trzeci sektor
nr 53 (01/2021) www.kwartalnik3sektor.pl

[ARTYKUŁ RECENZOWANY]

Medyczny Internet rzeczy a organizacje pozarządowe – wyzwania prawne[1]

Medical Internet of Things and Non-Governmental Organizations – Legal Challenges

DOI
10.26368/17332265-53-1-2021-1

JAROSŁAW GRESER
Uniwersytet im. Adama Mickiewicza w Poznaniu
j.greser@greser.pl

WYDAWCY
Fundacja Akademia Organizacji Obywatelskich
Szkoła Główna Handlowa w Warszawie

SŁOWA KLUCZOWE
Internet rzeczy, wyroby medyczne, RODO, cyberbezpieczeństwo, nowe technologie

KEYWORDS
Internet of Things (IoT), medical devices, GDPR, cybersecurity, new technologies

ABSTRAKT

Celem artykułu jest przybliżenie problematyki prawnej wdrażania medycznego Internetu rzeczy w działania organizacji pozarządowych. Praca jest podzielona na trzy części. Pierwsza z nich, dotycząca pojęcia Internetu rzeczy i jego podtypu - medycznego Internetu rzeczy, ukazuje różnorodność tego zjawiska, szczególnie w formie wyrobów medycznych. Druga część pokazuje przykładowe zastosowania tych urządzeń w działaniach organizacji pozarządowych z użyciem istniejących technologii. Trzecia część odnosi się do prawnych aspektów tego zjawiska z perspektywy organizacji pozarządowej, zwłaszcza obowiązków wynikających z RODO i przepisów o cyberbezpieczeństwie, które należy uwzględnić, implementując nowe technologie do swoich działań.

ABSTRACT

The aim of this paper is to shed light on legal problems of implementing the Internet of Medical Things into activities of non-governmental organizations. The article consists of three parts. Part one addresses the notion of the Internet of Things and its subtype – Internet of Medical Things, describes the diversity of this phenomenon, in particular with regard to medical devices. Part two presents examples of applying such devices in the non-governmental organizations' practice, with the use of existing technologies. Part three discusses legal aspects related to the Internet of Medical Things from the non-governmental organizations' perspective, especially obligations resulting from GDPR and cybersecurity legislation, which should be taken into consideration while incorporating new technologies into NGO activities.

Rozwój nowych technologii komunikacyjnych jest jednym z procesów charakterystycznych dla współczesności. Jak się wskazuje, jesteśmy na etapie przechodzenia do Internetu czwartej generacji, który cechuje automatyzacja procesów z wykorzystaniem technologii sztucznej inteligencji

[1] Tekst powstał na podstawie badań prowadzonych w ramach realizacji grantu „Cyberbezpieczeństwo urządzeń medycznego Internetu Rzeczy - perspektywa prawna", finansowanego ze środków Narodowego Centrum Nauki (umowa nr 2020/04/X/HS5/00135).

i uczenia maszynowego, wymagających do poprawnego działania wielkich ilości danych (*Komunikat*... 2018). Dynamika tego zjawiska przyspieszyła z powodu obostrzeń związanych z pandemią COVID-19, jakie wymusiły ograniczenie kontaktów międzyludzkich i przeniosły wiele działań do przestrzeni wirtualnej. Konieczność zmian objęła sfery aktywności ludzkich, które w okresie przed pandemią opierały się na osobistym uczestnictwie, takich jak kultura, edukacja czy ochrona zdrowia. Ich skutki będą widoczne w długim okresie, ale można przyjąć, że proces adaptacji opierający się na wykorzystaniu istniejących rozwiązań technologicznych dotknął wszystkich branż i sektorów.

Dotyczy to również organizacji pozarządowych. Wyniki badań analizujących postawy polskich podmiotów trzeciego sektora wobec pandemii wskazują, że 49 procent organizacji podjęło lub planuje podjąć nowe działania w reakcji na COVID-19 (Charycka, Gumkowska 2020, s. 14), jednocześnie 80 procent badanych podmiotów zamierza wykorzystywać nowe technologie w swoich działaniach, z czego 38 procent w dużym stopniu (*ibidem*, s. 28). Trzeba zwrócić uwagę, że istotną częścią polskiego trzeciego sektora są organizacje działające na rzecz seniorów lub osób chorych i z niepełnosprawnością - odpowiednio 39 procent i 25 procent organizacji działających w Polsce (*ibidem*, s. 11). Można więc przyjąć, że znaczna grupa organizacji operujących w tym sektorze podejmie działania z wykorzystaniem nowych technologii, a jednocześnie, że przynajmniej część z nich będzie dalej je wykorzystywała, gdy pandemia dobiegnie końca.

Zmiana w podejściu do nowych technologii w trzecim sektorze może się przekładać na szersze wdrożenie technologii wspierających opiekę nad seniorami i leczenie osób chorych oraz z niepełnosprawnościami. Rozwiązania w tym zakresie są wprowadzane zarówno przez podmioty działające dla zysku, które chcą zwiększyć w ten sposób swoją przewagę konkurencyjną (Sobieski 2020, s. 35), jak i przez samorządy w ramach realizowanych przez nie zadań publicznych (Warchała 2019). Dodatkowo zwiększanie udziału usług cyfrowych, szczególnie w opiece zdrowotnej, jest priorytetem w krajowych i unijnych politykach rozwoju (Kokocińska 2020).

