ЦИВІЛІСТИЧНІ ПРОБЛЕМИ ІТ-ПРАВА

УДК 347.77:(007:004.0565):004738.5

Некіт Катерина Георгіївна,
кандидат юридичних наук, доцент, доцент кафедри цивільного права
Національного університету «Одеська юридична академія»

ДЕЯКІ ПРАВОВІ ПРОБЛЕМИ ІНТЕРНЕТУ РЕЧЕЙ І НАПРЯМИ ЇХ ВИРІШЕННЯ

Постановка проблеми. Вплив технологій на життя людини та розвиток суспільства важко переоцінити. Наприкінці XX століття історія людства поділилася на дві епохи завдяки появі Інтернету, і швидкість розвитку технологій набирає таких обертів, що вже сьогодні, на початку XXI століття, ми впевнено можемо говорити про нову епоху в нашій історії – епоху Інтернету речей. Так, якщо кількість пристроїв, підключених до Інтернету у 2003 р., становила 500 мільйонів, то вже у 2010 р. їх кількість зросла до 12,5 мільярдів, а до 2020 р., за різними даними, прогнозують підключення до Інтернету від 26 до 50 мільярдів пристроїв [1]. Це, з одного боку, відкриває величезні перспективи для розвитку суспільства, але з іншого, як і будь-яке нове явище, породжує низку проблем, зокрема в правовій сфері, оскільки сьогодні немає жодного комплексного рішення щодо правового регулювання відносин у сфері Інтернету речей, як немає й самого легального визначення цього поняття.

Стан дослідження теми. Проблеми Інтернету речей останнім часом уже доволі часто привертають увагу дослідників, однак усе ще залишаються недостатньо недослідженими, численні питання залишаються відкритими. Серед сучасних дослідників, які приділяють увагу дослідженню проблематики Інтернету речей, можна згадати О. Баранова, А. Білощицького, Н. Віндерських, С. Грінгарда, І. Дороніна, Є. Харитонова, О. Харитонову й інших. Утім, проблеми Інтернету речей потребують подальших поглиблених досліджень.

Метою статті є аналіз системи правових проблем у сфері Інтернету речей і визначення напрямів їх вирішення з урахуванням останніх досліджень у цій сфері.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів. Для початку зупинимося детальніше на аналізі деяких технічних аспектів цього явища, які дозволяють скласти цілісне уявлення про Інтернет речей, що необхідно для вирішення правових проблем у цій сфері.

Термін «Інтернет речей» з'явився в 1999 р., коли працівником компанії Procter & Gamble Кевіном Ештоном було запропоновано покращити логістику корпорації за допомогою радіочастотних міток (radio-frequency identification, RFID) [2]. Щоправда, сьогодні цей термін піддається критиці на тій підставі, що Інтернет фактично є ім'ям власним, яке використовується для позначення глобальної Мережі мереж, побудованої на певних стандартах, тоді як існує ще Всесвітня павутина (WWW) – найбільш популярна Інтернет-платформа, яка забезпечує доступ до документів і технічно не містить перепон для підключення до цієї мережі речей-пристроїв, тобто для створення мереж, які складаються з речей із використанням технології Інтернет. Як зазначають критики, підміна понять виникла й зміцнилася через відсутність належного розуміння відмінностей між Інтернетом і WWW. Всесвітня павутина – це розподілена система, що надає доступ до зв'язаних між собою документів, розташованих на різних комп'ютерах, підключених до Інтернету. Говорячи про IoT, зазвичай мають на увазі не просто комунікації, а щось аналогічне WWW, щось на зразок павутини речей. Ця обставина була усвідомлена відносно недавно, після чого з'явився відповідний термін Web of Things (WoT), який точніше підходить до ідеального уявлення про IoT [3] (саме тому в багатьох джерелах використовується поняття «інтернет речей» – з маленької літери).

