

Internet Rzeczy – zjawisko rewolucjonizujące życie. Znajomość tej technologii i jej zagrożeń wśród osób 30+

Internet of Things – a revolution of life. Awareness and level of saturation with the Internet of Things technology among people 30+

Key words: Internet of things, IoT, Big data.

Summary: The Internet of Things (IoT) is a technology that surrounds us from every angle. It is used in many areas of life. It seems to make our life easier, but also raises concerns, especially in the area of privacy. The article presents the results of research on the awareness of respondents regarding the existence of the Internet of Things and the willingness and the need to use devices and solutions based on this technology.

Słowa kluczowe: Internet Rzeczy, Internet of things, IoT, Big data.

Streszczenie: Internet Rzeczy to technologia, która otacza nas z każdej strony. Wykorzystywana jest w wielu obszarach życia. Wydaje się być ułatwieniem, ale także budzi obawy, szczególnie w obszarze prywatności. W artykule przedstawiono wyniki badań dotyczące świadomości badanych w zakresie istnienia Internetu Rzeczy (IoT) oraz chęci i potrzeby wykorzystywania urządzeń i rozwiązań bazujących na tej technologii.

Wstęp

Technologiczna rewolucja dzieje się na naszych oczach. Nazwy procesów, które w niej zachodzą, jak sądzę, dla przeciętnego Kowalskiego nie są znane mimo codziennego korzystania z nich. Standardowy obywatel korzysta z automatycznego dostosowywania temperatury w domu do tej, która ma miejsce na dworze, ale czy zdaje sobie sprawę, w jaki sposób to działa? Czekając na tramwaj, patrzymy na tablicę z informacją, kiedy przyjedzie. I nie zastanawiamy się, jak to się dzieje. Korzystając z technologii mobilnych, rzadko kiedy zdajemy sobie sprawę z rozbudowanych mechanizmów za nimi stojących, a termin 5G często traktujemy jedynie jako chwyt marketingowy operatorów sieci komórkowych. Bo tak już jest, to jest nasza „normalność”.

Internet Rzeczy

Termin „Internet of Things” przypisuje się osobie Kevina Ashtona, brytyjskiego badacza MIT⁴, który w 1999 roku stwierdził: „gdyby wszystkie przedmioty w codziennym życiu były wyposażone w identyfikatory i łączność bezprzewodową, mogłyby porozumiewać się ze sobą i być zarządzane za pomocą komputera”¹.

Podstawowym celem Internetu Rzeczy jest stworzenie inteligentnych przestrzeni, tj. inteligentnych miast, transportu, produktów, budynków, systemów energetycznych, systemów zdrowia czy rozwiązań związanych z życiem codziennym. Podstawą rozwoju inteligentnych przestrzeni jest dostarczenie technologii, która zapewni ich realizację².

Rozwiązania IoE bazują na podłączaniu do Internetu różnych urządzeń, które budują coraz bardziej wyrafinowane systemy dysponujące siecią rozproszonych czujników, kamer, baz danych, systemów zdalnego sterowania oraz przetwarzania informacji. Fakt ten jest olbrzymią zaletą tego rozwiązania, ale jednocześnie stanowi jego olbrzymią słabość. Większość z „rzeczy” nie posiada solidnych zabezpieczeń w postaci firewalli, systemów wielostopniowej autoryzacji czy zaawansowanych systemów antywirusowych³.

Największy potencjał wykorzystania Internetu Rzeczy do tworzenia wartości w funkcjonowaniu społeczno-gospodarczym obserwowany jest w rozwiązaniach przeznaczonych dla⁴:

- ludzi (*human*),
- mieszkań (*home*),
- handlu detalicznego (*retail environments*),
- biur (*office*),
- fabryk (*factories*),
- miejsc pracy/placów budowy (*worksites*) np. miejsca wydobycia ropy naftowej,
- pojazdów (*vehicles*),
- miast (*cities*),
- obszarów zewnętrznych (*outside*), tj. obszarów znajdujących się pomiędzy środowiskami zurbanizowanymi⁵.

¹ M. Goodman, *Zbrodnie przyszłości: jak cyberprzestępcy, korporacje i państwa mogą użyć technologii przeciwko Tobie*, Gliwice 2016, s. 250.

² A. Brachman, *Raport Obserwatorium ICT Internet przedmiotów*.

³ M. Piwiński, *Internet Rzeczy – rozwiązania przyszłości*, Informatyka w Edukacji, XIV, UMK Toruń, 2019, 30, s. 50, <https://iwe.mat.umk.pl/tom-iwe2019/06.pdf> [14.04.2020].

⁴ Bauer H., Patel M., Veira J. (2014), *The Internet of Things: Sizing up the Opportunity*, McKinsey&Company, <http://www.mckinsey.com/industries/high-tech/our-insights/the-internet-of-things-sizing-up-the-opportunity> [dostęp: 12.05.2017].

⁵ A. Rot, B. Blaicke, *Bezpieczeństwo Internetu rzeczy. Wybrane zagrożenia i sposoby zabezpieczeń na przykładzie systemów produkcyjnych*, Zeszyty Naukowe Politechniki Częstochowskiej, Zarządzanie, Nr 26 (2017), s. 191.

Jedna z firm⁶ wypuściła serię reklam obrazujących, jak technologia Internetu Rzeczy (*Internet of Things*, IoT) dostępna jest w naszym życiu i jak bardzo je ułatwia – rolety, które podnoszą się w tym samym momencie, w którym dzwoni budzik, zaparzenie porannej kawy w odpowiedzi na włączenie aplikacji w telefonie...

