УДК 681.3, 314.1, 004.6

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

ПРОБЛЕМА ПЕРСОНАЛЬНИХ ДАНИХ ПРИ ВИКОРИСТАННІ СИСТЕМ ІНТЕРНЕТУ РЕЧЕЙ В ГАЛУЗІ ОХОРОНИ ЗДОРОВ'Я

Анотація. *В роботі розглядаються можливі механізми неконтрольованої генерації наборів персональних даних системами Інтернету речей при використанні в галузі охорони здоров'я.*

Ключові слова: *інформаційні технології, Інтернет речей, персональні дані, охорона здоров'я.*

Summary. *The paper considers possible mechanisms of uncontrolled generation of personal data sets by the Internet of Things when used in the field of health care.*

Keywords: *information technology, the Internet of Things, personal health data.*

Аннотация. *В работе рассматриваются возможные механизмы неконтролируемой генерации наборов персональных данных системами Интернета вещей при использовании в области охраны здоровья.*

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

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 з 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.

Основною темою при аналізі даної проблеми в наявній літературі є ситуації, пов'язані з безпосереднім отриманням даних за допомогою датчиків ІР та їх можливе несанкціоноване розповсюдження шляхом використання мережних технологій. Зазначимо, що ця тема як така є надзвичайно широкою і містить в собі цілу низку окремих проблем, кожна з яких заслуговує на окреме обговорення.

Однією з них слід вважати доступ до персональних даних громадян системами ІР, які використовуються в галузі охорони здоров'я. В її основі лежить те, що машина може оперувати даними, які вона самостійно збирає та опрацьовує в процесі вирішення задач, що за певних умов можуть виходити за межі стандартного їх набору, передбаченого розробниками та експлуатаційниками. Особливість ситуації полягає в тому, що в медицині (на відміну від більшості інших сфер застосування) системи ІР мають

безпосередній доступ до персональних даних пацієнтів. Маємо на увазі дані, що характеризують стан здоров'я пацієнта і підлягають захисту [9].

В пропонованій роботі ми проаналізуємо принципову здатність систем ІР формувати непередбачені набори даних, які за своєю природою мають бути віднесені до категорії персональних даних. Результатом може бути створення якісно нових комплексів персональних даних, які відсутні в інших наявних джерелах. Такі комплекси утворюються за рахунок поєднання стандартних персональних даних пацієнта, що використовуються працівниками медичного закладу в рамках, передбачених законом, з даними, отриманими шляхом використання різноманітних датчиків. Причому це поєднання здійснює машина без участі (а отже і контролю) людини.

Ми покажемо, що сама природа подібних комплексів даних передбачає необхідність їх зберігання в структурованому вигляді в різноманітних базах даних, що створює значні ризики отримання до них несанкціонованого доступу за допомогою різноманітних мережних технологій. Ситуація ускладнюється тим, що можливість доступу в даному випадку реалізується без відома не лише пацієнта, але й медичного персоналу. Отже питання про відповідальність за наслідки такої можливості є нетривіальним.

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 ІР, 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.

Вважаємо, що в рамках обраної нами теми ключовим чинником є здатність машини самостійно приймати рішення. Підкреслимо, що йдеться не про імітацію прийняття рішення, що, взагалі кажучи, на наш час не є чимось особливим (прикладом може служити комп'ютер, що грає в шахи). Ми маємо на увазі здатність машини приймати рішення, яке однозначно не визначається 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.

Загрози та ризики, що виникають в сфері використання IP, 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 Європейській Комісії [11]:

- 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; 12; 13]. IP за своєю природою орієнтований на збирання великих обсягів даних. Серед них 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 [14].

Основні аспекти сучасної проблеми захисту персональних даних містяться, наприклад, в матеріалах звіту Федеральної торгової палати США [15]:

- 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.

Галузь охорони здоров'я вважається однією з найперспективніших щодо запровадження технологій IP [10]. Головна причина полягає в тому, що кількість осіб, що потребують медичних послуг значно перевищує кількість осіб, здатних ці послуги надати. Більше того, пацієнти та потенційні пацієнти розподілені по значних територіях і часто змінюють свою локацію, тоді як медичні заклади централізовані.