Проте сьогодні вже є усталений термін «Інтернет речей», який набув широкого застосування у 2008–2009 рр., коли відбувся перехід від «Інтер-

нету людей» до «Інтернету речей», коли кількість підключених до Мережі предметів перевищила кількість населення Землі, і який, очевидно, буде використовуватися в подальшому, що викликає потребу введення його й у правову реальність.

Сьогодні є безліч технічних визначень поняття «Інтернет речей», зокрема, Інтернет речей визначається як мережа фізичних об'єктів, які мають вбудовані технології, що дозволяють здійснювати взаємодію із зовнішнім середовищем, передавати відомості про свій стан і приймати дані ззовні (Gartner) [3]. Також Інтернет речей визначають як «речі», такі як пристрої та датчики, відмінні від комп'ютерів, смартфонів або планшетів, які поєднуються, взаємодіють один з одним або передають інформацію один від одного завдяки Інтернету [4]. Інтерес для нашого подальшого дослідження викликає визначення, згідно з яким Інтернет речей – це концепція комунікаційної мережі фізичних або віртуальних об'єктів («речей»), які мають технології для взаємодії між собою та з навколишнім середовищем, а також можуть виконувати певні дії без втручання людини. Сутність цієї концепції полягає в тому, щоб усі предмети побуту, товари, вузли технологічних процесів тощо були оснащені вбудованими комп'ютерами та сенсорами, мали змогу обробляти інформацію, що надходить із навколишнього середовища, обмінюватися нею та виконувати різні дії залежно від отриманої інформації [5]. Звернемо увагу, що у визначенні поняття «Інтернет речей» часто використовується поняття віртуальної речі. Так, відповідно до Рекомендації Y2060 Відділу стандартів зв'язку Міжнародного союзу електрозв'язку «Огляд Інтернету речей», під Інтернетом речей пропонується розуміти глобальну інфраструктуру для інформаційного суспільства, яка забезпечує можливість надання більш складних послуг шляхом з'єднання між собою речей (фізичних і віртуальних) на підставі наявних і таких, що розвиваються, функціонально сумісних інформаційно-комунікаційних технологій [6].

Серед визначень поняття «Інтернет речей» з урахуванням правового аспекту, що пропонуються сучасними дослідниками, варто виділити визначення, запропоноване О. Барановим, згідно з яким під Інтернетом речей варто розуміти комплекси й системи, що складаються із сенсорів, мікропроцесорів, виконавчих пристроїв, локальних та/або розподілених обчислювальних ресурсів і програмних засобів, програм штучного інтелекту, технологій хмарних обчислювань, передача даних між якими здійснюється за допомогою мережі Інтернет, і призначені для надання послуг і проведення робіт в інтересах суб'єктів (фізичних або юридичних осіб) [7, с. 7].

Наведене визначення видається цілком прийнятним для розуміння поняття Інтернету речей у правовій площині, хіба що з тим уточненням, що Інтернет речей варто визначати як вищевказану сукупність компонентів, що використовуються для задоволення інтересів фізичних, юридичних осіб або інтересів держави й суспільства (з урахуванням того факту, що Інтернет речей є багатогранним поняттям та може використовуватись у різних сферах, із різними цілями, а тому тут можуть виникати різноманітні правові відносини з різними учасниками, про що буде йтися далі).

Серед проблем, пов'язаних з Інтернетом речей, можна виділити такі, як правовий режим інформації, персональні дані й приватне життя, інформаційна безпека, розроблення понятійного апарату, проблема ідентифікації осіб, відповідальність учасників цих відносин, проблема збору доказів тощо. Деякі з проблем, що виникають у сфері Інтернету речей, зокрема проблема відповідальності за шкоду, заподіяну пристроями, що входять до системи IoT, уже розглядалися нами раніше [8].

Ще одним чи не найважливішим проблемним питанням у сфері Інтернету речей є питання захисту персональних даних.

