Bogdanna Krupińska

Członek SIODO

PANDEMICZNY INTERNET RZECZY – ZA CZY PRZECIW?

1. Wstęp

XXI wiek jest wiekiem społeczeństwa informacyjnego, którego siłą napędową jest Internet. Społeczeństwo informacyjne jest stosunkowo nową formą społeczną, która rozwija się wraz ze stale rosnącym dostępem do informacji i stale rosnącym jej znaczeniem w społeczeństwie[1]. Gwałtowne nasilenie tendencji globalizacyjnych w gospodarce świata, przemiany polityczne oraz dynamiczny rozwój Internetu – zjawiska dające się szczególnie zauważyć od początku lat 90. XX w. sprawiły, że nikogo nie trzeba przekonywać o roli jaka odgrywa informacja w życiu współczesnych społeczeństw[2]. Internet przeniósł relacje międzyludzkie na wirtualny poziom w kilku różnych płaszczyznach, począwszy od życia zawodowego, aż po życie prywatne, szczególnie kontakty towarzyskie. Internet Rzeczy (Internet Przedmiotów - IoT) dodaje nowego znaczenia temu procesowi, umożliwiając komunikację nie tylko ludzi z inteligentnymi przedmiotami (*smart objects*), lecz także komunikację pomiędzy tymi urządzeniami.

Celem opracowania jest omówienie zagadnienia IoT, a także jego zastosowań w różnych obszarach działalności człowieka, jak również jego zalet oraz zagrożeń z nim związanych.

2. Czym tak naprawdę jest Internet Rzeczy?

Termin „Internet rzeczy" może się wydawać dla wielu osób terminem nowym, a tym czasem pojawił się w Stanach Zjednoczonych w 1999 r. Kevin Ashton (twórca m.in. systemu

[1] Sylwia Buregwa-Czuma, Katarzyna Garwol, *Definicje, właściwości i funkcje społeczeństwa informacyjnego, The Central European Journal of Social Sciences and Humanities, 2011,* str. 30. Pobrano z: http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-6910f2e3-7aea-47b2-aa01-45ac38ad4a65 (11.05.2020)

[2] Mariusz Grabowski, Agnieszka Zając, *Dane, informacja, wiedza - próba definicji, Zeszyty Naukowe / Uniwersytet Ekonomiczny w Krakowie nr 798, 2009,* str. 99

radiowej identyfikacji - RFID[3]) użył go jako tytułu prezentacji[4]. W prezentacji tej autor zaproponował wykorzystanie transmisji danych przez Internet z wykorzystaniem RFID do sterowania łańcuchem dostaw w Procter&Gamble. Podkreślił, że obecnie komputery - a zatem i Internet - są niemal całkowicie zależne od ludzi, od informacji przez nich dodawanych do sieci. Praktycznie wszystkie dane dostępne w Internecie zostały zebrane i utworzone – poprzez wpisanie, nagranie, zrobienie zdjęcia cyfrowego lub zeskanowanie kodu kreskowego, a następnie umieszczone w sieci. Dostępność komputerów, które dysponowałyby wiedzą o rzeczach, zebraną bez ludzkiej aktywności, umożliwiłaby śledzenie i zliczenie wszystkiego, a także znacznie zmniejszyłaby straty, koszty i ilość odpadów produkcyjnych.

Dlatego też konieczne jest wyposażenie komputerów w umiejętność samodzielnego gromadzenia informacji o świecie, a w szczególności o poszczególnych produktach. Powinno się to sprowadzać do umożliwienia komputerom patrzenia na świat, słuchania go i rozpoznawania jego zapachów. Radiowy system identyfikacji (RFID) i technologia czujników[5] pozwalają komputerom obserwować, identyfikować i rozumieć świat oraz poszczególne rzeczy bez ograniczeń wynikających z niepełnych, często szczątkowych informacji wprowadzanych do sieci przez człowieka. Dlatego Internet Rzeczy posiada potencjał zrewolucjonizowania świata, najprawdopodobniej w znacznie większym stopniu, niż zrobił to Internet[6].