Також важливим є те, що сучасна медицина має справу з великим обсягом різноманітних даних, які характеризують стан пацієнта та отримуються з різних джерел, як технологічних, так і "традиційних".

Основними є такі напрямки використання IP:

- діагностика;
- моніторинг стану пацієнта;
- лікування пацієнта.

Програмні комплекси здатні не лише отримувати і зберігати дані, але й обробляти їх (підраховувати прогрес від активності, будувати графіки тощо).

Тому можливість використання мережевих технологій для збирання, агрегування, зберігання та опрацювання відповідних даних є вкрай актуальною. Слід також прийняти до відома, що в сучасному світі медицина належить до числа найбільш фінансованих сфер людської діяльності, внаслідок чого виникають сприятливі можливості для різноманітних розробок, зокрема і в галузі ІР.

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 – 9].

Метою статті є визначення можливих механізмів генерації системами ІР, що працюють в медичній галузі, наборів персональних даних, заснованих на інтеграції стандартних персональних даних пацієнтів з даними, отриманими використовуваними датчиками.

Виклад основного матеріалу. Нижче ми проаналізуємо один із аспектів проблеми несанкціонованого поширення персональних даних системами ІР. А саме, принципову здатність систем ІР формувати непередбачені набори даних, які за своєю природою мають бути віднесені до категорії персональних даних. Результатом може бути створення якісно нових комплексів персональних даних, які відсутні в інших наявних джерелах. Такі комплекси утворюються за рахунок поєднання стандартних персональних даних пацієнта з даними, отриманими шляхом використання різноманітних датчиків, які входять до складу систем ІР.

Перш за все зазначимо, що важливою особливістю проблеми персональних даних в медицині є те, що результати роботи датчиків завжди жорстко прив 'язуються до конкретної особи, щодо якої передбачене використання її персональних даних. Отже, використання систем ІР неодмінно призведе до формування комплексів даних стосовно конкретної особи. При чому значна частина даних є непередбачуваною, оскільки визначається станом пацієнта, який заздалегідь невідомий. Але саме можливість несанкціонованого використання таких даних і зумовлює головні ризики.

Підкреслимо 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” [16]. 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.

В медицині ситуація з персональними даними є досить складною і має специфічні характерні риси. Причина полягає в тому, що в цьому випадку до "стандартних" персональних даних додаються дані іншої природи, що, взагалі кажучи, не є очевидним.

З точки зору чинного законодавства розглядається три категорії даних, що підлягають захисту [9]:

- медична таємниця;
- лікарняна таємниця;
- власне персональні дані.

До медичної таємниці відноситься інформація про

- факт звернення особи за медичною допомогою;
- стан здоров'я особи;
- функціональні особливості організму;
- фізичні недоліки;
- особливості психіки;
- діагноз захворювання особи;
- методи лікування особи;
- інші відомості, включаючи й інформацію про сімейне та інтимне життя.

До лікарняної таємниці відноситься інформація медичного характеру, яка стала відома в зв'язку з виконанням службових обов'язків чи з інших джерел

На перший погляд, перші дві категорії не належать до персональних даних, принаймні в звичайному розумінні. Але вони завжди стосуються особи, яка безперечно є ідентифікованою, а отже (як ми зазначили вище) повинні вважатися персональними даними.

Значна частина подібних відомостей зараз отримується в автоматичному чи автоматизованому режимах шляхом використання відповідних технічних засобів. Більш того, часто в такий самий спосіб здійснюється і первинна обробка отриманих даних. В результаті роботи системи утворюються набори даних, які постійно оновлюються, і заздалегідь неможливо передбачити, яка саме інформація стосовно тієї чи іншої особи буде в них накопичена.

Надання повноцінних медичних послуг передбачає здійснення постійного моніторингу за станом пацієнта. А тому всі дані, що систематично отримуються протягом значних проміжків часу, мають зберігатись у структурованому вигляді в спеціальних базах даних, асоційованих з профілями пацієнтів. Тому йдеться не просто про епізодичне отримання разових даних, а про доступ до конфіденційних баз даних.

