Правова інформатика

УДК 681.3, 314.1, 004.6

БРАЙЧЕВСЬКИЙ С.М., *кандидат фізико-математичних наук.*

ПЕРСОНАЛЬНІ ДАНІ ТА МУЛЬТИМЕДІА

Анотація. *В роботі розглядаються можливі механізми неконтрольованої генерації наборів персональних даних системами Інтернету речей у випадку використання в них мультимедійних технологій.*

Ключові слова: *інформаційні технології, Інтернет речей, персональні дані, мультимедійні технології, мультимедійні дані.*

Summary. *The paper considers possible mechanisms of uncontrolled generation of sets of personal data by Internet of Things systems in case of using multimedia technologies in them.*

Keywords: *information technology, Internet of Things, personal data, multimedia technologies, multimedia data.*

Аннотация. *В работе рассматриваются возможные механизмы неконтролируемой генерации наборов персональных данных системами Интернета вещей в случае использования в них мультимедийных технологий.*

Ключевые слова: *информационные технологии, Интернет вещей, персональные данные, мультимедийные технологии, мультимедийные данные.*

Постановка проблеми. Швидкий розвиток сучасних інформаційних технологій породжує нові виклики і нові ризики, що потребують ретельного вивчення. До їх числа відносяться і проблеми правового регулювання, пов'язані з використанням Інтернету речей (далі – ІР) [1 – 6]. Вони пов'язані з наявністю (принаймні, гіпотетичною) в поведінці систем ІР елементів соціальної поведінки [2]. Питання про природу соціальних відносин між людиною та технологічною системою є, взагалі кажучи, досить нетривіальне. В пропонованій роботі ми не маємо наміру обговорювати цю проблему в повному обсязі.

Однією з проблем, які активно обговорюються у зв'язку з розвитком ІР, є захист персональних даних [7; 8]. Причина полягає перш за все в тому, що системи ІР за своєю природою призначені для збирання різноманітних даних, причому відповідно до певних алгоритмів, які не завжди відповідають загальноприйнятим нормам оперування конфіденційними відомостями. Важливо, що значна частина ризиків, що виникають, взагалі не пов'язані зі штатними режимами експлуатації систем ІР. Дійсно, кібернетична система може оперувати даними, "не усвідомлюючи", що вони означають чи можуть означати в суб'єктивному сприйнятті людиною. Машина використовує дані з певною метою, тоді як хтось може використати ці ж самі дані зовсім з іншою метою.

Основні загрози, що обговорюються в наявній літературі, пов'язані з безпосереднім отриманням даних за допомогою датчиків ІР та їх можливе несанкціоноване розповсюдження шляхом використання мережних технологій. При цьому маються на увазі стандартні персональні ("паспортні") дані.

Але тут виникає проблема, яка, наскільки нам відомо, на цей час не є предметом обговорення. Вона полягає в тому, що сучасні технології швидко розвиваються, створюючи

тим самим умови для виникнення якісно нових ситуацій. В цих ситуаціях виникають принципово нові ризики та загрози, зумовлені особливостями не функціональних, а технічних можливостей. І це може призводити до формування наборів даних, які за своєю природою мають підстави вважатися персональними даними. Іншими словами, технологічний розвиток інструментальних засобів за певних умов може породжувати нові категорії персональних даних, які потребують відповідних заходів для захисту. Головна складність полягає в тому, що такі ситуації, як правило, виникають там, де їх не очікують. Адже вони не пов'язані з цілеспрямованим досягненням певної мети – персональні дані виникають як побічний ефект функціонування комплексу складних компонентів кібернетичної системи. Більше того, від початку певна інформація може взагалі не мати прямого відношення до персональних даних. Персональні дані виникають внаслідок її обробки в поєднанні з іншою інформацією. Такі ефекти можуть взагалі не усвідомлюватися людиною, і це становить додаткову загрозу, оскільки експлуатаційники системи не бачать необхідності в додаткових заходах безпеки.

