Etyczne problemy wdrażania medycznego Internetu rzeczy

dr Jarosław Greser[1]

W niniejszym opracowaniu autor porusza problematykę związaną z wdrażaniem medycznego Internetu rzeczy, przy czym z etycznego punktu widzenia. W literaturze podkreśla się, że problemy etyczne związane z korzystaniem z urządzeń H-IoT cieszą się zainteresowaniem badaczy od początków rozwoju tej technologii i są analizowane z różnych perspektyw, z których każda naświetla inne obawy[2]. Przedstawione zatem zostały wybrane problemy etyczne z perspektywy producentów urządzeń mających swoją siedzibę na terenie UE. Artykuł podzielono na cztery części, z których pierwsza jest wprowadzeniem do zagadnień związanych z etyką biznesu – swoistego zespołu norm, którego adresatem są przedsiębiorcy. Następnie przeanalizowano prywatność w wymiarze związanym ze stygmatyzacją związaną z korzystaniem z urządzeń H-IoT oraz problemy dotyczące własności danych zbieranych przez te urządzenia, a także zapewnienia cyberbezpieczeństwa ich użytkownikom.

Uwagi wstępne

Rozwój Internetu rzeczy stworzył nowe sposoby świadczenia usług medycznych. Technologia ta, którą w literaturze określa się jako *Health – Related Internet of Things* (H-IoT)[3] obejmuje bardzo szerokie spektrum urządzeń: od złożonych systemów podtrzymywania życia czy prowadzenia badań klinicznych do nieskomplikowanych konstrukcji monitorujących jeden parametr życiowy, na przykład temperaturę lub ciśnienie krwi. Równie szeroki jest zakres zastosowania takich urządzeń, który obejmuje monitorowanie pacjentów nie tylko w przypadkach nagłych, lecz również tych cierpiących na choroby przewlekłe czy też rejestrację zachowań mających wpływ na zdrowie takich jak sen lub nawyki żywieniowe. Badania wskazują, że wdrożenie rozwiązań H-IoT zmniejsza koszt opieki zdrowotnej[4], wskaźnik hospitalizacji[5] oraz poprawia standard opieki nad osobami przewlekle chorymi[6]. Dlatego ich wdrożenie jest priorytetem zarówno podmiotów prywatnych, które chcą zwiększyć w ten sposób swoją przewagę konkurencyjną[7], jak i celem stawianym w krajowych i unijnych politykach rozwoju[8]. Prowadzi to do coraz szerszego wykorzystania tych urządzeń w procedurach medycznych, a trend ten ma tendencję dynamicznie wzrostową.

Jednocześnie funkcjonowanie urządzeń medycznego Internetu rzeczy nie zostało w sposób kompleksowy uregulowane w żadnym akcie prawnym. Jedną z przyczyn jest zróżnicowanie tych urządzeń. Należy zauważyć, że do kategorii H-IoT są zaliczane zarówno wyroby medyczne, których wprowadzanie na rynek i użytkowanie jest regulowane odpowiednimi przepisami prawa[9], jak i rozwiązania, które mogą zmienić dowolne urządzenie w H-IoT na przykład aplikacje do monitorowania aktywności fizycznej instalowane na smartfonach, które nie posiadają dedykowanej regulacji. Ponadto, ze względu na specyfikę ich działania, do urządzeń tych mogą być stosowane przepisy dotyczące ochrony danych osobowych, cyberbezpieczeństwa, odpowiedzialności za produkt niebezpieczny, praw konsumenta czy regulujące problematykę własności intelektualnej.

Brak wprowadzenia regulacji prawnych dotyczących problematyki medycznego Internetu rzeczy może stanowić ponadto wynik świadomej decyzji prawodawcy czy też przejaw niemożności jego szybkiej reakcji na postępujące zmiany technologiczne. Obszary pozostające poza regulacją prawną mogą być jednak normowane środkami pozaprawnymi, wśród których pierwszoplanowe znaczenie mają normy

[1] Uniwersytet im. Adama Mickiewicza w Poznaniu.

[2] *B. Mittelstadt*, Ethics of the health-related internet of things: a narrative review, Ethics and Information Technology 2017, Nr 19(3), s. 157–175.

[3] *B. Mittelstadt*, Ethics of the health-related internet of things…, s. 157–175.

[4] *C. Henderson*, *M. Knapp*, *J.-L. Fernandez*, *J. Beecham*, *S.P. Hirani*, *M. Cartwright*, et al, Cost effectiveness of telehealth for patients with long term conditions (whole systems demonstrator telehealth questionnaire study): Nested economic evaluation in a pragmatic, cluster randomised controlled trial, British Medical Journal 2013, Nr 346, s. 1–19.