Із метою забезпечення захисту персональних даних у Європейському Союзі було розроблено нові правила оброблення персональних даних і прийнято Загальний регламент із захисту даних (Регламент ЄС 2016/679 від 27 квітня 2016 р. або GDPR – General Data Protection Regulation), який набув чинності в травні 2018 року, після чого компанії, що порушують правила щодо оброблення персональних даних, ризикують бути притягнутими до відповідальності з накладенням штрафів до 20 мільйонів євро, або 4% річного доходу компанії. Основні принципи оброблення персональних даних за GDPR такі:

1) законність, справедливість і прозорість: персональні дані повинні оброблятися законно, справедливо й прозоро. Будь-яку інформацію про цілі, методи й обсяги опрацювання персональних даних слід висловлювати максимально доступно й просто;

2) обмеження мети: дані повинні збиратися й використовуватися виключно в тих цілях, які заявлені компанією (онлайн-сервісом);

3) мінімізація даних: не можна збирати особисті дані в більшому обсязі, ніж це необхідно для цілей оброблення;

4) точність: особисті дані, які є неточними, повинні бути видалені чи виправлені (на вимогу користувача);

5) обмеження зберігання: особисті дані повинні зберігатися у формі, яка дозволяє ідентифікувати суб'єкти даних на строк не більший, ніж це необхідно для цілей оброблення;

6) цілісність і конфіденційність: під час оброблення даних користувачів компанії необхідно забезпечити захист персональних даних від несанкціонованої чи незаконної обробки, знищення й пошкодження [9].

Однією з важливих для належного розвитку IoT новацій, закріплених у GDPR, є так звані дружні для інновацій правила, відповідно до яких гарантії захисту даних у продуктах і послугах, що розробляються, повинні бути забезпечені на найбільш ранніх стадіях розвитку, тобто ще на стадії проектування. Це правило має назву Privacy by Design або Data Protection by Design. Основними принципами Privacy by Design є такі:

1) превентивні заходи, а не тільки усунення наслідків: вбудовування конфіденційності в конструкцію системи повинне бути активним, а не обмежуватися лише заходами з усунення наслідків. Такий підхід запобігає випадкам порушення конфіденційності ще до того, як вони відбуваються. Іншими словами, особиста інформація повинна бути захищена до того, як система запущена в роботу, а не після виявлення порушень конфіденційності;

2) конфіденційність як стандартна установка: Privacy by Design прагне досягти максимального ступеня захисту особистої інформації, гарантуючи, що персональні дані захищені автоматично в тій або іншій інформаційній системі чи ділових відносинах. Навіть якщо індивідуум не вживає ніяких заходів, його особиста інформація залишається надійно захищеною. Не вимагається ніяких дій із боку індивідуума для захисту особистої інформації, адже система вже на початку містить у собі необхідні установки;

3) конфіденційність як частина структури: захист особистої інформації повинен стати невід'ємною частиною архітектури будь-якої інформаційної системи чи ділових відносин. Це не якийсь додатковий компонент, внесений у систему постфактум;

4) повна функціональність із сумарним позитивним результатом: Privacy by Design не шукає приводів для помилкової дихотомії, таких, наприклад, як зміцнення безпеки системи на противагу захисту особистої інформації, демонструючи, що можна забезпечити й те, і інше;

5) захист особистої інформації впродовж усього циклу її збору, зберігання, оброблення й знищення: конфіденційність повинна бути вбудована в систему ще до початку збору даних. Більше того, цей захист повинен надійно розповсюджуватися на весь цикл зберігання й оброблення даних; іншими словами, збереження даних має важливе значення для конфіденційності від моменту запуску системи й до кінця її існування. Це гарантує надійне зберігання даних, а після закінчення їх використовування – надійне й своєчасне знищення;

6) доступність і відвертість: усі компоненти й операції залишаються відкритими й доступними (як для користувачів, так і для тих, хто забезпечує цей вид сервісу);

7) дотримання конфіденційності користувачів: система повинна бути орієнтована на користувача. Це досягається такими заходами, як захист особистої інформації за умовчанням, своєчасне повідомлення про збір особистої інформації, надання користувачу свободи вибору в зручній і зрозумілій формі [10].

