

УДК 002.6:004:340.1+316.329.8

БАРАНОВ О.А., доктор юридичних наук,
старший науковий співробітник
БРИЖКО В.М., доктор філософії (Ph.D) з юридичних наук,
старший науковий співробітник

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В СФЕРІ ІНТЕРНЕТ РЕЧЕЙ

***Анотація.** Про правові проблеми захисту персональних даних в сфері Інтернет речей в умовах становлення інформаційної індустрії електронно-цифрових технологій та інформаційних ресурсів.*

***Ключові слова:** Інтернет речей, захист персональних даних, інформаційні технології, постіндустріальне суспільство.*

***Аннотация.** О правовых проблемах защиты персональных данных в сфере Интернет вещей в условиях становления информационной индустрии электронно-цифровых технологий и информационных ресурсов.*

***Ключевые слова:** Интернет вещей, защита персональных данных, информационные технологии, постиндустриальное общество.*

***Summary.** About the legal problems of personal data protection in a sphere of the Internet of Things in the conditions of forming the information industry of electronic and digital technologies and information resources.*

***Keywords:** Internet of Things, personal data protection, information technologies, postindustrial society.*

Постановка проблеми. В останні роки у перспективах розвитку Інтернет-сфери набуває активного поширення словосполучення “Інтернет речей”. Як зазначається у [1] поняття “Інтернет речей” (скорочено ІР, англ. – Internet of Things (IoT)) розглядається як “мережа різних об’єктів, що росте, – від промислових пристроїв до споживацьких товарів, які можуть обмінюватися інформацією і виконувати свої задачі, поки людина працює, спить або займається спортом. Інтернет речей складається з мільйонів датчиків і різних пристроїв, що генерують безперервні потоки даних, які можна використовувати для поліпшення як життя взагалі, так і для підвищення ефективності бізнесу зокрема”.

Вперше термін “Інтернет речей” запропонував Кевін Ештон в 1999 році. Тоді був створений Центр автоматичної ідентифікації (Auto-ID Center), який займався сенсорними технологіями і радіочастотною ідентифікацією (RFID) [2].

Оцінка перспектив та проблем, пов’язаних з застосуванням мережі Інтернет та Інтернет-технологій, за допомогою яких забезпечується реалізація волевиявлення суб’єктів суспільства та у рамках техніко-технологічних можливостей задовольняються інформаційні, економічні та ін. потреби, здійснюється багатьма фахівцями з кінця 1980 рр. Провідні позиції у світі щодо правового забезпечення використання технологій ІР займають країни Європейського Союзу, США, Японія, КНР, Італія. До вчених, які здійснюють зазначені дослідження, можна віднести таких, як: Е. Барбі, С. Халлер, Ф. Блум, Б. Гофф, К. Росе, С. Чен, Е. Гудмэн, О. Джанджакомо, Р. Камілі, Дж. Кассано, Дж. Девей, М. Довден, З. Луксзо, Р. Вебер, Д. Бохн тощо. Про результати поглядів деяких зарубіжних авторів йдеться, зокрема у [3 – 6, 8, 12, 13, 16].

Разом з цим, як постановка юридичних проблем, так і шляхи їх вирішення все ще знаходяться на початковому етапі.

Варто звернути увагу на те, що мова все частіше йде не тільки про технологічний, але й про соціальний аспект застосування ІР. При цьому, у звіті одного з семінарів Інтернет-інституту Оксфорда [6] було прямо висловлено побоювання про те, що в дослідженнях щодо Інтернету речей приділяється першочергова увага технологічним консультаціям і зневажливо мало вивчаються соціальні наслідки впровадження і використання технологій ІР. Це в повній мірі відноситься і до правової тематики, серед якої однією з актуальних проблем є проблема захисту персональних даних.

Метою статті є визначення сучасного стану та правових проблем Інтернету речей в сфері захисту персональних даних.