В пропонованій роботі ми проаналізуємо принципову здатність систем ІР, що використовують мультимедійні технології (далі – ММТ), формувати специфічні набори даних, які під певним кутом зору можуть розглядатись як персональні. Такі набори даних виникають не за рахунок виконання системою тих чи інших функцій, а внаслідок наявних у неї додаткових технічних можливостей. Важливо, що в даному випадку ці технічні можливості застосовуються саме до мультимедійних даних (далі – ММД).

Результати аналізу наукових публікацій. Правове регулювання в галузі використання технологічних (в тому числі інформаційних) систем саме по собі не є чимось новим. Мається на увазі правове регулювання відносин між людьми, які здійснюються за допомогою технологічних систем або у зв'язку з їх використанням.

При цьому виділяють дві основні категорії проблем:

- особливості функціонування технологічних систем як причина виникнення особливостей у додатковому правовому регулюванні;
- забезпечення захисту від наслідків нештатного функціонування технологічних систем.

Тобто суб'єктом права в будь-якому випадку є людина, а технологічна система виступає лише в ролі знаряддя в її руках. Отже, в ситуаціях, коли функціонування системи призводило до негативних наслідків, вважалося, що відповідальність за її дії несуть розробники, виробники та експлуатаційники, тобто люди.

Але сьогодні (принаймні, теоретично) розглядаються ситуації, в яких відповідальність може бути покладена саме на машину, незалежно від участі людини [2; 3]. Такий погляд на технологічні системи є принципово новим, оскільки передбачає можливість того, що їх функціонування може мати соціальні наслідки, а отже, вони самі можуть розглядатися як суб'єкти суспільних відносин. Фактично, сказане означає, що за певних умов технологічна система набуває елементів суб'єктності. На перший погляд, це суперечить загальноприйнятим уявленням про сутність технологічних систем. Адже вважається, що машина лише виконує програму, закладену в неї людиною. І разом з тим, розвиток сучасних інформаційних технологій, зокрема Інтернету речей, свідчить, що такі ситуації можливі. Якщо не вдаватися до наукової фантастики, то мова, очевидно, йде не про повноцінну суб'єктність машини, а про наявність в її функціонуванні окремих рис, характерних для справжнього суб'єкта – людини.

Загрози та ризики, що виникають в сфері використання ІР, широко обговорюються в експертному середовищі. Стислий виклад поточного стану речей міститься, наприклад,

в звітах групи *Alliance for Internet of Things Innovation*, (AIPI), створеної 2015 року у складі Європейської Комісії [9]:

- існуюча нормативно-правова база і регуляторні рамки, в основному, відповідають вимогам сучасного цифрового середовища;
- ключ до розвитку IP полягає у встановленні балансу між гарантуванням безпеки споживачів і стимулюванням інновацій;
- частина ризиків пов'язана з відповідальністю за якість продукції, якій надається особливе значення, хоча вона й застосовує IP, але це не є чимось унікальним для цієї продукції і платформ;
- виникають питання, викликані наявністю відмінності в поняттях "продукт" і "сервіс", тому необхідні чіткі роз'яснення, щоб уникнути невизначеності;
- забезпечити такий розвиток регуляторної політики, щоб вона була досить гнучкою для можливості врахування схильності промисловості до постійного розвитку, що є для неї ключовим.

Окрему категорію становлять ризики, пов'язані з проблемою захисту персональних даних [7; 8; 10; 11]. IP за своєю природою орієнтований на збирання великих обсягів даних. Серед можуть бути і дані, які слід кваліфікувати як персональні.

Важливою є особливість систем IP, яка полягає в тому, що активне використання великої кількості датчиків створює умови для формування комплексів даних, в тому числі і персональних [12].

