Małgorzata Gradek Lewandowska[1]

Internet rzeczy (IoT – Internet of Thing) i o innych zagrożeniach cyberbezpieczeństwa

(Czwarta część cyklu: „Technologie jutra już dziś w życiu rzecznika patentowego”[2])

W filmie Stevena Spielberga „Raport mniejszości” akcja dzieje się w roku 2054, gdy ludzkość jest w stanie zgromadzić tak wiele danych, że może przewidzieć przyszłość, pewną skłonność, wyeliminować sprawców zanim popełnią zbrodnię[3]. Dzisiaj to fikcja, ale czy na pewno tak zawsze będzie? Już teraz, dzięki danym pochodzącym od pacjentów i wykorzystaniu sztucznej inteligencji możliwe jest prognozowanie 80 chorób na rok przed ich wystąpieniem.[4] W tym celu nie wykorzystuje się jasnowidzów, ale sztuczną inteligencję. Ta predykcja nie byłaby możliwa, gdyby algorytmy AI nie mogły „uczyć się” na danych pozyskanych od chorych, zapisywanych przez urządzenia monitorujące stan zdrowia. Spektrum tych urządzeń jest szerokie: od złożonych systemów podtrzymywania życia czy prowadzenia badań klinicznych, do smart zegarków czy opasek treningowych (smart bandy), wag łazienkowych czy ciśnieniomierzy - monitorujących jeden parametr życiowy (np. temperaturę lub ciśnienie krwi) czy też całą gamę zachowań mających wpływ na zdrowie takich jak sen lub nawyki żywieniowe. Pozyskiwanie danych może obejmować pacjentów w przypadkach nagłych, lecz również tych cierpiących na

1 Małgorzata Gradek Lewandowska - radca prawny, rzecznik patentowy

2 Pierwsza część tego cyklu została opublikowana w numerze 1/2022 (str.61-72), druga część - w numerze 2/2022 (str.73-84) zaś trzecia część - w numerze 3/2022 (str.33-48)

3 Film S. Spillberga „Raport mniejszości” (Minority Report) z 2002 r. oparty został o opowiadanie P.K. Dicka o takim samym tytule opublikowane w 1956 r. w czasopiśmie „Fantastic Universe”

4 Raport Riccardo Miotto: https://www.researchgate.net/publication/303317731_Deep_Patient_An_Unsupervised_Representation_to_Predict_the_Future_of_Patients_from_the_Electronic_Health_Records [dostęp 30.12.2022]

choroby przewlekłe[5], czy osób starszych bądź leczonych najnowszymi metodami terapeutycznymi, takimi jak medycyna precyzyjna.[6]

Trudno wyobrazić sobie dzisiejszy świat bez tych urządzeń, bez Internetu czy po prostu bez smartfona. Technologia pozwalająca na gromadzenie i wymianę danych odgrywa ogromną rolę i nie można odmówić jej wielu zalet. Dzięki nim możemy kontrolować wiele parametrów, zautomatyzować reakcje. Niemniej, cyberprzestrzeń, w której dane są przesyłane, stanowi również źródło wielu zagrożeń, od tych, które mogą rozprzestrzeniać się „wirusowo" w celu szerzenia dezinformacji, aż po te, które służą wykradaniu naszych danych wrażliwych. Nie sposób pokazać wszystkich zagrożeń dla przedmiotów ochrony własności intelektualnej w świecie technologii. Stąd, skupmy się na przedstawieniu „Internetu rzeczy", z którego istnienia często nie zdajemy sobie sprawy i związanych z tym prawnych skutków.

Koncepcja Internetu rzeczy (**IoT – Internet of Thing**) zakłada powstanie globalnej, bezprzewodowej zintegrowanej sieci inteligentnych przedmiotów[7], czyli urządzeń i maszyn, najróżniejszych czujników i elementów mechanicznych, w której dokonuje się komunikacja z jednej strony pomiędzy przedmiotami, a z drugiej pomiędzy przedmiotami i ludźmi. Internet rzeczy to sytuacja, w której każde fizyczne urządzenie czy przedmiot codziennego użytku będzie mogło być włączone w globalną sieć i będzie mogło dostarczać różnorakich usług poprzez analizę potrzeb użytkowników i ich zwyczajów. Koncepcja bazuje na trzech kryteriach: Anytime (w każdej chwili), Anyplace (w każdym miejscu), Anything (wszystko)[8].

