Dydaktyka Informatyki 15(2020)
ISSN 2083-3156; e-ISSN 2543-9847
DOI: 10.15584/di.2020.15.4
http://www.di.univ.rzeszow.pl

Uniwersytet Rzeszowski

Aleksander PIECUCH

ORCID: 0000-0001-5889-9643. Prof. nadzw. dr hab., Uniwersytet Rzeszowski, Laboratorium Zagadnień Społeczeństwa Informacyjnego, ul. prof. S. Pigonia 1, 35-310 Rzeszów; e-mail: apiecuch@ur.edu.pl

ŻYCIE SMART – MA SWOJĄ CENĘ
SMART LIFE – HAS THEIR PRICE

Słowa kluczowe: Smart, smartfon, smartlive, smartcity.
Keywords: Smart, smartphone, smartlive, smartcity.

Streszczenie

Globalna cyfryzacja zmieniła sposoby funkcjonowania społeczeństw, ale przede wszystkim zmieniła relacje międzyludzkie. Możliwości, które pojawiły się wraz z rozwojem IT, z jednej strony stały się ważnym przyczynkiem dla rozwoju gospodarczego i społecznego, z drugiej zaczęły gwałtownie wkraczać w sferę prywatną. Mnogość dostępnych darmowych aplikacji na urządzenia stacjonarne i mobilne otworzyła przy okazji nowe możliwości dla gigantów branży IT. Oferta, jaką składają użytkownikom swoich wyrobów, teoretycznie jest darmowa, jednak rzeczywistość wskazuje na inne praktyki. Za udostępnione nam udogodnienia płacimy utratą własnej prywatności.

Abstract

Global digitization has changed the way of societies function, but, above all, has changed interpersonal relationships. Opportunities that arose with the development of IT, on the one hand, have become an important contribution to economic and social development, on the other hand, they have rapidly entered to the private sphere. A lot of free applications available for stationary and mobile devices has opened up new opportunities for IT giants. The offer they make to users of their products is theoretically free, but reality points to other practices. We pay for the facilities provided to us by losing our privacy.

Wstęp

„Obyś żył w ciekawych czasach" – mówi przysłowie i bynajmniej nie wieści ono nic dobrego. Prawdopodobnie przyszło nam żyć właśnie w takich czasach, kiedy tempo rozwoju techniki wyprzedziło ludzką świadomość konsekwencji

tegoż rozwoju. Cyfryzacja, która w założeniach miała ułatwiać funkcjonowanie człowieka w XXI wieku, sprawiać, by życie stało się nieco wygodniejsze, w istocie przekształca nas obywateli – w cyfrowe obiekty. Nadano nam numery PESEL, NIP, ORCID, PIN-y do bankomatów, domofonów. Wciąż zmieniamy hasła do kont bankowych, poczty e-mail i wielu innych usług cyfrowych, których wyliczyć tu nie sposób. W rzeczywistości bez przypisanych nam numerów nie „istniejemy" w realnym świecie i nie możemy w nim sprawnie funkcjonować na dotychczasowych zasadach. Technika, która miała ułatwiać życie, osaczyła i wciąż osacza nas z coraz większą dynamiką.

Według Ministerstwa Cyfryzacji liczba i jakość usług publicznych świadczonych drogą elektroniczną jest wyznacznikiem otwartości, sprawności i efektywności funkcjonowania państwa. Nieodłącznym elementem tych działań jest stymulowanie stałego wzrostu cyfrowych kompetencji mieszkańców oraz obsługujących ich pracowników administracji publicznej, na wszystkich jej szczeblach[1].

Do technologii, które zdominują najbliższą przyszłość należeć będą:

- technologie SMAC (ang. **S**ocial, **M**obile, **A**nalytics, **C**loud),
- Internet rzeczy (ang. *Internet of Things* – IoT),
- wielokanałowe (ang. *Multi-channel*) modele dystrybucji produktów i usług,
- automatyzacja (ang. *Automation*) oraz robotyzacja (ang. *Robotisation*)[2].

Przyspieszenie technologiczne wskazuje jednoznacznie na kierunek ekspansji ku technologiom inteligentnym SMART. W najbliższym otoczeniu coraz więcej jest urządzeń tego typu (inteligentnych) wzrasta również liczba różnorakich usług, w których wykorzystywana jest sztuczna inteligencja. Przykładów jej wykorzystania nie trzeba szukać daleko. Smartfon posiada już dzisiaj każdy. Treść wiadomości SMS możemy po prostu wypowiedzieć, a ta zostanie automatycznie przetworzona na formę tekstową. Korzystając z translatorów językowych uzyskujemy niemal bezbłędne tłumaczenia. Samodiagnozujące się obrabiarki stają się podstawą dla przemysłu 4.0[3].

Technologie Smart

Termin „Smart" pochodzi z języka angielskiego i znaczy tyle co *elegancki, inteligentny*. Ze wspomnianym terminem stykamy się już od wielu lat w kontek-

[1] *Program zintegrowanej informatyzacji państwa*, Ministerstwo Cyfryzacji, Warszawa 2016.

[2] Zob:. Ch. Perera, R. Ranjan, L. Wang, S. Khan, A. Zomaya, *Privacy of Big Data in the Internet of Things Era*, IEEE IT Professional Magazine, PrePrint (Internet of Anything). Retrieved 1 February 2015; P. Corcoran, S.K. Datta, *Mobile-edge computing and the Internet of Things for consumers*: *Extending cloud computing and services to the edge of the network*, „IEEE Consumer Electronic Magazine", Vol. 5, No. 4/2016.

[3] A. Piecuch, *Szkoła XXI wieku – problemy i wyzwania*, Wydawnictwo UR, Rzeszów 2019, s. 43.

ście technologii inteligentnych. Chociaż ujmując rzecz precyzyjniej powinniśmy raczej mówić o pewnej idei, którą literatura przedmiotu nazywa *smart living*. „Obszar smart living to bardzo szerokie pojęcie, na które składają się m.in. kategorie związane z inteligentnym zarządzaniem i funkcjonowaniem w mieście (smart city), pracą (smart workplace), przemieszczaniem się (smart transport), domem (smart home). (…) Termin smart living jest bardzo pojemny, nie ma jednej, obowiązującej definicji. (…) choć trzonem pojęcia jest hasło smart łączone głównie z technologią i internetem, to o smart living musimy myśleć w szerszym kontekście i pamiętać, że celem wdrażania tej idei nie jest technologizacja każdego obszaru naszego życia, a raczej stworzenie bezpiecznej, efektywnej, energooszczędnej, spersonalizowanej, ekologicznej i lepiej zarządzanej przestrzeni życiowej (przy czym rozumiana jest ona bardzo szeroko: jako przestrzeń domu, środowiska pracy, funkcjonowania w mieście czy obszary związane z transportem). Idea smart living wymaga zatem otwartości nie tylko na nowe technologie, ale także przedefiniowania niektórych obszarów życia czy nawet stosunków społeczno-ekonomicznych. Jak podkreślają eksperci, smart living to koncepcja, która dąży do jak najlepszego, inteligentnego i efektywnego zarządzania środowiskiem i obszarami, w których funkcjonujemy”[4].

Bardziej wirtualni niż realni

Coraz bardziej żyjemy w świecie wirtualnym niż rzeczywistym. Bardziej cenimy sobie kontakty za pośrednictwem mediów cyfrowych niż osobiste. Liczba kontaktów na kontach mediów społecznościowych z całą pewnością jest o wiele większa od liczby osób, które faktycznie znamy osobiście i z którymi utrzymujemy bezpośredni kontakt. Z pozoru łatwość, z jaką nawiązujemy nowe kontakty w sieci, w rzeczywistości może okazać się zgubna dla naszej sfery prywatnej. Informacje na własny temat, które sami dobrowolnie umieszczamy w sieci w istocie udostępniamy bliżej nam nieznanemu gronu osób. Przy tym, nie zważamy na to, że od strony technicznej naszym kontem zarządza bliżej nieznany nam podmiot i w każdej chwili może zrobić użytek z informacji, które sami dostarczamy.