Основні аспекти сучасної проблеми захисту персональних даних містяться, наприклад, в матеріалах звіту Федеральної торгової палати США [13]:

- переваги впровадження IP зводяться до мінімуму наявністю негативних наслідків, наприклад, загрозами конфіденційності персональних даних;
- зайве регулювання в питаннях захисту персональних даних може призвести до уповільнення інвестицій в будь-який сектор;
- прийняття необхідного регулювання для гарантованого захисту персональних даних підвищить довіру споживачів до нових технологій;
- необхідно дочекатися проявів негативних наслідків і, тільки після цього, вживати заходів з регулювання;
- доцільно використовувати механізми саморегулювання замість регулювання законодавчими нормами.

Зазначимо також, що на наш час саме поняття персональних даних зазнало певного розширення в порівнянні з традиційним розумінням їх як "паспортні дані". Відповідно до Загального регламенту про захист даних (GDPR), діючого в межах законодавства Європейського Союзу щодо захисту персональних даних, це поняття визначається як "…будь-яка інформація, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати" [14]. Аналогічно це поняття визначається і Законом України "Про захист персональних даних".

Для нас в цьому визначенні важливі два моменти:

- персональними даними може бути будь-яка інформація;
- визначальним чинником є ідентифікованість відповідної особи, або принципова можливість такої ідентифікації.

Прийнято вважати, що персональні дані належать до одного з таких видів даних:

- літери;
- числа;
- графічні зображення (малюнки або картини);

- фото;
- аудіо;
- відео.

Також останнім часом до персональних відносять такі специфічні дані:

- файли cookies;
- IP адреси.

Таким чином, персональні дані в сучасному розумінні мають досить широкий спектр.

Аналіз широкого кола джерел свідчить про те, що останнім часом проблема захисту персональних даних у використанні систем ІР активно переходить в сферу прийняття безпосередньо правових рішень [7; 8].

Метою статті є визначення можливих ризиків та загроз в сфері захисту персональних даних, пов'язаних з використанням мультимедійних технологій в системах Інтернету речей.

Виклад основного матеріалу. Вище ми зазначили, що за певних умов технологічна система набуває елементів суб'єктності. Одним з найважливіших таких елементів, безумовно, є здатність самостійно приймати рішення. Підкреслимо, що йдеться не про імітацію прийняття рішення, що, взагалі кажучи, на наш час не є чимось особливим, а про здатність машини виконувати дії, які однозначно не визначаються алгоритмом, обраними значеннями його параметрів та структурою вхідних даних. Саме така поведінка машини дає підстави говорити про її відповідальність за власні дії, що є предметом правового регулювання.

В цьому плані, на наш погляд, слід розрізняти принаймні дві можливості. Перша – власне прийняття рішення, яке безпосередньо впливає на перебіг реальних подій. Друга – створення машиною специфічних наборів даних, непередбачених закладеними в неї алгоритмами та умовами її експлуатації. Ці дані машина сама, можливо, не використовує, але їх може використати людина. Машина формує їх сама, причому це може мати характер побічного ефекту. В цьому випадку рішення стосується не виконання тих чи інших операцій, а формування й зберігання певних наборів даних. І частина цих даних може підпадати під категорію персональних. Дійсно, для цього досить [14] лише виконання двох умов:

- дані повинні стосуватися конкретної особи;
- повинна бути забезпечена можливість ідентифікації цієї особи.

В роботі [15] нами були розглянуті ризики, пов'язані з обробкою персональних даних системами ІР з елементами штучного інтелекту. В ній розглядався один із аспектів проблеми несанкціонованого поширення персональних даних системами ІР. А саме, принципова можливість системи ІР генерувати якісно нові набори персональних даних, заснована на використанні алгоритмів, що в певний спосіб здійснюють агрегування вхідної інформації.

Подібні ризики можуть виникати і в простіших системах ІР (що не містять елементів штучного інтелекту). В них агрегування даних здійснюється за рахунок використання сучасних розвинених технологій, які створюють можливості для виконання складних операцій з великими обсягами даних.

Нижче ми проаналізуємо один із аспектів проблеми несанкціонованого поширення персональних даних системами ІР, пов'язаний з використанням ММТ.