[5] *C. Lomas*, Telehealth system slashes hospital admissions in COPD patients, Nursing Times 2009, Nr 105(9), http://www.nursingtimes.net/nursing-practice/clinical-zones/copd/telehealth-system-slashes-hospital--admis-sions-in-copd-patients/5005885.article (dostęp z 24.7.2020 r.).

[6] *D. Su*, *J. Zhou*, *M.S. Kelley*, *T.L. Michuad*, *M. Siahpush*, *J. Kim*, *F. Wilson*, *J.P. Stimpson*, *J.A. Pagánde*, Does telemedicine improve treatment outcomes for diabetes? A meta-analysis of results from 55 randomized controlled trials, Diabetes Research and Clinical Practice 2016, Nr 116.

[7] *L. Sobieski*, Koncepcja e-zdrowia w świetle regulacji publicznoprawnych, [w:] *K. Kokocińska* (red.), Innowacyjne technologie w ochronie zdrowia. Aspekty prawne, Warszawa 2020, s. 35.

[8] *K. Kokocińska*, Działania władzy publicznej na rzecz rozwoju innowacyjnych technologii w sektorze zdrowia (polityka unijna i krajowa), [w:] *K. Kokocińska* (red.), Innowacyjne technologie w ochronie zdrowia. Aspekty prawne, Warszawa 2020, s. 16–32.

[9] Od maja 2021 r. kwestie związane z wyrobami medycznymi będzie regulować rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/745 z 5.4.2017 r. w sprawie wyrobów medycznych, zmiany dyrektywy 2001/83/WE, rozporządzenia (WE) Nr 178/2002 i rozporządzenia (WE) Nr 1223/2009 oraz uchylenia dyrektyw Rady 90/385/EWG i 93/42/EWG, Dz.Urz. UE L Nr 117, s. 1; dalej jako: rozporządzenie 2017/745. Akt ten nie odnosi się w szczególny sposób do urządzeń IoT. Zob. *J. Greser*, Cyberbezpieczeństwo wyrobów medycznych w świetle rozporządzenia 2017/745, iKAR 2020, Nr 2, *passim*.

etyczne oraz normy typu *soft-law*, w szczególności działalność samoregulacyjna uczestników rynku w postaci kodeksów postępowań lub zaleceń branżowych i wytyczne organów władzy publicznej.

Etyka biznesu jako źródło obowiązków przedsiębiorstw

Kwestia przypisania odpowiedzialności etycznej przedsiębiorstwu jest przedmiotem sporu wśród etyków[10]. Zwolennicy jej istnienia twierdzą, że podmiot ten jako jednostka czyniąca dobro i zło nie może całkowicie uciec od ponoszenia odpowiedzialności moralnej za swe czyny. Przeciwnicy wskazują, że osobowość prawna zwalnia z posiadania zobowiązań moralnych, gdyż osoba prawna nie jest podmiotem moralnym, ponieważ nie ma sumienia.

Oczywiste jest, że przedsiębiorstwo nie może posiadać intencji ani motywów analogicznych do zachowań człowieka. Natomiast gdy potraktujemy je jako korelat jednostek, możemy jej przypisać cechy intencjonalne. Przyjmując, że jest to wysoko zorganizowana struktura, w której działania jednostek ukierunkowane są na osiągnięcie celu organizacji, można przyjąć, że istnieje pewien nadrzędny poziom intencji przedsiębiorstwa. Jest on jednak czymś więcej niż sumą intencji pojedynczych jednostek, ponieważ kształtują go również nieformalne relacje pomiędzy pracownikami oraz wartości, normy i przekonania, które są w przedsiębiorstwie akceptowane i przestrzegane[11]. Łącznie składają się one na kulturę organizacyjną, która jest podstawą przypisania odpowiedzialności etycznej przedsiębiorstwu.