Ale czy IoT to tylko ułatwienie? Inna firma udostępniła film⁷ dla odmiany pokazujący zagrożenia/niedogodności związane z IoT. Czy łatwo zrezygnować nam ze standardowych rozwiązań czy z prywatności na rzecz wygody? Korzystamy z Internetu. Najprostsza strona www ma obowiązek informować nas o ciasteczkach, o zbieraniu danych, dając nam jednocześnie wybór – akceptujemy taki stan czy nie. Jeśli nie, możemy nie wchodzić na taką stronę. Ale jeśli na niej są informacje, które bardzo nas interesują? Odruchowo, nie czytając rozwinięcia komunikatu naciskamy zgodę i wchodzimy na stronę. Nie powinno nas dziwić, że za moment pojawiają się reklamy produktów związanych z tematyką, o której przed chwilą czytaliśmy. Tak działa Internet i mechanizmy komercyjne, które pozwalają w pewien sposób go finansować. Nasze dane wykorzystywane są do realizacji celów marketingowych. Czasem jest to dla nas wygodne, czasem zastanawiamy się, dlaczego raptem wyświetlają nam się informacje powiązane z ostatnio wyszukiwanymi wiadomościami/przedmiotami, a czasem bardzo nas to denerwuje, czujemy się inwigilowani. Wszystko zależy od sytuacji i świadomości danej osoby, ale również akceptacji dla nowej cyfrowej rzeczywistości. Dane, które udostępniamy świadomie lub nie w Internecie, mogą służyć do celów marketingowych, ale mogą zostać także użyte nielegalnie, do np. różnych wyłudzeń lub podszywania się pod daną osobę.

Dzisiaj nie jest tak, jak ponad dekadę temu, kiedy za tworzenie informacji odpowiedzialne były profesjonalne media, pozostawiając pewien margines dla entuzjastów technologii czy dziennikarstwa. Dziś każdy z nas jest twórcą i wydawcą informacji w jednym dzięki rozwojowi portali społecznościowych, platform CMS, ale również demokratyzacji dostępu do Internetu. Część z nich tworzymy świadomie, pisząc do znajomych lub nieznanym komunikaty w mediach społecznościowych. Część nie – nawet zdjęcie, które robimy aparatem komórkowym jest daną, która zawiera w sobie zapisane informacje, takie jak: czas i miejsce wykonania, nazwa aparatu, z którego wykonano zdjęcie itp. Istnienia części z danych, które wytarzają przedmioty przez nas używane, nie jesteśmy świadomi. Dane takie w naszym imieniu wytwarzają i przekazują dalej tzw. smart urządzenia, np. poprzez przekazywanie dalej odczytów z naszych liczników elektrycznych czy gazowych. Istnienie takowych, w pierwszej chwili przyjęliśmy z wdzięcznością. Zwalniało nas to z konieczności np. wcześniejszego wyjścia z pracy na czas wykonywania stosownych pomiarów przez uprawnionego pracownika. Jednak bardziej się nad tym zastanawiając, możemy dojść do wniosku, że na podstawie danych, które przekazujemy, łatwo zdobyć informację o tym, w jakich godzinach zwiększony jest pobór mocy w naszym domu,

⁶ https://www.youtube.com/results?search_query=like+a+bosh

⁷ <https://www.youtube.com/watch?v=6LELq9ZbS8o>

a więc najpewniej jesteśmy wtedy w domu, a co za tym idzie, jeśli takowe dane zostały przechwycone przez niepowołane osoby, łatwo zorientować się, kiedy nas w domu nie ma, co może z kolei być interesującą informacją np. dla włamywaczy czy telemarketerów.

Kilka lat temu czytaliśmy z niedowierzaniem o inteligentnych domach czy sprzętach AGD. Dziś są one naszą rzeczywistością, znakiem naszych czasów. Bardzo wygodną, ale czy bezpieczną? Bo o ile IoT w mieście (np. za ile czasu nadjedzie tramwaj) nie korzysta z naszych danych osobistych, o tyle sprzęty domowe korzystają z nich, a dane te mogą zostać z nich wykradzione.

Dziś wraz z docierającymi do nas informacjami o Internecie Rzeczy, o „rozmawiających ze sobą urządzeniach”, o handlu informacjami (a wszystko to przy funkcjonujących zasadach RODO) zastanawiamy się, w jakim kierunku zmierza ta technologia oraz bezpieczeństwo danych związanych z użytkownikiem.

W wywiadzie, jakiego udzieliła w marcu 2010 roku hiszpańska posłanka Maria Badia i Cutchet z Parlamentu Europejskiego, poza wypowiedaniem się o oczekiwanych zaletach Internetu Rzeczy, zaznaczyła, że nie mamy jeszcze (i wciąż po 10 latach⁸) wyników badań wpływu na ludzkie zdrowie fal radiowych, za pomocą których urządzenia się porozumiewają⁹. „Badania nad wpływem promieniowania elektromagnetycznego na zdrowie są niezwykle trudne. Głównym tego powodem jest fakt, że ze względów etycznych nie jest możliwe poddawanie ludzi wpływom badanych czynników w warunkach kontrolowanych w pełnym zakresie mocy i w odpowiedniej skali czasowej¹⁰”. W chwili obecnej nie można jednoznacznie potwierdzić negatywnego ani pozytywnego wpływu promieniowania elektromagnetycznego na człowieka, a w środowisku naukowym istnieją duże rozbieżności odnośnie do wniosków płynących z wyników badań prowadzonych w tej dziedzinie¹¹.

⁸ M. Karaboytcheva, *Skutki bezprzewodowej łączności 5G dla zdrowia ludzkiego*, BRIEFINGEPRS | Biuro Analiz Parlamentu Europejskiego, luty 2020, 3[https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/646172/EPRS_BRI\(2020\)646172_PL.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/646172/EPRS_BRI(2020)646172_PL.pdf) [dostęp: 23.04.2020].

⁹ Parlament Europejski, *Internet przedmiotów, czyli rzecz w sieci*, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+IM-PRESS+20100312STO70527+0+DOC+XML+V0//PL> [dostęp: 29.01.2019].

¹⁰ *Pole elektromagnetyczne a człowiek. O fizyce, biologii, medycynie, normach i sieci 5G*, Biała Księga 2019, s. 58, <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKewiXh-Tav6jnAhWCjosKHffwDREQFjABegQIBRAB&url=https%3A%2F%2Fwww.gov.pl%2Fattachmen-t%2F856baf55-3ec2-40ed-8ea8-ed88cd81a7f&usq=AOvVaw0u8dKUMNpLjT-VI0x9Zz64> [dostęp: 29.01.2020].