Już w 2017 roku szacowano, że „do 2020 roku co sekundę będzie się produkować 1,7 MB danych na każdego człowieka na Ziemi i osiągnie wartość 44 ZB (zetta bajtów). Użytkownicy w samej tylko wyszukiwarce Google zadają 40 000 zapytań w ciągu sekundy, co daje 1,2 biliona zapytań rocznie. Od sierpnia br. [październik 2015 r. – przyp. A.P.] ponad miliard ludzi używa Facebooka co-

[4] M. Jaskulska, M. Trapp, *Główne wnioski* [w:] *Smart living*, red. N. Hatalska, Infuture Hatalska Foresight Institute, Gdańsk 2019, s. 6.

dziennie zostawiając około 31 milionów wiadomości i prawie 3 miliony filmów na minutę. Na YouTube przybywa około 300 godzin materiałów filmowych na minutę"[5]. Na podstawie powyższych danych uświadamiamy sobie, jak potężnymi zasobami informacji milionów użytkowników zarządza tak popularny na świecie, jak i w naszym kraju portal społecznościowy. Według *Global Digital Raport 2019* ogółem z mediów społecznościowych w Polsce, w roku 2019 korzystało 18 mln użytkowników, co stanowi 47% populacji. Zdecydowanym liderem na polskim rynku social mediów okazuje się być Facebook, z którego korzysta 17 mln użytkowników, w tym 52% użytkowników to kobiety, a pozostałe 48% – mężczyźni[6].

Pytanie, które bardzo rzadko się stawia i jeszcze rzadziej na nie odpowiada dotyczy sfery gromadzenia i przetwarzania informacji o obywatelu. Naruszeń sfery prywatnej użytkowników zebrało się znacznie więcej przez 17 lat funkcjonowania portalu[7]. Zwróćmy uwagę na niektóre z nich:

- W 2007 roku Facebook program *Beacon* udostępniał użytkownikom informacje o tym, co i gdzie kupili znajomi. Po protestach użytkowników portalu dodano możliwość wyłączenia tejże funkcjonalności.
- W 2011 roku odkryto, że Facebook udostępnia pełne dane użytkowników podmiotom trzecim, nawet jeśli ci nigdy nie korzystali z usług takiego podmiotu i nie wyrazili na to zgody.
- W 2013 roku na skutek błędów w oprogramowaniu Facebooka prawdopodobnie wyciekły dane 6 mln użytkowników w postaci adresów e-mail i numerów telefonów.
- W 2018 roku wyciekły dane ok. 87 mln użytkowników z serwisu społecznościowego[8].
- W marcu 2018 roku dowiedzieliśmy się o kolejnych praktykach FB. Jak się okazuje, portal prowadzi rejestr połączeń telefonicznych: są numery, daty, czas trwania rozmowy, są również nazwiska osób, z którymi była prowadzona rozmowa, jest również historia wysłanych i odebranych SMS-ów. Portal wszedł również w posiadanie wszystkich kontaktów znajdujących się w telefonie komórkowym (nr telefonów, adresy e-mail)[9]. Facebook co prawda udostępnił

[5] https://www.dobreprogramy.pl/mikolaj_s/Big-Data-gwaltownie-rosnie-ilosc-gromadzonych--danych,67205.html (dostęp: 27.08.2017 r.).

[6] Zob.: https://datareportal.com/reports/digital-2019-poland (dostęp: 25.03.2020 r.).

[7] Serwis Thefacebook został uruchomiony w dniu 4 lutego 2003 roku, natomiast w roku 2005 z nazwy serwisu zniknął człon The, by ostatecznie stać się Facebookiem.

[8] Zob.: *Facebook ma już 16 lat. Wszystkie grzechy serwisu Marka Zuckerberga,* https://www.geekweb.pl/inne/kartka-z-kalendarza/item/908-facebook-ma-16-lat

[9] Zob.: R. Teklak, *Co wie o mnie Facebook? Ściągnąłem dane i zdrętwiałem. Kasuję aplikację, która czyta nawet moje SMS-y*, Onet (dostęp: 28.03.2018 r.).

użytkownikom narzędzie *off-facebook activity,* dające wgląd do informacji, co zostało zgromadzone na ich temat, niemniej jednak niewielu wie o jego istnieniu.

Z pozoru niewinne, mające urozmaicić, wzbogacić wirtualne życie i ożywić profil na FB, wyzwania *wstaw zdjęcie z dzieciństwa na Fejsa* w rzeczywistości ma inne ukryte cele. Znana jest już wcześniejsza akcja *10 Year Challenge,* zachęcającą do umieszczenia oprócz aktualnych zdjęć także tych sprzed 10 lat. Pamiętając o wcześniejszych praktykach udostępniania stronom trzecim danych wrażliwych i tym razem najprawdopodobniej chodzi o taką praktykę. Nieświadomi niczego użytkownicy chętnie umieszczają na własnych profilach tego rodzaju zdjęcia. W konsekwencji powstaje niemalże kompletna informacja na temat naszego rozwoju osobowego. Baza tak zgromadzonego materiału fotograficznego służy uczeniu maszynowemu. Inaczej ujmując problem, algorytmy sztucznej inteligencji (SI) doskonalą się w technice rozpoznawania twarzy. Na marginesie dodajmy, że jedna z chińskich firm zajmująca się technologią rozpoznawania twarzy, dopracowała tak własny algorytm, że może poszczycić się 95-procentową skutecznością w rozpoznawania twarzy osób z nałożonymi maseczkami[10]. Przywołajmy w tym miejscu jeszcze jedno pojęcie, z którym możemy się spotkać w kontekście nielegalnego wykorzystywania danych osobowych i wizerunku, a mianowicie *deepfake*. To nowe i bardzo niebezpieczne narzędzie, a sam omawiany termin ma dość krótką historię bo sięgającą zaledwie końca 2017 roku. „Samo słowo *deepfake* pochodzi od dwóch angielskich zwrotów: *deep learning* (głębokie uczenie) oraz *fake* (fałsz, podróbka). I już to dobrze tłumaczy, czym jest *deepfake* – obróbką dźwięku i obrazu, która ma na celu utworzenie fałszywych obrazów i dźwięków przy użyciu technik z zakresu sztucznej inteligencji**.** W założeniu pozwala to na stworzenie materiałów, które będą trudne lub niemożliwe do odróżnienia od filmów lub zdjęć, które zostały zrealizowane w tradycyjny sposób – z udziałem żywych osób.

Cechy charakterystyczne *deepfake*:

– w większości przypadków dotyczy obrazów lub filmów, na których występują ludzie;

– nie tworzy obrazów czy filmów, ale bazuje na wcześniej utworzonym materiale, który jest przerabiany;

– najczęściej przerabiane są materiały filmowe, ale do deepfake'ów zaliczamy także przeróbki głosu oraz zdjęć;

[10] Zob.: https://arstechnica.com/tech-policy/2020/03/how-china-built-facial-recognition-for--people-wearing-masks/ (dostęp: 25.03.2020 r.).

– to nowe zjawisko: sama nazwa pojawiła się pod koniec 2017 r., choć pierwsze rozwiązania wykorzystujące głębokie uczenie w obróbce obrazu pojawiły się już co najmniej 5 lat wcześniej.

Sposoby wykorzystania *deepfake*:

– rozrywka, zabawa – aplikacje, które w jakiś sposób przerabiają twarz, podmieniają ją we fragmentach znanych filmów itp.;

– wirtualne postacie – np. kreacje prezenterów telewizyjnych, występujących w chińskiej telewizji (zjawisko z pogranicza deepfake'ów);

– fake news – tworzenie fałszywych materiałów z wypowiedziami polityków i osób publicznych;

– pornografia – podmiana twarzy osób występujących w filmach pornograficznych. Zagrożone są zwłaszcza kobiety – aktorki, celebrytki, ale także osoby prywatne (zjawisko *revenge porn*). Tak jak w przypadku wielu innych technologii, to branża pornograficzna jest w tym momencie jednym z głównych motorów napędowych rozwoju technologii i popularyzacji zjawiska deepfake'ów;

– logowanie, autoryzacja – oszukiwanie systemów posługujących się twarzą użytkownika, ale zabezpieczających się poprzez konieczność wykonania ruchu głową, mrugnięcia okiem albo wypowiedzenia krótkiej kwestii;

– ataki finansowe – podszycie się pod menedżera wysokiego szczebla i wydawanie przez telefon lub podczas rozmowy wideo poleceń finansowych (np. wykonanie przelewu)"[11].

Przykłady wykorzystania *deepfake*:

– „film z twarzą Kita Haringtona, w którym grany przez niego Jon Snow przeprasza za zakończenie serialu »Gra o tron«,

– wideoklipy, w których twarz Nicholasa Cage'a została nałożona na słynne sceny z filmów (początek 2018 r.),

– nagranie przedstawiające Baracka Obamę, wypowiadającego ostrzeżenia (których w rzeczywistości nigdy nie powiedział) przed zagrożeniami, jakie niesie nieetyczne zastosowanie technologii cyfrowych (kwiecień 2018 r.),

– nagranie z twarzą Marka Zuckerberga, ostrzegającego przed zagrożeniami, jakie niosą cyfrowe technologie (czerwiec 2019 r.),

– udostępnienie kontrowersyjnej aplikacji internetowej DeepNude pozwalającej na tworzenie naturalistycznych obrazów nagich kobiet za pomocą przesłanych do aplikacji zdjęć prawdziwych osób (czerwiec 2019 r.)"[12].

