Internet Rzeczy – czy mamy zacząć się bać?

Jarogniew Rykowski

Streszczenie: Wszyscy dostrzegamy dobre strony nowoczesnych technologii, spotykanych na każdym kroku: wygodę, stosunkowo niewielkie koszty, miniaturyzację i wszechobecną pomoc, coraz lepsze dopasowanie do człowieka. Modne ostatnio hasło Internetu Rzeczy znają wszyscy, którzy choć trochę mają do czynienia z nowinkami technicznymi. Internet Rzeczy tworzą urządzenia i systemy, które w założeniu mają pomagać ludziom. „Inteligentne" domy i miejsca pracy, ułatwiające wykonywanie codziennych i rutynowych czynności, a nawet zastępujące w tym człowieka stają się coraz widoczniejsze i popularniejsze, a ich cena nieustannie spada.

Jednakże, obok wielu zalet, Internet Rzeczy ma też ciemną stronę. W artykule przedstawiono szereg problemów związanych z masowym wykorzystywaniem niewidocznych i pomocnych urządzeń, wskazując, że na razie nie ma na nie skutecznego lekarstwa. Problemy te przede wszystkim są związane z szeroko rozumianym naruszeniem prywatności, brakiem odpowiedniej ochrony prawnej i organizacyjnej, zestawieniem rosnących możliwości technologii z jednoczesnym spadkiem jej widoczności przez potencjalnych użytkowników, związaną z tym coraz większą nieświadomością faktu świadczenia pomocy ze strony urządzeń, a także ekonomią i socjologią. Tekst jest jedną z pierwszych prób wskazania nietechnicznych ograniczeń Internetu Rzeczy oraz sygnalizacją potrzeby wprowadzenia zmian w sposobie jego wdrażania i wykorzystywania w życiu codziennym.

1. Wprowadzenie

W ostatnich latach nawet najwięksi sceptycy co do postępu technologicznego musieli przyznać, że Internet Rzeczy staje się codziennością. „Inteligentne" urządzenia i systemy, jeszcze kilka lat temu traktowane jako ciekawostka i obietnica bliżej nieokreślonej przyszłości, zostały zaakceptowane jako część naszego życia. Nikogo już nie dziwią pralki, które „mówią ludzkim głosem" i którym można wydawać głosowe polecenia, telewizory sterowane ruchem ręki zamiast pilotem, a nawet projekt autonomicznego samochodu, który można wynająć na godziny i który sam, bez udziału kierowcy, podjeżdża pod dom [1]. O ile jednak ciekawostki cieszyły się powszechną akceptacją, o tyle masowe wprowadzenie „inteligencji"[1] maszyn zaczyna uświadamiać społeczeństwu, że sama technologia to nie wszystko.

Czy ktokolwiek z czytających ten tekst zastanawiał się głębiej, jak duża jest ta „inteligencja" i komu ona w rzeczywistości służy? Podobnie jak nie zastanawiamy się, na czym polega zachowanie zwierząt, które odbieramy jako rozumne (na przykład reagowanie psa lub kota na polecenia głosowe, wyczuwanie nastroju, choroby itp.), tak do tej pory nie zapoczątkowaliśmy większej dyskusji na temat „rozumu" otaczających nas maszyn i komputerów. Wydaje się jednak, że nadszedł czas, w którym będziemy musieli z tym problemem się zmierzyć i go „ucywilizować", czyli w pierwszej kolejności przedyskutować i zrozumieć, a dalej ubrać w stosowne ramy prawne, organizacyjne i ekonomiczne.

Internet Rzeczy w takiej analizie wysoko stawia poprzeczkę. Do tej pory urządzenia komputerowe i maszyny mieliśmy pod pełną kontrolą. Nasz telewizor się sam nie włączy tylko dlatego, że wykryje naszą obecność w pokoju, tylko cierpliwie będzie czekać na wciśnięcie czerwonego przycisku na klawiaturze pilota. Nasz samochód także biernie czeka na nas w garażu lub na parkingu, co niestety oznacza, że zawsze wsiadamy do zimnego lub gorącego wnętrza (w zależności od pory roku i miejsca), które stanie się w miarę komfortowe dopiero po przejechaniu kilku kilometrów. Nasz komputer nie zredaguje za nas tekstu i nie zrealizuje przelewu bankowego, pozwoli nam tylko na uruchomienie odpowiednich aplikacji, które nam to umożliwią. Nawet tak „inteligentne" urządzenie jak smartfon nie poprowadzi za nas negocjacji biznesowych, nie zasygnalizuje, że na zakupy, za które właśnie zapłaciliśmy zbliżeniowo, nas po prostu nie stać, a nawet, że w czasie planowanego spaceru po parku przestanie działać, bo skończy się energia baterii, więc zawczasu przed wyjściem z domu powinniśmy je podłączyć do ładowarki.

Dopóki urządzenia są zauważalne i odpowiednio reagują na polecenia (na przykład w domu), mamy nad nimi kontrolę lub przynajmniej iluzję takiej kontroli. Dlaczego tylko iluzję? W celu wyjaśnienia warto wskazać kilka przykładów. I tak, przyjmujemy automatycznie, że kamera w wyłączonym telewizorze, która służy nam do sterowania wyborem programu za pomocą gestów rąk, jest wyłączona, podobnie jak kamera w naszym laptopie lub tablecie. Nie musi to być jednak prawda [2]. Więcej, niektóre systemy, takie jak analizator głosu lub gestów, muszą być cały czas aktywne, nawet jeśli urządzenie sprawia wrażenie wyłączonego. Jak inaczej moglibyśmy wydać polecenie włączenia telewizora lub pralki – analizatory są zmuszone obserwować otoczenie i nasłuchiwać poleceń, po rozpoznaniu których mają się uaktywnić. Jednocześnie muszą sprawiać wrażenie nieaktywnych, czyli utrzymywać iluzję. Dochodzi to tego,

że w większości urządzeń przycisk ich wyłączenia jest obsługiwany wyłącznie programowo – urządzenie bez względu na stan tego przycisku i tak jest aktywne (choć może wyłączyć pewne podzespoły, jak ekran telewizora lub smartfonu), może być także zdalnie pobudzone do pełnej aktywności.

Jeszcze gorzej z punktu widzenia szeregowego obywatela sytuacja wygląda w miejscach publicznych. O ile zdajemy sobie sprawę z obecności urządzeń w domu, bo najczęściej sami je kupiliśmy i uruchomiliśmy, o tyle urządzenia publicznego dostępu są całkowicie poza naszą kontrolą. Najczęściej w ogóle nie wiemy, że one istnieją, w najlepszym przypadku je ignorujemy. Kto na przykład zwraca uwagę na kamery monitoringu w sklepie, na przystanku czy też w tramwaju? Może to i dobrze, że nie mamy w większości przypadków świadomości funkcjonowania tych urządzeń, bo nie mamy na ich działanie jakiegokolwiek wpływu ani żadnych możliwości kontroli ich pracy, nawet jeśli praca ta wiąże się nierozerwalnie z naszą osobą. Nie możemy chociażby zablokować możliwości nagrywania naszej twarzy na wspomnianym wyżej przystanku lub w tramwaju, nie możemy uniemożliwić podsłuchania naszej rozmowy przez pokładowy mikrofon monitoringu tegoż tramwaju, nie możemy pozbawić naszego samochodu tablicy rejestracyjnej przy przejeździe przez każde skrzyżowanie w mieście z „inteligentnym" sterowaniem ruchem, która to tablica zostanie uwieczniona na zdjęciu lub filmie itd.