W raporcie stworzonym przez Grupę Roboczą działającą przy Ministrze Gospodarki[9] czytamy, że IoT *to* „sieć łącząca przewodowo lub bezprzewodowo urządzenia charakteryzujące się autonomicznym (niewymagającym zaangażowania człowieka) działaniem w zakresie pozyskiwania, udostępniania, przetwarzania danych lub wchodzenia w interakcje z otoczeniem pod wpływem tych danych. Jest to koncepcja budowy sieci telekomunikacyjnych i systemów informatycznych o wysokim stopniu rozproszenia, które służyć mogą między innymi tworzeniu inteligentnych

5 J.Greser „Etyczne problemy wdrażania medycznego Internetu rzeczy", PME 2020, Nr 3, Legalis [dostęp 30.12.2022]

6 J.Greser Cyberbezpieczeństwo wyrobów medycznych w świetle rozporządzenia 2017/745, IKAR 2020, Nr 2, Legalis [dostęp 30.12.2022]

7 Opinia Europejskiego Komitetu Ekonomiczno-Społecznego w sprawie komunikatu Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: „Internet przedmiotów – plan działań dla Europy" COM(2009) 278 wersja ostateczna (2010/C 255/21); Sprawozdawca: Zenonas Rokus Rudzikas

8 N.Gupta, J.Gupta, Internet of Things (IoT): A Vision of Any-Time Any-Place for Any-One, International Robotics & Automation Journal 2017, Vol.2, Issue 6.

9 IoT w polskiej gospodarce. Raport Grupy Roboczej do spraw Internetu Rzeczy przy Ministerstwie Cyfryzacji do pobrania z https://www.gov.pl/web/cyfryzacja/grupa-robocza-ds-internetu-rzeczy-internet-of-things-iot [dostęp 30.12.2022]

systemów kontrolnopomiarowych, analitycznych, czy układów sterowania, praktycznie w każdej dziedzinie życia, gospodarki czy nauki."

W innym ujęciu, to koncepcja architektury informatycznej, która umożliwia współpracę (interoperacyjność) różnorodnych systemów teleinformatycznych wspierających rozmaite zastosowania dziedzinowe i jest oparta na następujących warstwach:

- sprzęt – urządzenia (lub przedmioty w nie wyposażone), w szczególności sensory, elementy wykonawcze, ale także sterowniki, smartfony, tablety, laptopy czy komputery, które zdolne są do komunikacji i przetwarzania danych bez zaangażowania człowieka lub w ograniczonej z nim interakcji;
- komunikacja – infrastruktura telekomunikacyjna oraz sieć telekomunikacyjna (przewodowa lub bezprzewodowa), pracująca w oparciu o dowolne standardy transmisji danych o dowolnym zasięgu (tu Internet);
- oprogramowanie – systemy informatyczne urządzeń IoT oraz oprogramowanie służące do wymiany danych, ich przetwarzania, zarządzania systemem i jego zabezpieczenia;
- integracja – zbiory zdefiniowanych usług informatycznych zapewniających interoperacyjność oprogramowania na wszystkich poziomach architektury[10]

Konkretyzując, Internet rzeczy składa się z urządzeń i przekazów wirtualnych zapewniających:

- komunikację: sieć bezprzewodowa i przewodowa, podczerwień;
- pamięć: bazy danych, zdecentralizowane systemy rozproszone DHT[11];
- identyfikację: obraz video, kody, odczyty biometryczne, informacje z tagów i kodów kreskowych;
- lokalizację: sygnały GSM, GPS i procesy: serwis, sieci czujników, obsługa sieci)[12].

Zawarte w urządzeniach mechanizmy śledzące zbierają dane za pomocą różnych działań w sieci, m.in.:

- ustalanie lokalizacji;
- śledzenie działalności w sieci; śledzenie zachowań konsumenckich;
- dostęp do prywatności w sieciach społecznościowych; smartfonu;
- przejmowanie poczty e-mail;
- prywatność medyczna i genetyczna;

10 ibidem

11 ang.*Distributed Hash* Table, tł. rozproszona tablica mieszająca. Jest to rozproszony system używany do przechowywania informacji o dużych ilościach danych

12 A.Rot, B.Bleicke, Bezpieczeństwo Internetu Rzeczy. Wybrane zagrożenia i sposoby zabezpieczeń na przykładzie systemów produkcyjnych, Zeszyty Naukowe Politechniki Częstochowskiej Zarządzanie 2017, Nr 26, s. 189–190.