Na tym tle pojawia się pytanie o gotowość prawną i organizacyjną podmiotów trzeciego sektora do wdrażania nowoczesnych technologii do swojej działalności. Niniejszy artykuł jest próbą odpowiedzi na to pytanie, przy czym koncentruje się on na jednej z nowoczesnych technologii - medycznym Internecie rzeczy i jego wykorzystaniu w działaniach organizacji pracujących na rzecz seniorów i osób chorych. Praca została podzielona na trzy części. Dwie pierwsze poświęcono opisowi zjawiska przez zdefiniowanie medycznego Internetu rzeczy oraz wskazanie istniejących i możliwych sposobów wykorzystania tej technologii w działaniach

organizacji pozarządowych. Część trzecia dotyczy prawnych aspektów tego zagadnienia w zakresie istniejących norm prawnych, które nakładają określone obowiązki na organizacje.

Pojęcie medycznego Internetu rzeczy

Technologię Internetu rzeczy (Internet of Things, IoT) definiuje się jako połączoną ze sobą sieć urządzeń w sensie fizycznym, wyposażonych w czujniki, oprogramowanie i możliwość połączenia z Internetem, co pozwala tym urządzeniom zbierać i wymieniać dane oraz wchodzić w interakcje ze sobą przez Internet (Strous, von Solms, Zúquete 2021, s. 1). Urządzenia te mają bardzo szerokie zastosowanie i są wykorzystywane zarówno w przemyśle, na przykład jako część automatyki przemysłowej lub urządzeń dozoru, jak i w transporcie, przykładowo w pojazdach autonomicznych i przy świadczeniu usług typu dostawy paczek. Stały się one również częścią współczesnych gospodarstw domowych jako lodówki smart, autonomiczne odkurzacze czy niektóre zabawki. Liczbę tych urządzeń ocenia się na 25–30 miliardów, zakłada się również, że będzie ona stale rosła (https://www.gartner.com). Jednocześnie technologia ta jest uznawana za kluczową w procesach przetwarzania danych, a tym samym niezbędną dla rozwoju gospodarki cyfrowej (*Europejska strategia w zakresie danych* 2020, s. 2).

Medyczny Internet rzeczy (Health-Related Internet of Things, HIoT) można zdefiniować jako podzbiór urządzeń Internetu rzeczy, które gromadzą informacje o stanie zdrowia w celach *stricte* związanych z diagnozą lub leczeniem albo do innych zadań (Mittelstadt 2017, s. 157). Kategoria ta obejmuje całą paletę rozwiązań i zastosowań: od konstrukcji monitorujących jeden parametr życiowy, na przykład tętno lub ciśnienie krwi, do wielomodułowych systemów podtrzymywania życia na oddziałach intensywnej terapii. Trzeba zauważyć, że tak skonstruowana definicja obejmuje rozwiązania pozwalające zamienić dowolne urządzenie Internetu rzeczy w takie, które gromadzi i przetwarza dane o stanie zdrowia. Przykładem mogą być smartfony, które po zainstalowaniu odpowiednich aplikacji zamieniają się w urządzenia do monitorowania nawyków żywieniowych, jakości snu czy aktywności fizycznej.

Specyficzną grupą urządzeń medycznego Internetu rzeczy są wyroby medyczne. Pojęcie to odnosi się do kategorii urządzeń, które w wyniku spełnienia określonych wymogów mogą być używane do świadczenia usług medycznych. Ustawa o działalności leczniczej w art. 17 ust. 1 pkt 2 i 18 ust. 3 pkt 2 wskazuje wprost, że podmiot leczniczy i lekarz wykonujący działalność leczniczą jako indywidualną praktykę lekarską, udzielając świadczeń zdrowotnych, mogą korzystać wyłącznie z wyrobów medycznych. Tym samym podstawą prowadzenia diagnostyki lub leczenia chorób nie mogą być dane pochodzące

z innych urządzeń Internetu rzeczy, szczególnie ze smartfonów. Biorąc pod uwagę, że sektor wyrobów medycznych jest ściśle regulowany, a uzyskanie takiego statusu wymaga przejścia skomplikowanych procedur certyfikacyjnych (Żywicka 2021), producenci wielu urządzeń, których funkcje mogłyby być przydatne we wsparciu procesów leczenia, nie decydują się na taki krok.

Zastosowanie medycznego Internetu rzeczy w działalności organizacji pozarządowych

Konstrukcja urządzeń medycznego Internetu rzeczy powoduje, że możliwości ich wykorzystania w działaniach organizacji pozarządowych wydają się nieograniczone. Skupię się na kilku obszarach, aby zarysować omawianą problematykę. Jako pierwszy można wymienić sektor profilaktyki zdrowotnej. Od wielu lat się wskazuje, że wdrożenie rozwiązań medycznego Internetu rzeczy zmniejsza wskaźnik hospitalizacji wśród osób chorych (https://www.nursingtimes.net). Jednocześnie odpowiednio przystosowane programy profilaktyczne mogą wykorzystywać informacje na przykład o aktywności fizycznej lub nawykach żywieniowych do monitorowania i utrwalania zmian prozdrowotnych. Jednym z aspektów zapobiegania chorobom są kwestie związane z monitorowaniem jakości powietrza (Jastrzębowska 2020). Dane pozyskiwane w ramach czujników powietrza z sieci tworzonych i animowanych przez organizacje pozarządowe i ruchy nieformalne, takich jak Polski Alarm Smogowy, są wykorzystywane do tworzenia map zagrożeń i pozwalają grupom najbardziej narażonym na unikanie zagrożeń (Liczbińska, Kosińska, Greser 2020, s. 35-36). Mogą być również wykorzystane do kształtowania polityk środowiskowych lub w procesach sądowych i postępowaniach administracyjnych związanych z ochroną środowiska (Robakowska 2019).