Nadszedł już jednak czas, żebyśmy rozpoczęli dyskusję na temat ogólnie rozumianej ochrony prywatności i bezpieczeństwa (naszego, nie urządzeń i systemów) oraz innych zagrożeń w kontekście wszechobecnego Internetu Rzeczy i jego „inteligentnych" urządzeń i usług. Niniejszy artykuł jest próbą zwrócenia uwagi na te problemy, ze wskazaniem na te technologie, które w najbliższej przyszłości (najprawdopodobniej) staną się z tego powodu kontrowersyjne, przynajmniej dla tej części społeczeństwa, które sygnalizowane w tekście problemy zacznie dostrzegać, może nawet postulować wprowadzenie zmian. Z powyższych względów w dalszej części tekstu szczególną uwagę poświęcamy modnym i szeroko dyskutowanym technologiom typu autonomiczny samochód, elektroniczne liczniki poboru energii, systemy monitoringu, systemy automatyki domowej, a dla porównania – także tak z pozoru dalekie od Internetu Rzeczy tematy, jak elektroniczne płatności i karty lojalnościowe.

2. Internet Rzeczy

U podstaw Internetu Rzeczy leżą badania amerykańskiego socjologa Marka Weisera. Pod koniec XX wieku sformułował on pewne twierdzenia, które potem przyjęły nazwę zasad Weisera. Zasady te mówią, że urządzenia powinny działać na zasadzie „dobrego służącego", który, sam niewidoczny, stara się ze wszystkich sił pomóc swojemu panu. Podobnie urządzenia powinny pozostać niezauważalne i uaktywniać się tylko w tych momentach, w których mają świadczyć pewne usługi ludziom [3].

Naturalną konsekwencją stosowania się projektantów urządzeń Internetu Rzeczy do zasad Weisera jest konieczność nieustannego śledzenia przez te urządzenia aktywności ludzi i zmian otoczenia. Im lepiej urządzenia śledzą ludzi, tym lepiej są w stanie określić ich potrzeby i tym lepiej śpieszyć im z pomocą. Urządzenia nie mogą się zapytać lub upewnić, że robią coś dobrze lub źle – mogą tylko wyciągać wnioski z obserwacji, która musi być dogłębna. Dodatkowo urządzenia mogą między sobą wymieniać wiedzę na temat ludzi i otoczenia.

Aby w pełni wyjaśnić zasady działania Internetu Rzeczy w kontraście do tradycyjnych systemów automatyki, posłużmy się przykładem automatycznego włącznika światła, który ma zaświecić lampę w przypadku stwierdzenia obecności ludzi w jej pobliżu. W tradycyjnym ujęciu lampa jest na stałe sprzężona (w automatyce mówimy – sparowana) z sensorem obecności (np. wykrywaczem ruchu). Sygnał z sensora włącza lampę, brak sygnału po określonym czasie ją wyłącza. Sygnał ten jest ważny tylko dla lampy i inne urządzenie (np. grzejnik lub wentylator) nie może z niego skorzystać, chyba że taką możliwość wprowadzi

projektant na etapie budowy instalacji.

W systemie Internetu Rzeczy też mamy sensor i lampę. Jednakże te urządzenia nie są ze sobą na stałe połączone, a tylko obserwują otoczenie. Sensor, po wykryciu ruchu, nadaje sygnał „stwierdzono obecność osoby". Sygnał ten dociera do wszystkich urządzeń w pobliżu, w tym do sterownika lampy. Sterownik ten ma za zadanie włączyć lampę po odebraniu takiego sygnału – robi to, ale nie musi wiedzieć, który sensor był odpowiedzialny za wysłanie tej informacji. Co takie podejście zmienia? Można powiedzieć, że wszystko. Po pierwsze, jeśli do pomieszczenia wniesiemy drugą lampę, reagującą na sygnały sensorów w ten sam sposób, lampa ta też automatycznie się zaświeci po wykryciu ruchu, bez jakiejkolwiek konieczności jej przeprogramowania lub parowania w nowym otoczeniu. Po drugie, jeśli do sensora ruchu dołożymy czujnik hałasu, to ten drugi też może generować sygnał wykrycia obecności osoby po wykryciu odgłosów ruchu lub rozmowy – znowu bez żadnych dodatkowych czynności akceptowany przez pobliskie lampy. Po trzecie, jeśli do tego dołożymy jeszcze czujnik poziomu oświetlenia, to sterownik lampy może sygnał tego czujnika też uwzględnić w swoim algorytmie pracy, jeśli wcześniej poinstruujemy nasz smartfon o preferencjach osobistych w zakresie poziomu jasności – smartfon rozgłosi te preferencje, wymuszając na lampie zmianę poziomu jasności itd. W ten sposób możemy zwiększać poziom "inteligencji" w pomieszczeniu stopniowo i przy minimalnym wysiłku – urządzenia znajdujące się blisko siebie „dogadają" się ze sobą i będą świadczyć usługi efektywniej, szybciej, lepiej itp., nawet w przypadkowych i z góry niedających się przewidzieć sytuacjach.

W teorii opisany wyżej sposób wymiany wiedzy przez urządzenia Internetu Rzeczy ma służyć człowiekowi, dokładnie temu, który znajduje się w pobliżu tych urządzeń i może skorzystać z ich usług. Jest to jednak tylko teoria – jak pokazuje życie, praktyka jest nieco inna. Pojawiają się dwie kwestie: co się dzieje z danymi, które urządzenia zbierają podczas rozpoznawania otoczenia po zakończeniu świadczenia usługi (np. gdy opuściliśmy wspomniane wyżej pomieszczenie) i kto jest ich właścicielem?

Nominalnie po zakończeniu świadczenia usługi dane monitoringu otoczenia przestają być potrzebne. Na przykład rozgłaszane przez smartfon preferencje jego właściciela służą tylko do określenia poziomu oświetlenia, poniżej którego nastąpi zaświecenie lampy. Zatem po podjęciu decyzji dane te powinny zostać usunięte z systemu. Co jednak w sytuacji, gdy ten sam człowiek wróci za chwilę do pomieszczenia, w którym w międzyczasie zgasło światło? System powinien szybko przywrócić poprzednie warunki świadczenia usługi. Może w tym celu ponownie wymienić określoną wiedzę w ramach zbioru urządzeń, ale może też skorzystać z poprzednich ustaleń, co w większości przypadków będzie prostsze i szybsze. Czyli dane, które jeszcze przed chwilą były zbędne, nagle znowu okazują się potrzebne. Zatem dane te powinny być gdzieś przechowane i udostępnione, gdy tylko będą ponownie potrzebne. Pytanie – gdzie je przechowywać i w jakim zakresie, kto za to zapłaci, a także kto będzie ten proces nadzorować?