- bezpieczeństwo cybernetyczne;
- bańki informacyjne;
- Internet rzeczy;
- profilowanie użytkowników.

O ile na pierwsze punkty z listy mamy mniej lub bardziej realny wpływ, o tyle Internet rzeczy i profilowanie użytkowników z jednej strony ułatwią czy ratują życie, z drugiej powodują, że stajemy się źródłem danych dla wielkich korporacji. Przykładem może być wszczepienie programowalnego bionanochipa (*programable-bio-nano-chip)*, który może wykrywać choroby serca lub markery nowotworowe z próbki śliny pacjenta. Wszczepienie takiego chipa do ciała pacjenta, mogłoby zapewnić system wczesnego powiadamiania o tych chorobach, na długo przed odkryciem jakichkolwiek symptomów przez pacjenta. Dane te oczywiście trafiają do lekarza, ale co stanie się jeśli trafią do firmy ubezpieczeniowej?

Koncentrując się na dobrych stronach zastosowania IoT można wskazać inne przykłady z medycyny (np. zdalny monitoring pacjentów, reagowanie na sytuacje alarmowe, szybsze udzielanie pomocy, wspomaganie życia osób starszych i niepełnosprawnych). Tutaj pojawia się pojęcie *Health – Related Internet of Things* (H-IoT), które odnosi się do urządzeń wymagających zamontowania na ciele pacjenta. Będzie to dotyczyło zarówno urządzeń zintegrowanych na stałe, np. rozruszniki serca, jak i takich, które można łatwo usnąć, np. pompy insulinowe, opaski ułatwiające znalezienie osób cierpiących na zaburzenia pamięci[13] czy czujnik znajdujący się np. w zegarku, przyklejany do powierzchni ciała ale też wszczepiony chip[14]. Zastosowanie bezprzewodowego, zdalnego systemu monitorowania parametrów życiowych pacjenta pozwala na pomiar i transmisji danych przez Internet (audio lub wideo), a zebrane dane przekazywane są lekarzowi. Do najczęściej monitorowanych parametrów życiowych zalicza się m.in.: ciśnienie tętnicze, częstość pracy serca, saturację tlenem, temperaturę ciała, pojemność wydechową (pojemność płuc) i poziom glukozy we krwi.[15]

Ciekawy przykład podaje E.M.Kwiatkowska odnosząc się do pilotażowego programu monitorowania przyjmowania leków przez pacjentów. Zastosowanie silikonowych mikroczujników zamontowanych w tabletkach pozwala na monitorowanie przyjmowania przez pacjentów przepisanych leków. Z opisu przez nią przedstawionego wynika, że chip wielkości ziarenka piasku, umieszczony na każdej tabletce, zawiera niewielkie ilości miedzi i magnezu. Po połknięciu chipa, metale

13 J.Greser „Etyczne problemy wdrażania medycznego Internetu rzeczy", PME 2020, Nr 3, Legalis [dostęp 30.12.2022]

14 E.M.Kwiatkowska „Rozwój Internetu rzeczy – szanse i zagrożenia", IKAR 2014, Nr 8, Legalis [dostęp 30.12.2022]

15 Ibidem

w nim zawarte reagują z sokiem żołądkowym wytwarzając napięcie elektryczne. Impuls ten zostaje odczytany przez rejestrator medyczny umieszczony na powierzchni ciała (plaster naklejony na skórze). Dzięki wykorzystaniu telefonu komórkowego, rejestrator ten wysyła sygnał informujący o przyjęciu leku. W sytuacji, gdy pacjent nie zażyje przepisanych lekarstw, lekarz lub inna upoważniona do tego osoba – opiekun pacjenta, jest informowana i może zareagować. Rejestrator to właśnie ta „rzecz", która przesyła dane przez Internet.