Мультимедійні технології уже протягом багатьох років відіграють в нашому житті значно важливішу роль, ніж прийнято вважати [16]. В тому числі вони починають

активно впроваджуватись спільно з ІР. На наш час найбільш плідним є поєднання ММТ та ІР в галузі медіа індустрії [17; 18]. І, як не важко помітити, суттєву роль тут відіграють саме аспекти роботи систем, пов'язані з персоніфікацією користувачів. Медійні технології в стандартному варіанті дозволяють:

- ідентифікувати споживача, в тому числі суто технологічними засобами (наприклад, за допомогою геолокації);
- забезпечити персоналізоване постачання контенту;
- створення контенту на основі зібраних статистичних даних.

Медійні компанії вже зараз на практиці отримують досить широкий спектр інформації щодо окремих осіб (місцеперебування, переміщення, інтереси та уподобання, коло контактів тощо). Отже, проблема дійсно є актуальною.

Як правило, в контексті обговорення ММТ на перший план виноситься саме технологічний бік справи. Але нас вони цікавитимуть дещо з іншої точки зору. А саме, для нас важливими є в першу чергу властивості ММД, незалежно від того, як і чим вони обробляються. Те, що ми маємо на увазі, до певної міри корелює з так званою проблемою Big Data (укр. – "Великі Дані") [19].

Саме поняття Великих Даних досі не є остаточно визначеним, і ми не будемо обговорювати це питання. Зазначимо лише, що маються на увазі набори структурованих і неструктурованих даних, що визначаються таким комплексом характеристик:

- фізичний обсяг даних;
- швидкість зростання обсягу даних;
- можливість одночасної обробки різних типів даних.

Значення перших двох характеристик мають таку величину, що обробка їх традиційними інструментальними засобами (СУБД тощо) стає неможливою.

Проблема Великих Даних полягає перш за все в тому, що їх обсяг зростає швидше, ніж розширюються фізичні можливості стандартної обробки. Іншими словами, технології генерації даних стають ефективнішими, ніж технології їх обробки. Тому для роботи з Великими Даними використовуються горизонтально масштабовані рішення, які дозволяють підвищувати ефективність апаратно-програмних комплексів за рахунок постійного розширення технічних ресурсів.

Але для нас, як уже було зазначено, проблема обробки даних не є суттєвою. Світова практика неодноразово засвідчувала, що технічні складнощі, які здаються непереборними, з часом легко долаються внаслідок подальшого розвитку нових технологій. Отже, ми виходимо з того, що недосяжні сьогодні можливості обробки даних через рік-два стануть повсякденною рутиною. А отже і загрози, що на даний час виглядають надуманими та нереальними, дуже скоро можуть набути актуальності.

Ключовою в рамках даної роботи є остання характеристика – можливість одночасної обробки різних типів даних. Саме це становить для нас основний інтерес. Адже ММД за своєю природою (і за визначенням) характеризуються поєднанням в єдиному комплексі різних видів інформації, які передбачають її представлення в різних формах. Основними є такі типи даних:

- текст;
- гіпертекст;
- зображення;
- відеоряди;
- звукові ряди;
- анімація (як засіб візуалізації).

ММД в рамках сучасних технологій призначені в кінцевому рахунку для сприйняття їх безпосередньо людиною за допомогою природних органів відчуттів. Виділення (або побудова) семантично наповнених інформаційних блоків здійснюється вищою нервовою діяльністю людини, при чому цей процес, як правило, не піддається вербалізації. Переглядаючи відеоролик, ми впізнаємо Президента України, але не можемо пояснити, за якими конкретно ознаками. Ми не здійснюємо порівняння елементів відеоряду з елементами еталонних наборів, чи ще щось в такому плані. Ми просто впізнаємо знайоме обличчя.