Zespół norm regulujący kwestie etyczne związane z prowadzeniem działalności gospodarczej nazywany jest etyką biznesu. Definiowana jest ona jako działania, które są zgodne z prawem i oczekiwaniami społecznymi[12]. O ile zakres pierwszej z tych przesłanek jest względnie łatwy do ustalenia, o tyle w przypadku drugiej może rodzić to problemy. Punktem wyjścia do ustalenia zakresu etycznej odpowiedzialności przedsiębiorstw jest założenie, że działają one na podstawie tak zwanej społecznej licencji na funkcjonowanie (*social license to operate*). Wyznacza ona obszar aktywności ludzkiej, w którym operują podmioty gospodarcze, i zasady, w jakich powinno się to odbywać. Działanie zgodnie z nią wymaga zarówno przestrzegania norm narzuconych, jak np. normy prawne, czy dobrowolnie przyjętych, jak np. normy społecznej odpowiedzialności biznesu[13], jak i takich, które zgodnie ze społecznym oczekiwaniem powinny być przestrzegane[14]. Należy jednak zauważyć, że interpretacja norm etyki biznesu nie ma charakteru uniwersalnego, ponieważ są one formułowane przez pryzmat historii lub kultury danego kraju. Tym samym ma ona charakter krajowy lub wręcz regionalny[15]. Pojawia się zatem możliwość relatywizacji pojęć poprzez nadawanie im autonomicznego znaczenia w etyce biznesu. Tym samym przypisanie odpowiedzialności za naruszenie norm etycznych może być niemożliwe ze względu na trudności z jednoznacznym ustaleniem treści tych norm lub sprzeczność ich treści w różnych miejscach. Jako przykład przywołać można wdrożony w Chinach system do oceny zachowań obywateli (*social credit system*). Jeśli założymy, że takie rozwiązanie jest zgodne z prawem krajowym, to dostarczanie urządzeń do realizacji tego celu nie rodzi konfliktu etycznego z perspektywy przedsiębiorstw chińskich, ale w przypadku przedsiębiorstw europejskich możemy mówić o jego istnieniu ze względu na inne rozumienie koncepcji prywatności.

W przypadku H-IoT sytuację dodatkowo komplikuje fakt globalnego charakteru powiązań związanych z ich tworzeniem i wykorzystywaniem. Jak zauważyła *M. Ossowska*, do osiągnięcia skuteczności sankcji za naruszenie norm etycznych konieczne jest, aby skład grupy społecznej dokonującej oceny postępowania naruszyciela był względnie stały[16]. Zależności w obrębie współczesnego systemu gospodarczego utrudniają, a niejednokrotnie uniemożliwiają ustalenie podmiotu, który dokonał naruszenia norm. Tym samym można przyjąć, że etyka nie jest źródłem norm, na podstawie którego można dochodzić skutecznie jego odpowiedzialności. Nie oznacza to jednak, że istnienie norm etycznych lub powoływanie się na nie jest bezprzedmiotowe. Ich rolą jest zwracanie uwagi na problemy, które pozostają poza sferą regulacji prawnych wraz z przedstawianiem propozycji ich rozwiązań. W tym znaczeniu są one niezwykle przydatne dla ustalenia reguł tworzenia i korzystania z H-IoT, ze względu na możliwość wypełnienia treścią normatywną elementów niedoprecyzowanych przez prawo. Przywoływane w dalszej części artykułu problemy etyczne będę analizował przez ten pryzmat.

[10] Por. *J. Filek*, Wprowadzenie do etyki biznesu, Kraków 2001, s. 110; *G.D. Chryssides*, *J.H. Kaler*, Wprowadzenie do etyki biznesu, Warszawa 1999, s. 248.

[11] *M. Kapusta*, *M. Sukiennik*, *P. Bąk*, Wybrane determinanty kształtujące kulturę korporacyjną, Finanse, Rynki Finansowe, Ubezpieczenia 2017(89), Nr 5, cz. 2, s. 486.

[12] *W. Gasparski*, Wykłady z etyki biznesu. Nowa edycja uzupełniona, Warszawa 2007, s. 95 oraz 108.

[13] *J. Filek*, Wprowadzenie do…, s. 111; *C. Dierksmeier*, *P. Seele*, Cryptocurrencies and Business Ethics, J Bus Ethics 2018, Nr 152, s. 1–14.

[14] *J. Ruggie*, Protect, Respect and Remedy: a Framework for Business and Human Rights, Report of the Special Representative of the United Nations Secretary-General on the issue of human rights and transnational corporations and other business enterprises, 2008, https://www.mitpressjournals.org/doi/pdf/10.1162/itgg.2008.3.2.189 (dostęp z 24.7.2020 r.).

[15] *W. Gasparski*, Wykłady z etyki…, s. 196.

[16] *M. Ossowska*, Socjologia moralności: zarys zagadnień, Warszawa 1969, s. 109–112.