Jakie urządzenia wpisują się w definicję Internetu Rzeczy? Jest to sprzęt, który oferuje łączność internetową i pozwala za wysyłanie i odbieranie informacji, korzystając z których

[3] **RFID** (ang. *Radio-frequency identification*, **Systemy (zdalnej) identyfikacji radiowej**, **Technologie radiowych identyfikatorów**) – technologia, która wykorzystuje fale radiowe do przesyłania danych oraz zasilania elektronicznego układu (etykieta RFID) stanowiącego etykietę obiektu przez czytnik, w celu identyfikacji obiektu. Technika umożliwia odczyt, a czasami także zapis układu RFID. W zależności od konstrukcji umożliwia odczyt etykiet z odległości do kilkudziesięciu centymetrów lub kilku metrów od anteny czytnika. System odczytu umożliwia identyfikację wielu etykiet znajdujących się jednocześnie w polu odczytu. RFID przytwierdzony do przedmiotu może być jedną z form zabezpieczenia przedmiotów przed ich fałszowaniem. Pobrano z: https://pl.wikipedia.org/wiki/RFID (04.05.2020)

[4] Kevin Ashton, *That 'Internet of Things' Thing. In the real world, things matter more than ideas, „RFID Journal"*, 22.06.2009. Pobrano z: http://www.rfid journal.com/articles/pdf?4986 (04.05.2020)

[5] Czujnik (sensor) fizyczne bądź biologiczne narzędzie będące najczęściej elementem składowym większego układu, którego zadaniem jest wychwytywanie sygnałów z otaczającego środowiska, rozpoznawanie i rejestrowanie ich. W naukach technicznych czujnik to urządzenie dostarczające informacji o pojawieniu się określonego bodźca, przekroczeniu pewnej wartości progowej lub o wartości rejestrowanej wielkości fizycznej. Pobrano z: https://pl.wikipedia.org/wiki/Czujnik (04.05.2020)

[6] Kevin Ashton, *That 'Internet of Things' Thing. In the real world, things matter more than ideas, „RFID Journal"*, 22.06.2009. Pobrano z: http://www.rfid journal.com/articles/pdf?4986 (04.05.2020)

urządzenie jest w stanie zaoferować dodatkowe korzyści. Mimo tego, że znaczna część społeczeństwa nie zna pojęcia Internet Rzeczy, to większość korzysta z niego na co dzień.

3. Internet Rzeczy – zastosowanie praktyczne

Gdzie więc dokładnie możemy wykorzystać Internet Rzeczy? Wykorzystujemy go m.in. do użytku prywatnego. Do tej kategorii można zaliczyć mnóstwo urządzeń, z których korzystamy na co dzień. Są to smartfony, smartwatche, smartbandy, lodówki z dostępem do sieci, Smart TV, inteligentne głośniki, inteligentne kamery, elementy tworzące zestawy inteligentnego domu – m.in. czujniki inteligentne, inteligentne gniazdka, inteligentne oświetlenie, inteligentne ogrzewanie, inteligentne sterowniki, wideodomofony, inteligentne piloty, włączniki inteligentne, systemy alarmowe, których zadaniem jest ułatwienie życia oraz obniżanie wydatków na rachunki za prąd lub wodę.

W coraz większej liczbie nieruchomości stosowany jest zdalny odczyt liczników mediów (energii elektrycznej, wody). Umożliwia on sprawdzenie zużycia mediów bez potrzeby wchodzenia na teren danej nieruchomości. Korzyścią takiego systemu jest możliwość sprawdzenia stanów wszystkich liczników w jednym momencie, bez względu na nieobecność użytkowników. Oszczędza to czas, a tym samym koszt odczytu.

Ważną kwestią dla społeczeństwa informacyjnego jest możliwość przewidywania różnych zdarzeń możliwie wcześnie i przeprowadzenie akcji ratunkowej o jak największej skuteczności. Służą do tego inteligentne systemy, do zadań których należą m.in.:

- zapewnienie bezpieczeństwa publicznego (np. w związku z katastrofami, takimi jak pożary, powodzie, tsunami lub trzęsienia ziemi, monitoring miejski),
- ochrona środowiska (np. monitorowanie zanieczyszczeń środowiska, w szczególności wody i powietrza, monitorowanie, raportowanie i weryfikacja emisji dwutlenku węgla, gospodarka odpadami oraz efektywne wykorzystanie różnych rodzajów energii i zasobów naturalnych),
- ochrona zdrowia i życia (np. monitorowanie pacjenta, ochrona zdrowia sportowców, chłodziarki i zamrażarki medyczne, w stanie zagrożenia epidemicznego aplikacje do walki z pandemią, które w tym celu wykorzystują lokalizację obywateli i takie, które mają pomóc

w kontrolowaniu rozprzestrzeniania się choroby, wykorzystujące technologię Bluetooth oraz kamery termowizyjne do pomiaru temperatury ciała).

IoT ma również szerokie zastosowanie mi.in. w przemyśle. Są to różnego rodzaju roboty na liniach produkcyjnych, które mogą udostępniać dane między sobą. Jest wykorzystywany również w handlu (np. aplikacje zakupowe i sprzedażowe, płatności NFC), w transporcie i logistyce (np. śledzenie floty, lokalizacja przedmiotu, automatyzacja zamówień).