Особливістю такого способу сприйняття інформації є вибірковість. Людина сприймає лише те, що відповідає її конкретним інтересам в даному контексті. Решта інформації лишається поза увагою. Але ця інформація містить величезну кількість різноманітних відомостей, які можуть виявитись важливими в іншому контексті. Звідси випливає специфічна проблема: як таку інформацію вилучити з загального масиву даних, систематизувати і забезпечити споживачу прямий доступ до неї. Очевидно, що єдиний шлях вирішення її лежить через розробку методів автоматичного аналізу всього масиву інформації. Зараз нас не цікавить, як це зробити. Важливо те, що в разі реалізації такої програми ми отримаємо незрівнянно більше відомостей, ніж при традиційному сприйнятті за допомогою нашої перцептивної системи. В тому числі, ми можемо отримати і такі відомості, про існування яких ніхто навіть не підозрював. Такий ефект можливий при обробці будь-якого виду інформації, яку ми звикли сприймати безпосередньо, але у випадку поєднання різних форм представлення даних він значно посилюється. Наприклад, при обробці відеоряду, що містить звукову доріжку. Отже, комплексний аналіз ММД в автоматичному режимі може постачати нам величезну кількість відомостей, значна частина яких є непередбачуваною і тому здатна суттєво розширити коло наших інтересів. З іншого боку вона здатна забезпечити нас більш ефективними засобами вирішення широкого спектру проблем.

Практична реалізація таких програм виглядає нереалістичною з точки зору наявних технічних можливостей. Але протягом останніх десятиліть інформаційні технології досягли значного прогресу в галузі розпізнавання образів, а це дає підстави вважати, що повноцінна автоматична обробка ММД цілком можлива.

Очевидно, що ММД можуть містити різноманітні персональні дані, причому про необмежену кількість осіб (точніше кажучи, кількість осіб обмежена лише фізичними межами доступного носія інформації). Дійсно, те, що відтворено в певному наборі ММД, є інформацією щодо зафіксованих в ньому людей, які або вже ідентифіковані, або принципово можуть бути ідентифікованими на основі:

- розпізнання образу, що входить до відеоряду;
- розпізнання звукової картини, що входить до аудіоряду, синхронізованого з відеорядом;
- використання текстових даних як допоміжної інформації;
- використання гіпертексту як інструментального засобу розширення обсягу доступної інформації.

Аналіз таких даних дозволяє не лише отримати конкретні персональні дані конкретної особи, але й розширити загальний масив персональних даних (в тому числі й конфіденційних). Наведемо два найпростіших приклади, які ілюструють сказане нами вище. Нехай маємо камеру стеження, яка фіксує частину вулиці, де знаходиться відділення банку. Шляхом автоматичного аналізу її записів, зроблених за певний час, ми можемо отримати список постійних клієнтів цього банку, а також визначити, коли вони його відвідують. Якщо ми цікавимося цим банком, такі відомості можуть виявитися

корисними для вирішення тих чи інших проблем, отже ми отримуємо їх свідомо, знаючи, що нам потрібно. Далі, нехай в кадр камери потрапляє частина сусіднього будинку, де міститься вхід до спеціалізованої клініки. І в той самий спосіб ми додатково отримуємо список пацієнтів цієї клініки. Якщо один із них буде ідентифікований (теж в автоматичному режимі), ми дізнаємося дещо про стан його здоров'я. І ці відомості ми отримаємо неочікувано, оскільки від початку не знаємо, що дана камера фіксує також і клініку. І ті, і ті дані, взагалі кажучи, належать до кола конфіденційних.

Суттєво те, що камеру, про яку йде мова, можливо, ставили не ми, а інші люди з зовсім іншими цілями. Наприклад, камера може входити до складу системи IP "розумний дім" в будинку навпроти і мати своїм призначенням відстежувати наближення його власника, щоб вчасно ввімкнути світло в вестибюлі. Для цього система фіксує всіх перехожих, що потрапляють в заданий кут спостереження, ідентифікує їх особи та, в разі необхідності, визначає характеристики траєкторій їх руху. Тобто для виконання заданої програми необхідна лише незначна частина даних. Але внаслідок застосованих технологій записи містять всю інформацію, яку система спроможна отримати. І в цьому полягає вкрай важливий момент: інформація накопичується не тому, що це комусь потрібно, а лише тому, що це дозволяють доступні технології. А оскільки інформація отримана, використовувати її може в принципі хто завгодно з якою завгодно метою, і далеко не завжди легально і санкціоновано. Ми лише користуємося тим, що нам пропонують доступні технології.