[11] https://mitsmr.pl/serie/czy-wiesz-ze/co-to-jest-deepfake/ (dostęp: 30.03.2020 r.).

[12] J. Ciszewski, *Deepfake – co to jest*, https://publicrelations.pl/deepfake-co-to-jest/ (dostęp: 30.03.2020 r.).

Smart-telewizor

Na to, co niesie ze sobą idea smart living, spójrzmy z perspektywy użytkownika. Z nieco innej perspektywy przyglądnijmy się SMART-telewizorowi marki Samsung. Tylko decydenci firmy znają prawdziwy powód, dla którego w matryce telewizorów wbudowano kamery internetowe, o istnieniu których przeciętny użytkownik nie ma pojęcia. „Niniejszy wynalazek ujawnia moduł wyświetlacza LED, telewizor LED i system LED TV, w którym komponent kamery jest osadzony w module wyświetlacza LED; w ten sposób telewizor LED może wykonywać zdjęcia od środka ekranu; ponieważ uczestnicy patrzą na ekran wyświetlacza, w wyniku czego uczestnicy na poziomie lokalnym i na drugim końcu mogą spojrzeć w oczy, co poprawia zmysłowe odczucie interakcji wideo i pozwala uzyskać więcej informacji z wyrazu oczu; ponieważ komponent kamery może robić zdjęcia od przodu (…)”[13]. Do powyższego dodajmy, że omawiane rozwiązanie objęte jest ochroną patentową[14] z dnia 30.04.2015 roku. Przykładem na użycie tejże technologii niech będzie wypowiedź Billa Waltona, spikera stacji telewizyjnej ESPN: „»jedną z wielkich nowych technologii, które mamy tutaj w ESPN, jest to, że możemy patrzeć na ciebie w twoim domu przez twój telewizor«. Wypowiedź pojawiła się w kontekście tego, gdy sieć szpiegowała rodzinę koszykarza Dusana Ristica przez telewizor z ich salonu w Serbii”[15]. Z oficjalnych wypowiedzi przedstawicieli firmy dowiadujemy się, że dzięki wbudowanym komponentom mikrofonu i kamery możliwa jest komunikacja wideo, np. dzięki aplikacji Skype. Drugim powodem, dla którego owe komponenty znalazły się w odbiornikach telewizyjnych są inteligentne funkcje służące do głosowego sterowania odbiornikiem TV. „Wiosną 2015 roku eksperci ds. cyberbezpieczeństwa Ken Munro i David Lodge postanowili przekonać się, czy telewizory Samsunga z funkcją rozpoznawania mowy mogą służyć do podsłuchiwania rozmów użytkowników. Jak udało się im ustalić, telewizory cyfrowe pozostają nieaktywne, gdy nie są włączone – to dobra wieść dla użytkowników – ale nagrywają wszystko to, co zostaje powiedziane w ich pobliżu po otrzymaniu polecenia »Hi TV, włącz się«. Innymi słowy, rejestrują każdą naszą rozmowę do momentu wyłączenia. (…) Co gorsza, treści nagrywane po wydaniu polecenia uruchomienia telewizora nie są szyfrowane”[16]. W polityce

[13] *Telewizory mają wbudowane kamery szpiegujące! Śledzą twój każdy ruch,* https://newsbook.pl/2018/02/16/telewizory-maja-wbudowane-kamery-szpiegujace-sledza-twoj-kazdy-ruch/ (dostęp: 31.03.2020 r.).

[14] https://patentimages.storage.googleapis.com/4f/0b/4d/84f8b560d4d1d9/US20150116196A1.pdf (dostęp: 31.03.2020 r.).

[15] *Telewizory mają wbudowane kamery…*

[16] K. Mitnick, R. Vamosi, *Niewidzialny w sieci. Sztuka zacierania śladów,* Pascal, Bielsko-Biała 2017, s. 341.

prywatności firmy można odnaleźć następujący zapis dotyczący omawianej kwestii: „Sterowanie urządzeniem SmartTV oraz obsługa jego wielu funkcji są możliwe przy użyciu poleceń głosowych (...) W celu zapewnienia funkcjonalności rozpoznawania mowy niektóre polecenia głosowe (wraz z informacjami o urządzeniu, w tym jego identyfikatory) mogą być wysyłane do zewnętrznej usługi (…) Dodatkowo Samsung może gromadzić polecenia głosowe i towarzyszący zapis tekstowy rejestrowane przez Twoje urządzenie (…). Pamiętaj, że jeśli wypowiadane przez Ciebie słowa obejmują dane osobowe lub inne poufne informacje, znajdą się wśród informacji zapisanych i wysłanych zewnętrznemu podmiotowi”[17]. Oficjalnie firma nie ujawnia nazwy zewnętrznego podmiotu, natomiast wspomina o niej K. Mitnick: „Samsung pobiera te dane nie tylko na własne serwery, ale przekazuje je również firmie Nuance, dostarczającej oprogramowanie do rozpoznawania głosu. I to właśnie one będą dysponować przechwyconymi od ciebie informacjami (…). A jeśli zdradzisz coś sprzecznego z prawem? Wówczas istnieje duże prawdopodobieństwo, że firmy te zawiadomią organy ścigania. Gdybyś już wcześniej znalazł się w kręgu zainteresowania policji, funkcjonariusze mają prawo zażądać od nich – na podstawie nakazu sądowego – udostępnienia pełnych zapisów twoich rozmów. A potem usłyszysz: »Przykro nam, wpadłeś przez swój smart-telewizor…«”[18].

Często zapominamy, że współczesne smart-telewizory to w rzeczywistości komputery o nieco innym przeznaczeniu. Oprócz tego, że posiadają gniazdo do podłączenia z Internetem i/lub moduł WiFi, są także wyposażone w typowe dla komputerów porty USB. Dzięki nim można podłączać do telewizora zewnętrzne nośniki danych. O ile dbamy o własne komputery PC, instalując w nich oprogramowanie antywirusowe i firewalle, o tyle w przypadku telewizorów takich możliwości już nie posiadamy i w kwestiach bezpieczeństwa jesteśmy zdani na zabezpieczenia zaimplementowane do odbiornika TV przez producenta. Podłączony zewnętrzny nośnik danych może stać się przyczyną zainfekowania odbiornika wirusem. Na tym jednak nie koniec. Potencjalnie istnieje taka możliwość, że podczas cyberataku hacker uzyska dostęp nie tylko do telewizora, ale również do zgromadzonych danych na zewnętrznym nośniku. Warto w tym miejscu nadmienić, że problemy poruszone do tej pory dotyczą także innych producentów smart-telewizorów. „Telewizory LG zbierają nie tylko informacje o oglądanych przez ich posiadacza kanałach, ale nawet nazwy plików przechowywanych na nośnikach USB. Może się to odbywać również wówczas, gdy

[17] M. Maj, *Telewizor Samsunga podsłuchuje i wysyła dane innej firmie,* http://di.com.pl/telewizor-samsunga-podsluchuje-i-wysyla-dane-innej-firmie-51465 (dostęp: 31.03.2020 r.).

[18] K. Mitnick, R. Vamosi, *Niewidzialny…,* s. 342.

w ustawieniach telewizora funkcja zbierania danych jest wyłączona”[19]. Fakt ten zauważa również K. Mitnick w książce *Niewidzialny w sieci*: „Testując smart-telewizor LG, jeden z ekspertów zauważył, że za każdym razem, gdy użytkownik zmienia kanał, informacja ta przesyłana jest za pośrednictwem Internetu do producenta. Telewizor ma w ustawieniach domyślnie włączoną funkcję *Collection of watching info* (zbieranie informacji o oglądanych kanałach). Informacje te zawierają między innymi nazwy plików zapisanych na zewnętrznym dysku USB podłączonym do telewizora, na którym mogą się znajdować na przykład zdjęcia z rodzinnych wakacji. Dodatkowo badacze wykonali kolejny eksperyment – stworzyli własne nagranie, zapisali je na dysku USB, a następnie podłączyli go do telewizora. Analizując ruch sieciowy, zauważyli, że nazwa tego pliku wideo została przesłana w niezaszyfrowanym ruchu http pod adres GB.smartshare.lgtvsdp.com. Firma Sensory, producent narzędzi do rozpoznawania mowy przeznaczonych dla inteligentnych produktów, uważa, że wolno jej jeszcze więcej. »Jesteśmy zdania, że fenomen [inteligentnych telewizorów] polega na tym, by urządzenia te cały czas czuwały i słuchały – przyznaje Todd Mozer, dyrektor generalny Sensory. W obecnej chwili to [ciągłe nasłuchiwanie] jest jeszcze niemożliwe, bo pochłania zbyt dużo energii. Samsungowi udało się opracować niezwykle inteligentne rozwiązanie w postaci trybu czuwania. My chcemy jednak pójść o krok dalej i sprawić, by urządzenia słuchały nas przez cały czas, bez względu na to, gdzie jesteśmy«”[20].