¹¹ S.A.R. Mortazavi, A. Tavakkoli-Golpayegani, M. Haghani, S.M.J. Mortazavi, *Looking at the other side of the coin: the search for possible biopositive cognitive effects of the exposure to 900 MHz GSM mobile phone radiofrequency radiation*, J. Environ. Heal. Sci. Eng. 2014; 12: 75. Por. *Pole elektromagnetyczne a człowiek. O fizyce, biologii, medycynie, normach i sieci 5G*, Biała Księga 2019, s. 58 <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKewiXh-Tav6jnAhWCjosKHffwDREQFjABegQIBRAB&url=https%3A%2F%2Fwww.gov.pl%2Fattachmen-t%2F856baf55-3ec2-40ed-8ea8-ed88cd81a7f&usq=AOvVaw0u8dKUMNpLjT-VI0x9Zz64> [dostęp: 29.01.2020].

Niewątpliwym faktem jest, że w ostatnich latach notuje się większą zapadalność na różne choroby¹². Póki co, otwartym zostaje pytanie, czy jest to związane z wszechobecnym oddziaływaniem promieniowania, czy rozwój medycyny daje możliwość wcześniejszego wykrycia różnych chorób i przedłużenia życia mimo wielu współtowarzyszących niedogodności towarzyszących choremu.

Program Big Brother cieszył się dużym zainteresowaniem części populacji za sprawą możliwości bezkarnego podglądania innych we wszystkich możliwych sytuacjach życia. Ilu jednak z nas, oglądając wówczas ten program, pomyślałoby, że za kilka lat sami będziemy uczestnikami życia na podglądzie? Obserwacja, w której bierzemy udział, nie jest co prawda transmitowana przez żadną stację telewizyjną, ale jesteśmy obserwowani przez sprzęty, w posiadanie których weszliśmy sami, z własnej woli. Zapewne nie wszyscy wiedzą, że są podsłuchiwanie przez własny smartfon (o fakcie tym donosiły media¹³), czy też, że kamery w naszych laptopach podglądają¹⁴. Wraz ze wzrostem ilości technologii w życiu przeciętnego Kowalskiego oraz ilością danych, które są przez nie generowane, dużą popularność zyskał termin Big Data.

Istota działania Internetu Rzeczy

Każdego dnia wytwarzamy i przekazujemy dalej dziesiątki, setki informacji. Tak wiele, że stan ten doczekał się własnej nazwy – żyjemy w erze Big Data.

Bez względu na sposób przesyłania danych, aby mogło dojść do przesyłania informacji pomiędzy dwiema „rzeczami”, muszą być spełnione trzy następujące warunki (Kokot i Kolenda, 2015, s. 8):

1. Urządzenie musi być wyposażone w sensor (różnego rodzaju czujniki np. GPS, drgań ruchu), dzięki któremu może zbierać informacje z otoczenia i przysyłać je dalej. Najpopularniejszym, najczęściej używanym nadajnikiem może być opaska na rękę typu smartband monitorująca tętno czy pokonany dystans.
2. Konieczne jest akcesorium (np. smartfon), które jest w stanie odebrać przesłany sygnał, przerobić go i w konsekwencji wywołać określoną czynność (akcję). Np. ekspres do kawy, który zaparza kawę po tym, jak odebrał informację od budzika, że pora wstawać i rozpocząć dzień.
3. Niezbędne jest wykorzystanie sieci teleinformatycznej, za pomocą której odbywa się dialog pomiędzy urządzeniami, np. Wi-Fi czy Bluetooth¹⁵.

¹² RZĄDOWA RADA LUDNOŚCIOWA, *Zachorowalność i umieralność na nowotwory a sytuacja demograficzna Polski*, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwjfmpym0KjnAhWCjosKHfFwDREQFjAAegQIBhAB&url=https%3A%2F%2Fbip.stat.gov.pl%2Fdownload%2Fgfx%2Fbip%2Fpl%2Fdefaultstronaopisowa%2F805%2F1%2F1%2Fzachorowalnos_na_nowotwory.pdf&usq=AOvVaw3yvONrOGS16S0khcYxV_C3, Warszawa 2014, s. 27 [dostęp: 29.01.2020].

¹³ <https://www.spidersweb.pl/2019/07/asystent-google-podsluchuje.html> [dostęp: 13.01.2019].

¹⁴ <https://www.ochronatozsamosci.pl/blog/one,3,,40,czy-nalezzy-obawiac-sie-kamery-w-laptopie-.html> [dostęp: 13.01.2019].

¹⁵ W. Kokot, P. Kolenda, (2015), *Czym jest Internet rzeczy, IAB Polska Raport: Internet Rzeczy w Polsce*, <http://iab.org.pl/wp-content/uploads/2015/09/Raport-Internet-Rzeczy-w-Polsce.pdf> [dostęp: 10.02.2017].

Big Data pochodzą z czujników, urządzeń multimedialnych, dzienników aktywności programów komputerowych, aplikacji transakcyjnych, stron internetowych i mediów społecznościowych – większość z nich generowana jest w czasie rzeczywistym i na bardzo dużą skalę.

Podłączanie coraz większej liczby urządzeń skutkuje pojawieniem się coraz większej ilości danych, które muszą być zapisywane, przesyłane i analizowane. W sposób naturalny narzuca to wymogi dotyczące wydajnej infrastruktury sieciowej oraz systemów będących w stanie przetwarzać taką ilość informacji. Zjawisko to, powiązane bezpośrednio z IoT opisywane jest jako Big Data¹⁶.

IoT - szanse i zagrożenia

Urządzenia IoT mogą padać łatwym łupem przestępców zainteresowanych kradzieżą danych osobowych. Większość cyberprzestępców nieustannie skupia się na kradzieży danych, które po pierwsze – są wartością samą w sobie, a po wtóre będąc już w ich posiadaniu, można łatwo realizować nielegalne działania¹⁷. Już w 2012 roku dane okrzyknięto „nową ropą naftową”, a slogan ten jest szeroko powtarzany w środowiskach naukowych i publicystycznych¹⁸.