Drugim obszarem jest poprawa opieki nad osobami przewlekle chorymi. W literaturze przedmiotu mówi się o tym, że urządzenia medycznego Internetu rzeczy mogą przynieść znaczne korzyści w tym zakresie (Su *et al*. 2016). Można wykorzystywać je do nadzorowania zachowań pacjentów, na przykład częstotliwości brania leków lub lokalizowania miejsca przebywania osób z demencją. Innym zastosowaniem jest prowadzenie monitoringu określonych parametrów zdrowotnych. Jako przykład należy przywołać urządzenie do ciągłego badania poziomu glukozy oraz wyznaczania tendencji w tym zakresie bez konieczności pobierania krwi z palca, które wyświetla wyniki w czasie rzeczywistym na współpracujących z nim smartfonach (https://www.dexcom.com). Istotą takich rozwiązań jest możliwość alarmowania zarówno osoby chorej, jak i innych osób, takich jak personel medyczny czy opiekunowie. Dotyczy to sytuacji, w której przekroczono określone wskaźniki, na przykład poziom glukozy we krwi, jak

i przewidywania powstania określonych stanów na podstawie analiz danych dostarczanych przez urządzenie w ramach działania algorytmów sztucznej inteligencji. Pozwala to na zmniejszenie liczby osób zaangażowanych w opiekę oraz poprawę jakości życia osoby chorej, na przykład przez obniżenie nasilenia i częstotliwości ataków astmy.

Te cechy urządzeń medycznego Internetu rzeczy otwierają kolejne pole ich wykorzystania, jakim jest przeniesienie opieki zdrowotnej z placówek opieki medycznej do domu. Przykładem mogą być urządzenia typu CPAP, które stosowane są do leczenia bezdechu sennego. Składają się one z pompy powietrznej i specjalnej maski, która wspomaga oddychanie w czasie snu. Obecnie dostępne na rynku modele zaopatrzane są w funkcje przesyłania danych do urządzeń mobilnych, co pozwala śledzić pacjentowi jego wyniki i korygować swoje zachowania w celu zwiększenia skuteczności terapii (https://www.resmed.com). Przed ich rozpowszechnieniem leczenie wymagało odbycia hospitalizacji. Podobne możliwości dotyczą badań, które dotychczas mogły być prowadzone jedynie w czasie wizyt ambulatoryjnych. Jako przykład można przywołać urządzenia do kardiotokografii (KTG). Ich zadaniem jest monitorowanie akcji serca płodu i czynności skurczowej macicy w celu wykrycia sytuacji zagrożenia życia płodu. Poza porodem i sytuacjami bezpośredniego zagrożenia życia badanie to wykonywane było w trakcie wizyt lekarskich, co dawało cząstkowy obraz sytuacji. Obecnie są dostępne urządzenia pozwalające wykonać badanie w domu, w dowolnym czasie i przez wybrany przez pacjentkę okres, a wyniki są analizowane przez algorytmy i dyżurujących lekarzy (https://www.pregnabit.com).

Powiązanym zagadnieniem jest wsparcie rehabilitacji w warunkach domowych. Problem ten dotyczy szczególnie osób starszych oraz ze sprzężonymi niepełnosprawnościami, które wymagają stałej rehabilitacji lub mają problem z dostępem do fizjoterapii stacjonarnej zarówno z powodów finansowych, jak i ze względu na ograniczenia systemowe, takie jak wykluczenie komunikacyjne uniemożliwiające dojazd do placówek świadczących rehabilitację lub ich zamknięcie spowodowane pandemią. W literaturze wskazuje się, że za pomocą urządzeń medycznego Internetu rzeczy można uzyskać porównywalne lub lepsze wyniki niż w wypadku rehabilitacji prowadzonej w placówce (Burridge *et al.* 2017). Ponadto do ich osiągnięcia może w określonych wypadkach wystarczyć posiadanie smartfona lub smartwatcha i odpowiedniej aplikacji (Chae *et al.* 2020). Dodatkowym problemem występującym w trakcie długotrwałej rehabilitacji jest zniechęcenie pacjentów powtarzalnością ćwiczeń, małym tempem postępów i brakiem informacji zwrotnej w zakresie poprawności ćwiczeń, co przekłada się na wysoki wskaźnik zaprzestawania terapii. Jedną z metod zapobiegających temu zjawisku jest gamifikacja rehabilitacji, czyli dodanie elementu

rozrywkowego do ćwiczeń. Odpowiednio skonfigurowane urządzenia medycznego Intermetu rzeczy mają możliwość prowadzenia rehabilitacji przy wsparciu gier dostępnych na najpopularniejsze platformy – zarówno u dorosłych, jak i u dzieci (Janssen 2017). Rozwiązania tego typu są dostępne na rynku (https://raccoon.world).