Головна особливість маніпуляції персональними даними в системах IP полягає в тому, що її здійснює машина, яка, взагалі кажучи, "не знає", який сенс мають ті або інші дані з точки зору людини. Саме ця особливість породжує специфічні ризики, зумовлені тим, що людині надзвичайно важко контролювати такі аспекти функціонування кібернетичних пристроїв.

На рівні технологічної реалізації IP є набором датчиків, що отримують певні дані та пристроїв, що їх обробляють. Для нас суттєво, що обмін даними здійснюється за допомогою мережі Інтернет. Метою створення такої системи є виключення безпосередньої

участі людини принаймні в частині функціональних можливостей системи. Це, в свою чергу означає, що система ІР повинна на основі обробки отриманих вхідних даних приймати рішення, результатом яких буде отримання додаткових даних. Ці додаткові дані можуть мати різні джерела, які більш чи менш строго розподіляються на дві групи:

- дані датчиків, які входять до складу даної системи ІР;
- дані, що знаходяться в мережі Інтернет, до якого дана система ІР має доступ.

Саме доступність даних другої групи може створювати складні неконтрольовані ситуації. Адже проектувальник системи не може передбачити, запит на які дані сформує машина в певній ситуації, навіть, якщо сама ситуація прогнозована. Прикладом може бути зовнішня система діагностики, яка на підставі певного набору симптомів ставить діагноз хворому. І ця процедура може і не бути передбачена заздалегідь.

Отримання машиною додаткових даних гіпотетично є актуальним для систем з елементами штучного інтелекту [1]. Але у нашому випадку такі ситуації можуть виникати і в значно простіших системах внаслідок, з одного боку, більш вагомої ролі природного інтелекту проектувальників і експлуатаційників, а з другого боку, специфічними особливостями функціонування датчиків, які отримують інформацію, характер якої залежить від багатьох зовнішніх чинників. Прикладом якісно нового елементу даних може бути діагноз, який машина автоматично фіксує на основі "стандартних" показників (температура, тиск, пульс, біохімія крові тощо), які самі по собі змістовного значення не мають і не можуть використовуватися зловмисником у протиправних цілях.

Безпосередньо нас цікавить ситуація, в якій машина використовує персональні дані, не передбачені при її створенні. В "звичайних" кібернетичних системах такі ситуації не виникають. Кожний конкретний програмно-апаратний комплекс від початку призначений для обробки певного набору даних, серед яких можуть бути і персональні. Процеси несанкціонованого збирання та поширення персональних даних є доволі простими і зрозумілими. Ми розуміємо їх причини і механізми. Проблема полягає лише в тому, щоб віднайти адекватні засоби відповідних дій.

Зовсім інший стан справ виникає тоді, коли машина здатна сама генерувати персональні дані, використовуючи інші дані, на перший погляд такі, що не мають відношення до персональних. При цьому, очевидно, так чи інакше машина повинна використовувати додаткові дані, які вона збирає самостійно, використовуючи алгоритми власного виробництва (наприклад, в рамках можливості самонавчання). Джерелами таких даних, звичайно, можуть бути і власні датчики системи ІР, і доступні для неї ресурси мережі Інтернет.

З точки зору проектувальників, дана система ІР може оперувати персональними даними в обмежених рамках у повній відповідності з існуючими правовими нормами.. Але ми вже казали, що до персональних даних можуть бути віднесені будь-які відомості, так чи інакше пов'язані з тією чи іншою особою. І вони можуть складатися з кількох компонентів. Частина з них передбачена штатним режимом експлуатації системи, а частина – ні.

В медичній сфері також необхідно мати на увазі можливість специфічної форми зловживань, пов'язаних з несанкціонованою модифікацією даних, які використовуються для лікування пацієнтів. Така модифікація може здійснюватись свідомо (наприклад, шляхом зламу системи) з метою завдання шкоди конкретному пацієнту. Зрозуміло, що такі ситуації можливі лише за умови відсутності належного захисту персональних даних пацієнтів.