Przykładami wykorzystania IoT spoza świata medycznego są systemy inteligentnych budynków (w zakresie sterowania automatyką domową, zapewniania bezpieczeństwa, dostarczania rozrywki, monitorowania domowników), inteligentne sieci energetyczne i czy sieci liczników (w zakresie dynamicznego rynku taryf energii elektrycznej, sterowania odbiornikami energii, sterowania i bilansowaniem źródeł odnawialnych), inteligentne miasta (sterowanie ruchem, monitorowanie dróg i zasobów, stanu środowiska, wspomaganie procesów biznesowych, wspomaganie handlu, bezpieczeństwo miast)[16]. Te ostanie *smart systemy* są przedmiotem zainteresowania Unii Europejskiej, która promuje m.in. „Inteligentne miasta" w ramach programu ramowego „Horyzont 2020". Celem tego programu jest zastosowanie technologii cyfrowych i telekomunikacyjnych do poprawy bezpieczeństwa i poprawy skuteczności tradycyjnych sieci i usług.[17] Przykładami takiego wykorzystania IoT są Mysłowice i Bydgoszcz. W Mysłowicach pojemniki na odpady zostały podpięte do Internetu i dzięki zastosowaniu działającej w oparciu o sieć mobilną 4G Orange Polska technologii CAT-M1 przekazują sygnał, że zostały zapełnione. W Bydgoszczy zamontowano na skrzyżowaniach ulic ponad czterdzieści szybkoobrotowych kamer CCTV, które wraz z ponad pięćdziesięcioma kamerami typu ANPR rejestrują cechy pojazdów co usprawnia zarządzanie ruchem.[18]

Pojazdy, zwłaszcza te nowoczesne wyposażone w elektronikę już teraz mogą generować ogromne ilości danych. Są to dane dotyczące sposobu jazdy, telemetrii, eksploatacji samochodu, warunków pogodowych lub drogowych, a nawet dane o zdrowiu kierowców (w przypadku systemów monitorujących stan kierowcy i ostrzegających przed zmęczeniem) lub o ich cechach biometrycznych (np. w przypadku niektórych funkcji sterowanych głosem lub informacji związanych ze stylem jazdy, np. używaniem hamulca.[19] Dane te mogą pozostawać w samochodzie, ale też są przesyłane do producenta. Jedno jest pewne: z założenia – mają być wymieniane z innymi użytkownikami dróg lub z infrastrukturą drogową

16 A. Brachman, Ekspertyza Obserwatorium ICT, Internet rzeczy – wybrane zastosowania, SO RIS, Sieć Regionalnych Obserwatoriów Specjalistycznych, Katowice 2015, s. 9

17 Europejska Agenda Cyfrowa, Digital Single Market, s. 7

18 M. Gadomski, Internet rzeczy dociera do miast. Uwaga na zagrożenia, https://www.portalsamorzadowy.pl/spoleczenstwo-informacyjne/Internet-rzeczy-dociera-do-miast-uwaga-na-zagrozenia,114495.html (dostęp: 1.1.2020 r.).

19 A.Szeliga, M.Kupczak-Strzelecka, M.Rudzińska „Connected cars – wybrane problemy i wyzwania regulacyjne", MOP 2020, Nr 20, Legalis [dostęp 30.12.2022]

(np. ostrzegając zbliżające się samochody o sobie lub odpowiednio modyfikując ustawienia świateł, aby zapewnić ich efektywny i bezkolizyjny przejazd). Różna może być technika czy technologia przekazywania danych: za pomocą instalowanych w samochodach urządzeń zapewniających transmisję danych przy wykorzystaniu sieci komórkowych (np. modemy LTE czy 5G), ale też urządzeń własnych kierowcy lub pasażera (np. smartfonów), które dzięki połączeniu z Internetem zapewniają łączność systemów samochodowych z zewnętrznymi systemami podmiotów trzecich, czy też za pomocą innych czujników instalowanych w samochodach.[20] Na przykład samochody marki Mercedes w ramach systemu SOS/eCALL przesyłają dane na serwer przedsiębiorstwa Bosch. Mogą więc stać się pewnego rodzaju „świadkami" w wypadkach drogowych[21].