Do głosu zatem, obok techniki, dochodzi ekonomia. W analizie ekonomicznej już na pierwszy rzut oka można zauważyć różne cele biznesowe dostawcy usługi i usługobiorcy. Jak już wspomniano, we własnym domu jesteśmy jednocześnie usługodawcą i biorcą, zatem problemu określenia własności i praw nie ma. Jednakże w miejscu publicznym te dwie funkcje ulegają całkowitemu rozdzieleniu – urządzenia należą do określonego operatora, świadczącego za ich pomocą pewne usługi klientom. Dane są przechowywane i przetwarzane zawsze po stronie operatora, a nie klienta. Można z dużym prawdopodobieństwem założyć, że cele biznesowe operatora i klienta są całkowicie różne. Ten pierwszy będzie chciał zarobić jak najwięcej pieniędzy jak najmniejszym kosztem, ten drugi będzie przede wszystkim dbał o swoją wygodę i bezpieczeństwo, co z kolei będzie mało znaczące dla tego pierwszego. W efekcie będziemy mieć sytuację bardzo niesymetryczną i niesprawiedliwą dla klienta – wszystkie mechanizmy kontroli będą po stronie operatora, więcej, być może klient w ogóle nie będzie sobie zdawał sprawy z faktu świadczenia usługi w danym miejscu i czasie, bo usługa ta będzie realizowana głównie dla osiągnięcia celów operatora, naruszając w tym celu prywatność użytkownika.

Stawiając powyższy problem inaczej, możemy się zapytać – czy publicznym urządzeniom Internetu Rzeczy można będzie wierzyć? Czy urządzenia te nie będą klientów/użytkowników oszukiwać, realizując cele swoich właścicieli? Czy zgromadzone przez nie dane posłużą tylko do lepszego świadczenia usługi, czy zostaną potem wykorzystane także w innych celach? Niestety, jest więcej niż prawdopodobne, że będzie to pole do nadużyć, w dużej mierze bezkarnych i z nikłymi możliwościami obrony.

Żeby lepiej zilustrować problem, posłużmy się prostym przykładem turysty, który szuka w nieznanym sobie mieście miejsca, gdzie mógłby coś zjeść. Tradycyjnie osoba taka pyta się przypadkowego przechodnia na ulicy: „Przepraszam, gdzie tu jest w pobliżu jakaś dobra restauracja?", raczej nie spodziewając się, bo i dlaczego, że zostanie oszukana i skierowana gdzieś indziej. Co najwyżej, w takich sytuacjach spodziewamy się, że się mogliśmy pomylić lub źle zrozumieć instrukcje, w razie niepowodzenia zrzucając winę na siebie. Nic też nie stoi na przeszkodzie, żeby o drogę zapytać się kilka razy i „wyciągnąć średnią" z uzyskanych porad.

Teraz załóżmy, że wykorzystujemy nasz smartfon, który rozgłasza w sieci lokalnej pytanie o pobliskie restauracje i odbiera odpowiedzi nadawane przez usłużne urządzenia Internetu Rzeczy, które znajdują się w pobliżu. Czy mamy szansę uzyskać w miarę wyważoną odpowiedź, być może nawet uwzględniającą opinie poprzednich użytkowników? Odpowiedź jest prosta – nie mamy takich szans. Urządzenia, które udzielą nam odpowiedzi, będą w tym miejscu umieszczone tylko w jednym celu – żeby zachęcić do odwiedzenia restauracji, do której są przypisane. Urządzenia te będą w pełni kontrolowane przez swych właścicieli i będą „łowić ofiary". Każde takie urządzenie będzie kłamać (to znaczy w języku biznesowym – przedstawi

nam bogatą i wyważoną ofertę marketingową), stwarzając przy tym pozory przypadkowości i prawdomówności. Sytuację mogłoby uratować jakieś zewnętrzne forum społecznościowe, niezwiązane biznesowo z właścicielami restauracji, które w miarę obiektywnie przedstawiłoby opinie poprzednich użytkowników. Jednak żeby skorzystać z takiego forum, trzeba znać punkt wejścia (adres serwera lub nazwę grupy dyskusyjnej), a także mieć czas na przeanalizowanie wypowiedzi poprzedników, nie mówiąc o połączeniu online z siecią publiczną.

Jak widzimy, stawianie prostych analogii między światem tradycyjnym („rzeczywistym") i kontrolowanym przez Internet Rzeczy jest dość ryzykowne. Zwróćmy dodatkowo uwagę, że w powyższym przykładzie pokazaliśmy tylko stronę klienta, pomijając w analizie inne cele, dla których warto postawić na urządzenia Internetu Rzeczy – ciągłe badanie rynku (urządzenie raportuje, kto i czego szuka w pobliżu, informując, jak dopasować ofertę do zmieniającej się sytuacji), personalny marketing (urządzenie, znając lub wnioskując z kontekstu o preferencjach klienta, jest w stanie przedstawić ofertę jak najatrakcyjniejszą z jego osobistego punktu widzenia, przy czym dla innej osoby chwilę później oferta może już być inna) itp.

Aby w pełni przedstawić problem, w następnym rozdziale tę prostą analizę przypadku pogłębiamy, odnosząc ją do konkretnych, ostatnio bardzo nośnych medialnie technologii.

3. Konsekwencje masowego użycia „inteligentnych" technologii i urządzeń

3.1. „Inteligentne samochody"

„Inteligentny samochód" – to hasło, ostatnio w połączeniu z „autonomicznością", wyznacza trendy w motoryzacji. Samochody są wyposażane w komputerowe systemy sterowania, które w razie potrzeby pomagają kierowcy lub nawet przejmują sterowanie pojazdem, żeby uniknąć katastrofy. Wyznacznikiem nowoczesności stają się trzy- i czteroliterowe skróty: ABS, EDS, ESP, ASR, ACC, BAS, GPS, BLIS, TPMS – to tylko wierzchołek góry lodowej. Elektronika i mikroprocesory znacząco wpływają na

Rys. 1. Znaki drogowe „poprawione" przez pogodę i „żartownisiów"

cenę nowoczesnego samochodu, część z wyżej wymienionych systemów jest wymagana prawem, a większość jest ceniona przez kierowców, którzy chętnie dopłacają do ceny, żeby móc wygodniej i bezpieczniej korzystać z pojazdu. Rodzina udogodnień nieustannie rośnie, a ceny systemów maleją dzięki miniaturyzacji, standaryzacji i masowemu zastosowaniu. Nikogo już nie dziwią takie propozycje, jak asystent parkowania, który sam ustawia samochód na parkingu, asystent linii na jezdni, który ostrzega o zjeżdżaniu z pasa ruchu, asystent awaryjnego hamowania, który może zapobiec stłuczce w miejskim korku, i inne podobne systemy. Na pewno nie można ich nazwać niezbędnymi (przecież przez prawie sto lat doskonale się bez nich obywaliśmy), ale zwiększenie wygody i bezpieczeństwa na skutek ich masowego wykorzystania nie jest już dziś przez nikogo kwestionowane.

Rozważmy nowoczesny pojazd, wyposażony w nawigację GPS, wspomaganie kierownicy, radary (tylny, czołowy i boczne), kamery monitoringu i podobne systemy, w tym układ wykrywający znaki drogowe i przekroczenie linii na jezdni, układ pomiaru zużycia paliwa, siły hamowania itp. Dopóki nic się nie stanie, taki samochód bardzo pomaga kierowcy – nie tylko pokazuje, gdzie ma jechać (nawigacja), ale także ostrzega o innych pojazdach w pobliżu (kamery i radary) oraz przypomina o przepisach (na przykład podaje informacje o ignorowanych lub niezauważonych przez kierowcę znakach drogowych) i ułatwia oszczędzanie paliwa.