Podsumowując – Internet Rzeczy znalazł zastosowanie w takich obszarach działalności człowieka jak sprzęt AGD i multimedialny, inteligentny dom, systemy bezpieczeństwa, systemy ochrony zdrowia i życia, marketing w handlu detalicznym, systemy produkcyjne, logistyka, inne zastosowania np. w hodowli i uprawach roślin.

4. Zalety Internetu Rzeczy i jakie niesie zagrożenia

Zastosowanie IoT otwiera przemysł, usługi oraz wiele innych branż na nowe możliwości. Przed wieloma organizacjami otwiera nowe możliwości biznesowe. Zastosowanie IoT umożliwia zbieranie informacji zwrotnej od klienta w celu wprowadzenia nowych rozwiązań i innowacji, jak również umożliwia wprowadzenie nowych produktów.

Na rynku, który jest nastawiony na potrzeby klienta, IoT pozwala śledzić zachowania konsumentów. Poznanie preferencji klientów umożliwia prowadzenie marketingu ukierunkowanego na konkretne ich potrzeby oraz rozwój nowych biznesowych strategii. W produkcji Internet Rzeczy pozwala zoptymalizować procesy, dostawy i zasoby oraz dostarcza nowe rozwiązanie w celu poprawy efektywności operacyjnej oraz pomaga zwiększyć dochody poprzez m.in. monitorowanie i poprawę jakości, zwiększenie wydajności maszyn oraz ograniczenie ilości odpadów.

Dla konsumentów zaletą zastosowania IoT jest możliwość zaoszczędzenia czasu poprzez ułatwienie wielu czynności i oszczędności na rachunkach np. poprzez gaszenia świateł. Automatyzacja domu, czyli Smart Home to nowa perspektywa oszczędności i bezpieczeństwa.

Mówiąc o zaletach Internetu Rzeczy i o jego bezpieczeństwie nie można zapomnieć o zagrożeniach jakie ze sobą niesie. W ramach IoT udostępniana i wykorzystywana jest przez sprzęty duża ilość danych, z jednej strony może być to traktowane jako korzyść dla rozwoju technologii, z drugiej strony może stanowić zagrożenie. IoT gromadząc dużą ilość informacji staje się

zagrożeniem dla naszej wolności i prywatności, poszanowanie której i ochrona danych osobowych mają charakter praw podstawowych[7]. Etymologicznie słowo prywatność wywodzi się od łacińskiego słowa privus tłumaczonego jako własny, wolny od, pojedynczy. To z niego wykształcił się przymiotnik privatus, służący do oznaczenia prywatnej własności czy też osób nie pełniących funkcji publicznych[8].

IoT gromadzi o nas informacje dot. naszych finansów, zdrowia, przyzwyczajeń, preferencji zakupowych, informacji z portali społecznościowych, oglądanych stron www, oglądanych programów telewizyjnych, mieszkania, lokalizacji i tras podróży. Innym zagrożeniem dla naszej wolności i prywatności jest wykorzystywanie systemów do rozpoznawania twarzy. Tysiące kamer w miastach, sklepach, dworcach, lotniskach, na drogach dają możliwość rozpoznania nas, śledzenia nas on line i prześledzenia historii naszych podróży, wykorzystując do tego system rozpoznawania twarzy.

Coraz większą popularnością cieszą się chipy RFID, które są wykorzystywane w celu identyfikacji osób, kontroli pracowników, w coraz większej ilości towarów i urządzeń. Taka ilość informacji może powodować zagrożenie, że informacje te mogą być wykorzystywane nie tylko przez osoby do tego uprawnione. Problemem współczesnego świata jest fakt, że ogromna zcentralizowana wiedza o obywatelach znajduje się w rękach kilku firm komercyjnych, dla których celem działalności nie są korzyści społeczne, lecz wypracowanie zysku[9]. I tu nasuwa się pytanie, czy jako społeczeństwo XXI wieku jesteśmy gotowi na *chipowanie* ludzi, na pełną inwigilację naszego życia prywatnego i jaką zapłacimy cenę za wygodę i oszczędność czasu?