Виникає запитання: а для чого використовувати ММТ в системах IP? Відповідь може виявитись простою: тому, що використовувати вже розроблені надійні технології (нехай навіть з надлишковими функціональними можливостями) простіше і дешевше, ніж створювати щось якісно нове під конкретну мету. Це рівною мірою стосується як апаратної частини, так і програмного забезпечення. Якщо стандартна камера стеження дозволяє здійснювати повний моніторинг всього, що відбувається в заданій локації, то краще використати її, а не розробляти програмно-апаратний комплекс, який опрацьовує лише певну частину вхідної інформації.

Аналізуючи функціональні можливості (прямі та непрямі) систем IP, ми повинні врахувати, що їх розвиток відбувається загалом в темпі розвитку інформаційних технологій в цілому. Центральна ідея IP передбачає створення складної організації набору технологічних елементів, яка зумовлюється обміном даними між ними через мережу Інтернет. Саме нетривіальний обмін певними даними між певними елементами забезпечує можливість принципово більш складної поведінки систем IP, ніж "звичайних" кібернетичних пристроїв. Самі ж елементи (датчики, аналізатори тощо) принципово не відрізняються від тих, що використовуються в інших технологічних комплексах, а також індивідуально самі по собі. А це, в свою чергу, означає, що центр ваги переміщається в бік процесу проектування системи IP як такої. Тому і її функціональні можливості (в тому числі виконання несанкціонованих операцій) визначаються властивостями структури зв'язків між елементами системи, а не технічними характеристиками самих елементів. І це набуває особливого значення у випадку застосування технологій, пов'язаних з використанням Великих Даних, оскільки вони створюють умови для реалізації надзвичайно складних інформаційних процесів.

Отже, застосування ММТ в системах IP відкриває широкий спектр можливостей, здатних породжувати якісно нові загрози та ризики.

Головна особливість маніпулювання персональними даними в системах IP полягає в тому, що його здійснює машина, яка "не знає", який сенс мають ті або інші дані з точки зору людини. Відповідно, вона, взагалі кажучи, не може відрізнити персональні

дані від даних інших категорій. У випадку використання ММТ ситуація ускладнюється тим, що персональні дані можуть взагалі формально не виокремлюватися в окремі семантично окреслені блоки. Причина полягає в тому, що агрегація даних виникає не в результаті компонування окремих блоків, серед яких присутні й персональні дані, а внаслідок формування цілісних наборів шляхом використання технологій, які обробляють неперервні вхідні потоки. В свою чергу, вхідні потоки генеруються комплексами датчиків і тому принципово не передбачають контроль за отримуваним контентом. Вони лише фіксують те, що потрапляє в їх поле зору. Загальні набори даних містять, сказати б, "сирий" матеріал, із якого можуть бути отримані зокрема й персональні дані. Але це, можливо, потребуватиме застосування або спеціальних алгоритмів, або безпосередньої участі людини.

А тому поширення персональних даних не обов'язково має носити цілеспрямований характер. Поширюватись можуть великі масиви інформації, які окрім іншого містять в собі й персональні дані. А це надзвичайно ускладнює контроль над роботою системи.

В результаті маємо суттєве ускладнення питання про відповідальність за таке несанкціоноване поширення персональних даних. Адже заздалегідь невідомо, поширюються персональні дані чи ні. Поширюються великі обсяги ММД, а в них гіпотетично можуть бути присутні й персональні дані, агреговані в загальний масив суто технологічним способом, причому за певних обставин.

В рамках зазначеної проблеми головний акцент зміщується на роботу датчиків, які постачають системі ІР вхідні дані. Мається на увазі не тільки технічний бік справи (технічні характеристики самих датчиків), але й експлуатаційні чинники, такі як розташування датчиків та режим їх роботи.