Крім того, що наведені положення щодо захисту персональних даних варті уваги українського законодавця з метою забезпечення захисту персональних даних українських громадян шляхом прийняття аналогічного акта, необхідно пам'ятати, що Регламент ЄС 2016/679 має екстериторіальний характер, тобто застосовується до всіх компаній, що обробляють персональні дані громадян і резидентів ЄС, незалежно від місця знаходження такої компанії.

Пильної уваги потребує проблема забезпечення інформаційної безпеки у сфері Інтернету речей. Раніше нами вже обговорювалися випадки порушень правил інформаційної безпеки у сфері Інтернету речей і причини, з яких такі порушення трапляються. Наводилися також і приклади судових спорів із причини незабезпечення належної безпеки пристроїв, що входять до системи Інтернету речей [8, с. 109]. Як зазначалося нами раніше, для забезпечення інформаційної безпеки у сфері Інтернету речей одним із ключових завдань є взяття на себе професійним співтовариством відповідальності щодо цього питання. Припускається, що допомогти в забезпеченні інформаційної безпеки зможуть засоби саморегуляції та сертифікація пристроїв, що входять у систему Інтернету речей.

На думку дослідників, проблему узгодження співіснування різноманітних компонентів Інтернету речей допоможе вирішити введення певних стан-

дартів у сфері Інтернету речей. Так, зазначається, що сьогодні необхідним є перехід до нового рівня технологій, де виникає новий підключений світ. Так само, як раніше різні патентовані мережеві протоколи IBM, Novell, Bay Networks, Cisco Systems усе ж зникли, залишивши замість себе спільний стандарт IP, патентовані та закриті системи Інтернету речей повинні поступитися місцем більш відкритому простору. Ситуація, коли є безліч різноманітних не стандартизованих пристроїв, аналогічна ситуації, коли б, наприклад, кожен виробник автомобілів використовував свою систему управління, в одному автомобілі б установлювалося кермо, а в іншому – джойстик чи панель управління. Або якби системи електронної пошти були б несумісними, а телефоном було б неможливо телефонувати на номери інших операторів, і для побутової техніки різних брендів були б потрібні різні типи підключення води чи електричної енергії. Так само й у світі Інтернету закритих чи патентованих речей, у якому пристрої не підключені один до одного, власник будинку не зможе керувати освітленням, системою безпеки, терморегулятором, замками тощо за допомогою центрального додатка чи панелі управління. І сьогодні дедалі більше визнається необхідність стандартів для Інтернету речей. Із цією метою Асоціацією зі стандартизації було розроблено низку стандартів і протоколів, покликаних допомогти розвитку підключених систем. Сьогодні також ведеться робота над розробленням для технологій, систем і пристроїв Інтернету речей платформи з відкритим кодом [11, с. 120–121].

Отже, серед заходів забезпечення інформаційної безпеки у сфері IoT насамперед необхідно виділити саморегуляцію, яка повинна забезпечуватися за допомогою тісної співпраці технологічних компаній і громадянського суспільства. Це мінімізує втручання держави в цю сферу, що сприятиме швидкому розвитку інноваційних технологій. Виникає лише потреба в правовому регулюванні відносин між громадянським суспільством, організаціями із захисту прав споживачів і технологічними компаніями. Насамперед зусилля мають бути спрямовані на охорону прав людини від порушень, пов'язаних із функціонуванням Інтернету речей, що передбачає необхідність профілактики таких порушень шляхом контролю за встановленням належного захисного програмного забезпечення на всі пристрої, що входять до екосистеми IoT.