Smartfon

Telefon komórkowy przeszedł długą ewolucję od 1973 roku, by stać się współcześnie smartfonem. Z danych statystycznych wynika, że w 2019 roku liczba abonentów telefonii komórkowej (8,3 mld abonamentów na całym świecie)[21] przekroczyła liczbę ludności, która wynosiła 7,6 mld. Tylko z powyższych danych wynika, że smartfon jest urządzeniem powszechnego użytku, a w jego posiadaniu (statystycznie) jest każdy mieszkaniec Ziemi. Telefon komórkowy to już wielofunkcyjne urządzenie integrujące ze sobą: telefon, książkę telefoniczną, aparat fotograficzny, kamerę wideo, cyfrowe albumy ze zdjęciami, komunikator internetowy, nawigację satelitarną, skaner odcisków palca, a nawet latarkę.

[19] M. Maj, *Telewizory LG ostro szpiegują widzów, nawet gdy użytkownik wyłączy śledzenie?,* http://di.com.pl/telewizory-lg-ostro-szpieguja-widzow-nawet-gdy-uzytkownik-wylaczy-sledzenie-49122 (dostęp: 31.03.2020 r.).

[20] K. Mitnick, R. Vamosi, *Niewidzialny…,* s. 343–344.

[21] Zob.: *Number of mobile (cellular) subscriptions worldwide from 1993 to 2019,* https://www.statista.com/statistics/262950/global-mobile-subscriptions-since-1993/ (dostęp: 10.05.2020 r.).

Oczywiście wymienione funkcjonalności zostały wbudowane w urządzenie, a jego i tak już duże możliwości poszerzają dziś już miliony aplikacji, które można doinstalować na własnym urządzeniu. Pytanie, które stawiamy w tym miejscu, brzmi: jakie inne niż te przypisane do telefonu funkcjonalności są przez niego jeszcze wykonywane? – chociaż ściślej byłoby pytać o oprogramowanie, bo to ono w rzeczywistości odpowiada za to, co zostanie przesłane z naszą lub bez naszej wiedzy do innych podmiotów. Z badań przeprowadzonych przez Francuskie Narodowe Centrum Informatyczne wynika, że naruszeń prywatności jest nadspodziewanie dużo. Przypomnijmy, że o funkcjonalności współczesnego telefonu decydują trzy komponenty. Są nimi:

- system operacyjny,
- przeglądarka internetowa,
- aplikacje[22].

Na każdym z tych poziomów możliwe jest ingerowanie w dane wrażliwe użytkownika. „Użytkownik jest »szpiegowany« z wielu stron – przez operatora infrastruktury telefonii komórkowej, producenta urządzeń – ale informacje na jego temat zbierają także system operacyjny i wreszcie aplikacje”[23].

Pierwszy komponent, tj. system operacyjny, stanowi punkt wyjściowy, bowiem na tym poziomie odbywa się konfiguracja urządzenia. Tutaj właśnie użytkownik (wyraża zgodę) na wykonywanie przez urządzenie określonych akcji. Między innymi przypisuje się do telefonu: konta mediów społecznościowych, konta Google, adresy e-mail, zezwalamy na automatyczne aktualizacje systemu, tworzenie kopii zapasowych kontaktów, galerii ze zdjęciami itd., a wszystkie na ogół te informacje gromadzone są w chmurze. Konfigurujemy również wbudowane w smartfon dodatkowe urządzenia typu: mikrofon, kamera, żyroskop, czytnik biometryczny czy GPS. Każde z tych urządzeń może dostarczać producentowi urządzenia określonego rodzaju danych, w tym także tych wrażliwych.

Przeglądarka internetowa też stanowi cenne źródło informacji o użytkowniku. W 2018 roku „użytkownicy smartfonów Vivo NEX odkryli, że po otwarciu niektórych aplikacji, w tym przeglądarki chińskiego giganta internetowego Tencent – QQ, aparat samoczynnie wysuwa się z obudowy. W odróżnieniu od większości innych telefonów komórkowych, w których kamera może aktywować się bez wiedzy użytkownika, Vivo NEX posiada mały aparat na górnej części urzą-

[22] Zob.: S. Czubkowska, A. Pawluć, *Szpieg, którego kochamy. Co wie o tobie twój smartfon,* https://serwisy.gazetaprawna.pl/nowe-technologie/artykuly/1071166,smartfon-dane-osobowe.html (dostęp: 10.05.2020 r.).

[23] Ł. Ostruszka, *Jak sprawdzić, co wie o nas smartfon, i jak pozbawić go tej wiedzy,* https://www.polityka.pl/tygodnikpolityka/ludzieistyle/1776896,1,jak-sprawdzic-co-wie-o-nas--smartfon-i-jak-pozbawic-go-tej-wiedzy.read (dostęp: 10.05.2020 r.).

dzenia, który wysuwa się, gdy jest włączony i chowa, gdy telefon z niego nie korzysta. (…) Inny użytkownik smartfona Vivo NEX odkrył, że po zainstalowaniu aplikacji Baidu aparat w telefonie oraz funkcja nagrywania dźwięku aktywowała się za każdym razem, gdy otworzył on jakąkolwiek aplikację – włączając w to przeglądarki czy komunikatory – które umożliwiają wprowadzenie wiadomości tekstowych”[24].

Wyszukiwane w Internecie frazy w połączeniu z danymi lokalizacyjnymi zebranymi przez BTS'y pozwalają algorytmom SI określić miejsca, w których najczęściej przebywamy, poznać nasze zainteresowania, upodobania, określić stopień naszej aktywności i w konsekwencji w dość prosty sposób zbudować profil użytkownika, po to, by zarzucić go w odpowiednim czasie spersonalizowanymi reklamami. „Tak naprawdę użytkowników smartfonów nie inwigiluje się po to, żeby poznać pikantne szczegóły ich życia, bo przecież nikogo Kowalski nie interesuje, ale po to, żeby jak najwięcej zarobić na reklamach, które są do Kowalskiego kierowane. Sprofilowane reklamy są lepsze i cenniejsze, więc konieczne jest pozyskanie wiedzy o użytkownikach”[25]. „Potentatami na rynku reklamy internetowej są dwa koncerny – Google, a właściwie Alphabet (taką nazwę ma od kilku lat konglomerat), i Facebook, czyli właściciel największego portalu społecznościowego na świecie, z którego korzysta ponad 2 mld osób. Agencja GroupM, czołowa grupa mediowa należąca do reklamowego potentata WPP, obliczyła, że w 2017 r. aż 84% globalnych wydatków na reklamę w Internecie trafiło właśnie do Facebooka i Google”[26]. Według Associated Press problem „dotyczy około dwóch miliardów urządzeń z Androidem na pokładzie i siłą rzeczy kolejnych setek milionów użytkowników iPhone'ów. Google śledzi nas nawet wtedy, gdy w ustawieniach prywatności odznaczymy opcje lokalizacji i śledzenia! Doniesienia te zostały już potwierdzone przez informatyków z uniwersytetu Princeton”[27].

Trzeci z komponentów jest chyba najwrażliwszym elementem systemu składającym się na funkcjonalność telefonu komórkowego. W konfrontacji człowiek – urządzenie, na ogół ten pierwszy stanowi najsłabsze ogniwo[28]. Od

[24] *Jak chińskie smartfony podsłuchują swoich użytkowników,* https://zaufanatrzeciastrona.pl/post/jak-chinskie-smartfony-podsluchuja-swoich-uzytkownikow/; przytoczoną sytuację można zobaczyć na filmie w popularnym serwisie YT pod adresem: https://www.youtube.com/watch?v=D8y4fRPVBCw&feature=youtu.be (dostęp: 26.04.2020 r.).

[25] https://niebezpiecznik.pl/post/polityka-jak-sprawdzic-co-wie-o-nas-smartfon/?similarpost (dostep: 10.05.2020 r.).

[26] Ł. Ostruszka, *Jak sprawdzić, co wie o nas…*

[27] J. Snoch, *Google śledzi nas czy tego chcemy, czy nie, https://www.komputerswiat.pl/aktualnosci/internet/google-sledzi-nas-czy-tego-chcemy-czy-nie/9v045mx* (dostęp: 10.05.2020 r.).