Oprócz wspomnianych zagrożeń należy podkreślić, że inteligentne urządzenia i Internet Rzeczy dają nam niezwykłą wygodę oraz bezpieczeństwo, np. w zakresie ochrony zdrowia, a czasem nawet życia. Odpowiednie urządzenia są w stanie monitorować nasze funkcje zdrowotne czy nawet sprawdzać, czy po domu ktoś się porusza. W przypadku osób mieszkających samotnie, np. starszych i schorowanych, wykrycie odstępstw od normy, np. w przypadku upadku czy innych niż normalnie wskaźników zdrowia, czy braku ruchu w pomieszczeniu po zawiadomieniu odpowiednich służb może nawet przyczynić się do uratowania czyjegoś życia.

Jednak dostępne sprzęty medyczne monitorujące stan człowieka i brak wiedzy odnośnie do interpretacji wyników w połączeniu z coraz większą liczbą leków dostępnych bez recepty oraz skłonnością do poszukiwania porady medycznej w wyszukiwarce Google może prowadzić do utarty zdrowia przez nierozważnych, ślepo ufających technologii pacjentów.

Wyniki badań

Dla sprawdzenia stanu nasycenia urządzeniami wykorzystującymi Internet Rzeczy przeprowadzono ankietowe badania diagnostyczne. Badanie przeprowadzono

¹⁶ M. Piwiński, *Internet rzeczy – rozwiązania przyszłości*, s. 47. Informatyka w Edukacji, XVI, UMK Toruń, 2019 <https://iwe.mat.umk.pl/tom-iwe2019/06.pdf> [dostęp: 29.01.2020 r.].

¹⁷ M. Decyk, *Internet rzeczy-wistych zagrożeń*, SECURO, Nr 5, Cyberbezpieczeństwo w XXI wieku, Warszawa 2018, s. 27, https://www.academia.edu/35840213/SECURO_2018_5_CYBERBEZPIECZE%C5%83STWO_W_XXI_WIEKU_red._A._Gasztold_i_J._Saba%C5%82a [dostęp: 29.04.2020].

¹⁸ <https://www.forbes.com/sites/perryrotella/2012/04/02/is-data-the-new-oil/#2cdac4587db3> [dostęp: 29.04.2020].

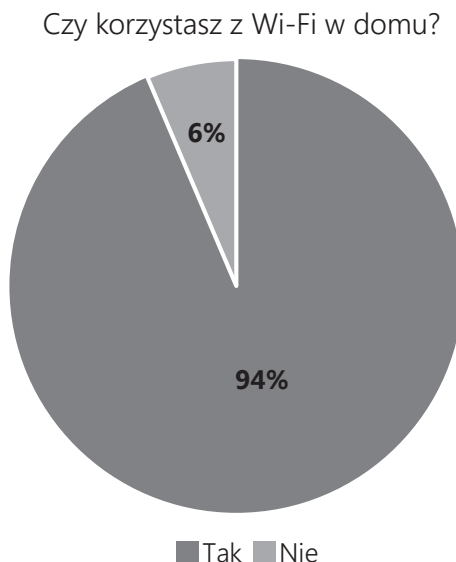
w Internecie w marcu 2020 roku przy pomocy narzędzia badawczego webankieta.pl. Swoim zasięgiem badanie objęło losowo wybranych 78 osób mających co najmniej 30 lat. **Przedmiotem** przeprowadzonego badania była świadomość istnienia i korzystanie z Internetu Rzeczy wśród osób 30+.

Celem badania było sprawdzenie, czy osoby 30+ znają pojęcie Internetu, czy kiedykolwiek zetknęły się z tą technologią, czy potrafią określić potencjalną wartość tworzoną przez tę technologię w ich życiu prywatnym lub zawodowym oraz czy korzystają lub w przyszłości chciałyby korzystać z narzędzi/urządzeń wykorzystujących technologię kategoryzowaną jako IoT.

Głównym problemem badawczym było postawione pytanie: Czy osoby 30+ znają pojęcie Interetu Rzeczy (IoT) oraz czy używają lub chciałyby używać narzędzi wykorzystujących IoT i jaką wartość technologia ta może wnieść do ich życia prywatnego bądź zawodowego.

Badanym zadano 11 pytań, z czego wszystkie z nich były obowiązkowe.

Pytanie pierwsze dotyczyło wykorzystywania w domu sieci Wi-Fi, co wydaje się być niezbędne przy korzystaniu z narzędzi IoT. Ponadto technologia WiFi wydaje się bardziej powszechną niż Bluetooth, która w dużej mierze stosowana jest w urządzeniach IoT¹⁹. 94% badanych korzystało z Wi-Fi w domu (rys. 1).

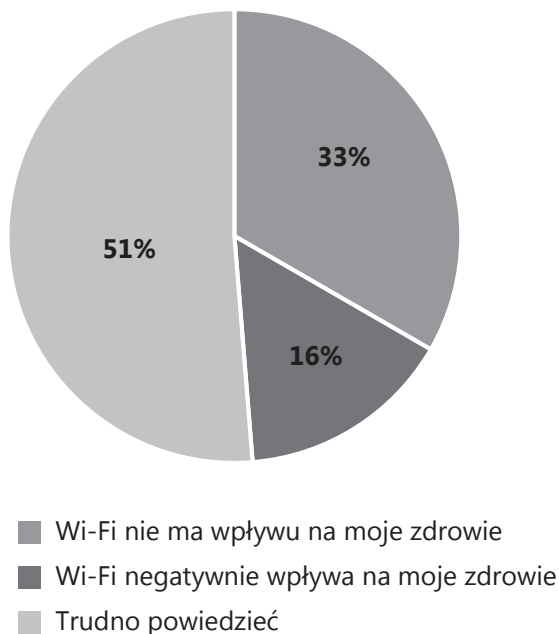


Rys. 1. Czy korzystasz z Wi-Fi w domu?

