальність та розмитість, але прямо вказав, що відповідальність за недоторканість приватного життя користувачів пристроями лежить на виробниках, які і мають забезпечувати належний захист від зламу та попереджувати можливість несанкціонованого доступу до персональних даних. Також ним висунуто вимогу до розробників щодо наповнення пристрою функціоналом з безпеки задля попередження можливих зміни чи вилучення даних [5].

Доцільно приділити увагу Доповіді Федеральної торгової комісії США «Принципи добросовісної інформаційної практики» («Fair Information

Practice Principles»), адже висвітлені у ній концепції стусуються справедливого використання інформації та безпеки персональних даних в інтернеті, виголошені у Доповіді ідеї знайшли відображення у багатьох сучасних директивах: «Загальному положенні про захист даних» (General Data Protection Regulation) ЄС; Законі про захист персональних даних та електронних документів» (Personal Information Protection and Electronic Documents Act) Канади; Керівних принципах Організації економічного співробітництва та розвитку (OECD Privacy Guidelines) [6].

Окремо варто зазначити про Новий Регламент з кібербезпеки ЄС. Даним положенням передбачено схему індивідуальної сертифікації продукції та послуг у сфері IoT та систему довіри щодо виробника для користувача. Наразі носить рекомендаційний характер [7]. Варто зазначити, що запропонована система гарантій є вкрай ефективною, адже зазвичай компанії дбають про власний гудвіл, тож запорукою їхнього ефективного функціонування буде довіра споживачів, яка будується на взаємних правах та обов'язках щодо безпеки та поваги до приватності.

Ера інформатизації привнесла зміни до традиційного розуміння природи конфіденційності та балансу між приватними інтересами та інтересами владних органів. У ході розгляду справи Riley v. California постало питання права поліції піддавати обшуку цифрові дані з телефона, вилученого (конфіскованого) під час затримання, які згодом були використані для висунення обвинувачень. ВС США постановив, що інформація на засобі зв'язку підлягає захисту, проте поліцейський має право проводити обшук вилученого телефона після отримання на це відповідного ордеру [8].

Ще одним прецедентом стосовно балансу інтересів стала справа Apple v. Federal Bureau of Investigations. FBI висунув вимогу Apple надати доступ до телефону особи, котру звинувачують у вчиненні особливо тяжкого умисного злочину. Компанія відмовила, вважаючи такі дії надмірним розширенням повноважень органів влади. Адже отримавши доступ до одного девайсу, владні органи зможуть надалі використовувати ключ доступу та зламувати інші пристрої [9].

Черговим правовим викликом від IoT є розмиття інституту персональної відповідальності. Автоматизовані пристрої взаємодіють між собою без втручання людини, тож невідомо, хто у разі спричинення збитків девайсами IoT буде нести відповідальність, — власник чи виробник. У випадках ДТП за участі авто Tesla Inc. компанія наголошувала, що функція автопілоту має допоміжний характер та не передбачає повністю автономного руху. Проте, технології розвиваються, законодавстом необхідно чітко передбачити можливі загрози для життя і здоров'я людини та виокремити, яка зі сторін буде нести відповідальність за ті чи інші випадки.

Окрім проблеми відсутності приватості у користувачів IoT, постає також питання можливої дискримінації. Немає гарантій, що інформація, зібрана IoT, не буде використовуватись страховиками, роботодавцями чи кредиторами у власних економіко-орієнтованих цілях, адже наразі трекери, смартфони зберігають та передають інформацію про фінасовий стан особи, залежності, негативні звички, стан здоров'я загалом тощо [2].

Конфіденційність персональних даних передбачає право споживача інтернет-послуг на повагу до його персональних даних та право визначати

спосіб використання таких даних іншими особами чи організаціями. За стрімкого розвитку системи IoT конфіденційність забезпечити вкрай важко або навіть неможливо, адже дані, згенеровані «розумними» передбачають включення до процесу обробки даних багатьох сторін: виробників, розробників додатків, соціальних платформ.

Висновки. У підсумку зазначимо, що нові технології завжди продукуватимуть виклики для світових правових систем. Поставатиме питання балансу між безпекою приватних даних конкретного індивіда та загальнодержавною безпекою. Нові законодавчі акти у сфері IoT мають забезпечувати дотримання такого балансу. Подальшого врегулювання потребує проблематика непрозорості угод користувача, суб'єкти мають розуміти взаємні права та обов'язки, тож доцільно виробити певні принципи етичного та функціонального характеру.