Виклад основних положень. Чим обумовлено активний розвиток Інтернет-проектів і технологій ІР? Причин на це дві: можливості економії різних ресурсів та перспективи в бізнесі [7].

Перша з них виходить з прагнення економити фізичні і економічні ресурси: здоров'я, сили та час людей, електроенергію, воду. Друга причина визначається прагненням різних фірм підключитися до багатомільярдного і перспективного бізнесу, який надає можливості диверсифікаційних змін і оптимізації бізнес-процесів, про що йдеться, зокрема у [8, с. 110-129].

Сьогодні різних інформаційних технологій ІР досить багато. Ось деякі їх моделі.

ІР для будинку (технології “розумний будинок”). Передбачає можливість віддаленого керування за допомогою Інтернет-технологій побутовими приладами, віддалений моніторинг і управління, зокрема програмованого, системами освітлення, опалювання, кондиціонування, медіапристроями, протипожежними системами, кухонними пристроями і ін. Для цього використовують різні пристрої та датчики – спеціалізовані контролери, датчики вогкості повітря, температури, руху, які допомагають збирати інформацію, обробляти її і передавати дані, за допомогою Інтернет та радіо-технологій.

ІР для медицини. Для діагностики вже застосовуються методи телемедицини, коли є зв'язок з лікарем, поліклінікою або лабораторією, що знаходяться в іншому районі [8, с. 140]. Розроблені протези кінцівок, керовані за допомогою сигналів мозку. Існують бездротові пристрої, які дозволяють паралізованим пацієнтам керувати телевізорами, комп'ютерами та інвалідними кріслами [9].

ІР у фінансовому секторі і страхуванні, охоронній сфері і дослідницькому бізнесі також активно розвивається. Як наголошується в [10], близько 10 % компаній у всьому світі застосовують будь-яку ІР-технологію в своєму бізнесі. Найшвидше використання ІР простежується у виробничому секторі – з 2013 року використання технологій Інтернету речей в ньому виросло на 204 %. Підприємства починають з підключення камер і датчиків для моніторингу безпеки на виробництвах і спостереження за його ходом та процесом поставки. Тепер компанії, які виробляють сервісне обладнання та здійснюють поставки великогабаритного устаткування, використовують ІР, щоб стежити за ним і запобігати дорогим поломкам. Це допомагає економити на регулярних техоглядах, які дорого коштують.

ІР для транспорту. Безліч рішень для безпечнішої експлуатації створено для ж/д та авіатранспорту. Для автомобіля вже використовуються системи відстеження його маршруту, моніторинг вантажоперевезень, контроль відвантаження, складування та ін. Компанія Microsoft розробила проект операційної системи Windows для “розумного” автомобіля. Головним інструментом спілкування водія з бортовим комп'ютером є голосовий асистент Cortana. Він позбавляє людину від необхідності відволікатися від дороги. Графічна інформація проектується прямо на лобове скло машини [9].

За прогнозами впровадження технологій IP матиме наслідком появу до 100 мільярдів технічних пристроїв до 2025 року, які, напевно, будуть оснащені бездротовими технологіями передачі даних, обмін якими буде здійснюватися за допомогою мережі Інтернет [12].

Наведені та багато інших прикладів свідчить, що IP розглядається пріоритетним напрямом розвитку в багатьох країнах.

В березні 2015 року у Європейській Комісії була створена група високого рівня зацікавлених представників галузі ІКТ – Альянс для інновацій в Інтернет речей (Alliance for Internet of Things Innovation, API) для консультування Генерального директорату комунікаційних мереж, контенту і технологій (Directorate General for Communications Networks, Content and Technology, DG Connect). Метою Альянсу є виведення Європейського Союзу в лідери в області IP шляхом створення динамічної європейської IP екосистеми. Альянс складається з одинадцяти робочих груп, які 26 жовтня 2015 р. опублікували доповіді, що містять широке коло питань, пов'язаних з IP, включаючи підготовку майбутніх досліджень в області IP. Основні рекомендації цих звітів зводяться до наступного [13]:

- 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.