¹⁹ T. McKinney, *Bluetooth, WiFi czy Zigbee? Wybór optymalnego standardu transmisji bezprzewodowej*, <http://www.elektroonline.pl/a/8479,Bluetooth-WiFi-czy-Zigbee-Wybor-optymalnego-standardu-transmisji-bezprzewodowej,,Automatyka> [dostęp: 15.04.2020].

Mimo dość dużego nasycenia technologią Wi-Fi domostw badanych osób jedynie 33% z badanych jest przekonanych, że nie ma ona negatywnego wpływu na ich zdrowie. Najwięcej osób badanych – 51% – uważa, że trudno określić, jaki jest jej wpływ na zdrowie (rys. 2).

Czy sądzisz, że Wi-Fi ma wpływ na Twoje zdrowie?

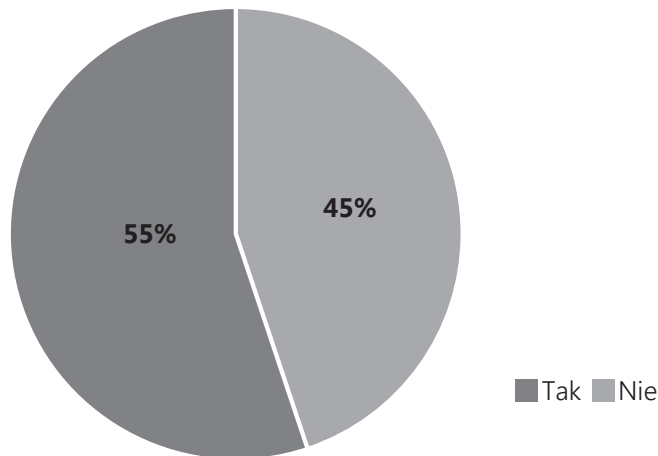


Rys. 2. Wpływ Wi-Fi na zdrowie

Urządzenia IoT jawią się jako takie, które wprowadzają wygodę w nasze życie poprzez wykonywanie pewnych czynności bez każdorazowego udziału człowieka, w sposób niejednokrotnie automatyczny. O ogólną chęć korzystania z tego typu urządzeń badani byli pytani w kolejnym pytaniu (rys. 3). 55% badanych wyraziło opinię, iż nie chciałoby, aby pewnymi zadaniami, np. wyłączeniem światła, można było sterować automatycznie. Świadczyć to może o dużym przywiązaniu do samodzielnego wykonywania czynności oraz – można zaryzykować stwierdzenie – o strachu przed utratą kontroli nad tą sferą rzeczywistości, a może także nieumiejętnością wyobrażenia sobie sposobu, w jaki ta samodzielność urządzeń mogłaby się odbywać. Podobny nastrój społeczny towarzyszyły nam przy wejściu na rynek elektronicznych książek. Dziś jadąc w Warszawie komunikacją miejską, bez trudu można zauważyć ludzi (w każdym wieku) korzystających z czytników elektronicznych książek (choć wg raportu Biblioteki Narodowej jedynie 3% czytelników sięgnęło po e-book²⁰).

²⁰ Kuba, Jak wyglądało czytelnictwo w Polsce w roku 2018? Podsumowanie najnowszego raportu Biblioteki Narodowej, <https://www.naczytniku.pl/jak-wygladalo-czytelnictwo-w-polsce-w-roku-2018-podsumowanie-najnowszego-raportu-biblioteki-narodowej/> [dostęp: 14.04.2020].

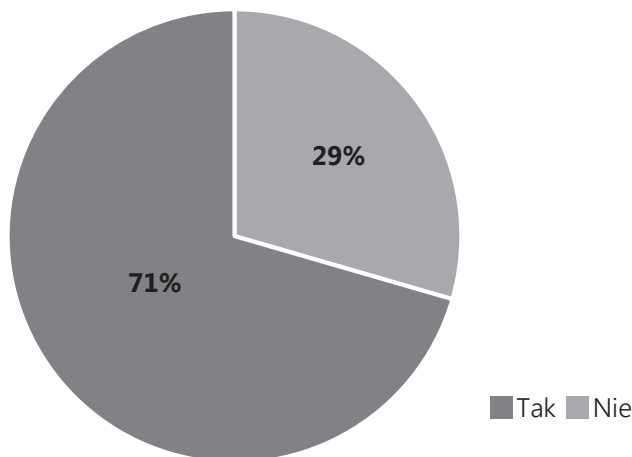
Czy chciałbyś, aby pewnymi zadaniami, np. wyłączeniem światła, można było sterować automatycznie, korzystając tylko z telefonu/tabletu?



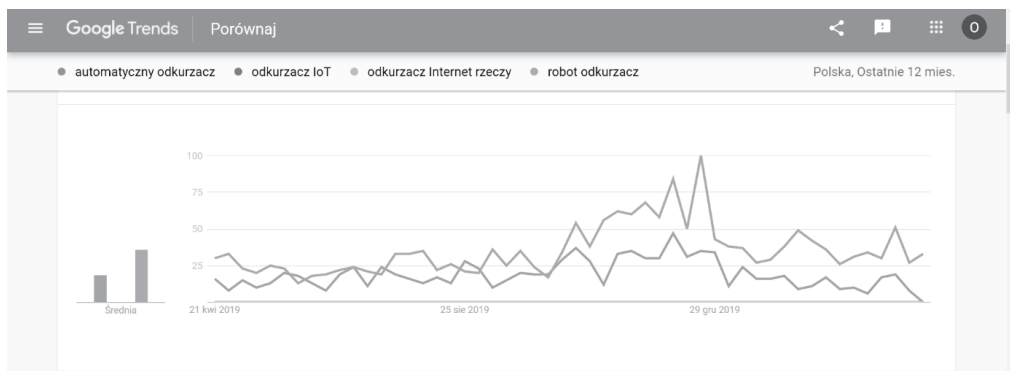
Rys. 3. Chęć do wykorzystywania przedmiotów IoT

Większość osób badanych nie spotkała się ani z określeniem Internet Rzeczy/ani z jego angielskim odpowiednikiem czy akronimem (rys. 4). Świadczyć to może o tym, iż sprzęty czy rozwiązania wykorzystujące IoT, mimo coraz szerszego zastosowania, nie wykorzystują wspomnianych nazw do promocji. Aplikacja Google Trends, służąca do sprawdzania, czego wyszukujemy w wyszukiwarce wskazuje, że np. samosprzątający odkurzacz czy odkurzacz robot były wielokrotnie wyszukiwane, a odkurzacz IoT wcale (rys. 5).