[28] Warto sięgnąć do publikacji najsłynniejszego i na szczęście już byłego hakera Kevina Mitnicka pt. *Sztuka podstępu.* We wstępie do wydania polskiego możemy przeczytać: „Autorzy

rozwagi użytkownika zależy, co zadecyduje się zainstalować na własnym urządzeniu i jakich uprawnień udzieli instalowanej aplikacji. Chociaż, jak wynika z przywoływanego już francuskiego raportu[29] Narodowego Centrum Informatycznego, „zainstalowane na telefonach aplikacje najczęściej uzyskiwały dostęp do danych na temat lokalizacji użytkownika. Takie zapytania stanowiły 30% wszystkich prób zdobycia prywatnych danych podczas testu. Niektóre z wykorzystywanych przez użytkowników telefonów programów podchodziły do tematu szczególnie gorliwie. Chociażby oficjalna aplikacja Facebooka – u jednego z użytkowników zanotowano 150 tys. zapytań o położenie w ciągu 3-miesięcznego okresu testów. Częściej niż raz na minutę – non stop, przez cały czas! A nie była ona nawet rekordzistką – w innym przypadku oficjalny sklep Google Play sprawdzał miejsce przebywania użytkownika 10 razy na minutę. Równie chętnie korzystały z tych danych inne aplikacje, nawet jeżeli same nie zbierały ich tak często. Wykorzystywały jednak to, czego mogły dowiedzieć się o właścicielu telefonu – przede wszystkim do serwowania mu dopasowanej do jego zainteresowań reklamy. Autorzy raportu podają przykład zainstalowanego przez samego producenta telefonu programu, który sprawdził miejsce przebywania użytkownika ponad milion razy w ciągu zaledwie miesiąca. Chociaż, powiedzieć można, dane te zbierane są tylko w teoretycznie niegroźnych celach reklamowych, to pamiętać trzeba, że sposób ich użycia może być różny”[30].

Internet rzeczy (IoT)

Koncepcja *Internetu rzeczy* (ang. *Internet of Things*, IoT), pojawiła się już w 1991 roku, a jej twórcą był Mark Weiser[31], natomiast po raz pierwszy ów termin został użyty w Stanach Zjednoczonych przez Kevina Ashtona w roku

przedstawiają metody genialne w swojej prostocie, a dzięki licznym przykładom uświadamiają czytelnikowi, jak potężną bronią jest inżynieria społeczna i do czego może doprowadzić umiejętne jej stosowanie przez intruza. Z drugiej strony, pokazują jak katastrofalne w skutkach może być lekceważenie tej wiedzy, zarówno przez duże korporacje, jak i pojedynczych ludzi”.

[29] W badaniach udział wzięło dziesięć osób, które w ciągu trzech miesięcy użytkowały powierzone im smartfony wyposażone w narzędzie Mobilitics. Celem specjalnie przygotowanego do badań narzędzia było rejestrowanie każdego przypadku, gdy aplikacja uzyskiwała dostęp do jakichkolwiek danych użytkownika. Ponadto Mobilitics rejestrował każdorazowe przesłanie takich danych na zewnętrzny serwer. Użytkownicy w badaniach skorzystali ze 121 aplikacji, a telefony eksploatowali jak swoje własne.

[30] *Co wie o tobie twój telefon z Androidem? To przerażające*!, https://tech.wp.pl/co-wie-o-tobie--twoj-telefon-z-androidem-to-przerazajace-6034835236930689a (dostęp: 10.05.2020 r.).

[31] Zob.: R. Tadeusiewicz, *Internet rzeczy – co wynika z tego, że użytkownikami Internetu staną się też przedmioty?,* „Utrzymanie Ruchu” 2017, nr 1, s. 28.

1999[32]. Trudno znaleźć jedną jednobrzmiącą definicję IoT, natomiast w literaturze przedmiotu odnajdujemy szereg definicji opisowych. Przykładowo *Internet rzeczy* opisuje się jako: „sieć fizycznych przedmiotów (rzeczy), które dzięki wbudowanym czujnikom i dostępowi do Internetu mogą komunikować się zarówno między sobą, jak i z człowiekiem. IoT wykorzystują praktycznie wszystkie branże: od motoryzacji po medycynę"[33]. Według firmy Cisco Internet Business Solutions Group (IBSG) „Internet Rzeczy jest po prostu momentem, w którym więcej »rzeczy lub przedmiotów« jest podłączonych do Internetu niż ludzi"[34].

Polskie Ministerstwo Cyfryzacji IoT opisuje jako: „falę innowacji wykorzystujących sieć inteligentnych przedmiotów (obiektów wyposażonych w zdolność do przetwarzania danych i kooperacji), której istotą jest nie tylko zaspokajanie znanych dzisiaj potrzeb. Podobnie, jak miało to miejsce w przypadku pierwszej »rewolucji internetowej«, mamy również do czynienia z kreowaniem nowych obszarów zastosowań, nieoczekiwanych zachowań konsumenckich i nowych modeli biznesowych. Jest to z pewnością obszar ogromnych szans, choć również wielkiego ryzyka charakterystycznego dla masowych fal innowacji"[35]. Dodajmy, że według prognoz Cisco w 2020 roku liczba podłączonych do Internetu urządzeń podwoi się w stosunku do 2015 roku i osiągnie wartość 50 miliardów[36]. Mimo braku jednobrzmiącej definicji, intuicyjnie rozumiemy, co kryje się pod określeniem *internetu rzeczy*.

Równolegle do terminu *Internet rzeczy* funkcjonuje jeszcze termin *Internet wszechrzeczy*, którym często zastępuje się ten pierwszy, chociaż nie są to terminy tożsame. Przez *Internet wszechrzeczy* (ang. *Internet of Everything*, IoE) rozumie się „sieć łącząca ludzi, procesy, dane i przedmioty, dająca zupełnie nowe możliwości. Kolejne etapy rozwoju technologicznego, w tym mobilna rewolucja, cloud computing i przetwarzanie big data, uzupełniając się, pozwalają na korzystanie z zalet IoE"[37]. Wzajemne relacje pomiędzy ludźmi, procesami, danymi i przedmiotami pokazano na rys. 1.

---

[32] Zob.: E. Kwiatkowska, *Rozwój Internetu rzeczy – szanse i zagrożenia*, „internetowy Kwartalnik Antymonopolowy i Regulacyjny", 8/3/2014, s. 61.

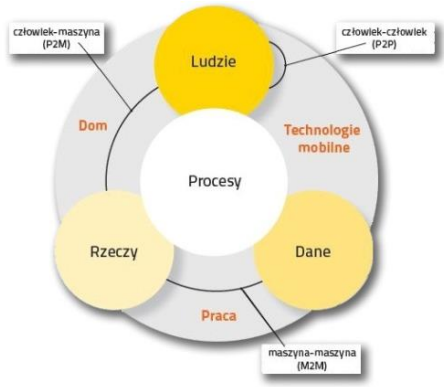
[33] N. Hatalska (red.), *Smart…,* s. 44.

[34] D. Evans, *The Internet of Things. How the Next Evolution of the Internet Is Changing Everything*, Cisco Internet Business Solutions Group (IBSG) 2011, s. 2.

[35] Ministerstwo Cyfryzacji, *Internet rzeczy*, https://www.gov.pl/web/cyfryzacja/internet-rzeczy (dostęp: 10.05.2020 r.).

[36] Por.: D. Evans, *The Internet of…,* s. 3.

[37] S. Kuniszewski**,** *Internet wszechrzeczy – kolejna faza rozwoju internetu*, http://www.it-professional.pl/o-miesieczniku/ (dostęp: 10.05.2020 r.).