Problematyka prywatności pacjentów korzystających z H-IoT

Prawo do prywatności jest ugruntowanym pojęciem na poziomie prawnym. Ma status prawa człowieka chronionego umowami międzynarodowymi, jak również umocowanie w konstytucjach wielu państw, w tym Polski[17]. W kontekście H-IoT konkretyzacją tego prawa są przepisy chroniące autonomię informacyjną pacjenta zawarte w przepisach o ochronie danych osobowych i regulujących tajemnicę lekarską[18]. Wyznaczają one zakres zachowań poszczególnych podmiotów, który ma gwarantować zachowanie odpowiedniego poziomu prywatności jednostek. Z perspektywy etycznej prywatność ujmowana jest szerzej niż w normach prawnych. W literaturze oprócz zagadnień związanych z prawem do posiadania i ochrony przestrzeni osobistej i bycia pozostawionym w spokoju wskazuje się również, że to pojęcie ma swój materialny wymiar[19]. Inaczej mówiąc, będzie odnosić się do fizycznej obecności urządzeń, których działanie wkracza w sferę prywatności jednostki. Na tym tle rodzą się problemy z wykorzystaniem urządzeń H-IoT, które są na stałe zamontowane w określonych miejscach. W literaturze wskazuje się, że takie rozwiązania mogą prowadzić do stopniowej utraty prywatności i wywoływać uciążliwe poczucie bycia obserwowanym[20]. Jednocześnie instalacja urządzeń w taki sposób, że są one niewidoczne dla osób monitorowanych, tak jak przykładowo czujników w domach opieki, również wywołuje pewne problemy etyczne. Wskazuje się, że w takich przypadkach informacja o działaniu urządzeń oraz ewentualne zgody na ich wykorzystywanie powinny być ponawiane[21]. Należy zauważyć, że takie ponawiane uzyskiwanie zgody wykracza poza obowiązki nałożone normami prawnymi. Przykładowo art. 7 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE[22] zakłada jednorazowe udzielenie zgody, która uprawnia administratora do przetwarzania danych dopóty, dopóki zgoda taka nie zostanie wycofana. W przypadku obowiązków informacyjnych zarówno art. 13 ust. 4, jak i art. 14 ust. 5 lit. a RODO wskazują, że jeżeli osoba już dysponuje informacjami wymaganymi przez przepisy, to nie ma potrzeby ponownego ich przekazywania. Będzie to miało szczególne znaczenie w przypadku przetwarzania danych osobowych przez urządzenia H-IoT, gdyż podstawą prawną tego działania zasadniczo nie będzie zgoda – administrator raczej powoła się na konieczność zapewnienia opieki zdrowotnej lub leczenia (art. 9 ust. 1 lit. h RODO) lub ochrony żywotnych interesów (art. 9 ust. 1 lit. c RODO) w przypadku danych wrażliwych, a w przypadku danych zwykłych wykonanie umowy (art. 6 ust. 1 lit. b RODO), obowiązek prawny (art. 6 ust. 1 lit. c RODO) lub uzasadniony interes administratora (art. 6 ust. 1 lit. f RODO). Może to więc prowadzić do sytuacji, w której wykonanie obowiązku informacyjnego jest jedynym momentem przekazywania informacji o wykorzystywaniu urządzeń H-IoT.

Inny problem etyczny jest związany z wykorzystaniem urządzeń H-IoT, których używanie wymaga zamontowania urządzenia na ciele pacjenta. Będzie to dotyczyło zarówno urządzeń zintegrowanych na stałe, np. rozruszniki serca, jak i takich, które można łatwo usnąć, np. pompy insulinowe czy opaski ułatwiające znalezienie osób cierpiących na zaburzenia pamięci. W literaturze wskazuje się, że widoczność urządzeń może prowadzić do stygmatyzacji ich użytkowników, podobnie jak alarmy i raportowanie przez nie o sytuacjach zagrożenia[23]. Obniża to chęć korzystania z tych urządzeń w długim okresie, tym samym może prowadzić do pogorszenia stanu opieki nad pacjentem zamiast jej polepszenia[24]. Należy zauważyć, że problem ten dotyczy w szczególności urządzeń do zastosowań klinicznych. Badania wskazują, że jeżeli jako H-IoT jest wykorzystywane urządzenie mające w odbiorze społecznym inny cel, np. smartfon, to chęć pacjentów do wykorzystania rozwiązań jest dużo wyższa[25]. Prowadzi to do wniosku, że kluczowym aspektem jest sposób zaprojektowania urządzenia, w trakcie którego koniecznie jest branie pod uwagę wartości i doświadczeń pacjentów, ponieważ od nich będzie zależał poziom akceptacji urządzenia[26]. Należy zauważyć, że rozporządzenie 2017/745 odnosi się do ergonomii wyrobu medycznego w zakresie dotyczącym eliminowania