Jednak wyobraźmy sobie, że samochód zostaje wyposażony w pewien zespół

decyzyjny, który ocenia postępowanie kierowcy i w razie potrzeby je koryguje. Na przykład asystent pasa ruchu automatycznie „prostuje" tor ruchu po przekroczeniu linii ciągłej i powiadamia o tym kierowcę sygnałem dźwiękowym, przyjmując, że zasnął on za kierownicą. Inny przykład – asystent hamowania uruchamia hamulec w momencie, gdy wykryje sylwetkę człowieka przed maską samochodu. Jednak co się stanie w przypadku, gdy spadł śnieg i na jezdni pojawiły się czarne koleiny, a pozostały śnieg wygląda jak linie? Dla człowieka jest to sytuacja trudna, ale zrozumiała na pierwszy rzut oka – pojedzie on tak, jakby nic się nie stało. Dla komputera będzie to przeszkoda nie do pokonania – przez całą drogę będzie on starał się „obudzić" kierowcę, więcej, może nawet podejmować aktywne próby zmiany toru ruchu pojazdu, co szybko będzie skutkować poślizgiem i wypadkiem, bo kierowca będzie machinalnie te próby kontrować. Podobnie asystent rozpoznawania znaków drogowych, który między innymi ma za zadanie uniemożliwić prowadzenie pojazdu z większą niż nakazana prędkością. Co się stanie, jeśli błędnie rozpozna on na drodze znaki, które wyglądają jak na rys. 1? A asystent hamowania – czy nie potraktuje zdjęcia modelki z przydrożnej reklamy jako kogoś, kto chce nagle wtargnąć na jezdnię i nie zahamuje pojazdu na środku drogi szybkiego ruchu, doprowadzając tym samym do zderzenia z pojazdem jadącym z tyłu?

Dopóki działanie wyżej opisanych systemów zamyka się we wnętrzu pojazdu, jest to dla kierowcy nieoceniona pomoc, i przymyka on oko na opisane powyżej niedogodności. Co jednak w sytuacji, gdy system zablokuje przyspieszenie na skutek rozpoznania znaku ograniczenia prędkości akurat w momencie wyprzedzania, gdy z naprzeciwka pojawi się inny pojazd? Czy programista tego systemu na pewno przewidział wszystkie takie sytuacje i zaprogramował odpowiednie reakcje? Czy system zachowa się jak człowiek, nie stosując się w sytuacjach awaryjnych do przepisów, czy też będzie ich przestrzegał bez względu na konsekwencje? Więcej, czy nasz samochód nie powiadomi policji, że przekroczyliśmy dozwoloną prędkość, a może nawet wystawi nam mandat?

To nie koniec – dane o naszych manewrach i sytuacji na drodze mogą być zapamiętane, a potem udostępnione na przykład policji lub ubezpieczycielowi, który na ich podstawie może mieć pretekst do odmowy wypłaty odszkodowania. Niektórzy producenci samochodów zaczynają już w nich montować „czarne skrzynki" na wzór podobnych systemów stanowiących obowiązkowe wyposażenie samolotów. „Czarna skrzynka" jest niedostępna dla właściciela samochodu, nie może on jej nawet wyłączyć ani uzyskać dostępu do zapisanych w niej danych. Jednocześnie dane, np. po wypadku, mogą świadczyć na niekorzyść kierowcy, który w ten sposób niejako składa sam przeciwko sobie obciążające go zeznania. Na podstawie danych uzyskanych z „czarnej skrzynki" ubezpieczyciel może ocenić styl jazdy kierowcy i odpowiednio zwiększyć (rzadziej – zmniejszyć) jego składkę [4].

„Czarna skrzynka" niekoniecznie musi być osobnym systemem, niezależnym od innych systemów pojazdu, czyli dodatkiem, który kierowca może, ale nie musi posiadać. Możliwa jest także sytuacja, w której zapamiętywanie danych z czujników odbywa się w komputerze pokładowym samochodu. Dane te mogą być następnie transmitowane online (z wykorzystaniem np. systemu pokładowego asystenta nawigacyjno-antykradzieżowego i transmisji GSM) lub offline (np. podczas cyklicznych wizyt kontrolnych w warsztacie) do producenta lub serwisanta samochodu, gdzie teoretycznie służą do lepszego poznania samochodu i ewentualnego wprowadzenia usprawnień. Kto jednak zagwarantuje, że dane te nie zostaną skopiowane przez nieuczciwego mechanika i nie posłużą do zanalizowania zachowania kierowcy pod kątem chociażby ustalenia dla niego indywidualnej stawki ubezpieczeniowej lub wyznaczenia dokładnego profilu marketingowego? Kto zagwarantuje, że właściciel floty samochodów nie będzie w ten sposób śledził swoich kierowców (co zresztą jest dziś nagminne, oczywiście w „trosce o ich bezpieczeństwo", choć z wykorzystaniem innych systemów śledzenia, za które trzeba płacić),

Rys. 2. „Inteligentny" licznik energii elektrycznej [5]

żona – męża (i odwrotnie) itp.? Czyli nawet jeśli nic się nie stanie i policja lub ubezpieczyciel nie będą dbali o odczyt „czarnej skrzynki", jej zapisy mogą być użyte przeciwko posiadaczowi samochodu, także całkowicie bez jego wiedzy.

Wybiegając dalej w przyszłość, rozważmy wykorzystanie samochodu autonomicznego, który nie potrzebuje kierowcy do poruszania się po drodze. Jest to już rzeczywistość, a nie tylko fantastyka naukowa, o której każdy z nas może przeczytać w gazecie, a nieliczni na razie szczęściarze – zobaczyć na własne oczy. Jednak nie wszyscy zdają sobie sprawę ze zmian, jakie wprowadzi masowe wykorzystanie tej technologii, zwłaszcza w połączeniu z napędem elektrycznym lub wodorowym. Takiego samochodu nie będzie się opłacało posiadać na własność – najlepiej będzie go wypożyczać do przejechania konkretnej trasy, tak jak dziś korzystamy z taksówek. O ile jednak taksówkarz zna nas tylko z jednego kursu i raczej tej informacji do niczego nie wykorzysta, o tyle pojazd autonomiczny zapamięta i łatwo zidentyfikuje klienta na podstawie adresu, identyfikatora przywołania lub metody płatności. Sieć pojazdów będzie zatem w posiadaniu dokładnych danych o tym, jak i gdzie jeżdżą jej klienci. Znowu: można takie informacje wykorzystać statystycznie do usprawnienia pracy sieci, ale można też sprzedać tym, których interesuje konkretna osoba lub jej profil marketingowy, może także pozycja biznesowa i rodzinna. Niektóre uzyskane w ten sposób dane będzie można wykorzystać w negocjacjach biznesowych lub nawet do szantażu.