До основних проблем Інтернету речей можна віднести безпеку і захист персональних даних. Технології IP значно посилюють ризики порушення конфіденційності персональних даних внаслідок того, що вони передбачають накопичення, циркулювання і використання великого, просто величезного територіально і технологічно розподіленого обсягу інформації (даних) про конкретну людину. Це викликає цілком закономірні питання про надійність зберігання таких даних та забезпечення їх захисту від несанкціонованого використання.

У наш час багато пристроїв вже мають датчики, що дозволяють збирати інформацію про фізичний світ і людину – камери, гіроскопи, акселерометри, термометри, пристрої розпізнавання мови та ін. Активне використання різних гаджетів, що забезпечують інформаційну взаємодію, призводить до того, що за допомогою Інтернет-технологій можна стежити практично за кожним куточком і за кожною подією в світі, збирати різні персональні дані [14]. Описано випадок, коли в Нідерландах було відхилено проект зі створення інтелектуальних електромереж на основі “розумних” лічильників спожитої електроенергії в квартирах і будинках. Відхилений на підставі підозри про те, що збір кожні 7 секунд інформації про рівень споживання електроенергії, зберігання такої інформації і її подальший аналіз може привести до розкриття в деталях способу життя споживачів електроенергії та до можливого її незаконного використання зловмисниками.

В умовах домашнього використання технологій IP кожен датчик, підключений до мережі – це не тільки величезні можливості. Коли нові інформаційні технології розміщуються на тому або іншому предметі, який раніше не був “розумним”, виникають

проблеми, яких раніше не було. Несанкціонований доступ до системи подачі повітря або до регулювання температури в приміщенні, “розумні” дверні замки, сигналізації, автомобілі, телевізори – всі ці та інші пристрої можуть бути використані не так, як їх було запрограмовано. І якщо з “розумними” лампочками ситуація не дуже критична, то, коли мова заходить про захист персональних даних, медичне устаткування, смарт-автомобілі тощо, картина стає іншою [15]. При цьому, що більше пристроїв з ІР будуть з’єднані між собою, то більше можливостей буде у хакерів для злому будинків і збору інформації, що цікавить їх.

Сьогодні практикується імплантація датчиків всередину тіла людини, які можуть автоматично передавати медичну інформацію на видалені сервери. Ці дані надалі аналізуються за допомогою технології постачальника, і, нерідко, спільно з третіми сторонами. Хоча така діяльність несе певну користь всім зацікавленим, проте, для суб’єкта персональних даних стає дедалі відстежувати і контролювати те, де і як вони зберігаються, ким і коли використовуються, і з якою метою.

Дослідники відзначають такі факти, про які ми не замислюємося в звичайному житті без технологій ІР. Наприклад, коли виникає випадок автоаварії і вирішується питання про страхові виплати, то страхові компанії можуть мати доступ до даних “розумного” автомобіля, зокрема, отримати дані про місцезнаходження, час, відстані, швидкості та інші параметри, які можуть впливати на страхову премію. Без сумніву, ці дані розкривають і інформацію про приватне життя (персональні дані) водія [16].

Багато даних, які надають відомості, що характеризують приватне життя, використовується і буде використовуватися в найрізноманітніших системах ІР. Й тому, вирішення проблеми забезпечення інформаційної безпеки в частині захисту персональних даних в разі застосування ІР не можна очікувати як просте завдання. Поєднання пристроїв, послуг і мереж технологій ІР призводить до необхідності багаторівневої і багатооб’єктної системи забезпечення інформаційної безпеки, що значно складніше, ніж відома донині мережева безпека, а це в свою чергу потребує створення алгоритмів шифрування з низькою вартістю, низькою латентністю і високою енергоефективністю [17].