Rys. 1. Relacje IoE

Źródło: S. Kuniszewski, *Internet wszechrzeczy…*

Z punktu widzenia problematyki, którą zajmujemy się w niniejszym opracowaniu interesuje nas przede wszystkim relacja człowiek – urządzenie, a mówiąc ściślej smart-dom. „System inteligentnego domu składa się zwykle ze swojego rodzaju serwera (jednostki sterującej) oraz kontrolowanych urządzeń – czujników i sterowników. Czujniki, jako urządzenia wejściowe (np. termometr), dostarczają do systemu dane potrzebne do podjęcia decyzji o sterowaniu urządzeniami wyjściowymi (np. ogrzewaniem). Podłączone urządzenia mogą być zarówno analogowe, jak i cyfrowe, często będące dodatkowym sterownikiem, wymagającym osobnego oprogramowania. Możliwe jest też sterowanie ręczne – z poziomu manipulatora (fizycznego urządzenia), aplikacji bądź strony web. Każdy z tych interfejsów pozwala również na konfigurację systemu zgodnie z oczekiwaniami użytkownika”[38]. Jakkolwiek postrzegamy nasze inteligentne otoczenie, to jednak zawsze dostrzeżemy analogię do komputera. Niech świadczy o tym definicja samego komputera „wszelkie obiekty przeznaczone do przechowywania danych lub komunikacji bezpośrednio związane lub współdziałające z takimi urządzeniami”[39]. Nie ma wątpliwości, że inteligentne domy wraz ze swoim elektronicznym wyposażeniem należą do tej właśnie grupy. Nie podajemy w wątpliwość, że inteligentne otoczenie, w tym smart – dom charakteryzuje wiele zalet. Przede wszystkim podwyższa komfort życia domowników, maksymalizuje funkcjonalność budynku oraz pozytywnie wpływa na gospodarowanie energią. Instalacja systemu inteligentnego domu niestety nie czyni użytkownika

[38] P. Pańczyk, J. Smołka, *Porównanie rozwiązań inteligentnego budynku na wybranych platformach sprzętowych,* „Informatyka. Automatyka. Pomiary w Gospodarce i Ochronie Środowiska” 2017/T7, nr 2, s. 58.

[39] M. Siwicki, *Cyberprzestępczość*, C.H. Beck, Warszawa 2013, s. 10.

autonomicznym. W dalszym ciągu pozostaje on uzależniony od zewnętrznych podmiotów branży IT. Jak twierdzi K. Mitnick „wraz z rozwojem tzw. internetu rzeczy (IoT) firmy takie jak Google, walczą o zdobycie w nim jak największego udziału, czyli o zostanie właścicielem platform wykorzystywanych przez inne produkty. Mówiąc krótko, dążą do tego, by urządzenia IoT korzystały przede wszystkim z ich usług. (…) Korzyść, jaka z tego wynika – przynajmniej dla Google – to dostęp do jeszcze większej liczby danych o użytkownikach i ich codziennych nawykach”[40]. O takiej strategii Google mówił już w 2006 roku Richard MacManus, zapowiadając dążenie do przechowywania 100% danych użytkownika dzięki nieskończonej przestrzeni dyskowej, a w tym: e-maile, historię online, zdjęcia, zakładki itp., które następnie będzie można udostępniać z dowolnego miejsca (dowolnego urządzenia, dowolnej platformy itp.)[41]. Zatem z jednej strony mamy do czynienia z polityką gromadzenia przez usługodawcę wszelkich możliwych informacji użytkownika, a tym samym i o użytkowniku, z drugiej zaś to realne zagrożenia natury techniczno-informatycznej wynikające z użytkowania systemu smart-dom. W tym miejscu wtrąćmy jeszcze jedną uwagę. Zakładając, że słowa R. MacManusa urzeczywistnią się, nasze domowe (firmowe) komputery staną się faktycznie tylko terminalami komputerowymi, a wszystkie wygenerowane przez użytkownika dane będą zlokalizowane poza jego własną jednostką centralną. Nietrudno wyobrazić sobie sytuację, kiedy z bliżej nieokreślonych powodów dostęp do własnych cyfrowych zasobów zostałby utrudniony, ograniczony lub uniemożliwiony. W obecnej dobie informacja jest takim samym jak każdy inny bądź nawet cenniejszym towarem. Dostęp do informacji w określonych okolicznościach np. dla firmy może decydować o jej przyszłości.

Powróćmy jednak do głównego wątku. Potencjalnym zagrożeniem dla tego rodzaju obiektów jest hacking, który można rozumieć na kilka sposobów: *sensu stricto*, czyli zachowanie polegające na uzyskaniu dostępu do systemu informatycznego lub danych komputerowych, *sensu largo*, a więc jako wszelkie zamachy na bezpieczeństwo systemów i danych informatycznych (czyli również np. zakłócenie pracy systemu informatycznego, modyfikacja lub zniszczenie danych komputerowych) oraz w znaczeniu najszerszym, potocznym – jako zbiorcze określenie praktycznie wszystkich przestępstw popełnianych w sieci (…)[42].

[40] K. Mitnick, R. Vamosi, *Niewidzialny…,* s. 333.

[41] Zob.: R. MacManus, *Store 100% – Google's Golden Copy,* ReadWriteWeb, 5.03.2006 r., https://web.archive.org/web/20110501063541/http://www.readwriteweb.com/archives/store_100_googl.php (dostęp: 10.05.2020 r.).

[42] R. Radoniewicz, *Odpowiedzialność karna za przestępstwo hackingu,* „Prawo w Działaniu. Sprawy Karne”, 13/2013, s. 122.

Wspomniane zagrożenia techniczno-informatyczne w zasadzie można sprowadzić do dwóch kategorii. Na pierwszą kategorię składają się nieprzemyślane działania użytkownika, natomiast druga kategoria to ingerencja osób trzecich w system informatyczny smart-domu. Zakładamy przy tym, że wszelkie instalacje zostały wykonane zgodnie ze sztuką. Przejdźmy zatem do pierwszej kategorii zagrożeń. Powszechnie wiadomo, że sterowanie automatyką domową może odbywać się z wykorzystaniem typowych już dziś urządzeń mobilnych, takich jak smartfony, tablety, laptopy. Zagubienie takiego urządzenia lub pozostawienie go bez nadzoru może skutkować przejęciem kontroli nad instalacją inteligentnego domu. Dość powszechnym grzechem użytkowników systemów informatycznych jest ustalanie wręcz banalnych haseł dostępu do własnych zasobów lub pozostawianie haseł fabrycznie nadanych przez producenta, a te są raczej powszechnie znane wśród hakerów. „Ważne jest również odpowiednie zorganizowanie elementów Smart Home, które może zwiększyć ryzyko utraty poufnych informacji. Przykładowo takie technologie wykorzystują usługi serwisu chmurowego do przechowywania informacji. Im większa liczba połączeń zewnętrznych, tym większa szansa wycieku informacji. Występuje również ryzyko, że usługodawcy, którzy zbierają informacje płynące z urządzeń Smart Home, a następnie je przetwarzają, mogą zostać wykupieni przez inne przedsiębiorstwa i nie do końca wtedy wiadomo, co może stać się z danymi”[43]. Z pewnością to tylko niektóre z ważniejszych uchybień ze strony użytkowników. Z obsługą urządzeń informatycznych jest tak samo jak z jazdą samochodem. Poruszający się po drodze mają prawo jazdy, zatem znają przepisy o ruchu drogowym, a jednak pomimo to liczba wypadków i kolizji drogowych jest w dalszym ciągu zbyt duża, a wynika to wprost z lekceważenia obowiązujących przepisów. Podobnie z urządzeniami informatycznymi, teoretycznie wszyscy wiedzą, jak powinni zadbać o bezpieczeństwo własnych danych, tylko mało kto stosuje się do takich zaleceń.

Druga kategoria zagrożeń w zasadzie wynika z pierwszej. „Specjalista ds. bezpieczeństwa IT Bruce Schneier w wywiadzie wyraził następującą opinię na temat *Internetu rzeczy*: »Przypomina mi do złudzenia branżę komputerową z lat dziewięćdziesiątych. Nikt nie przejmuje się bezpieczeństwem, nikt nie zawraca sobie głowy aktualizacjami, nikt nic nie wie. Sytuacja wygląda naprawdę nieciekawie i obawiam się, że kiedyś to wszystko runie z wielkim hukiem (…). Nie da się tego uniknąć – pojawią się niemożliwe do naprawienia luki w zabezpieczeniach, z których ochoczo skorzystają hakerzy«”[44]. Wśród najczęstszych zagrożeń ze strony hakerów można wymienić:

[43] *Bezpieczeństwo w inteligentnym domu* [*ANALIZA*], https://tech.wp.pl/bezpieczenstwo-w-inteligentnym-domu-analiza-6201059637847681a (dostęp: 10.05.2020 r.).

[44] Za: K. Mitnick, R. Vamosi, *Niewidzialny w sieci …,* s. 333–334.

– kradzież tożsamości – odbywa się w sposób pośredni na drodze włamania do baz danych dystrybutorów inteligentnych urządzeń. Z nich pozyskiwane są dane osobowe użytkowników, które następnie haker może wykorzystać w różny sposób.

– śledzenie lokalizacji – urządzenia mobilne (stacjonarne), za pomocą których steruje się smart-domem, jeśli zostały zainfekowane złośliwym oprogramowaniem mogą przekazywać dane lokalizacyjne w czasie rzeczywistym.