Наявність певних даних в конкретній системі ІР сама по собі не означає їх поширення. Така система може накопичити значний обсяг персональних даних, непередбачених штатними функціональними можливостями, але вони лишаються невикористаними, оскільки алгоритми системи з ними не працюють. На перший погляд, ця обставина свідчить про те, що фактично ніяких загроз не існує. Але проблема полягає в тому, що обмін даними між елементами системи ІР здійснюється через мережу Інтернет, а отже, вона принципово є відкритою до зовнішніх зв'язків. І вони практично є неконтрольованими. Принаймні контроль над ними вимагає застосування достатньо складних (і тому дорогих) рішень, що робить його в більшості випадків нерентабельним. Ми повинні визнати, що використання Великих Даних, в тому числі ММД, на практиці несе специфічні загрози, які вимагають значного переосмислення правового аспекту технологічного прогресу.

Висновки.

Отже, ми бачимо, що за певних умов характер взаємодії систем ІР з оточуючим середовищем може призводити до формування наборів даних, які можуть бути віднесені до категорії персональних. Такі набори даних містяться в більш широких інформаційних масивах і не призначаються для явної обробки системою. Вони потрапляють в загальні обсяги вхідної інформації виключно за рахунок наявних технологічних можливостей. Тим не менш, ці дані можуть бути використані саме як персональні в рамках нецільового використання систем.

Типовим прикладом подібних ситуацій може служити використання в системах ІР ММТ. Головна особливість полягає в тому, що ці технології за своєю природою здатні накопичувати і обробляти великі обсяги даних, до складу яких може входити різноманітна інформація щодо людей, які потрапляють (в тому числі випадково) в поле

зору датчиків, наприклад, камер стеження. Така інформація автоматично зберігається в стандартних форматах незалежно від призначення системи лише внаслідок того, що так влаштовані відповідні технології Зрозуміло, що вона є доступною для обробки.

Як правило, ця інформація містить графічні та відео дані, що принципово дозволяє ідентифікувати зображених там осіб. Отже, незалежно від призначення системи та характеру її функціонування, вона може працювати на поширення персональних даних.

Такі ситуації породжують додаткові загрози в плані захисту персональних даних, важливість яких в першу чергу обумовлена принциповою неконтрольованістю наборів даних, якими фактично маніпулює машина. Отже, виникає необхідність врахування таких загроз при розробці правових норм щодо захисту персональних даних, а також адекватних механізмів реалізації цих норм на практиці.

Використана література

1. Баранов А.А. Интернет вещей и искусственный интеллект: истоки проблемы правового регулирования: збірник матеріалів ІІ-ї Міжнародної науково-практичної конференції *Проблеми та перспективи розвитку в Україні*, м. Львів, 17 лист. 2017 р. Львів: НУ "Львівська політехніка", 2017. С. 18-42.

2. Рекомендации МСЭ-Т Y.2060 (06/2012). Серия Y: Глобальная информационная инфраструктура, аспекты протокола Интернет и сети последующих поколений. Сети последующих поколений. *Структура и функциональные модели архитектуры. Обзор Интернета вещей*. URL: http://handle.itu.int/11.1002/1000/11559 (дата звернення: 23.10.2020).

3. Баранов О.А. "Інтернет речей" як правовий термін. *Юридична Україна*. 2016. № 5 – 6. С. 96-103. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/urykr_2016_5-6_16.pdf (дата звернення: 23.10.2020).

4. Черняк Леонид. Платформа Интернета вещей. *Открытые системы. СУБД*. 2012. № 7. URL: https://www.osp.ru/os/2012/07/13017643 (дата звернення: 23.10.2020).

5. Kevin Ashton. That 'Internet of Things' Thing. In the real world, things matter more than ideas. (англ.). *RFID Journal.* Jun 22. 2009. URL: http://www.rfidjournal.com/articles/view?4986 (дата звернення: 23.10.2020).