Czy spotkałeś się z określeniem Internet Rzeczy / Internet of things / IoT?



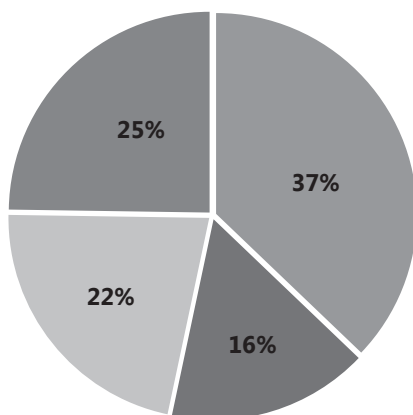
Rys. 4. Czy spotkałeś się z określeniem Internet Rzeczy/ Internet of Things/ IoT



Rys. 5. Google Trends

Kolejne pytanie sprawdzało, czy osoby badane są w stanie wskazać, czym jest Internet Rzeczy, a więc z danych odpowiedzi wskazać właściwą. 25% osób badanych wskazało ostatnią opcję, deklarując, że nie wiedzą, czym jest Internet Rzeczy.

Internet Rzeczy to:

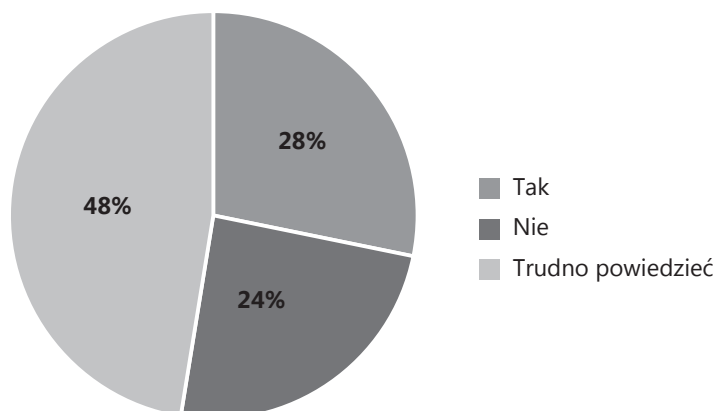


- Koncepcja urządzeń mogących połączyć się z Internetem lub innymi urządzeniami, korzystając bezpośrednio z sieci bezprzewodowych
- Sieć komunikujących się ze sobą i z ludźmi inteligentnych, uczących się urządzeń, na bieżąco zbierających dane i podejmujących działania
- Sieć czujników, elementów wykonawczych i układów sterowania, które są ze sobą połączone, umożliwiając uzyskanie wyższego poziomu wydajności, bezpieczeństwa lub komfortu w stosunku do stanu sprzed zastosowania takiego rozwiązania
- Nie wiem

Rys. 6. Definicja Internetu Rzeczy

Przekonanie badanych odnośnie do wpływu urządzeń IoT na zdrowie koreluje z pytaniem nr 3 w aspekcie niepewności odnośnie do samej technologii. W pozostałych opcjach odpowiedzi różnice procentowe są większe, ale trend jakościowy zostaje zachowany.

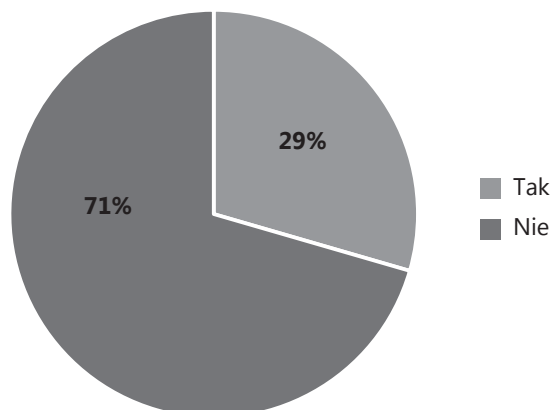
Czy sądzisz, że korzystanie z urządzeń IoT pozostaje bez wpływu na Twoje zdrowie?



Rys. 7. Wpływ urządzeń IoT na zdrowie

Wydaje się, że znajdujemy się o krok od wypuszczenia na nasze drogi autonomicznych samochodów. Z dużym entuzjazmem przyjmujemy samoparkujące samochody, traktując je jako spore ułatwienie, szczególnie w miejskich, zawsze przepelnionych parkingach. Jednak na autonomiczne samochody patrzymy z nieufnością. Nawet przy założeniu, że zostały świetnie zaprojektowane i nauczone właściwych zachowań, ciągle boimy się, że na naszych ulicach przepisy są bardzo często łamane, a wyczyny kierowców są trudne do przewidzenia, jak np. kierowca, który przeleciał rekordowy dystans nad rondem²¹.

Czy myślisz, że byłbyś w stanie zaufać autonomicznemu / samokierującemu się samochodowi?