– smart-włamania – to włamania rzeczywiste. Złamanie zabezpieczeń lub wykrycie luk w oprogramowaniu w połączeniu z możliwością śledzenia lokalizacji daje hakerom możliwość bezproblemowego wtargnięcia do inteligentnego domu bez pozostawiana fizycznych śladów włamania.

Małe AGD też jest Smart

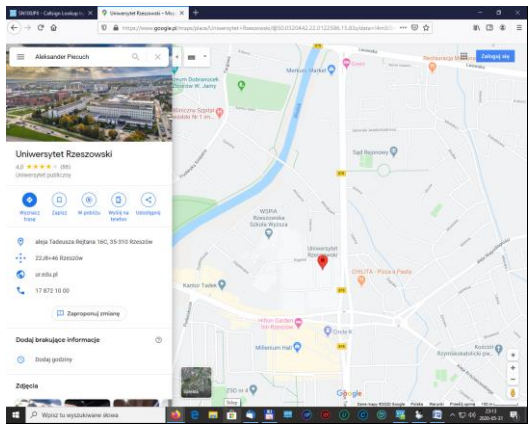
Prawdopodobnie nikt nie przypuszczałby, że artykuły AGD również mogą być narzędziami inwigilacji. Na opis takiego przypadku natrafiłem przeglądając strony internetowe związane z problematyką artykułu. Okazuje się, że robot kuchenny *Monsieur Cuisine Connect* sprzedawany w sieci Lidl – także na terenie Polski, posiadał wbudowany mikrofon. Jak donosi jeden z portali internetowych produktem zainteresował się francuski portal Numerama, który specjalizuje się w przeprowadzaniu testów urządzeń elektronicznych. Przy czym należy zaznaczyć, że proces testowania nie dotyczy tylko badania funkcjonalności urządzenia, ale urządzenie jest badane kompleksowo włącznie z jego demontażem i badaniem poszczególnych komponentów składowych. Testujący po rozłożeniu robota, stwierdzili zainstalowanie w nim mikrofonu podłączonego do panelu sterowania. Dla rozwiania wszelkich wątpliwości robot nie posiadał funkcji sterowania głosem, a dostarczana z produktem dokumentacja nie wspominała o wbudowanym module nasłuchującym[45]. W cytowanym artykule autor zawarł bardzo trafną własną konkluzję „To, że słuchać nas mogą także urządzenia małego AGD, jest jednak pewną nowością. Niestety, z takimi przypadkami niechcianej inwigilacji będziemy mieć do czynienia coraz częściej. Upowszechnianie się »internetu rzeczy«, czyli wyposażanie w moduły Wi-Fi nawet takich urządzeń jak pralki czy lodówki – a jak się okazuje dziś – także najmniejsze urządzenia kuchenne, którymi są roboty, będzie za sobą pociągać przynajmniej teoretyczną możliwość stałego, zewnętrznego monitoringu tego, co robimy w domu”[46].

[45] Zob. S. Tokarczuk, *Twój dom na podsłuchu. Jak inwigilują nas sprzęty domowe,* https://facetpo40.pl/nowoczesny-dom/twoj-dom-na-podsluchu-jak-inwigiluja-nas-sprzety-domowe/ (dostęp: 10.05.2020 r.).

[46] Tamże.

Usługi Google też są ciekawe

Jeśli nie wszyscy, to z pewnością większość z nas korzysta z map Googla, które z powodzeniem zaczynają wypierać z rynku nawigacje satelitarne. Wyznaczenie trasy z miejsca „A" do miejsca „B" jest czymś oczywistym, ale czy oczywiste jest, jeśli w miejsce wyszukiwanego adresu wpiszemy własne imię i nazwisko, a w odpowiedzi otrzymamy oznaczoną lokalizację własnego miejsca pracy? – rys. 2.



Rys. 2. Nieoczekiwany wynik wyszukiwania

Czy tak zdefiniowane przez firmę usługi nie idą zbyt daleko, ingerując jakby nie było, w dość prywatną sferę swoich użytkowników. Korzystający z usług poczty elektronicznej zapewne spotkali się również z sytuacją, w której użytkownicy są zachęcani do podania dodatkowych informacji na swój temat, np. adresu zamieszkania lub numeru telefonu – rys. 3, oczywiście – tylko dla bezpieczeństwa własnych danych.

Rys. 3. Dodatkowe informacje mile widziane

Na podstawie przewijających się informacji o firmie Google, chyba bez sprzeciwu zgodzimy się z opinią A. Szewczyk: „(…) Google wie o każdym z nas:

- Google wie, czego szukasz,
- Wie, co kupujesz,
- Wie, co czytasz,
- Wie, co Cię interesuje,
- Wie, co oglądasz,
- Wie, kto jest Twoim przyjacielem; wie, o czym z nim rozmawiasz,
- Wie, jakie masz poglądy,
- Wie, gdzie w danej chwili się znajdujesz,
- Wie, kto odwiedza Twoje strony internetowe,
- Wie, jak wyglądasz Ty i Twoi bliscy,
- Wie, jaką muzykę lubisz,
- Wie, co zamierzasz opatentować,
- Wie, jakie strony przeglądasz,
- Wie, jakie książki czytasz”[47].

SMART na ulicy

Do widoku kamer na ulicach miast zdążyliśmy się już przyzwyczaić. O ile do tej pory pełniły funkcje prewencyjne, o tyle teraz będą nas rozpoznawały na ulicach. Jak doskonali się technologia w tym kierunku widać na przykładzie Chin. „Naukowcy z dwóch chińskich uczelni stworzyli nową superkamerę, którą wyposażono w sensor o rozdzielczości 500 megapikseli. Urządzenie w czasie rzeczywistym jest w stanie monitorować dziesiątki tysięcy ludzi jednocześnie.

Nowa kamera Chińczyków zapewnia dokładność do pięciu razy lepszą od ludzkiego oka. Jeden z twórców, Xiaoyang Zeng, twierdzi, że urządzenie jest w stanie wykrywać ludzkie twarze i może znaleźć konkretne cele nawet na zatłoczonym stadionie. Sprzęt w trakcie monitorowania może wykonywać zdjęcia, a nawet nagrywać wideo”[48]. Również w Londynie mają zostać zainstalowane kamery miejskiego monitoringu do skanowania i rozpoznawania twarzy. Będą rozlokowane w pobliżu centrów handlowych i atrakcji turystycznych[49]. Nie trzeba dodawać, że system kamer pracuje pod nadzorem sztucznej inteligencji.

[47] A. Szewczyk, *Problemy moralne w świecie informacji,* Difin, Warszawa 2008.

[48] D. Długosz, *Chiny opracowały super kamerę 500 MP, która może śledzić tysiące osób jednocześnie,* https://www.komputerswiat.pl/aktualnosci/sprzet/chiny-opracowaly-super-kamere-500-mp-ktora-moze-sledzic-tysiace-osob-jednoczesnie/p4p8ftq (dostęp: 10.05.2020 r.).

[49] Zob. D. Długosz, *Londyn zainstaluje miejskie kamery do skanowania i rozpoznawania twarzy*, https://www.komputerswiat.pl/aktualnosci/wydarzenia/londyn-zainstaluje-miejskie-kamery-do-skanowania-i-rozpoznawania-twarzy/9ddt2d2 (dostęp: 10.05.2020 r.).

W każdym z wymienionych powyżej przykładzie uzasadnienie podjętych działań odwołuje się do bezpieczeństwa i identyfikowania osób mających problemy z prawem. Wobec tego wypada zapytać, czy jako ludzkość stajemy się coraz mniej cywilizowani? – jeśli trzeba „czuwać" nad każdym krokiem obywatela, a w każdym z nich upatrywać potencjalnego przestępcy.

Zakończenie

Użycie każdej technologii można uzasadnić w mniej lub bardziej prawdopodobny sposób. Nie ma większego znaczenia, czy opisane sytuacje mają miejsce już na naszym rodzimym gruncie czy nie. Jeśli nawet nie, to z doświadczeń minionych lat wiemy, że wcześniej czy później owe zmiany obejmą wszystkich, bo taka jest natura postępu (wyścigu technologicznego). Podążamy ślepo za wszelkiego rodzaju nowinkami technicznymi, nie zważając na konsekwencje podejmowanych decyzji. Bywamy nieświadomi, jaką faktycznie cenę płacimy za bycie nowoczesnym. Niestety, świat został tak urządzony, że nie ma w nim nic za darmo. Nawet jeśli jakiś podmiot świadczący usługę nie żąda za nią zapłaty, to wcale nie oznacza, że nie odbierze jej z nawiązką w innej i najmniej spodziewanej przez nas formie. W dobie smart-live już płacimy własną prywatnością. Kierunki rozwoju współczesnych technologii informatycznych i informacyjnych wyraźnie zmierzają w kierunku przejęcia pełnej kontroli nad obywatelem. Z cyfrowych baz danych, o każdym z nas będzie można uzyskać informacje: w jakie produkty się zaopatrujemy, co gotujemy, co jemy, na co się leczymy, w jakie leki zaopatrujemy się w aptece, czym się interesujemy, z kim się spotykamy, jakie programy telewizyjne oglądamy, o czym rozmawiamy w domu itd. Jesteśmy lub niebawem będziemy obserwowani wszędzie, we własnym mieszkaniu, na ulicy i w miejscu pracy. Czyżby na naszych oczach urzeczywistniała się Orwellowska wizja świata?