Dane zbierane przez IoT podzielić możemy na te, które nie mają charakteru danych osobowych i nie stanowią jako takie zagrożenia dla prawa do prywatności (np. informacje o pogodzie) i takie, które wiążą się z przetwarzaniem danych osobowych (dane zbierane z social mediów, lokalizacji itd.). Zagrożeniami dla bezpieczeństwa użytkowników są niekontrolowana inwigilacja ludzi, działalność hakerów czy wrogie przejęcie kontroli nad urządzeniami.[22]

Inwigilacja zaczyna się zwykle niewinnie. Chcąc skorzystać z jakieś rzeczy czy aplikacji „płacimy" danymi najczęściej zezwalając na:

- dostęp do swoich kontaktów,
- dostęp do kalendarza,
- dostęp do historii przeglądanych stron i zakładek,
- dostęp do wrażliwych logów aplikacji systemowych,
- dostęp do aplikacji aktywnych na danym urządzeniu
- dostęp do historii wybieranych numerów,
- dostęp do wszystkich profili użytkownika na danym urządzeniu,
- dostęp do treści i metadanych wysyłanych SMS-ów,
- dostęp do załączników e-maili.

Dark patterns (w wolnym tłumaczeniu: „wredne praktyki")[23] to elementy interfejsów w aplikacjach i serwisach internetowych zaprojektowane tak, by skłonić użytkownika do wybrania opcji najkorzystniejszej dla firmy zarabiającej na

20 Ibidem

21 Prowadzi to do wprowadzenia nowego pojęcia: cyfrowego świadka (ang. digital witness), którym zwykle jest urządzenie osobiste potrafiące zidentyfikować i zebrać dowody cyfrowe.

22 O tym, że jest to problem faktycznie dotykający nas świadczy szybki przegląd prasy: https://cbzc.policja.gov.pl/bzc/aktualnosci, https://www.bankier.pl/wiadomosc/Poczta-Polska-Brak-powiadomienia-o-dostawie-oszusci-wysylaja-falszywe-maile-8050765.html czy https://www.bankier.pl/wiadomosc/NBP-utworzyl-departament-cyberbezpieczenstwa-8039336.html

23 https://panoptykon.org/sites/default/files/publikacje/panoptykon_raport_o_sledzeniu_final.pdf

komercjalizacji danych. Kolory, rozmieszczenie przycisków i sposób wyświetlania komunikatów mają doprowadzić do tego, że użytkownik (niekoniecznie świadomie) „zgodzi się" na głęboką ingerencję w prywatność (np. ciągłe śledzenie lokalizacji, czy dopuszczenie skryptów śledzących obsługiwanych przez podmioty trzecie).

Najczęściej stosowane *dark patterns*[24] to:

- niekorzystne dla użytkowników ustawienia domyślne,
- wydłużona ścieżka zmiany ustawień dla tych, którzy chcą zadbać o swoją prywatność,
- wyskakujące okienka z ustawieniami prywatności, w których kluczowe informacje zostały pominięte lub przedstawione w mylący sposób,
- grożenie utratą ważnych funkcjonalności lub usunięciem konta, jeśli użytkownik nie „zgodzi się" na przekazanie dodatkowych danych,
- interpretowanie nierzadko przypadkowych akcji (np. nieznacznego ruchu myszką) na korzyść aplikacji czy serwisu.

Dotychczasowe szacunki pokazywały, że wartość rynkowa ogółu danych przetwarzanych w Internecie na terenie Unii Europejskiej do 2020 r. to wysokość 739 miliardów euro.[25] Nawet jeśli szacunki te nie sprawdziły się, liczby są imponujące. Nic dziwnego, skoro badanie Eurobarometru pokazuje, że 60% Europejczyków, korzystających z Internetu, kupuje lub sprzedaje rzeczy on-line oraz korzysta z portali społecznościowych[26]. Pozostawiają przy tym swoje dane osobowe, w tym informacje biograficzne (prawie 90% badanych), informacje o swoim otoczeniu (prawie 50%) oraz informacje szczególnie chronione (prawie 10%). 70% badanych wyraziło obawy co do tego, w jaki sposób firmy korzystają z tych danych, oraz uważa, że ma jedynie częściową, jeśli w ogóle, kontrolę nad własnymi danymi. Natomiast 74% chciałoby, aby gromadzenie i przetwarzanie ich danych w Internecie wymagało ich wyraźnej zgody. Jednocześnie wg badania przeprowadzonego przez Kantar,[27] ponad połowa respondentów (zarówno w przypadku Polski, jak i Unii Europejskiej), obawia się, że ich dane osobowe w Internecie nie są chronione przez władze publiczne. Respondenci w wieku 25-39 lat (74%) oraz 40-54 lat (69%) częściej wyrażają taką obawę niż osoby w wieku 15-24 lat (52%).