[17] *M. Wujczyk*, Prawo pracownika do ochrony prywatności, Warszawa 2012, s. 28; *P. Sarnecki*, Komentarz do art. 47, [w:] *L. Garlicki* (red.), *K. Działocha*, *P. Sarnecki*, *W. Sokolewicz*, *J. Trzciński*, Konstytucja Rzeczypospolitej Polskiej. Komentarz. T. III, Warszawa 2001, s. 1.

[18] *J. Greser*, Ochrona danych dotyczących zdrowia a nowoczesne technologie medyczne, [w:] *K. Kokocińska*, Innowacyjne technologie w ochronie zdrowia. Aspekty prawne, Warszawa 2020, s. 137–158.

[19] *A. Essén*, The two facets of electronic care surveillance: An exploration of the views of older people who live with monitoring devices, Social Science & Medicine 2008, Nr 67, s. 128–136; *A. Bowes*, *A. Dawson*, *A. Bell*, Ethical implications of lifestyle monitoring data in ageing research, Information, Communication & Society 2012, Nr 15(1), s. 5–22.

[20] *R. Steele*, *A. Lo*, *C. Secombe*, *Y. Wong*, Elderly per-sons' perception and acceptance of using wireless sensor net-works to assist healthcare, International Journal of Medical Informatics 2009, Nr 78, s. 788–801; *A.M. Dorsten*, *S.K. Sifford*, *A. Bharucha*, *L.P. Mecca*, *H. Wactlar*, Ethical perspectives on emerging assistive technologies: insights from focus groups with stakeholders in long-term care facilities, Journal of Empirical Research on Human Research Ethics 2009, Nr 4, s. 25–36.

[21] *K. Ebersold*, *R. Glass*, The internet of things: A cause for ethical concern, Issues in Information Systems 2016, Nr 17, s. 145–151, http://www.iacis.org/iis/2016/4_iis_2016_145-151.pdf (dostęp z 24.7.2020 r.).

[22] Dz.Urz. UE L Nr 119, s. 1; dalej jako: RODO.

[23] *K.L. Courtney*, *G. Demiris*, *M. Rantz*, *M. Skubic*, Needing smart home technologies: The perspectives of older adults in continuing care retirement communities, Informatics in Primary Care 2008, Nr 16, s. 195–201.

[24] *G. Demiris*, *B.K. Hensel*, „Smart homes" for patients at the end of life, Journal of Housing for the Elderly 2009, Nr 23, s. 106–115.

[25] *B.K. Hensel*, *G. Demiris*, *K.L. Courtney*, Defining obtrusiveness in home telehealth technologies: A conceptual framework, Journal of the American Medical Informatics Association 2006, Nr 13, s. 428–431.

[26] *B. Mittelstadt*, Ethics of the health-related internet of things: a narrative review, Ethics and Information Technology 2017, Nr 19(3), s. 162.

ryzyka związanego z błędem użytkowym (załącznik 1 pkt 5 lit. a oraz pkt 14 ust. 2), wskazując, że wystąpienie takiego błędu trzeba zaliczyć do kategorii incydentu (art. 2 pkt 64). W konsekwencji należy stwierdzić, że inne wartości niż bezpośrednio związane z bezpieczeństwem użytkowania nie są brane przez prawodawcę pod uwagę. Tym samym działania mające na celu zapewnienie komfortu psychicznego użytkowników wykraczają poza obowiązki prawne, ale jednocześnie, ze względu na swój wpływ na jednostkę, można je zaliczyć do zobowiązań o charakterze etycznym.

Własność i dzielenie się danymi generowanymi przez urządzenia H-IoT

Ocenia się, że w 2019 r. ilość danych generowanych przez IoT wyniosła 500 zettabajtów i będzie w kolejnych latach rosła wykładniczo[27]. Jednocześnie wskazuje się na urządzenia H-IoT jako jedno z głównych źródeł tych danych[28]. Wśród problemów etycznych wskazywanych w literaturze, które są związane z gromadzeniem danych na pierwszy plan wysuwają się zagadnienia minimalizacji zbieranych danych oraz dostęp do zgromadzonych informacji przez pacjenta.