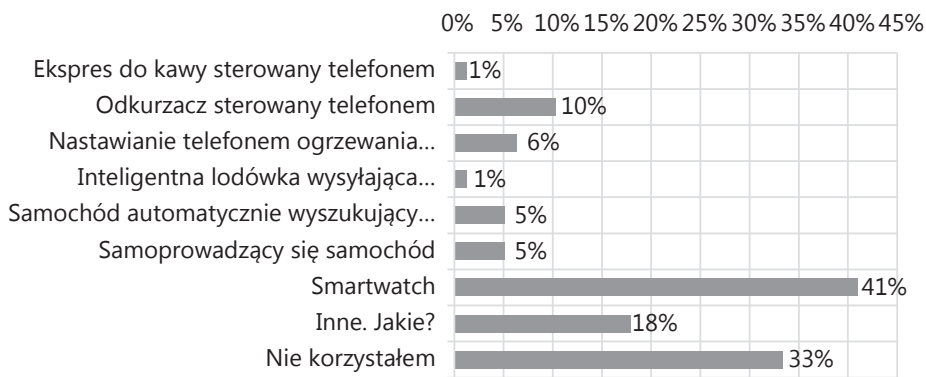
Rys. 8. Stopień zaufania do autonomicznych samochodów

71% z badanych deklaruje, że nie byłoby w stanie zaufać autonomicznemu samochodowi, przy deklarowanych 5% osób, które już korzystały z takiego samo-

²¹ <https://tvn24.pl/lodz/rabien-wypadek-wjechal-na-rondo-i-nad-nim-przelecial-4553654> [dostęp: 15.04.2020].

chodu (rys. 8–9). Najwięcej osób korzystało ze smart zegarków, co w odniesieniu do panującej mody na bieganie²² (smartwatche umożliwiają m.in. mierzenie i śledzenie swoich osiągnięć sportowych) i powszechności dostępu do nich u operatorów komórkowych²³ nie powinno dziwić. Z kolei badani najchętniej skorzystaliby (rys. 10) z samosterującego ogrzewania domu (62% badanych) oraz samochodu wyszukującego wolne miejsca parkingowe (51%). Widać, że są to obszary życia, w których chętnie skorzystalibyśmy ze wsparcia za pomocą technologii.

Czy korzystałeś z następujących inteligentnych urządzeń?



Rys. 9. Korzystanie z wybranych inteligentnych urządzeń

Zaznacz, z jakich urządzeń chciałbyś skorzystać

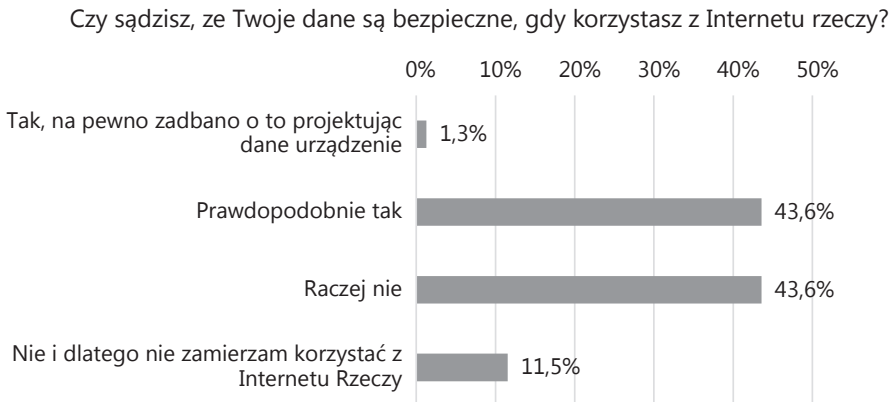


Rys. 10. Chęć do skorzystania z wybranych inteligentnych urządzeń w przyszłości

²² <https://forsal.pl/artykuly/1082697,boom-na-bieganie-w-polsce-socjolog-ta-moda-jest-zdominowana-przez-klase-srednia.html> [dostęp: 15.04.2020].

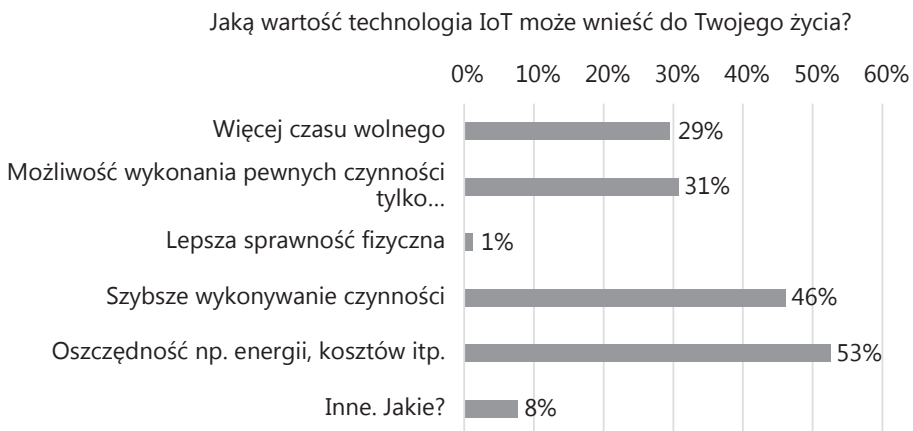
²³ <https://komorkomat.pl/promocja/play-abonament-smartwatche-od-1-zl/> [dostęp: 15.04.2020].

Często poruszonym teraz tematem, związanym z wejściem w życie rozporządzenia RODO²⁴, jest bezpieczeństwo danych osobowych. Ze względu na to, że przedmioty Internetu Rzeczy przetwarzają wiele danych, zasadnym było zapytanie badanych, czy uważają, że ich dane są bezpieczne podczas korzystania ze sprzętów Internetu Rzeczy. Badani skłaniają się do nieuznawania swoich danych za bezpieczne (rys. 11).



Rys. 11. Bezpieczeństwo danych osobowych podczas korzystania z Internetu Rzeczy

Na zakończenia badania respondenci zostali zapytani o wartość, jaką technologia IoT może wnieść do ich życia (rys. 12). Najczęściej dostrzegali oszczędność kosztów, związaną z np. lepszym dopasowaniem ogrzewania domu do faktycznych potrzeb, czy szybsze wykonywanie działań (oszczędność czasu) dzięki możliwości ich zaplanowania.



Rys. 12. Wartość wnoszona przez technologię IoT

²⁴ <https://www.gov.pl/web/cyfryzacja/rodo-informacje> [dostęp: 15.04.2020].

Zakończenie i wnioski

Technologia Internetu Rzeczy nie jest jeszcze bardzo popularna wśród przeciętnych użytkowników, ale wydaje się, że ze względu na wygodę używania rozwiązania wykorzystujące tę technologię przyjmą się.