Tymczasem urządzenia spokojnie zbierają nasze dane. Tworzony na podstawie zachowań w sieci profil człowieka nie zawiera danych bezpośrednio identyfikujących użytkownika, takich jak nazwisko czy adres. Te informacje z perspektywy reklamodawców mają niewielką wartość. Z punktu widzenia

24 Ibidem

25 Komisja Europejska, European Data Market Study, https://ec.europa.eu/digital-single-market/en/news/final-results-european-data-market-study-measuring-size-and-trends-eu-data-economy.

26 https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/yearFrom/1974/yearTo/2020/surveyKy/2207

27 http://www.tnsglobal.pl/archiwumraportow/files/2020/03/K.017_20_Czego-obawiamy-si%C4%99-w-sieci_EB.pdf

sprzedających dużo bardziej wartościowe się cechy decydujące o skłonności użytkownika do dokonania konkretnego zakupu. Na podstawie zebranych danych agencje mediowe ustalają, jakie cechy i zachowania charakteryzują osoby, które jeszcze reklamowanego produktu nie kupiły, ale mogą to zrobić w przyszłości. Budując profil potencjalnego klienta, agencje mediowe próbują ustalić nawyki, zainteresowania, słabości, ważne momenty z życia (takie jak ślub czy ciąża), cechy osobowościowe i demograficzne użytkowników, które posłużą do stworzenia kategorii powiązanych z cechami usługi czy produktu, który mają za zadanie sprzedać pewną potrzebę: „aktywny styl życia", „dom, zdrowe jedzenie", „przede wszystkim dzieci", „miejski styl życia, singiel" czy „ponadprzeciętny dochód, dobra luksusowe"[28].

Powstaje tzw. look-alike – hipotetyczny profil klienta[29] składający się z twardych danych pochodzących od reklamodawców („taki człowiek już u mnie kupił") i statystycznej wiedzy o ludziach („taki człowiek może chcieć to kupić"). W dużym uproszczeniu: gdy w sieci pojawi się użytkownik o konkretnych cechach zaczyna się licytacja o jego uwagę. Proces licytacji jest w pełni zautomatyzowany i z punktu widzenia profilowanego użytkownika pozostaje całkowicie niezauważalny – cała transakcja zajmuje 1/5 sekundy czyli 200 milisekund, a na mrugnięcie okiem przeciętnie potrzebujemy „aż" 300 milisekund. Następnie prezentowane są nam te komunikaty, które „powinnyśmy" otrzymać, skoro sieć zakwalifikowała nas jako „człowieka, który może chcieć to kupić".

Czy mamy jakikolwiek wpływ, aby ograniczyć przekazywanie danych o nas? Niewielki, jeśli wybieramy wygodę korzystania z urządzeń podłączonych do Internetu i sami "podłączamy" się do sieci. Trzeba być jednak świadomym tego, że ceną za wygodę tak korzystania Internetu, jak i z urządzeń podpiętych pod sieć, może być pełna inwigilacja. Nie jesteśmy zupełnie bezradni. Zwłaszcza, że niektóre możliwości kontroli czy ograniczenia zbierania prywatnych danych w Internecie są łatwe do zastosowania, takie jak:

- dostosowanie ustawień przeglądarki;
- dostosowanie ustawień poszczególnych serwisów;
- instalacja odpowiednich wtyczek zabezpieczających przed reklamami, ciasteczkami;
- korzystanie z usług zaufanego dostawcy;
- korzystanie z usług klienta pocztowego i szyfrowanie danych;
- szyfrowanie danych w ustawieniach komputera.