Problematyka leczenia chorób przewlekłych, wsparcia leczenia i rehabilitacji w warunkach domowych jest wspólna dla wielu organizacji pozarządowych. Dotyczy to szczególnie organizacji pacjenckich, które skupiają się na wsparciu osób z określonymi schorzeniami, organizacji działających na rzecz osób niepełnosprawnych psychicznie i fizycznie, w tym prowadzących warsztaty terapii zajęciowej, oraz działających na rzecz seniorów. W zależności od typu odbiorcy i rodzaju prowadzonych działań organizacje mogą w różny sposób wdrażać medyczny Internet rzeczy w swoje przedsięwzięcia. Możliwości jest kilka: pierwszą stanowi zakup lub użyczanie urządzeń, takich jak opaski ratunkowe czy pompy insulinowe, beneficjentom albo organizowanie zbiórek, loterii czy festynów, na których gromadzi się środki na ten cel. Drugą jest wyposażanie siedzib organizacji w urządzenia wspierające terapię, co stosować można na przykład w dziennych domach opieki lub warsztatach terapii zajęciowej, albo w urządzenia zwiększające bezpieczeństwo beneficjentów, jak czujniki monitorujące zakładane w domach opieki. Trzecią jest zwiększenie zakresu działania przez wyposażanie beneficjentów w urządzenia wspierające leczenie w domu wraz z zapewnianiem wsparcia w korzystaniu z nich. Oczywiście jest to tylko niewielki wycinek możliwości urządzeń medycznego Internetu rzeczy, które z powodzeniem mogą być stosowane w leczeniu nałogów za pomocą urządzeń monitorujących zachowania, w edukacji ze wsparciem rozszerzonej rzeczywistości czy w aktywnościach sportowych do badania postępów w treningach. Coraz większa dostępność tych urządzeń na rynku, a także zmiany spowodowane pandemią, mogą sprawić, że większa grupa organizacji będzie sięgać po tego typu rozwiązania.

Prawna strona wdrażania medycznego Internetu rzeczy w organizacjach pozarządowych

Wdrożenie urządzeń medycznego Internetu rzeczy w działania organizacji pozarządowej powinna poprzedzić analiza prawna konsekwencji takiego posunięcia. Trzeba zauważyć, że korzystanie z Internetu rzeczy nie jest materią regulowaną w jednym akcie prawnym. Sposób konstrukcji tych urządzeń powoduje, że mogą być w ich wypadku stosowane przepisy prawa własności intelektualnej, odpowiedzialności za produkt niebezpieczny, ochrony danych osobowych czy praw konsumenta. Do tych urządzeń medycznego Internetu rzeczy, które są wyrobami medycznymi, będą od maja 2021 roku

znajdować zastosowanie przepisy rozporządzenia 2017/746. Należy pamiętać, że większość obowiązków jest nałożona na producentów lub dystrybutorów urządzeń, a nie ich użytkowników końcowych. Z pespektywy organizacji pozarządowej w wypadku tradycyjnych wyrobów medycznych analiza prawna ogranicza się zazwyczaj do stwierdzenia, czy są spełnione kryteria bezpieczeństwa, a w wypadku urządzeń elektronicznych - do kwestii związanych z danymi osobowymi. Stosując urządzenia medycznego Internetu rzeczy mamy do czynienia z połączeniem tych dwóch obszarów, z których każdy ma swoje regulacje nakładające pewne obowiązki również na organizacje.

W odniesieniu do problematyki bezpieczeństwa należy zauważyć, że ze względu na stałe połączenie urządzeń medycznego Internetu rzeczy z siecią podstawowym zagadnieniem jest ich cyberbezpieczeństwo. Problem jest wyjątkowo istotny z powodu wskazywanej w literaturze (Weber, Studer 2016, s. 719) i opracowaniach branżowych (http://www8.hp.com, s. 3) podatności tej technologii na ataki ze strony cyberprzestępców. Dodatkowo pandemia COVID-19 spowodowała znaczny wzrost ataków z ich strony na sektor medyczny. Międzynarodowy Związek Telekomunikacyjny wskazuje, że w czasie pandemii do ataku hakerskiego dochodzi co trzydzieści dziewięć sekund, a liczba e-maili wykorzystywanych do ataków wzrosła o 600 procent (https://www.cyberdefence24.pl). Do potwierdzonych ataków doszło również w Polsce, gdzie ofiarą stała się największa sieć prywatnych klinik kardiologicznych (https://zaufanatrzeciastrona.pl).

Prawna strona cyberbezpieczeństwa medycznego Internetu rzeczy opiera się na trzech podstawach. Pierwszą są regulacje instytucjonalne. Ich źródłem jest dyrektywa 2016/1148 i przyjęta na jej podstawie Ustawa o krajowym systemie cyberbezpieczeństwa oraz oparte na niej akty wykonawcze. Stworzony na podstawie ustawy system nakłada obowiązki na dwie grupy podmiotów: operatorów usług kluczowych i dostawców usług cyfrowych. Operatorem takim mogą być, zgodnie z art. 5 ust. 1 ustawy, podmioty świadczące określonego rodzaju usługi. W sektorze ochrony zdrowia są to między innymi podmiot leczniczy, o którym mowa w art. 4 ust. 1 Ustawy o działalności leczniczej, i przedsiębiorca prowadzący działalność w formie apteki ogólnodostępnej w rozumieniu Prawa farmaceutycznego. Ponadto podmiot zaliczany do tej grupy musi świadczyć usługę kluczową, czyli taką, która ma fundamentalne znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, jest wymieniona w wykazie usług kluczowych i świadczona na dużą skalę. Teoretycznie organizacja pozarządowa może spełnić te warunki, w praktyce jednak trudno sobie wyobrazić taką sytuację. Podobny wniosek można sformułować w odniesieniu do dostawców usług cyfrowych. Zgodnie z definicją zawartą w ustawie są to podmioty świadczące usługi elektroniczne w rozumieniu Ustawy o świadczeniu usług

drogą elektroniczną, wymienione w załączniku numer 2 do ustawy, który obejmuje platformy handlowe, usługi przetwarzania w chmurze i wyszukiwarki internetowe. Obecnie trwają prace nad nowelizacją dyrektywy, która ma rozszerzyć zakres podmiotów o dodatkowe branże, ale nic nie wskazuje na to, by objęła ona w szerszym niż dotychczas zakresie organizacje pozarządowe korzystające z medycznego Internetu rzeczy.