Z podobną sytuacją mamy do czynienia w przypadku systemu eCall, który będzie obowiązkowo montowany

w nowych samochodach od marca 2018 roku[2]. System ten w założeniach ma bardzo szczytny cel – usprawnić pomoc dla ofiar wypadków przez wprowadzenie automatycznych powiadomień o zdarzeniu drogowym. Zdarzenie takie jest wykrywane po stwierdzeniu na przykład faktu odpalenia poduszki powietrznej i braku reakcji kierowcy na bodźce. Informacje o zdarzeniu, w tym miejsce i czas, są wysyłane o centrali, której pracownik może nawiązać zdalnie połączenie głosowe z pojazdem i w przypadku braku reakcji kierowcy wezwać odpowiednie służby. Do celów powiadamiania i łączności urządzenie eCall jest wyposażone w lokalizator GPS oraz mikrofon i głośnik, które można uaktywnić zdalnie. Jednak – powtarzając naszą analizę powyżej – kto zagwarantuje, że system nie będzie przesyłał danych nawet wtedy, gdy nie doszło do wypadku, umożliwiając tym samym niewykrywalne śledzenie pojazdu? W świetle uchwalonego w naszym kraju prawa o inwigilacji mogą to zrobić dowolne służby, a kierowca nawet po fakcie nie będzie o tym poinformowany. Więcej, kto zagwarantuje, że mikrofon nie zostanie zdalnie włączony, umożliwiając podsłuch wnętrza pojazdu? Przypominamy, że systemu tego nie będzie można wyłączyć, a kierowca nie będzie miał nad nim praktycznie żadnej kontroli. Ironiczne jest to, że najprawdopodobniej to sami kierowcy będą płacić za korzystanie z tego systemu (nie wiadomo jak – bezpośrednio, opłacając abonament GSM dla karty SIM, czy też pośrednio przez uiszczanie podatków), czyli niejako będą podsłuchiwani za własne pieniądze. Szkoda, że tak ważne decyzje zapadają bez udziału i wiedzy najbardziej zainteresowanych – czyli kierowców, z których większość nie zdaje sobie sprawy ze skutków masowego wprowadzenia tej usługi w życie.

3.2. „Inteligentne liczniki prądu" i inne udogodnienia „inteligentnego domu"

„Inteligentne liczniki prądu" to usprawnienie zafundowane obywatelom naszego kraju przez dostawców energii elektrycznej. Takie liczniki umożliwiają efektywniejsze i szybsze raportowanie zużycia energii przez gospodarstwo domowe lub przedsiębiorstwo (rys. 2), mogą też znacznie zmniejszyć czasokres rozliczenia – z miesięcy nawet do pojedynczych minut. Na pierwszy rzut oka jest to bardzo duża zaleta dla obu stron – rozliczającego i rozliczanego, być może pomijając tylko koszt wprowadzenia systemu, który prędzej czy później będą musieli pokryć klienci. Jednak jeśli zanalizujemy to zagadnienie trochę głębiej, to dojdziemy do kilku zaskakujących wniosków. „Inteligentny" licznik może mierzyć parametry linii zasilającej praktycznie w dowolnym odstępie czasowym, od milisekund do dni i tygodni. Jeśli okres pomiaru jest odpowiednio długi, dane są ujmowane statystycznie i zbiorczo, co zresztą jest podstawowym przedmiotem zainteresowania dostawcy (opłata za całość zużytej energii). Jeśli jednak okres pomiaru i raportowania zmniejszymy na przykład do milisekund, otrzymujemy na tyle dokładne dane o zużyciu energii w danym miejscu, że możemy określić typ, a nawet model odbiornika tej energii. Dalej, znając na przykład model telewizora, na podstawie charakterystyki poboru energii można nawet określić program, który przez ten telewizor jest aktualnie wyświetlany. Jest to wręcz wymarzone narzędzie dla firm zajmujących się reklamą telewizyjną, które mogą w ten sposób oceniać nie tylko popularność danych audycji, ale także określić indywidualny profil marketingowy klienta i jego podatność na reklamy. Pytanie, ile takie dane na temat każdego z nas będą warte i czy dostawca energii nie będzie ich sprzedawać (nie podlegają one ochronie prawnej, gdyż nie są danymi o charakterystyce personalnej, o których mówi ustawa o ochronie danych osobowych). Do ustalenia naszego profilu zresztą wystarczy informacja, z jakich urządzeń korzystamy i czy niedługo nie będziemy musieli/chcieli ich zmienić (np. lodówka jest starszego typu i konsumuje dużo energii – może reklama nowej energooszczędnej lodówki okaże się bardzo skuteczna?).

Podobnie inne instalacje „inteligentne" w naszym domu – dopóki informacje zbierane przez urządzenia i niezbędne do świadczenia przez nie usług nie opuszczą czterech ścian, jesteśmy bezpieczni. Jeśli jednak wydostaną się one na zewnątrz, staniemy się celem agresywnego marketingu personalnego – ktoś, znając nasze przyzwyczajenia i preferencje, będzie mógł je wykorzystać w swoich celach,

Rys. 3. Kamery systemu ITS [7]

prawie na pewno niezgodnych z naszymi.

Inny przykład – „inteligentny" telewizor ułatwi nam wybór programu do oglądania, ale też prześle komu trzeba informację, jakie reklamy wzbudziły nasze zainteresowanie (bo nie wyszliśmy w trakcie ich emisji do łazienki i ich nie przełączyliśmy pilotem). Wystarczy w tym celu analizować obraz z kamery zintegrowanej z odbiornikiem – kamera taka może wykrywać ruch, zliczać osoby znajdujące się w pomieszczeniu, a nawet sprawdzać, czy osoby te są wpatrzone w ekran. Takie śledzenie może także służyć użytkownikowi – na przykład jest możliwe „zamrożenie" filmu na czas pobytu w łazience. Jednak nigdy nie będziemy mieli pewności, czy kamera, której zadaniem miało być analizowanie gestów i wybór programów czy też zmiana głośności, nie prześle cyklicznie danych o naszym zachowaniu do bliżej nieokreślonego centrum. Zwróćmy uwagę, że wykorzystanie kamery do celów badania rynku jest znacznie skuteczniejsze niż metody tradycyjne, na przykład ankiety telefoniczne. Dodatkowo kamera analizuje zachowanie nieświadomych użytkowników, może wnioskować o ich zainteresowaniu (siedzą ze wzrokiem nieruchomo wpatrzonym w ekran, odwróciły się od ekranu i nie słuchają, rozmawiają lub robią coś innego – analizy takie mogą być w większości przypadków wykonywane automatycznie, nawet przy wykorzystaniu procesora sterującego telewizorem), o nastroju i odczuciach, o wrażeniach itp. Podobnie mogą zachowywać się panele reklamowe LED, które często widzimy stojące przy drodze – ich kamery, licząc wpatrzone w nie twarze i obserwując ruch mijających je ludzi, mogą ocenić skuteczność aktualnie wyświetlanej reklamy i siłę jej oddziaływania na słuchacza.

Idąc dalej, możemy sobie wyobrazić ofertę „telewizora za złotówkę" – odbiornika, którego użycie jest opłacane czasem oglądania reklam. W takim telewizorze obejrzenie na przykład filmu jest „nagrodą" za uważne wpatrywanie się przez określony czas w emitowane reklamy, co, jak pokazano powyżej, łatwo ocenić za pomocą aktualnie produkowanych i zainstalowanych w naszych domach urządzeń.