5. Wnioski

Po przyjrzeniu się zagrożeniom jakie niesie IoT nasuwa się wniosek, że żeby zapewnić bezpieczeństwo IoT konsumenci muszą zwrócić szczególną uwagę na bezpieczne korzystanie z Internetu. Muszą zrozumieć, że dbając o bezpieczeństwo komputerów i sprzętów mobilnych,

[7] Art. 7 i 8 Karty Praw podstawowych Unii Europejskiej, Dz. Urz. UE C 202/389 z 07.06.2016 oraz art. 47 i 51 Konstytucji Rzeczpospolitej Polski z dnia 2 kwietnia 1997 r. (Dz. U. z 1997 r. Nr 78, poz. 483 z późn. zm.)

[8] Marek Puwalski, *Prawo do prywatności osób publicznych*, wyd. Toruń, 2003, str. 14

[9] Jędrzej Wieczorkowski, *Akceptacja naruszenia prywatności w erze Big Data, Nierówności Społeczne a Wzrost Gospodarczy, nr 52 (4/2017)*, str. 323

rozważając zasadność korzystania z portali społecznościowych i poprzez kontrolę nad umieszczanymi na nich treściami w znacznym stopniu eliminują wiele zagrożeń ze strony cyberprzestępców.

Natomiast nie każde cyberzagrożenie jakie wiąże się z Internetem Rzeczy może wyeliminować użytkownik. Wiele zależy od zachowania standardów bezpieczeństwa sprzętu i oprogramowania, które wdroży firma, która proponuje dane rozwiązanie. Niezależnie od tego, jakie zagrożenia przyniesie ze sobą korzystanie z IoT można stwierdzić, że ma również wiele zalet. Dzięki niektórym rozwiązaniom życie staje się łatwiejsze, oszczędzamy na rachunkach. Jest to rozwiązanie dla osób, które wiedzą po co im jest potrzebne to rozwiązanie technologiczne, wiedzą jak z niego korzystać i w jaki sposób zapewnić bezpieczne z niego korzystanie.

Dobro, jakim jest nabywanie i posiadanie informacji stanowi nowe zjawisko w historii cywilizacji. Technologie informatyczne poza wieloma korzyściami, takimi np. jak poprawa jakości życia, niosą za sobą zagrożenia, takie jak: ryzyko naruszenia prywatności i bezpieczeństwa jednostki, rozwarstwienie społeczne, wytyczające podziały i prowadzące do izolacji jednostek o ograniczonym dostępie do technologii informacyjnych, zwrot kultury ku technicznym narzędziom i automatyzacji, zagrożenia intelektualne i bezkrytyczne zaufanie do źródeł informacji[10]. Pojęcie prywatności ewoluuje wraz z rozwojem technologii informacyjnych. Zmienia się także świadomość dotycząca zagrożenia prywatności wynikającego z masowego przetwarzania danych prywatnych, w tym osobowych[11].

Pandemiczny Internet Rzeczy – za czy przeciw? Za – pod warunkiem rozsądnego z niego korzystania. W XXI wieku nie unikniemy Internetu Rzeczy. Należy natomiast poświęcić uwagę na edukację społeczeństwa w celu uczynienia IoT bezpiecznym.

Bibliografia

1. Sylwia Buregwa-Czuma, Katarzyna Garwol, *Definicje, właściwości i funkcje społeczeństwa informacyjnego, The Central European Journal of Social Sciences and Humanities, 2011.*

[10] Sylwia Buregwa-Czuma, Katarzyna Garwol, *Definicje, właściwości i funkcje społeczeństwa informacyjnego, The Central European Journal of Social Sciences and Humanities, 2011*, str. 36. Pobrano z: http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-6910f2e3-7aea-47b2-aa01-45ac38ad4a65 (11.05.2020)

[11] Jędrzej Wieczorkowski, *Akceptacja naruszenia prywatności w erze Big Data, Nierówności Społeczne a Wzrost Gospodarczy, nr 52 (4/2017)*, str. 323

Pobrano z: http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-6910f2e3-7aea-47b2-aa01-45ac38ad4a65 (11.05.2020)
2. Mariusz Grabowski, Agnieszka Zając, *Dane, informacja, wiedza - próba definicji, Zeszyty Naukowe / Uniwersytet Ekonomiczny w Krakowie nr 798, 2009,* str. 99-116
3. Kevin Ashton, *That 'Internet of Things' Thing. In the real world, things matter more than ideas, „RFID Journal",* 22.06.2009. Pobrano z: http://www.rfid journal.com/articles/pdf?4986 (04.05.2020)
4. Marek Puwalski, *Prawo do prywatności osób publicznych*, wyd. Toruń, 2003
5. Jędrzej Wieczorkowski, *Akceptacja naruszenia prywatności w erze Big Data, Nierówności Społeczne a Wzrost Gospodarczy, nr 52 (4/2017),* str. 315-325