28 https://panoptykon.org/sites/default/files/publikacje/panoptykon_raport_o_sledzeniu_final.pdf

29 https://experienceleague.adobe.com/docs/audience-manager/user-guide/features/algorithmic-models/look-alike-modeling/understanding-models.html?lang=en

Oczywiście „kontrola" ze strony „maszyn" czasami może być przydatna jak wspomniane wcześniej przykłady medyczne czy jak dowód z nagrania Alexy. Popularny na całym świecie asystent głosowy Alexa opracowany przez Amazon, posiada wiele funkcjonalności, które można wywołać za pomocą komend głosowych. Alexa udzieli informacji na zadane pytanie a także umożliwi zdalne sterowanie różnymi domowymi urządzeniami oraz oświetleniem. Kompatybilne z Alexą są inteligentne głośniki Amazon Echo, które nadsłuchują i gromadzą dane. Jak się okazuje do tych danych wielokrotnie sięgali śledczy w trakcie oględzin miejsca zdarzenia[30].

Stąd trudno jednoznacznie ocenić IoT. Wykorzystanie zebranych danych jak i fakt ich przesyłania może mieć dobre i złe skutki. I tak, pompa powietrzna CPAP monitorująca sen osób cierpiących na zespół bezdechu przekazuje dane do ubezpieczyciela (zamiast do lekarza), który może odmówić wypłaty ubezpieczenia, jeśli pompa jest źle używana. Wspomniany Amazon Echo, to głośnik, który słucha i nagrywa rozmowy ingerując tym samym w prywatność. Podobnie, dane zbierane przez Fredi monitor dziecięcy, który transmituje dźwięk z pomieszczenia w którym przebywa dziecko, są źródłem wiedzy dla hakerów, z czego kilkukrotnie skorzystali[31]. Problemem jest najczęściej nie samo pozyskiwanie danych przez urządzenia IoT ale to gdzie te dane trafiają. Większość smart urządzeń wysyła dane na chmurę i niekoniecznie muszą to być serwery zlokalizowane w Polsce, a nawet w Unii[32].

W gronie rzeczników patentowych jedynie wspomnieć należy o ochronie rozwiązań o charakterze technicznym "zamkniętych" w urządzeniach IoT, o *design* tych urządzeń chronionym wzorami przemysłowymi, marketingu wzmocnionym dobrze prowadzoną strategią w zakresie ochrony i budowy renomy znaku towarowego dzięki czemu korzystamy z tych „rzeczy". O czynach nieuczciwej konkurencji i tajemnicy przedsiębiorstwa nie wspominając. A propos poufności: na razie stosunkowo niewiele danych z urządzeń IoT jest poddanych badaniom, co podkreślają badacze nazywając te niewykorzystane dane cyfrowe „ciemnymi danymi" (ang. *dark data)*[33] Jeśli zaś wierzyć statystykom to ok 52% wszystkich informacji wytwarzanych i przechowywanych przez organizację to dark data i szybko ta ilość rośnie. Prognozuje się, że w latach 2025-2030 poziomy danych wzrosną trzykrotnie[34].

Kwestie IoT i cyberbezpieczeństwa wiążą się z nurtem IBAC – *Internet of Things, Blockchain, Artificial Inteligence, Cybersecurity* – czyli problematyką maszyn

30 R.Prabucki „Prawo sztucznej inteligencji" pod red. prof. L.Lai, dr.M.Świerczyńskiego, Legalis [dostęp 30.12.2022] Rozdział XXI. „Inteligentne" rzeczy jako „świadkowie" w postępowaniu dowodowym

31 https://panoptykon.org/sites/default/files/publikacje/panoptykon_raport_o_sledzeniu_final.pdf

32 R.Prabucki „Prawo (…)"

33 Ibidem

34 https://www.slingshotsimulations.com/technical/dark-data-what-is-it/

cyfrowych. Tej problematyce poświęcony jest cykl „Technologie jutra już dziś w życiu rzecznika patentowego”, w tym dotychczasowe części cyklu zwracające uwagę na zagadnienia deepfake, Metaversum czy NFT. Omówienie nowoczesnych technologii byłoby niepełne, gdyby nie zostały zaprezentowane zagadnienia tematyki *Blockchain*. Obejmuje ona z jednej strony bazy rejestrów danych, z drugiej - platformy, na której działają programy nazwane „smart kontraktami”, zasilane nieczęsto danymi urządzeń IoT. O Blockchain więc w kolejnym artykule cyklu *„Technologie jutra już dziś w życiu rzecznika patentowego”.*