Ostatnim elementem, który warto przedyskutować, jest interfejs głosowy, w który wyposażane jest coraz więcej domowych urządzeń, nie tylko telewizorów, ale także pralek, kuchenek mikrofalowych i gazowych itp. W większości przypadków do realizacji takiego interfejsu wykorzystuje się zewnętrzne serwery oraz technikę „n-gram", która z grubsza polega na analizie prawdopodobieństwa występowania słów w kontekście konkretnej wypowiedzi [6]. Im więcej próbek głosu w takim systemie analizy, tym analiza ta jest dokładniejsza. Sposób ten stosuje na przykład firma Google w swoim asystencie/tłumaczu głosowym (*Google Voice Translate*). Aby zanalizować próbkę głosu, urządzenie nagrywa dźwięk i plik w odpowiednim formacie przesyła do serwera. Tam jest on analizowany, a wyniki analizy prawdopodobieństwa w postaci ciągu słów są odsyłane do urządzenia. Czyli w ogólności wszystko, co mówimy w domu, jest przesyłane do serwera – jest to podsłuch wręcz doskonały, a podsłuchiwana osoba najczęściej nie jest tego świadoma. Sytuacji nie zmienia wyłączenie urządzenia – interfejs głosowy działa w trybie ciągłym, gdyż jedną z obsługiwanych komend musi być uaktywnienie urządzenia, a bramka głosowa musi takie polecenie wykryć nawet mimo pozorów nieaktywności całego systemu. Pojawia się pytanie, czy dane uzyskane z podsłuchu są wykorzystywane tylko do celów ulepszenia analizy n-gramów, czy też są przedmiotem handlu na przykład w celu określenia profilu marketingowego klienta lub ich grupy, oceny popularności określonego produktu na podstawie analizy częstotliwości wypowiadania jego nazwy itp.?

3.3. Kamery i monitoring wizyjny

Nagrywanie obrazu przez kamery, zarówno w przestrzeni publicznej, jak i prywatnej, stało się naszą codziennością. Autor tego tekstu kilka lat temu podczas jednej z konferencji krótko podsumował ten trend, wskazując, że policjant, który do tej pory pytał świadków „kto widział wypadek", za chwilę będzie się pytać, kto go nagrał. Wtedy nie spotkało się to ze zrozumieniem, ale od pewnego czasu jest to praktycznie norma. Dziesięć lat temu na ulicach nie było tylu urządzeń, które potrafią nagrywać filmy i robić zdjęcia, nie było to też naturalnym odruchem, tak jak dziś – widząc niecodzienną sytuację, odruchowo chwytamy za smartfon i próbujemy uwiecznić tę chwilę. Kamery monitoringu zainstalowane w firmach, a nawet domach prywatnych są już tak mnogie, że praktycznie nie do policzenia, nawet w skali małego miasta. Duża część kierowców instaluje też kamery w pojazdach, żeby w razie wypadku mieć dowód swojej niewinności, co oznacza, że prawie cała przestrzeń publiczna, szczególnie na terenach miejskich, jest nieustannie monitorowana, oczywiście bez udziału i wiedzy „nagrywanych".

Na wykorzystanie kamer przez policję większość z nas patrzy przez pryzmat amerykańskich filmów, w których dzielni funkcjonariusze służb specjalnych w mgnieniu oka i po błyskawicznym wpisaniu komendy na klawiaturze (koniecznie na klawiaturze i koniecznie bardzo szybko – zwykłe ruchy myszką i wybór z menu nie są wystarczająco „filmowe") znajdują najbliższą kamerę w przestrzeni publicznej i uzyskują do niej natychmiastowy dostęp, dodatkowo uzyskany obraz magicznie powiększają i wyostrzają niemal w nieskończoność. Widzowie traktują to jako coś normalnego, ale to przecież olbrzymie naruszenie prywatności, praktycznie bez kontroli. Pytanie, kiedy filmy zaczną nas przyzwyczajać do instalacji kamer w domach i nieograniczonego dostępu do nich ze strony „uprawnionych" służb, oczywiście wszystko to w imię zwiększonego stopnia naszego bezpieczeństwa? Na razie to *science-fiction*, ale „Rok

1984" w latach 50. XX wieku też się taki wydawał, a dziś wszechobecność „Wielkiego Brata" już nikogo nie dziwi, więcej, zjawisko powszechnego podpatrywania i monitorowania jest raczej przedmiotem żartów, niż troski ze strony obywateli. Być może zmienimy zdanie dopiero wtedy, gdy nasza domowa kamera doniesie na nas do prokuratury, podobnie jak wspomniany wcześniej samochód, który sam z siebie wystawi nam mandat za zbyt szybką jazdę…

Wracając do kamer na ulicach – w wielu miastach wprowadza się systemy klasy ITS (ang. *Intelligent Transport Systems*) do optymalizacji ruchu drogowego, zarówno masowego (tramwaje i autobusy), jak i prywatnych samochodów. W ramach tych systemów kamery na głównych skrzyżowaniach rejestrują numery rejestracyjne przejeżdżających przez nie pojazdów, a także uwieczniają fakt wykroczeń drogowych typu wjazd na czerwonym świetle (rys. 3). Informacje te pozwalają następnie wyznaczyć tak zwane ścieżki ruchu, które w ujęciu statystycznym mogą posłużyć do usprawnienia działania świateł na skrzyżowaniach pod względem przepustowości, rozkładu jazdy komunikacji miejskiej, przewidywania i raportowania utrudnień drogowych, wyszukiwania „wąskich gardeł" transportowych itp., oczywiście dodając do tego wspomnianą powyżej możliwość karania niewłaściwie zachowujących się na drodze kierowców.

Dopóki informacje o numerach rejestracyjnych są przetwarzane wyłącznie statystycznie, system ITS jest bardzo użyteczny dla większości kierowców, oczywiście pomijając tych, którzy łamią prawo drogowe i zostaną na tym przyłapani. Jednakże kto zagwarantuje, że zgromadzone dane nie zostaną udostępnione osobom i firmom postronnym, przed czym nie chroni prawo?[3] Sytuacja z pozoru wydaje się niezbyt groźna – przecież każdy może stanąć na skrzyżowaniu, obserwować i zapamiętywać lub nawet zapisywać numery rejestracyjne mijających go pojazdów. Jednakże taka osoba zapamięta kilka numerów rejestracyjnych na czas kilku minut – kamera w tym samym miejscu zapamięta setki, jeśli nie tysiące pojazdów, praktycznie na zawsze (bo zapisze je w bazie danych), do tego doda możliwości wyszukiwania i grupowania faktów w celach analitycznych (np. jak „dobrymi" jesteśmy kierowcami z punktu widzenia agenta ubezpieczeniowego czy też policji). Jeśli dodamy do tego sygnalizowany wcześniej fakt, że dane te praktycznie nie podlegają ochronie prawnej, co więcej, jako dane publiczne są dostępne na każde żądanie i dla każdego, także potencjalnego przestępcy, to sytuacja staje się groźna. Analiza ścieżek ruchu konkretnego pojazdu pozwoli każdemu sprawdzić, kiedy statystycznie lub nawet realnie, czyli z wykorzystaniem analizy w czasie rzeczywistym, nie ma nas w domu, na przykład, żeby się do niego bezkarnie włamać.

3.4. Inne systemy monitorujące zachowanie i aktywność ludzi

Z podobnymi problemami jak opisane w poprzednich rozdziałach musieliśmy się już zmierzyć wcześniej, z różnym skutkiem. Poniżej pokazujemy szereg przykładów naruszania lub nadużywania danych prywatnych do celów biznesowych.