Слід зазначити, що в Європі розвитку технологій IoT уже загрожують регулятивні бар'єри. Із метою забезпечення безпеки в Європі на державному рівні планують ввести обов'язкову сертифікацію всіх пристроїв, які підключаються до IoT. Країни – учасниці ЄС розглядають можливість розроблення комплексу заходів, націлених на забезпечення кібербезпеки Інтернету речей. Заступник європейського комісара із цифрової економіки й суспільства Тібо Клейнер відзначив, що контролю потребують не тільки прилади, які, наприклад, можна захистити за допомогою чипів, що забезпечують віддзеркалення атак хакерів, але й мережі, до яких вони підключені, а також хмарні сховища [12].

Висновки з дослідження та перспективи подальших розвідок у цьому напрямі. У підсумку зазначимо, що оскільки Інтернет речей є складним і багатогранним поняттям, правові проблеми, що виникають у цій сфері, є досить різноманітними. До таких відносять проблеми захисту персональних даних і забезпечення невтручання у приватне життя, проблеми інформаційної безпеки, проблеми ідентифікації осіб, відповідальності учасників цих відносин, проблеми збору доказів тощо.

На вирішення проблеми захисту персональних даних у сфері Інтернету речей спрямовані, зокрема, норми GDPR шляхом закріплення дружніх для інновацій правил, відповідно до яких гарантії захисту даних у продуктах і послугах, що розробляються, повинні бути забезпечені на найбільш ранніх стадіях розвитку, тобто ще на стадії проектування (Privacy by Design або Data Protection by Design).

Проблему забезпечення інформаційної безпеки сьогодні пропонують вирішувати шляхом саморегуляції у сфері Інтернету речей і введенням стандартизації й обов'язкової сертифікації об'єктів, що входять до системи Інтернету речей. Остання позиція видається доцільною, хоча й піддається критиці, оскільки надмірна регуляція може завадити розвитку технологій у сфері IoT.

ЛІТЕРАТУРА:

1. Храмцов П. Всеобъемлющий интернет: прогнозы и реальность. Открытые системы. 2013. № 4. URL: http://www.osp.ru/os/2013/04/13035552/.
2. Інтернет вещей – что это такое и как применять IoT в реальном бизнесе. URL: https://rb.ru/longread/iot-cards/.
3. Что такое Интернет вещей. URL: http://www.tadviser.ru/index.php/(Internet_of_Things,_IoT)#cite_note-0.
4. Открытая концепция «Интернет вещей: правовые аспекты (Российская Федерация)». URL: http://www.dentons.com/ru/whats-different-about-dentons/connecting-you-to-talented-lawyers-around-the-globe/news/2016/june/dentons-develops-russias-first-ever-whitepaper-on-the-legal-aspects-of-the-internet-of-things.

5. Інтернет речей. URL: http://glossary.starbasic.net/index.php?title=%D0%86%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D1%80%D0%B5%D1%87%D0%B5%D0%B9.
6. Обзор Интернета вещей. URL: https://www.itu.int/rec/T-REC-Y.2060-201206-I.
7. Баранов О. Інтернет речей (IoT): огляд правових проблем. Інтернет речей: проблеми правового регулювання і впровадження: матеріали науково-практичної конференції (24 жовтня, 2017 р., м. Київ) / Упоряд. В. Фурашев, С. Петрячев. Київ: Національний технічний університет України «Київський політехнічний інститут ім. І. Сікорського», Вид-во «Політехніка», 2017. С. 7–16.
8. Некіт К. Проблеми забезпечення інформаційної безпеки та відшкодування шкоди, заподіяної пристроями, підключеними до Інтернету речей. Часопис цивілістики. 2017. № 27. С. 107–112.
9. GDPR – новые правила обработки персональных данных в Европе для международного IT-рынка. URL: https://habrahabr.ru/company/digitalrightscenter/blog/344064/.
10. Кавукиан Э. Privacy by Design: 7 основополагающих принципов. URL: https://online.zakon.kz/Document/?doc_id=31633216#pos=0;0.
11. Грингард С. Интернет вещей: будущее уже здесь. М.: Альпина Паблишер, 2016. 188 с.
12. ЕС отрегулирует интернет вещей. URL: https://roskomsvoboda.org/22079/.