Іншим ризиком є те, що в умовах взаємозв’язку великої кількості систем і комплексів ІР, які будуть надавати послуги або здійснювати роботи в інтересах великої кількості людей, з’являється досить легко здійсненна можливість комплексування персональних даних про людину з найрізноманітніших джерел [18]. Цілком очевидно, що широкомасштабне використання технологій ІР призведе до появи, та в подальшому, і до ідентифікації ще багатьох проблем, пов’язаних із захистом персональних даних.

У матеріалах звіту Федеральної торгової палати (США) відбивається практично весь спектр думок щодо проблеми захисту персональних даних [19]:

- переваги впровадження ІР 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.

Далі автори звіту дійшли висновку про потребу у спеціальному законодавстві в сфері ІР. Наявність деяких ризиків, пов’язаних з безпекою персональних даних, вимагає більш

уважного ставлення на федеральному рівні до цієї проблеми. Дотримуючись при цьому принципу технологічної нейтральності та не залишаючи осторонь питання захисту функціональності пристроїв, які використовуються в IP. У звіті, як і в ряді інших робіт, наводиться приклад кардіостимуляторів, несанкціоноване порушення роботи яких може призвести до загибелі людини.

Згідно основоположних принципів міжнародного права про захист персональних даних, затвердженими першою у світі Конвенцією Ради Європи № 108 від 28.01.81 р. та рядом директив Європейського Союзу, зокрема Директивою Європейського Парламенту і Ради 95/46/ЄС від 24.10.95 р., стосовно захисту персональних даних (див. [20]), захист прав людини у сфері персональних даних передбачає, зокрема, наступне: “Персональні дані, що піддаються автоматизованій обробці: а) отримуються та обробляються сумлінно та законно; б) зберігаються для визначених і законних цілей та не використовуються у спосіб, несумісний з цими цілями; с) мають бути адекватними, відповідними і не надмірними з точки зору цілей, для яких вони зберігаються” [21, с. 66]. Щодо створення відповідних умов в Україні про це та інше йшлося у [22], починаючи ще з 1998 року.

На початку 2016 року Європейський Парламент і Рада прийняли рішення про відміну Директиви 95/46/ЄС Європейського Парламенту і Ради від 24.10.95 р. “Про захист осіб у зв’язку з обробкою персональних даних і вільним обігом цих даних” та прийняли Регламент ЄС 2016/679 від 27.04.16 року “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 (Загальні Положення про захист даних)”. В офіційному прес-релізі ЄС зазначається, що “Європейська комісія висунула свою реформу ЄС про захист даних для того, щоб зробити Європу придатною для життя в цифрову епоху. Більше 90 % європейців говорять, що вони хочуть ті ж права захисту даних як в країнах ЄС – і незалежно від того, де обробляються їх дані” [23].

Цілі і принципи Директиви 95/46/ЄС залишаються співзвучними з положеннями нового міжнародного акту – Регламенту ЄС 2016/679. Разом з тим, економічна інтеграція і розвиток ринку ЄС в умовах активного застосування інформаційних технологій привели до значного збільшення трансграничних потоків персональних даних, зокрема завдяки можливостям Інтернету. Нові технології і глобалізація принесли з собою нові проблеми для захисту персональних даних. Масштаби їх збору і використання значно зросли. Технології змінюють як економіку, так і соціальне життя. Тому виникла необхідність в подальшій фрагментації і уніфікації законодавства про захист персональних даних у всіх державах Союзу. При цьому, у п. 1. преамбули Регламенту ЄС 2016/679 вказується, що захист фізичних осіб у зв’язку з обробкою персональних даних є їх фундаментальним правом.