Drugim filarem systemu cyberbezpieczeństwa są regulacje dotyczące wyrobów medycznych. Trzeba podkreślić, że znajdują one zastosowanie tylko do określonej grupy produktów, które uzyskały ten status w wyniku przeprowadzenia odpowiednich procedur. Zarówno w obecnie obowiązującej Ustawie o wyrobach medycznych, jak i w rozporządzeniu 2017/746 proces certyfikacji jest bardzo szczegółowo uregulowany i wymaga od producenta urządzenia spełnienia wielu wymagań. Jego celem jest zapewnienie bezpieczeństwa korzystania z wyrobu na wszystkich jego płaszczyznach, ale kwestia cyberbezpieczeństwa nie jest ujęta jako odrębne zagadnienie (Greser 2020a, s. 89). Jednocześnie przepisy nie nakładają na użytkownika wyrobu żadnych obowiązków w tym zakresie. Zatem z perspektywy organizacji pozarządowej korzystanie z medycznego Internetu rzeczy będącego wyrobem medycznym nie tworzy nowych wyzwań pod względem prawnym. Należy jednak pamiętać, że bezpieczne korzystanie z urządzenia może wiązać się z określonymi wymaganiami, przedstawionymi przez producenta w instrukcji. Dotyczy to również cyberbezpieczeństwa i może obejmować na przykład obowiązek aktualizacji oprogramowania lub odpowiedniego skonfigurowania sieci. Z tej perspektywy brak odpowiednich działań ze strony organizacji pozarządowej może się wiązać na przykład z odpowiedzialnością odszkodowawczą wynikającą z niedochowania należytej staranności.

Trzecim obszarem regulującym problematykę cyberbezpieczeństwa jest rozporządzenie 2016/679 (RODO). Będzie się ono odnosiło do każdego urządzenia medycznego Internetu rzeczy, niezależnie od tego, czy jest ono klasyfikowane jako wyrób medyczny, czy nie ma takiego charakteru. Regulacja ta ma za zadanie całościowe unormowanie problematyki danych osobowych, a więc wiąże się ze wskazanym wyżej obszarem ryzyka prawnego dla organizacji, jakim jest przetwarzanie tych danych. Ponieważ przepisy RODO nie wyróżniają kwestii cyberbezpieczeństwa jako osobnego zagadnienia, oba problemy poddam więc łącznej analizie.

Szukając podstaw normatywnych konieczności zapewnienia cyberbezpieczeństwa, należy zauważyć, że pierwszoplanowy charakter ma zasada integralności i poufności, która jest zawarta w art. 5 ust. 1 RODO. Nakłada ona na administratora danych obowiązek ich przetwarzania w sposób zapewniający bezpieczeństwo (Chmielewski, Waćkowski 2018, s. 79). Jednocześnie RODO nie wskazuje wiążących środków jej realizacji. Przywołane w art. 32 rozwiązania,

takie jak pseudoanonimizacja, szyfrowanie czy regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych, służące zapewnieniu bezpieczeństwa przetwarzania, mają charakter jedynie przykładowy. Dobór środków ochrony to zadanie administratora, a decyzja w tym zakresie zależy od poziomu zdefiniowanego ryzyka, do których środki te muszą być adekwatne (Litwiński 2017, s. 54; Greser 2018b, s. 21-22). W związku z tym trzeba zwrócić uwagę na dwie kwestie dotyczące użytkowania urządzeń medycznego Internetu rzeczy. Pierwszą jest wskazany w motywie szóstym RODO wzrost zagrożeń dla ochrony danych osobowych w związku z rozwojem Internetu. Tendencję tę wskazuje się również w literaturze (Konarski 2017, s. 13). Drugą jest założenie, że poziom cyberbezpieczeństwa jest procesem dynamicznym i w dużej mierze zależnym od czynników zewnętrznych (Banasiński 2018, s. 29). Można zatem uznać, że każdorazowe wdrożenie urządzeń medycznego Internetu rzeczy w działania organizacji będzie wymagało aktualizacji analizy ryzyka.

Kolejnym problemem jest stwierdzenie, jakie dane osobowe są przetwarzane przez urządzenia medycznego Internetu rzeczy. Kwestia ta ma fundamentalne znaczenie dla identyfikacji obowiązków organizacji pozarządowych jako podmiotów przetwarzających dane. Jednocześnie rodzi ona ogromne komplikacje praktyczne. Urządzenia tego typu często generują w medycznym Internecie rzeczy „niewidzialne dane", których istnienia użytkownik nie jest świadomy (Bietz *et al.* 2016, s. 42). Do takich informacji należą metadane czy adresy IP pozwalające zidentyfikować tożsamość użytkownika. W orzeczeniu C-582/14 Trybunał Sprawiedliwości Unii Europejskiej uznał, że dynamiczny adres IP jest daną osobową, o ile istnieją środki prawne umożliwiające ustalenie tożsamości osoby, która się nim posłużyła. Trzeba mieć na uwadze, że w Polsce takie środki istnieją, co potwierdził Naczelny Sąd Administracyjny w wyroku z 19 maja 2011 roku. Jednocześnie w polskiej doktrynie wskazuje się, że danymi osobowymi są tylko te informacje, które pozwalają na zidentyfikowanie osoby fizycznej w ramach środków własnych administratora danych (Litwiński 2017, s. 51-53). Po stronie organizacji będzie zatem obowiązek stwierdzenia, jakie nieoczywiste informacje generuje urządzenie, oraz podjęcia decyzji, czy są one danymi osobowymi, czy nie. Niejednokrotnie wymaga to specjalistycznej wiedzy z zakresu prawa i informatyki, a jednocześnie podmiotem odpowiedzialnym za prawidłowość decyzji jest administrator danych, czyli często sama organizacja pozarządowa.