6. The Internet of Things is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment . *Gartner IT glossary.* Gartner. 5 May. 2012. URL: https://www.gartner.com/it-glossary/internet-of-things/ (дата звернення: 03.11.2020).

7. Баранов О.А., Брижко В.М. Захист персональних даних в сфері Інтернет речей. *Інформація і право.* № 2(17)/2016. С. 85-91. URL: http://ippi.org.ua/sites/default/files/11_0.pdf (дата звернення: 03.11.2020).

Брижко В.М., Фурашев В.М. Конвергенція новітніх технологій: стан і перспективи змін у інформаційних відносинах. *Інформація і право.* № 1(20)/2017. С. 51-67.

8. Брижко В.М., Пилипчук В.Г. та ін. Становлення і розвиток правових основ та системи захисту персональних даних в Україні: монографія / за ред. В.М. Брижка, В.Г. Пилипчука. Київ: ТОВ "Видавничий дім "АртЕк". 2017. 226 с.

9. Charlie Hawes. *Hogan Lovells assists Internet of Things policy group in Brussels*, 28 October 2015. URL: http://www.hlmediacomms.com/2015/10/28/hogan-lovells-assists-internet-of-things-policy-group-in-brussels (дата звернення: 09.11.2020).

10. Интернет вещей: чем угрожает будущее. URL: http://igate.com.ua/news/3169-internet-veshhej-chem-ugrozhaet-budushhee (дата звернення: 09.11.2020).

11. Как в 2015 году был взломан Интернет вещей. URL: http://igate.com.ua/ news/12342-kak-v-2015-godu-byl-vzloman-internet-veshhej (дата звернення: 09.11.2020).

12. Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protectionof individuals with regard to automatic processing of personal data in the context of profiling (Adopted by theCommittee of Ministers on 23 November 2010 at the 1099th meeting of the Ministers' Deputies). URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cdd00 (дата звернення: 09.11.2020).

13. Internet of Things: Privacy & Security in a Connected. *World Federal Trade Commission (FTC) Staff Report*. January 2015. URL: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127IP rpt.pdf (дата звернення: 09.11.2020).

14. Про захист фізичних осіб у зв'язку з обробкою персональних даних та про вільне переміщення таких даних, а також про скасування Директиви 95/46/ЄС (Загальний Регламент про захист даних): Регламент (ЄС) 2016/679 від 27.04.16 р. URL: https://gdpr-text.com/ ?col=2& lang1=ukr&lang2=en&lang3=rumain (дата звернення: 09.11.2020).

Сучасні правові стандарти Євросоюзу у сфері захисту персональних даних: / І. Майстренко – перекл. з англ.; В. Брижко – перекл. та редагування тексту. – (Науково-дослідний інститут інформатики і права Національної академії правових наук України). Київ: ТОВ "Видавничий дім "АртЕк", 2018. 177 с. С. 2-103.

15. Брайчевський С.М. Проблема персональних даних в системах Інтернету речей з елементами штучного інтелекту. *Інформація і право.* № 4(31)/2019. С. 61-67. URL: http://ippi.org.ua/braichevskii-sm-problema-personalnikh-danikh-v-sistemakh-internetu-rechei-z-elementami-shtuchnogo-in (дата звернення: 09.11.2020).

16. Каптерев А.И. Мультимедиа как социокультурный феномен. Москва: Профиздат, 2002. 224 с.

17. Наден Клер. Развитие Интернета вещей в медиаиндустрии с новой серией международных стандартов ISO. 2019. URL: https://www.iso.org/ru/news/ref2449.html (дата звернення: 09.11.2020).

18. ISO/IEC 23093-1:2020 *Information technology. Internet of media things. Part 1: Architecture*. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:23093:-1:ed-1:v1:en (дата звернення: 09.11.2020).

19. Черняк Леонид. Большие Данные – новая теория и практика. *Открытые системы. СУБД*. 2011. № 10. URL: https://www.osp.ru/os/2011/10/13010990 (дата звернення: 16.11.2020).

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~