Регламент ЄС 2016/679 розглядається стратегією цифрового Єдиного ринку, яка вважається важливим кроком для зміцнення фундаментальних прав громадян в століття цифрових технологій і у сприянні розвитку бізнесу за рахунок спрощення правил для компаній в цифровому єдиному ринку. Фізичні особи повинні мати можливість контролювати використання своїх персональних даних. Юридична і практична визначеність для фізичних осіб, суб’єктів економічної діяльності і державних органів має бути розширеною. Також він передбачає позбавлення від дорогого адміністративного навантаження, що сприяє економії коштів бізнесу в розмірі біля € 2,3 млрд. в рік. Положення, зокрема, для сектора поліції і кримінального правосуддя, мають здійснювати захист основних прав громадян у сфері персональних даних всякий раз, коли вони порушуються правоохоронними органами. Передбачається створення таких умов, коли особисті дані потерпілих, свідків і підозрюваних в здійсненні злочину будуть

належним чином захищені. При цьому також передбачено сприяння прикордонній співпраці в боротьбі із злочинністю і тероризмом.

Таким чином, з одного боку, міжнародне і національне законодавство (див. [24]) передбачають обмежений збір персональних даних і на користь первинних цілей їх використання, а з іншої, в умовах стрімкого розвитку технологій ІР робить уразливим саме забезпечення захисту персональних даних.

Висновки.

До основних проблем Інтернету речей можна віднести інформаційну безпеку і захист персональних даних. Технології ІР значно посилюють ризики порушення конфіденційності персональних даних внаслідок того, що вони передбачають накопичення, циркулювання і використання великого, територіально і технологічно розподіленого обсягу інформації (даних) про конкретну людину. Це викликає цілком закономірні питання про надійність зберігання таких даних та забезпечення їх захисту від несанкціонованого використання.

Можна зазначити, що широке використання технологій Інтернету речей призводить до необхідності вирішення таких основних правових проблем:

- визначення механізмів реалізації принципу попередньої згоди на використання та “на стирання” персональних даних (ст. 17 Регламенту ЄС 2016/679 від 27.04.16 р.);
- правовий вплив на регулювання транскордонних потоків персональних даних, що передбачає не тільки цілеспрямовану діяльність по впорядковуванню інформаційних відносин, але і непряму дію правових засобів і методів на різних суб’єктів, що не підпадають безпосередньо під правове регулювання;
- використання персональних даних інтелектуальними комплексами, що функціонують без участі суб’єктів (юридичних або фізичних осіб).

Крім того, необхідність створення багаторівневої і багатооб’єктної системи захисту персональних даних потребує формування нової системи правового регулювання.

Використана література

1. Интернет вещей – аналитика вещей? – Режим доступа : <http://channel4it.com/blogs/Internet-veshchey-analitika-veshchey-7403.html>
2. Интернет вещей. – Режим доступа : <http://igate.com.ua/tag/internet-veshhej/4/>; <http://revo1verlab.com/chto-takoe-internet-veschey>
3. Адам Тернер. Интернет вещей и носимые технологии : решение тайны частной жизни и безопасности, не сорвать инноваций. – 21 Rich. – JL & Технология. – № 6 (2015), – Режим доступа : <http://jolt.richmond.edu/v21i2/article6.pdf>;
4. Интернет вещей. – Режим доступа : <http://www.Users/Home85/AppData/Local/Temp/EPIC%20-%20D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%20%D0%B2%D0%B5%D1%89%D0%B5%D0%B9%20%28IoT%29.html>
5. Будущее Интернета вещей, или Как будут управляться огромные объемы данных. – Режим доступа : <http://broadcast.net.ua/show/Infrastruktura/6155-buduweeinternetavewejilikakbudutupravliatsiaogromnyeobemydannyh13.04.2016>
6. The Societal Impact of the Internet of Things. A report of a workshop on the Internet of Things organized by BCS – The Chartered Institute for IT, on Thursday 14 February 2013. The Chairs were Jeremy Crump (BCS) and Ian Brown (Oxford Internet Institute, University of Oxford). Режим доступа : <https://www.bcs.org/upload/pdf/societal-impact-report-feb13.pdf>
7. Интернет вещей уже в Украине. Кто зарабатывает на работах? – Режим доступа : <http://www.epra.vda.com.ua/rus/publications/2015/08/13/554178>
8. e-будущее и информационное право / В. Брыжко, А. Орехов, О. Гальченко ; ред. д.ю.н., проф. Р. Калюжного и д.э.н, проф. Н. Швеца. – К. : Интеграл, 2002. – 264 с.