Następnym zagadnieniem, z którym muszą się zmierzyć organizacje pozarządowe, jest wybór podstawy przetwarzania danych. W trakcie wykorzystywania urządzeń medycznego Internetu rzeczy są gromadzone informacje o stanie zdrowia, które zalicza się do szczególnej kategorii danych, w doktrynie nazywanej danymi wrażliwymi. Zgodnie z art. 9 ust. 1 RODO

przetwarzanie tych danych jest zakazane, chyba że można wskazać jakąś przesłankę legalizacyjną enumeratywnie wymienioną w kolejnym ustępie tego artykułu. Jedną z nich jest zgoda osoby, której dane są przetwarzane, ale ze względu na możliwość wycofania takiej zgody w każdym momencie opieranie się na tej przesłance może być znacznym utrudnieniem w praktyce działania podmiotów trzeciego sektora, na przykład gdy istnieje konieczność przetwarzania tych informacji w związku z otrzymanym dofinasowaniem i obowiązkiem dokonania rozliczeń z grantodawcą.

Wydaje się, że lepszą podstawą będzie art. 9 ust. 2 lit. d RODO, który pozwala przetwarzać dane przez organizacje pozarządowe, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu albo osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą. Wybór tej podstawy rodzi dwa istotne problemy. Pierwszym będzie wykluczenie ze skorzystania ze świadczeń innych osób niż wskazane w tym przepisie. Można jednak uznać, że w wielu wypadkach korzystanie z urządzenia medycznego Internetu rzeczy będzie wymagało stałego kontaktu z organizacją, którego intensywność oceniana jest *ad casum* (por. Greser 2018a, s. 28-30). Z kolei zgoda osób na przekazanie danych innym podmiotom może rodzić te same komplikacje praktyczne w rozliczeniach z grantodawcami, jak wskazane powyżej. Inną podstawą, którą można wykorzystać, jest możliwość przetwarzania danych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą (art. 9 ust. 1 lit. e RODO), czy w związku z usługami opieki zdrowotnej (art. 9 ust. 1 lit. h RODO).

Wybór każdej z podstaw przetwarzania ma swoje wady i zalety, a o tym, którą wybierze organizacja, będzie decydować konkretna specyfika jej działań. Trzeba pamiętać, że zawsze jest to autonomiczna decyzja administratora, ale jednocześnie sam proces przetwarzania tych samych danych nie może mieć różnych podstaw przetwarzania. Należy jednak zauważyć, że w wypadku wdrożenia urządzeń medycznego Internetu rzeczy organizacje mogą posiłkować się przyjętymi u nich podstawami przetwarzania wobec innych procesów związanych ze swoją działalnością.

***

Internet rzeczy jest bez wątpienia technologią, która będzie zyskiwać na popularności. Jej specyfika, szczególnie łatwość adaptacji do różnych celów i relatywnie niska cena, powoduje, że technologia ta jest coraz szerzej wykorzystywana i śmiało wkracza na nowe obszary. Dodatkowo można oczekiwać przyspieszenia procesów cyfryzacji świadczenia wielu usług, co się wiąże ze zmianami społecznymi spowodowanymi pandemią COVID-19. Procesy te dotyczą również organizacji pozarządowych, dlatego należy się

spodziewać, że coraz większa liczba podmiotów trzeciego sektora w Polsce będzie korzystać z tej technologii.

Szczególną rolę odgrywają urządzenia medycznego Internetu rzeczy. Ich funkcje, które skupiają się na wsparciu diagnozowania i leczenia lub monitorowaniu innych zachowań związanych ze zdrowiem, mogą być przydatne dla wielu organizacji o różnych profilach. Ich umiejętne wykorzystanie może pozwolić na utrzymanie działania mimo obostrzeń epidemicznych, rozszerzenie zakresu świadczonych usług, zwiększenie liczby beneficjentów lub otwarcie się na nowe ich grupy. Zalety tej technologii powinny być analizowane przez pryzmat wyzwań prawnych, jakie są związane z ich wdrożeniem. Biorąc pod uwagę, że zdecydowana większość organizacji pozarządowych będzie nabywała gotowe produkty, w analizie można pominąć obowiązki nałożone na producentów tych urządzeń, które stanowią większość wymagań nakładanych przez prawo. Obszary, które muszą być w polu zainteresowania podmiotów trzeciego sektora, dotyczą cyberbezpieczeństwa i ochrony danych osobowych. Z perspektywy organizacji przenikają się one wzajemnie, ponieważ objęcie trzeciego sektora przepisami normującymi działanie krajowego systemu cyberbezpieczeństwa jest bardzo mało prawdopodobne. Podstawą wymagań wobec organizacji będzie zatem RODO, przez pryzmat którego należy analizować wybór urządzenia medycznego Internetu rzeczy i konsekwencje jego używania.