Niemal każdy z nas ma w portfelu co najmniej jedną kartę lojalnościową wybranego sklepu lub sieci. Karta taka oferuje pewne korzyści, na przykład zniżki w płatnościach lub specjalne towary w obniżonych cenach, w zamian za rejestrację zakupów w systemie. Dane o zakupach klientów są (w założeniu) przetwarzane statystycznie, głównie w celu uatrakcyjnienia oferty i zachęcenia do dalszych zakupów. Klient sklepu nie wie, gdzie, kiedy i w jakim celu dane zebrane za jego pośrednictwem będą wykorzystane, nie wie też, jaki zysk osiągnie z tego sklep. Jest to oczywiste naruszanie prywatności. Dodatkowo nie można być pewnym, czy dane na nasz temat nie zostaną sprzedane na zewnątrz (klient najczęściej podpisuje stosowną zgodę podczas rejestracji karty) i czy wtedy nie posłużą do wyznaczenia dokładnego profilu marketingowego, który może zostać wykorzystany do zachęcenia klienta do dalszych zakupów (także w innych sklepach). Jednakże większość klientów o to nie dba, skuszona „promocjami" i „specjalnymi ofertami" dostępnymi wyłącznie dla posiadaczy

kart – są to realne, a nie wirtualne korzyści, wyliczalne i obserwowalne.

Znacznie groźniejsze z punktu widzenia klienta jest śledzenie przeniesione z poziomu sklepu na poziom terminalu płatniczego. O ile w danym sklepie dokonujemy zakupu na przykład raz na tydzień, dane uzyskane z takiego śledzenia nie pozwalają na wyliczenie dokładnego profilu zakupowego klienta, więc są w zasadzie użyteczne tylko dla sklepu i to raczej w zbiorczym ujęciu statystycznym, o tyle zebranie takich danych dla wszystkich sklepów, w których klient dokonuje zakupów, pozwala już na zbudowanie bardzo dokładnego profilu, który może zostać wykorzystany w personalnym marketingu „na miejscu". Terminal płatniczy po przyjęciu płatności może sprawdzić w ogólnokrajowej bazie danych profil klienta i od razu zaproponować mu „w promocji" następne zakupy w sklepie w pobliżu, oferując zniżki lub inne zachęty. Taka forma promocji jest wyjątkowo skuteczna, bo wykorzystuje słabe punkty klienta, który na dodatek nie zdaje sobie sprawy z działania systemu i jego dalekosiężnych skutków, traktując „promocje" jako przypadkowe reklamy, które z jego punktu widzenia są wszechobecne. Zwróćmy uwagę, że takie postępowanie, mimo wątpliwej wartości etycznej, jest całkowicie zgodne z obowiązującym w naszym kraju prawem – numer karty bankowej nie jest daną osobistą i nie podlega ustawowej ochronie, a przetwarzanie imienia, nazwiska, adresu i innych danych personalnych w tym systemie jest bezprzedmiotowe, gdyż nie daje żadnych dodatkowych informacji. Jeśli jednak klient posługuje się tylko jedną kartą płatniczą (co jest regułą w Polsce), śledzenie wszystkich płatności kartą może dać bardzo dużo informacji o preferencjach i możliwościach zakupowych jej posiadacza. System jest skuteczny tak długo, jak długo klient nie uświadomi sobie, że jest „naciągany" na kolejne promocje – ma on jednak najczęściej zbyt mało wiedzy, żeby samemu dojść do takiego wniosku.

Inny przykład, który dobrze obrazuje nikły stopień świadomości klientów co do ochrony ich prywatności, to próba uzyskania odpowiedzi na proste pytanie: „Gdzie byłem i co robiłem dokładnie rok temu?" Prawie nikt z nas nie jest w stanie odpowiedzieć na takie pytanie z dokładnością do metrów (pozycja) i sekund (czas). A jednak nasz operator telekomunikacyjny nie miałby z tym najmniejszych kłopotów – pozycja telefonu komórkowego jest określana (w mieście) z dokładnością do kilkudziesięciu metrów, a uaktualniana w odstępie rzędu sekund. Jest to niezbędne do świadczenia usługi telekomunikacyjnej, a dane te nie mogą być udostępniane przez operatora na zewnątrz bez zgody zainteresowanego, zatem problem nie jest poważny i praktycznie nikt się tym nie przejmuje. Jednak takie naruszenie prywatności występuje i może być użyte przeciwko nam, chociażby jako dowód w sądzie.

Podobne pytanie: Kto wie o nas najwięcej? My sami? Nasza rodzina lub przyjaciele? Nie – najwięcej o nas wie Google! Dane są wykorzystywane oficjalnie do „lepszego świadczenia usługi wyszukiwania w sieci pod kątem zainteresowań danej osoby", tym niemniej system ten w praktyce pamięta wszystkie zapytania, jakie mu wydaliśmy w ciągu ostatnich lat. Więcej, Google wie także, gdzie byliśmy (o ile korzystamy z telefonu z Androidem), czym się interesujemy, z kim korespondujemy, jakie robiliśmy zakupy itp. Jest to bardzo duże, jeśli nie najpoważniejsze ze wszystkich opisywanych tutaj naruszenie prywatności, jednak każdy się na nie zgadza, albo go nie rozumiejąc w pełni (oczywiście do czasu), albo nie dbając o skutki (też do czasu – sieć niczego nie zapomina). Dlaczego więc Google nam nie płaci za dostęp do naszych danych, skoro zarabia na ich wykorzystaniu olbrzymie pieniądze? W ramach obsługi kart lojalnościowych sklepy dzielą się częściowo zyskami z klientem, operatorzy telekomunikacyjni muszą znać pozycję telefonu, żeby obsłużyć rozmowy telefoniczne, jednak Google ani nie dzieli się zyskami, ani nie musi personalnie wykorzystywać danych o swoich użytkownikach. Nie wiemy, w jakim zakresie to robi, nie wiemy, jakie są zyski z wykorzystania konkretnie naszych danych – co nie znaczy, że mamy się na takie postępowanie bezwarunkowo zgadzać.

Teraz wyobraźmy sobie, że powyższe zbieranie danych odbywa się nie raz na tydzień (zakupy kartą płatniczą) lub kilka razy dziennie (wyszukiwanie w Google czy też rozmowa przez telefon), ale wiele razy na minutę, na dodatek bez naszej świadomości – realizowane całkowicie automatycznie przez otaczające nas urządzenia Internetu Rzeczy i nasze urządzenia personalne typu smartfon. Określony w taki sposób profil klienta będzie niezwykle precyzyjny, można powiedzieć, że urządzenia będą o nas wiedzieć więcej, niż my sami wiemy o sobie. Dla przykładu: sklep, do którego zaraz wejdziemy, już w momencie wejścia będzie lepiej od nas wiedzieć, co w nim kupimy (bo będzie nami sterować, podsuwając oferty dokładnie dopasowane do naszego profilu). Oczywiście jest to sprawa przyszłości, pytanie – jak dalekiej? Na razie w analizie gigadanych na temat klientów dominuje podejście statystyczne, ale pojawienie się analiz personalnych jest tylko kwestią czasu.

Powyższe problemy niekoniecznie związane są *sensu stricte* z Internetem Rzeczy. Pokazują one jednak, że większość ludzi można przekonać nawet do udostępniania bardzo osobistych danych w zamian za mgliste i iluzoryczne korzyści, co w połączeniu z nowymi możliwościami technologii oraz praktycznym brakiem ochrony prawnej pokazuje, że sytuacja staje się bardzo poważna.

4. Ewolucja zagrożenia

Opisane w poprzednich rozdziałach systemy i przykłady ich wykorzystania jasno pokazują trend zmian – jest to ewolucja w stronę dokładnego określania profilu marketingowego i marketingu personalnego. Można się obronić, dopóki mamy świadomość zagrożenia, jednak im zagrożenie bardziej spersonalizowane, tym trudniej to zrobić lub tym mniejsze są chęci, żeby temu przeciwdziałać. Można powiedzieć, że im lepiej działa Internet Rzeczy, tym ryzyko staje się większe.