Некіт Катерина Георгіївна

ДЕЯКІ ПРАВОВІ ПРОБЛЕМИ ІНТЕРНЕТУ РЕЧЕЙ І НАПРЯМИ ЇХ ВИРІШЕННЯ

Стаття присвячена визначенню кола проблем, що виникають із розвитком Інтернету речей, і аналізу напрямів їх вирішення. Зазначено, що до таких проблем відносять проблеми захисту персональних даних і забезпечення невтручання у приватне життя, проблеми інформаційної безпеки, проблеми ідентифікації осіб, відповідальності учасників цих відносин, проблеми збору доказів тощо. Першочерговими серед них є проблема захисту персональних даних і забезпечення інформаційної безпеки. Цим проблемам приділена особлива увага, визначені шляхи запобігання порушенням у цій сфері.

Ключові слова: Інтернет речей, речі, пристрої, персональні дані, GDPR, інформаційна безпека, саморегулювання, сертифікація.

Некит Екатерина Георгиевна

НЕКОТОРЫЕ ПРАВОВЫЕ ПРОБЛЕМЫ ИНТЕРНЕТА ВЕЩЕЙ И НАПРАВЛЕНИЯ ИХ РЕШЕНИЯ

Статья посвящена определению круга проблем, которые возникают с развитием Интернета вещей, и анализу направлений их решения. Отмечено, что к таким проблемам относят проблемы защиты персональных данных и обеспечения невмешательства в частную жизнь, проблемы информационной безопасности, проблемы идентификации лиц, ответственности участников этих отношений, проблемы сбора доказательств и тому подобное. Первоочередной среди них является проблема защиты персональных данных и обеспечения информационной безопасности. Этим проблемам уделено особенное внимание, определены пути предотвращения нарушений в этой сфере.

Ключевые слова: Интернет вещей, вещи, устройства, персональные данные, GDPR, информационная безопасность, саморегулирование, сертификация.

Nekit Kateryna

SOME LEGAL PROBLEMS OF THE INTERNET OF THINGS (IoT) AND WAYS OF THEIR SOLUTION

The article is dedicated to definition of the range of problems which arise due to the development of the Internet of things and to the analysis of the ways of their solution. It is noted that the most important issues in this sphere are: problems of personal data protection and holding of the principle of non-interference into private life, problems of information security, a problem of user's identification, responsibility of participants of these relations, problems of collecting proofs and so forth. Among them the problem of personal data protection and information security is primary. Special attention is paid to these problems, ways of prevention of violations in this sphere are defined.

It is noted that recently adopted in European Union General Data Protection Regulation addressed the problem of personal data protection in the sphere of the Internet of things. In this legal act so-called friendly rules for innovations were enshrined, according to which data protection guarantees concerning products and services have to be provided at early stages of development, that is at a design stage (Privacy by Design or Data Protection by Design). To the basic principles of Privacy by Design refer, particularly: 1) preventive measures, that is orientation on prevention of violations, but not just elimination of consequences; 2) confidentiality, maximum protection of personal information; 3) simultaneous safety of a system and protection of personal information; 4) protection of personal information throughout the whole cycle of its collecting, processing, storage and so on; 5) availability and openness of components of a system.

The problem of information security is suggested to be resolved, particularly, by self-regulation in the sphere of the Internet of things. It is also offered to enter standardization and obligatory certification of objects which are part of the system of the Internet of things. In Europe for the purpose of safety there is considered to be enforced obligatory certification of all devices which are connected to IoT. The member countries of the EU consider the possibility of development of a complex of the actions aimed at ensuring of cyber security of the Internet of things. Such approach is advisable, though gives in to criticism as excessive regulation can interfere with development of technologies in the IoT.

Key words: Internet of things, things, devices, personal data, GDPR, information security, self-regulation, certification.