Wdrażanie medycznego Internetu rzeczy jest jedynie wąskim wycinkiem problemów związanych z implementacją nowych technologii w działania organizacji pozarządowych. Wiele organizacji stanie przed wyzwaniami związanymi z wykorzystaniem *blockchain*, uczenia maszynowego czy elektronicznego obiegu dokumentów. Każde z tych zagadnień ma swoje regulacje prawne, które należy brać pod uwagę. Niezależnie od tego, wprowadzanie nowych technologii wiąże się z kwestiami etycznymi, równie ważnymi jak zagadnienia prawne. Jest to szczególnie istotne w sektorze opieki zdrowotnej, w którym łatwo jest narzucać pewne rozwiązania pod pretekstem ochrony zdrowia (por. Mittelstad 2017; Greser 2020b).

BIBLIOGRAFIA

Banasiński, Cezary. 2018. *Podstawowe pojęcia i podstawy prawne bezpieczeństwa w cyberprzestrzeni*, [w:] Cezary Banasiński (red.), *Cyberbezpieczeństwo. Zarys wykładu*. Warszawa: Wolters Kluwer.

Bietz, Matthew, Bloss, Cinnamon, Calvert, Scout, Godino, Job, Gregory, Judith, Claffey, Michael. 2016. Opportunities and challenges in the use of personal health data for health research. *Journal of the American Medical Informatics Association*, 23: 42–48, DOI:10.1093/jamia/ocv118.

Burridge, Jane, Chong W. Lee, Alan, Turk, Ruth, Stokes, Maria Whitall, Jill, Vaidyanathan, Ravi, Clatworthy, Phil, Hughes, Ann-Marie, Meagher, Claire, Franco, Enrico, Yardley, Lucy. 2017. Telehealth, Wearable Sensors, and the Internet: Will They Improve Stroke Outcomes Through Increased Intensity of Therapy, Motivation, and Adherence to

Rehabilitation Programs?. *Journal of Neurologic Physical Therapy*, 41: 32-38, DOI: 10.1097/NPT.0000000000000183.

Chae, Sang Hoon, Yushin, Kim, Lee, Kyoung-Soub, Park, Hyung-Soon. 2020. Development and Clinical Evaluation of a Web-Based Upper Limb Home Rehabilitation System Using a Smartwatch and Machine Learning Model for Chronic Stroke Survivors: Prospective Comparative Study, *Journal of Medical Internet Research*, 8, DOI: 10.2196/17216.

Charycka, Beata, Gumkowska, Marta. 2018. *Kondycja organizacji pozarządowych*. Warszawa: Stowarzyszenie Klon/Jawor.

Charycka, Beata, Gumkowska, Marta. 2020. *Organizacje pozarządowe wobec pandemii. Raport z badań*. Warszawa: Stowarzyszenie Klon/Jawor.

Chmielewski, Jan Maciej, Waćkowski, Kazimierz. 2018. *Technologie teleinformatyczne - podstawy, rozwój i bezpieczeństwo systemów teleinformatycznych*, [w:] Cezary Banasiński (red.), *Cyberbezpieczeństwo. Zarys wykładu*. Warszawa: Wolters Kluwer.

Jastrzębowska, Aleksandra. 2020. *Wpływ zanieczyszczenia powietrza na zaburzenia psychiczne człowieka*, [w:] Lubomira Wengler, Daria Mirosławska (red.), *Polskie miasta dla zdrowego powietrza. Jak ograniczyć koszty zdrowotne generowane przez transport?*. T. 1. Gdańsk: Polskie Towarzystwo Programów Zdrowotnych.

Janssen, Joep, Verschuren, Olaf, Renger, Willem Jan, Ermers, Jose, Ketelaar, Marjolijn, van Ee, Raymond. 2017. Gamification in Physical Therapy: More Than Using Games. *Pediatric Physical Therapy*, 29: 95-99, DOI: 10.1097/PEP.0000000000000326.

Greser, Jarosław. 2018a. Zasady przetwarzania danych osobowych w ogólnym rozporządzeniu o ochronie danych osobowych, *Trzeci Sektor*, 41: 19-35, DOI:10.26368/17332265-041-1-2018-1.

Greser, Jarosław. 2018b. Obowiązki organizacji pozarządowych jako administratorów danych osobowych. *Trzeci Sektor*, 42: 20-36, DOI:10.26368/17332265-042-2-2018-1.

Greser, Jarosław. 2020a. Cyberbezpieczeństwo wyrobów medycznych w świetle rozporządzenia 2017/745. *Internetowy Kwartalnik Antymonopolowy i Regulacyjny*, 2: 79-90, DOI: 10.7172/2299-5749.IKAR.2.9.6.

Greser, Jarosław. 2020b. Etyczne problemy wdrażania medycznego Internetu Rzeczy. *Prawo Mediów Elektronicznych*, 3: 4-11.

Kokocińska, Katarzyna. 2020. *Działania władzy publicznej na rzecz rozwoju innowacyjnych technologii w sektorze zdrowia (polityka unijna i krajowa)*, [w:] Katarzyna Kokocińska (red.), *Innowacyjne technologie w ochronie zdrowia. Aspekty prawne*. Warszawa: Wolters Kluwer.

Konarski, Xawery. 2017. Rozporządzenie o e-Prywatności jako regulacja sektorowa względem ogólnego rozporządzenia o ochronie danych osobowych (RODO). *Monitor Prawniczy*, 20: 6-13.

Liczbińska, Grażyna, Kosińska, Magdalena, Greser, Jarosław. 2020. Podnoszenie świadomości społeczeństwa polskiego w zakresie zagrożeń zdrowia i życia spowodowanych zanieczyszczeniem powietrza. *Kwartalnik Trzeci Sektor*, 47: 28-40, DOI: 10.26368/17332265-047-3-2019-2.