9. Как технологии будут выглядеть через пять лет. – Режим доступа : <http://igate.com.ua/news/11402-kak-tehnologii-budut-vyglyadet-cherez-pyat-let>
10. Интернет вещей : всё подключается к сети. – Режим доступа : <http://igate.com.ua/news/6309-internet-veshhej-vse-podklyuchaetsya-k-seti>
11. 6 новостей из мира IT, которые нужно знать сегодня. – Режим доступа : <http://igate.com.ua/news/10123-6-novostej-iz-mira-it-kotorye-nuzhno-znat-segodnya>
12. K. Rose, S. Eldridge, L. Chapin The Internet of Things : An Overview. Understanding the Issues and Challenges of a More Connected World / The Internet Society (ISOC), October 2015. – 50 P. – Режим доступа : <http://www.internetsociety.org/sites/default/files/ISOC-IP-Overview-20151022.pdf>
13. Charlie Hawes. Hogan Lovells assists Internet of Things policy group in Brussels, 28 October 2015. – Режим доступа : <http://www.hlmediacomms.com/2015/10/28/hogan-lovells-assists-internet-of-things-policy-group-in-brussels>
14. Интернет вещей : чем угрожает будущее. – Режим доступа : <http://igate.com.ua/news/3169-internet-veshhej-chem-ugrozhaet-budushhee>
15. Как в 2015 году был взломан Интернет вещей. – Режим доступа : <http://igate.com.ua/news/12342-kak-v-2015-godu-byt-vzloman-internet-veshhej>
16. Eric Barbry. The Internet of Things, Legal Aspects: What Will Change (Everything) / Communications & Strategies, No. 87. – Pp. 83-100. – Quarter 2012. – Режим доступа : http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2304137
17. S. Chen et al. A Vision of IP : Applications, Challenges and Opportunities With China Perspective IEEE / Internet of Things Journal, vol. 1, No. 4. – Pp. 349-359. – August 2014. – Режим доступа : <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6851114>
18. Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (Adopted by the Committee of Ministers on 23 November 2010 at the 1099th meeting of the Ministers' Deputies). – Режим доступа : https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cdd00
19. Internet of Things: Privacy & Security in a Connected. – World Federal Trade Commission (FTC) Staff Report. – January 2015. – Режим доступа : <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127IPrpt.pdf>
20. Системна інформатизація правоохоронної діяльності : європейські нормативно-правові акти та підходи до упорядкування інформаційних відносин у зв'язку з автоматизованою обробкою даних : посіб. / В. Брижко, М. Швець [та ін.]. – Кн. 2. – К. : ТОВ “ПанТот”, 2006. – 509 с.
21. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Amendment to Convention ETS No. 108 allowing the European Communities to accede. – Strasbourg, 28.1.1981. – (Article 5 – Quality of data). – Режим доступа : <http://www.convention.coe.int/treaty/en/Treaties/Html/108.htm>
22. Права человека и защита персональных данных / А. Баранов. В. Брижко, Ю. Базанов. – (Финансовая помощь и содействие в издании Харьковской правозащитной группы и Национального фонда поддержки демократии (США). – Харьков : Фолио, 2000. – 280 с.
23. On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) : Regulation (EU) 2016/679 of the European Parliament and of the council of 27 April 2016. – Режим доступа : <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN>
24. Про захист персональних даних : Закон України від 01.06.10 р. № 2297-VI ; із змін та доп. // Відомості Верховної Ради України (ВВР). – 2010. – № 34. – Ст. 481