Окремою проблемою є невизначеність юрисдикції, що поширюється на учасників інтернету речей, зокрема у разі визначення застованого права, дії закону в просторі та за колом осіб, визначення місця вирішення спору тощо. Тож необхідне подальше вдосконалення на доктринальному та практичному рівнях приватно-правових міжнародних законів. Зокрема, як вже зазначалось, доцільним було б прийняття законодавчого акту нового покоління, котрий закріплював загальні вимоги до суб'єктів та об'єктів IoT і принципи їхньої діяльності та вирішував можливі інтертемпоральні, інтерлокальні та інтерперсональні колізії та був прийнятий за безпосереднього співробітництва законотворчих органів та представників ринку послуг інтернету речей. Такий консенсус допоможе уникнути складності або неможливості правореалізації та допоможе його підлаштувати під конкретні вимоги ринку та попередить можливі прогалини, які мають місце за недостатньої обізнаності правотворців у тій чи іншій проблематиці. Також необхідно чітко розмежувати рівні саморегулювання та окреслити можливі межі втручання державних органів у ринок IoT задля забезпечення подальшого безперебійного розвитку технологій, адже дуже жорсткі вимоги та регламенти з боку владних структур можуть неспівмірно здорожчувати виробництво чим знижувати якість пристрою і відповідно можливість захисту ними персональних даних споживача.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Баранов О. А. Інтернет речей і штучний інтелект: витоки проблеми правового регулювання. *ІТ-право: проблеми та перспективи розвитку в Україні: збірник матеріалів ІІ-ї Міжнародної науково-практичної конференції*. Львів: НУ «Львівська політехніка». 2017. С. 18-42.
2. C. P. Chike. The Legal Challenges of Internet of Things. 2017. URL: https://www.researchgate.net/publication/322628457
3. The official website of the Federal Trade Commission. URL: https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations
4. Justice Information Sharing. URL: https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285
5. A. Robertson. California just became the first state with an Internet of Things cybersecurity law. 2018. URL: https://www.theverge.com/2018/9/28/17874768/california-iot-smart-device-cybersecurity-bill-sb-327-signed-law
6. A. O`Driscoll. 5 core principles of fair information practices. *Comparitech blog*. 2017.

URL: https://www.comparitech.com/blog/vpn-privacy/fair-information-practices/

7. Proposal for a regulation of the European Parliament and of the Council on ENISA, the «EU Cybersecurity Agency», and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification («Cybersecurity Act»). URL: https://clck.ru/FEMLA

8. Riley v. California, 134 S. Ct. 2473. 573 US (2014).

9. A. Kharpal. Apple vs FBI: All you need to know. 2016. URL: https://www.cnbc.com/2016/03/29/apple-vs-fbi-all-you-need-to-know.html

10. Expanding the Internet of Things: Four Key Legal Issues October 2020. URL: https://www.jdsupra.com/legalnews/expanding-the-internet-of-things-four-65062/

11. Senatepasses bipartisan DIGIT Act. *Press*.2020.URL: https://www.fischer.senate.gov/public/index.cfm/2020/1/senate-passes-bipartisan-digit-act

REFERENCES:

1. Baranov, O. A. (2017). Internet rechey i shtuchniy intelekt: vitoki problemi pravovogo regulyuvannya. [Internet of Things: behind the problems of legal regulation]. Proceedings of the International Scientific and Practical Conference: *II Mizhnarodna naukovo-praktychna konferentsiia «IT-pravo: problemi ta perspektivi rozvitku v Ukraini» – The Second International Scientific and Practical Conference «IT law: challenges and perspectives»*. (18-42). Lviv: NU «Lvivska politehnika» [in Ukrainian].

2. Chike, C. P. (2017). The Legal Challenges of Internet of Things. *www.researchgate.net*. Retrieved from https://www.researchgate.net/publication/322628457 [in English].

3. The official website of the Federal Trade Commission. *www.ftc.gov*. Retrieved from https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations [in English].

4. Justice Information Sharing. *it.ojp.gov*. Retrieved from https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285 [in English].

5. Robertson, A. (2018). California just became the first state with an Internet of Things cybersecurity law. *www.theverge.com*. Retrieved from https://www.theverge.com/2018/9/28/17874768/california-iot-smart-device-cybersecurity-bill-sb-327-signed-law [in English].

6. O`Driscoll, A. (2017) 5 core principles of fair information practices. www.c*omparitech.com*. Retrieved from https://www.comparitech.com/blog/vpn-privacy/fair-information-practices/ [in English].

7. Proposal for a regulation of the European Parliament and of the Council on ENISA, the «EU Cybersecurity Agency», and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification («Cybersecurity Act»). *clck.ru*. Retrieved from https://clck.ru/FEMLA [in English].

8. Riley v. California, 134 S. Ct. 2473. 573 US (2014). [in English].

9. Kharpal, A. (2016) Apple vs FBI: All you need to know. *www.cnbc.com*. Retrieved from https://www.cnbc.com/2016/03/29/apple-vs-fbi-all-you-need-to-know.html [in English].

10. Expanding the Internet of Things: Four Key Legal Issues (2020). *www.jdsupra.com*. Retrieved from https://www.jdsupra.com/legalnews/expanding-the-internet-of-things-four-65062/ [in English].

11. Senatepasses bipartisan DIGIT Act. (2020). *www.fisher.senate.gov*. Retrieved from https://www.fischer.senate.gov/public/index.cfm/2020/1/senate-passes-bipartisan-digit-act [in English].