Zadaniem projektantów sprzętów IoT jest zwiększenie bezpieczeństwa tych urządzeń i naszych danych, które urządzenia generują i przetwarzają. Czyli ważne będzie znalezienie właściwej równowagi pomiędzy korzyściami a potencjalnymi zagrożeniami, które zawsze występują w przypadku korzystania z wysokich technologii.

Zdaje się, że nie uda się nam uniknąć kontaktów z Internetem Rzeczy na większą skalę.

Bibliografia:

1. Bauer H., Patel M., Veira J. (2014), *The Internet of Things: Sizing up the Opportunity*, McKinsey&Company, <http://www.mckinsey.com/industries/high-tech/our-insights/the-internet-of-things-sizing-up-the-opportunity> [dostęp: 12.05.2017].
2. *Boom na bieganie w Polsce. Socjolog: Ta moda jest zdominowana przez klasę średnią*, <https://forsal.pl/artykuly/1082697,boom-na-bieganie-w-polsce-socjolog-ta-moda-jest-zdominowana-przez-klase-srednia.html> [dostęp: 15.04.2020].
3. Brachman A., *Raport Obserwatorium ICT Internet przedmiotów*.
4. *Czy należy obawiać się kamery w laptopie?*, <https://www.ochronatozsamosci.pl/blog/one,3,,40,czy-nalezy-obawiac-sie-kamery-w-laptopie-.html> [dostęp: 13.01.2019].
5. Decyk M., *Internet rzeczy-wistych zagrożeń*, SECURO, Nr 5, Cyberbezpieczeństwo w XXI wieku, Warszawa 2018, s. 27 https://www.academia.edu/35840213/SECURO_2018_5_CYBERBEZPIECZE%C5%83STWO_W_XXI_WIEKU_red._A_Gasztold_i_J_Saba%C5%82a [dostęp: 29.04.2020].
6. Gajewski M., *To nie była plotka*, <https://www.spidersweb.pl/2019/07/asystent-google-podsluchuje.html> [dostęp: 13.01.2019].
7. Goodman M. (2016), *Zbrodnie przyszłości: jak cyberprzestępcy, korporacje i państwa mogą użyć technologii przeciwko Tobie*, Gliwice, s. 250.
8. https://www.youtube.com/results?search_query=like+a+bosh
9. <https://www.youtube.com/watch?v=6LELq9ZbS8o>
10. Karaboytcheva M., *Skutki bezprzewodowej łączności 5G dla zdrowia ludzkiego*, BRIEFINGEPRS | Biuro Analiz Parlamentu Europejskiego, luty 2020, 3 [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/646172/EPRS_BRI\(2020\)646172_PL.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/646172/EPRS_BRI(2020)646172_PL.pdf) [dostęp: 23.04.2020].
11. Kokot W. i Kolenda P. (2015), *Czym jest Internet rzeczy*, IAB Polska Raport: Internet Rzeczy w Polsce, <http://iab.org.pl/wp-content/uploads/2015/09/Raport-Internet-Rzeczy-w-Polsce.pdf> [dostęp: 10.02.2017].
12. McKinney T., *Bluetooth, WiFi czy Zigbee? Wybór optymalnego standardu transmisji bezprzewodowej*, <http://www.elektroonline.pl/a/8479,Bluetooth-WiFi-czy-Zigbee-Wybor-optymalnego-standardu-transmisji-bezprzewodowej,,Automatyka> [dostęp: 15.04.2020].
13. Mortazavi S.A.R., Tavakkoli-Golpayegani A., Haghani M., Mortazavi S.M.J. (2014), *Looking at the other side of the coin: the search for possible biopositive cognitive effects of the exposure to 900 MHz GSM mobile phone radiofrequency radiation*, J. Environ. Heal. Sci. Eng.; 12: 75.
14. Parlament Europejski, Internet przedmiotów, czyli rzecz w sieci <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+IM-PRESS+20100312STO70527+0+DOC+XML+V0//PL> [dostęp: 29.01.2019].

15. Piwiński M., *Internet Rzeczy – rozwiązania przyszłości*, Informatyka w Edukacji, XIV, UMK Toruń, 2019,30 s. 50 <https://iwe.mat.umk.pl/tom-iwe2019/06.pdf> [dostęp: 14.04.2020].
16. *Pole elektromagnetyczne a człowiek. O fizyce, biologii, medycynie, normach i sieci 5G*, Biała Księga 2019, s. 58, <https://www.gov.pl/web/5g/biala-ksiega1> [dostęp: 29.01.2020].
17. RODO – informacje, <https://www.gov.pl/web/cyfryzacja/rodo-informacje> [dostęp: 15.04.2020]
18. Rot A., Blaike B. (2017), *Bezpieczeństwo internetu rzeczy. Wybrane zagrożenia i sposoby zabezpieczeń na przykładzie systemów produkcyjnych*, Zeszyty Naukowe Politechniki Częstochowskiej, Zarządzanie Nr 26, s. 191.
19. Rotella P., *Is Data The New Oil?*, [shttps://www.forbes.com/sites/perryrotella/2012/04/02/is-data-the-new-oil/#2cdac4587db3](https://www.forbes.com/sites/perryrotella/2012/04/02/is-data-the-new-oil/#2cdac4587db3) [dostęp: 29.04.2020].
20. *Smartwatche w abonamencie Play od 1 zł* <https://komorkomat.pl/promocja/play-abonament-smartwatche-od-1-zl/> [dostęp: 15.04.2020].
21. *Wbił się na rondzie*, <https://tvn24.pl/lodz/rabien-wypadek-wjechał-na-rondo-i-nad-nim-przeleciał-4553654> [dostęp: 15.04.2020].
22. *Zachorowalność i umieralność na nowotwory a sytuacja demograficzna Polski*, RZĄDOWA RADA LUDNOŚCIOWA, Warszawa 2014, s. 27.

dr Olga Pawłowska – Naukowa i Akademicka Sieć Komputerowa (NASK) – Państwowy Instytut Badawczy,
Warszawa