Такі ситуації породжують додаткові загрози в плані захисту персональних даних, важливість яких в першу чергу обумовлена принциповою неконтрольованістю наборів даних, якими фактично маніпулює машина. І ці загрози можуть становити реальну небезпеку для здоров'я і життя людини.

Висновки.

Отже, ми бачимо, що за певних умов характер функціонування систем ІР в медичній сфері може призводити до використання машиною непередбачених наборів даних, серед яких можуть бути присутні і персональні дані.

Системи ІР в процесі експлуатації в принципі здатні розширювати штатний режим отримання та обробки даних, внаслідок чого машина стає здатна самостійно генерувати персональні дані, використовуючи інші дані, отримані в передбачений спосіб. При цьому машина так чи інакше повинна використовувати додаткові дані, які вона збирає самостійно, використовуючи специфічні алгоритми (в тому числі, створені нею в рамках можливості самонавчання). Джерелами таких даних, звичайно, можуть бути і власні датчики системи ІР, і доступні для неї ресурси мережі Інтернет.

В результаті виникають додаткові загрози в плані захисту персональних даних, важливість яких в першу чергу обумовлена принциповою неконтрольованістю наборів даних, якими фактично маніпулює машина. Ці загрози ускладнюються тією обставиною, що в сфері медицини вони можуть становити реальну загрозу здоров'ю та життю людини. 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. Інтернет вещей и искусственный интеллект: истоки проблемы правового регулирования: зб. матеріалів ІІ-ї Міжнародної науково-практичної конференції *ІТ-право: проблеми та перспективи розвитку в Україні*, м. Львів, 17 лист. 2017 р. Львів: НУ "Львівська політехніка", 2017. 318 с. 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

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&I21 DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/urykr_2016 _5-6_16.pdf

4. Черняк Л.. Платформа Интернета вещей. *Открытые системы. СУБД*. № 7. 2012. URL: https://www.osp.ru/os/2012/07/13017643

5. Kevin Ashton. That 'Internet of Things' Thing. In the real world, things matter more than ideas. RFID Journal. 22 June 2009. URL: http://www.rfidjournal.com/articles/view?4986

6. Internet of Things. Gartner IT glossary. Gartner. 5 May 2012. "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". URL: https://www.gartner.com/it-glos sary/ internet-of-things

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

8. Пилипчук В.Г., Брижко В.М. 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. Булеца С.Б. Персональні дані пацієнта. *Науковий вісник Ужгородського національного університету. Сер. Право.* 2013. Вип. 22. Ч. II. Т. 1. С 186-191. URL: https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/3366/1/%D0%91%D1%83%D0%BB%D0%B5%D1%86%D0%B0%20%D0%A1.%D0%91.%20%D0%9F%D0%B5%D1%80%D1%81%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%96%20%D0%B4%D0%B0%D0%BD%D1%96%20%D0%BF%D0%B0%D1%86%D1%96%D1%94%D0%BD%D1%82%D0%B0%20.pdf

10. Семанов А.О., Блинников М.А., Пирмагомедов Р.Я. Обзор технологий связи медицинских приложений Интернета вещей. *Информационные технологии и телекоммуникации.* 2018. Т. 6. № 1. С. 63-71. URL: http://www.sut.ru/doci/nauka/review/20185/63-71.pdf

11. 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

12. Интернет вещей: чем угрожает будущее. URL: http://igate.com.ua/news/3169-internet-veshhej-chem-ugrozhaet-budushhee

13. Как в 2015 году был взломан Интернет вещей. URL: http://igate.com.ua/ news/12342-kak-v-2015-godu-byl-vzloman-internet-veshhej

14. 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

15. 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/150127IPrpt.pdf

16. 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 (ЄС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 р. – (В кн. Сучасні правові стандарти Європейського Союзу у сфері захисту персональних даних: зб. документів; пер. з англ. І. Майстренко / за ред. В. Брижко; передмова В. Пилипчука. – (НДІ інформатики і права НАПрН України). Київ: ТОВ "Видавничий дім "АртЕк", 2018. 180 с.; URL: https://gdpr-text.com/?col=2&lang1=ukr&lang2=en&lang3=rumain

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