Personalny atak na naszą pozycję biznesową to w praktyce brak możliwości obrony. Jak wspomnieliśmy poprzednio, dla przykładu sklep będzie wiedzieć co kupimy, zanim jeszcze podejmiemy decyzję o zakupie, jeszcze w momencie

wejścia i rejestracji w tym czasie urządzenia personalnego. Zatem klienci już od wejścia (a nawet od wyjścia z samochodu na parkingu, który to samochód zostanie rozpoznany po numerze rejestracyjnym) zostaną podzieleni na lepszych i gorszych – tymi pierwszymi zainteresuje się doradca handlowy, usiłując ich nakłonić do zakupu „przypisanych" im towarów i usług, a tymi drugimi – strażnik, sprawdzając, czy nie zamierzają czegoś ukraść.

Inny poważny problem, pominięty w niniejszej analizie, stanowią ataki na same urządzenia Internetu Rzeczy i ich wykorzystanie przeciwko ludziom. Dla przykładu, ostatnio wykryto ataki typu „zombie botnet" realizowane nie przez komputery osobiste, ale przez urządzenia Internetu Rzeczy, nad którymi hakerzy przejęli kontrolę. W konsekwencji przestały działać takie serwisy, jak Amazon, Netflix, Twitter, ale również finansowa usługa PayPal. Na początku listopada hakerzy zablokowali system ogrzewania i dostawy ciepłej wody w dwóch inteligentnych apartamentowcach w Finlandii. To zaczyna przypominać scenariusz z głośnej książki „Blackout", która opisuje hipotetyczny, ale możliwy scenariusz ataku hakerskiego na dostawców prądu w Europie i USA, co skutkuje odcięciem prądu w niemal całym zachodnim świecie i nieuchronnie prowadzi do katastrofy [8].

Wnioski końcowe

Urządzenia Internetu Rzeczy oraz utworzone dzięki nim „inteligentne" miejsca, domy i systemy są dużą pomocą i udogodnieniem przez automatyzację codziennych i rutynowych czynności. Jednakże, obok ich niewątpliwych zalet, należy też podkreślać problemy związane z ich masowym wykorzystaniem, zwłaszcza duże niebezpieczeństwo utraty kontroli nad danymi personalnymi (przetwarzanymi przez „czarne skrzynki" i w chmurze), wysoką rozdzielczość danych o charakterystyce personalnej u operatorów, praktyczną niezauważalność faktu śledzenia (dla celów marketingu i monitoringu), nikłe możliwości reakcji, a przy braku świadomości – zerowe możliwości obrony, bez względu na wiedzę, pozycję, doświadczenie itp. Istotny jest też praktycznie całkowity brak odpowiedniej ochrony prawnej (na przykład numer karty bankowej nie jest daną osobistą i nie podlega ustawowej ochronie – śledzenie płatności kartą może dać bardzo dużo informacji o preferencjach i możliwościach zakupowych jej posiadacza). Niestety aktualna sytuacja, przede wszystkim porównanie praktycznie nieograniczonych możliwości technologii z bardzo ograniczonym prawem i niewielkimi indywidualnymi możliwościami obrony nie daje powodów do optymizmu.

Z drugiej strony urządzenia i dane personalne można wykorzystać np. w serwisach społecznościowych – wymieniając się opiniami, opisując własne odczucia, publikując porównania, ułatwiając innym wybór w zamian za inne porady – ogólnie wspólnymi siłami broniąc się przed nadużyciem możliwości technologii. Możemy także upowszechniać wiedzę na tematy szeroko rozumianego bezpieczeństwa i konieczności ochrony prywatności, czego wyrazem jest niniejszy tekst.

Przypisy

1. Autor celowo zaznacza umowność tego pojęcia w odniesieniu do maszyn, ujmując je w cudzysłów. Maszyny są tak „inteligentne", jak inteligentni byli ich projektanci. Nie można tu mówić o inteligencji w sensie klasycznym, możliwości uczenia się, wyciągania wniosków itp., nawet jeśli istnieją technologie, które udają, że są zdolne do takich zachowań. „Sztuczna inteligencja" jest w dalszym ciągu bardziej sztuczna, niż inteligentna.
2. W świetle analizy z niniejszego tekstu wypada się cieszyć, że data rozpoczęcia wdrożenia systemu eCall była sukcesywnie przekładana od roku (około) 2008–2009, być może także aktualnie wyznaczony termin na początku 2018 roku zostanie odsunięty w przyszłość.
3. Więcej – takie dane są gromadzone przez podmioty publiczne, a zatem w sposób praktycznie nieograniczony i z mocy prawa dostępne dla każdego, kto o nie poprosi. W niektórych analizach prawnych wskazuje się też, że numer rejestracyjny pojazdu nie podlega ochronie, gdyż nie jest klasyfikowany jako dana osobowa.

Literatura

[1] *Volvo – autonomiczne samochody dla Ubera.* Artykuł z serwisu moto.pl, http://moto.pl/MotoPL/1,88389,20580261,volvo-autonomiczne-samochody-dla-ubera.html, ostatni dostęp październik 2016.

[2] Jurczak T.: *Zaklejanie kamerki w laptopie? Lepiej kupić plaster na smartfon*. Artykuł z serwisu Gazeta Prawna, http://serwisy.gazetaprawna.pl/nowe-technologie/artykuly/941720,zaklejanie-kamerki-w-laptopie-lepiej-kupic-plaster-na-smartfon.html, ostatni dostęp październik 2016.

[3] Weiser M.: *The Computer for the 21st Century*. Scientific American Special Issue on Communications, Computers, and Networks, 1991.

[4] Szypulski P.: *Uważaj: Twoje auto to szpieg!* Artykuł z serwisu Auto Świat, http://www.auto-swiat.pl/eksploatacja/uwazaj-twoje-auto-to-szpieg-wyjasniamy-po-co-producentom-dane-o-autach-i-kierowcach/4e0b6d, ostatni dostęp październik 2016.

[5] *Rynek: pora na inteligentne liczniki energii*. Artykuł Polskiej Agencji Prasowej, http://nettg.pl/news/103326/rynek-pora-na-inteligentne-liczniki-energii, ostatni dostęp październik 2016.

[6] Rykowski J.: *Metody i narzędzia rozpoznawania mowy w zastosowaniach niekomercyjnych*. „Napędy i Sterowanie" 6/2014.

[7] *ITS „przyłapał" 30 tys. kierowców na czerwonym w Olsztynie*. Artykuł z serwisu Gazeta Olsztyńska, http://gazetaolsztynska.pl/277512,ITS-przylapal-30-tys-kierowcow-na-czerwonym-w-Olsztynie.html, ostatni dostęp październik 2016

[8] Kołodziej A.: *Cyberwojna jest w Polsce realnym zagrożeniem*. Artykuł z serwisu Money Wirtualnej Polski, http://www.money.pl/gospodarka/wiadomosci/artykul/cyberwojna-ataki-hakerskie-w-polsce,35,0,2188579.html, ostatni dostęp październik 2016.

Jarogniew Rykowski –
Katedra Technologii Informacyjnych;
Uniwersytet Ekonomiczny w Poznaniu;
e-mail: rykowski@kti.ue.poznan.pl