Bibliografia

Corcoran P., Datta S.K., *Mobile-edge computing and the Internet of Things for consumers*: *Extending cloud computing and services to the edge of the network*, "IEEE Consumer Electronic Magazine" 2016, Vol. 5, No. 4.

Evans D., *The Internet of Things. How the Next Evolution of the Internet Is Changing Everything*, Cisco Internet Business Solutions Group (IBSG) 2011.

Hatalska N. (red.), *Smart living,* Infuture Hatalska Foresight Institute, Gdańsk 2019.

Kwiatkowska E., *Rozwój Internetu rzeczy – szanse i zagrożenia,* „internetowy Kwartalnik Antymonopolowy i Regulacyjny", 8/3/2014.

Mitnick K., Vamosi R., *Niewidzialny w sieci. Sztuka zacierania śladów,* Pascal, Bielsko-Biała 2017.

Pańczyk P., Smołka J., *Porównanie rozwiązań inteligentnego budynku na wybranych platformach sprzętowych,* „Informatyka. Automatyka. Pomiary w Gospodarce i Ochronie Środowiska", 2017/T7, nr 2.
Perera Ch., Ranjan R., Wang L., Khan S., Zomaya A., *Privacy of Big Data in the Internet of Things Era*, IEEE IT Professional Magazine, PrePrint (Internet of Anything). Retrieved 1 February 2015;
Piecuch A., *Szkoła XXI wieku – problemy i wyzwania*, Wydawnictwo UR, Rzeszów 2019.
Program zintegrowanej informatyzacji państwa, Ministerstwo Cyfryzacji, Warszawa 2016.
Radoniewicz R., *Odpowiedzialność karna za przestępstwo hackingu,* „Prawo w Działaniu. Sprawy Karne" 2013, nr 13.
Siwicki M., *Cyberprzestępczość*, C.H. Beck, Warszawa 2013.
Szewczyk A., *Problemy moralne w świecie informacji,* Difin, Warszawa 2008.
Tadeusiewicz R., *Internet rzeczy – co wynika z tego, że użytkownikami Internetu staną się też przedmioty?*, „Utrzymanie Ruchu" 2017, nr 1.
Teklak R., *Co wie o mnie Facebook? Ściągnąłem dane i zdrętwiałem. Kasuję aplikację, która czyta nawet moje SMS-y*, Onet z 28.03.2018 r.

Netografia

Bezpieczeństwo w inteligentnym domu [*ANALIZA*], https://tech.wp.pl/bezpieczenstwo-w-inteligentnym-domu-analiza-6201059637847681a (dostęp: 10.05.2020 r.).
Ciszewski J., *Deepfake – co to jest*, https://publicrelations.pl/deepfake-co-to-jest/ (dostęp: 30.03.2020 r.).
Co wie o tobie twój telefon z Androidem? To przerażające!, https://tech.wp.pl/co-wie-o-tobie-twoj-telefon-z-androidem-to-przerazajace-6034835236930689a (dostęp: 10.05.2020 r.).
Czubkowska S., Pawluć A., *Szpieg, którego kochamy. Co wie o tobie twój smartfon,* https://serwisy.gazetaprawna.pl/nowe-technologie/artykuly/1071166, smartfon-dane-osobowe.html (dostęp: 10.05.2020 r.).
Długosz D., *Chiny opracowały super kamerę 500 MP, która może śledzić tysiące osób jednocześnie,* https://www.komputerswiat.pl/aktualnosci/sprzet/chiny-opracowaly-super-kamere-500-mp-ktora-moze-sledzic-tysiace-osob-jednoczesnie/p4p8ftq (dostęp: 10.05.2020 r.).
Długosz D., *Londyn zainstaluje miejskie kamery do skanowania i rozpoznawania twarzy*, https://www.komputerswiat.pl/aktualnosci/wydarzenia/londyn-zainstaluje-miejskie-kamery-do-skanowania-i-rozpoznawania-twarzy/9ddt2d2 (dostęp: 10.05.2020 r.).
Facebook ma już 16 lat. Wszystkie grzechy serwisu Marka Zuckerberga, https://www.geekweb.pl/inne/kartka-z-kalendarza/item/908-facebook-ma-16-lat (dostęp: 10.05.2020 r.).
https://arstechnica.com/tech-policy/2020/03/how-china-built-facial-recognition-for-people-wearing-masks/ (dostęp: 25.03.2020 r.).
https://datareportal.com/reports/digital-2019-poland (dostęp: 25.03.2020 r.).
https://mitsmr.pl/serie/czy-wiesz-ze/co-to-jest-deepfake/ (dostęp: 30.03.2020 r.).
https://niebezpiecznik.pl/post/polityka-jak-sprawdzic-co-wie-o-nas-smartfon/?similarpost (dostęp: 10.05.2020 r.).
https://patentimages.storage.googleapis.com/4f/0b/4d/84f8b560d4d1d9/US20150116196A1.pdf (dostęp: 31.03.2020 r.).
https://www.dobreprogramy.pl/mikolaj_s/Big-Data-gwaltownie-rosnie-ilosc-gromadzonych-danych, 67205.html (dostęp: 27.08.2017 r.).

Jak chińskie smartfony podsłuchują swoich użytkowników, https://zaufanatrzeciastrona.pl/post/jak-chinskie-smartfony-podsluchuja-swoich-uzytkownikow/; https://www.youtube.com/watch?v=D8y4fRPVBCw&feature=youtu.be (dostep: 26.04.2020 r.).

Kuniszewski S., *Internet wszechrzeczy – kolejna faza rozwoju internetu*, http://www.it-professional.pl/o-miesieczniku/ (dostęp: 10.05.2020 r.).

MacManus R., *Store 100% – Google's Golden Copy*, ReadWriteWeb, 5.03.2006r., https://web.archive.org/web/20110501063541/http://www.readwriteweb.com/archives/store_100_googl.php (dostęp: 10.05.2020 r.).

Maj M., *Telewizor Samsunga podsłuchuje i wysyła dane innej firmie*, http://di.com.pl/telewizor-samsunga-podsluchuje-i-wysyla-dane-innej-firmie-51465 (dostep: 31.03.2020 r.).

Maj M., *Telewizory LG ostro szpiegują widzów, nawet gdy użytkownik wyłączy śledzenie?,* http://di.com.pl/telewizory-lg-ostro-szpieguja-widzow-nawet-gdy-uzytkownik-wylaczy-sledzenie-49122 (dostep: 31.03.2020 r.).

Ministerstwo Cyfryzacji, *Internet rzeczy*, https://www.gov.pl/web/cyfryzacja/internet-rzeczy (dostęp: 10.05.2020 r.).

Number of mobile (cellular) subscriptions worldwide from 1993 to 2019, https://www.statista.com/statistics/262950/global-mobile-subscriptions-since-1993/ (dostęp: 10.05.2020 r.).

Ostruszka Ł., *Jak sprawdzić, co wie o nas smartfon, i jak pozbawić go tej wiedzy,* https://www.polityka.pl/tygodnikpolityka/ludzieistyle/1776896,1,jak-sprawdzic-co-wie-o-nas-smartfon-i-jak-pozbawic-go-tej-wiedzy.read (dostęp: 10.05.2020 r.).

Snoch J., *Google śledzi nas czy tego chcemy, czy nie,* https://www.komputerswiat.pl/aktualnosci/internet/google-sledzi-nas-czy-tego-chcemy-czy-nie/9v045mx (dostęp: 10.05.2020 r.).

Telewizory mają wbudowane kamery szpiegujące! Śledzą twój każdy ruch, https://newsbook.pl/2018/02/16/telewizory-maja-wbudowane-kamery-szpiegujace-sledza-twoj-kazdy-ruch/ (dostęp: 31.03.2020 r.).

Tokarczuk S., *Twój dom na podsłuchu. Jak inwigilują nas sprzęty domowe,* https://facetpo40.pl/nowoczesny-dom/twoj-dom-na-podsluchu-jak-inwigiluja-nas-sprzety-domowe/ (dostęp: 10.05.2020 r.).