Litwiński, Paweł. 2017. Pojęcie danych osobowych w ogólnym rozporządzeniu o ochronie danych osobowych - glosa do wyroku Trybunału sprawiedliwości z 19.10.2016 w sprawie c-582/14 Patrick Breyer, *Europejski Przegląd Sądowy*, 5: 51-57.

Mittelstadt, Brent. 2017. Ethics of the health-related internet of things: a narrative review. *Ethics and Information Technology*, 3: 157-175, DOI: 10.1007/s10676-017-9426-4.

Robakowska, Martyna. 2019. Udział organizacji ekologicznych w postępowaniach w sprawie wydania decyzji środowiskowej - uwarunkowania prawne. *Kwartalnik Trzeci Sektor*, 45: 28-39, DOI:10.26368/17332265-045-1-2019-2.

Sobieski, Leszek. 2020. *Koncepcja e-zdrowia w świetle regulacji publicznoprawnych*, [w:] Katarzyna Kokocińska (red.), *Innowacyjne technologie w ochronie zdrowia. Aspekty prawne*. Warszawa: Wolters Kluwer.

Strous, Leon, von Solms, Suné, Zúquete, André. 2021. Security and privacy of the Internet of Things, *Compter&Security*, 102: 1-3, DOI: 10.1016/j.cose.2020.102148.

Su, Dejun, Zhou Junmin, Kelley, Megan, Michuad, Tzeyu, Siahpush Mohammad, Kim, Jungyoon, Wilson, Fernando, Stimpson, Jim, Pagánde, Jose. 2016. Does telemedicine improve treatment

outcomes for diabetes? A meta-analysis of results from 55 randomized controlled trials, *Diabetes Research and Clinical Practice*, 116: 136-148.

Warchala, Magdalena. 2019. Inteligentne opaski pilnują bezpieczeństwa seniorów. Skorzystają kolejne osoby, *Gazeta Wyborcza*, 3 czerwca 2019 roku.

Weber, Ralph, Studer, Evelyne. 2016. Cybersecurity in the Internet of Things: Legal aspects, *Computer Law & Security Review*, 32: 719-721.

Żywicka, Agnieszka. 2021. *Uwarunkowania prawne bezpieczeństwa wyrobów medycznych. Certyfikacja wyrobów medycznych w świetle rozporządzenia Parlamentu Europejskiego i Rady* 2017/745 UE, [w:] Jarosław Greser, Katarzyna Kokocińska (red.), *Jakość w opiece medycznej. Teleporady, Internet Rzeczy, aplikacje śledzące, IP Boxy*. Warszawa: Wolters Kluwer [w druku].

AKTY PRAWNE I DOKUMENTY

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 roku w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U. UE z 19 lipca 2016, L 194/1).

Komunikat Komisji Europejskiej z dnia 25 kwietnia 2018 roku, *Communication From the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of The Regions „Towards a common European data space"*, COM(2018) 232 final.

Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z dnia 19 lutego 2020 roku, *Europejska strategia w zakresie danych*, COM(2020) 66 final.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/746 z dnia 5 kwietnia 2017 roku w sprawie wyrobów medycznych do diagnostyki in vitro oraz uchylenia dyrektywy 98/79/WE i decyzji Komisji 2010/227/UE (Dz.U. UE z 5.05.2017 L 117/176).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. UE z 4.5.2016, L 119/1).

Ustawa z dnia 15 kwietnia 2011 roku o działalności leczniczej (t.j.: Dz.U. z 2020 r. poz. 295, z późn zm.).

Ustawa z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa (t.j.: Dz.U. z 2020 r. poz. 1369).

Ustawa z dnia 6 września 2001 roku - Prawo farmaceutyczne (t.j.: Dz.U. z 2020 r. poz. 944).

Ustawa z dnia 18 lipca 2002 roku oświadczeniu usług drogą elektroniczną (t.j.: Dz.U. z 2020 r. poz. 344).

Ustawa z dnia 20 maja 2010 roku o wyrobach medycznych (t.j.: Dz.U. z 2020 r. poz. 186, z późn. zm.).

Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 19 października 2016 roku w sprawie C-582/14 Patrick Breyer przeciwko Niemcom.

Wyrok Naczelnego Sądu Administracyjnego z 19 maja 2011 roku, I OSK 1079/10.

ŹRÓDŁA INTERNETOWE

Hewlett Packard Internet of Things Research Study 2015, http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf [dostęp: 31 stycznia 2021 roku].

https://www.cyberdefence24.pl/onz-podczas-pandemii-liczba-zlosliwych-e-maili-wzrosla-o-600-proc [dostęp: 31 października 2020 roku].

https://zaufanatrzeciastrona.pl/post/atak-ransoware-na-najwieksza-siec-klinik-kardiologicznych-w-polsce [dostęp: 31 stycznia 2021 roku].

http://www.nursingtimes.net/nursing-practice/clinical-zones/copd/telehealth-system-slashes-hospital-admis-sions-in-copd-patients/5005885.article [dostęp: 31 stycznia 2021 roku].

https://www.dexcom.com/pl-PL [dostęp: 31 stycznia 2021 roku].

https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016 [dostęp: 31 stycznia 2021 roku].

https://www.resmed.com/en-us/sleep-apnea/cpap-parts-support/sleep-apnea-full-products-list/cpap-machines/airsense-10 [dostęp: 31 stycznia 2021 roku].
https://www.pregnabit.com/technologia [dostęp: 31 stycznia 2021 roku].
https://raccoon.world [dostęp: 31 stycznia 2021 roku].