Odnosząc się do pierwszej kwestii, należy zauważyć, że H-IoT zbierają i generują zarówno dane osobowe, jak i nieosobowe. W odniesieniu do tych drugich rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1807 z 14.11.2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w UE[29], wprost wskazuje w motywie 3, że swoboda przedsiębiorczości i swoboda świadczenia usług mają zastosowanie do usług przetwarzania danych. Tym samym nie można nakładać ograniczeń ani w zakresie ilości danych, które są gromadzone przez określony podmiot, ani w zakresie działań, które są na nich prowadzone, np. agregacji, analizy, obrotu czy dystrybucji.

W przypadku danych osobowych zagadnienie minimalizacji jest uregulowane prawnie. Artykuł 5 ust. 1 lit. c RODO wskazuje, że można przetwarzać tylko te dane, które są adekwatne, stosowne oraz ograniczone do tego co niezbędne do celów, w których są przetwarzane. Przepis ten ma status zasady przetwarzania, co oznacza, że ma nadrzędną moc wobec pozostałych przepisów, a jednocześnie stanowi dla nich dyrektywę interpretacyjną[30]. Na tej podstawie można przyjąć, że zakres zbieranych danych powinien być wyznaczany potrzebami terapeutycznymi określonego użytkownika. Jednocześnie zbieranie dodatkowych informacji może mieć wpływ na zwiększenie skuteczności terapii albo zmniejszenie częstotliwości występowania skutków ubocznych. Należy przez to rozumieć inne dane niż te, których przetwarzanie nie wynika z obowiązku prawnego lub uzasadnionego interesu administratora, jakim jest bezpieczeństwo urządzenia. Będą to np. metadane, które są źródłem do wyszukiwania ukrytych korelacji za pomocą algorytmów sztucznej inteligencji. Intuicyjnym rozwiązaniem do zastosowania w tym przypadku jest wyrażenie zgody przez użytkownika. Zasadą jest, że w licencjach końcowych producenci urządzenia zastrzegają sobie prawo do agregacji zebranych i udostępniania ich innym podmiotom zarówno dla celów naukowych, jak i komercyjnych. Zasadniczo zgoda jest udzielana na jednorazowe badanie. Jednocześnie etycy wskazują, że w przypadku HIoT bardzo trudno jest doprowadzić do sytuacji, w której zgoda jest świadoma[31]. Wynika to z braku odpowiedniej wiedzy i aparatu poznawczego pacjenta wymaganego, aby zrozumieć poziom szczegółowości zbieranych danych i konsekwencje przeprowadzonych analiz, które, jak się wskazuje, mogą prowadzić do wykluczenia ze świadczenia określonego rodzaju usług[32]. Podobny problem pojawia się przy uzyskaniu zgody na pozyskiwanie danych dotyczących stosowania H-IoT ze źródeł nieformalnych, jak opisy samopoczucia w mediach społecznościowych czy analizy zapytań do wyszukiwarek[33].

Alternatywą jest anonimizacja informacji, co pozbawia je statusu danych osobowych (motyw 26 RODO). Należy jednak pamiętać, że przeprowadzenie takiego procesu jest bardzo trudne, jeśli w ogóle możliwe. Przeprowadzone w 2013 r. testy potwierdziły, że odpowiednio gęste ułożenie anten BTS pozwala na jednoznaczną identyfikację 95% osób, które korzystały z telefonów komórkowych[34]. W przypadku urządzeń H-IoT, których konstrukcja wymaga stałego kontaktu z Internetem, można założyć, że wynik ten byłby porównywalny.

Drugim wskazywanym problemem jest dostęp pacjentów do zgromadzonych danych zbieranych przez urządzenia H-IoT. W typowej sytuacji można wyróżnić trzy grupy podmiotów. Pierwszą jest producent urządzenia, który dysponuje wszystkimi zebranymi informacjami, zarówno przetworzonymi, jak i nieprzetworzonymi, które są generowane przez urządzenie. Drugą grupę stanowią podmioty wykonujące działalność leczniczą. Zakres przekazywanych

[27] Cisco, Cisco Annual Internet Report (2018-2023) White Paper, 2020 https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.html (dostęp z 24.7.2020 r.).

[28] *J. Lima*, 10 of the biggest IoT data generators, Computer Business Review, 2015, https://www.cbronline.com/internet-of-things/10-of-the-biggest-iot-data-generators-4586937/ (dostęp z 24.7.2020 r.).

[29] Dz.Urz. UE L Nr 303, s. 59; dalej jako: rozporządzenie 2018/1807.

[30] *P. Drobek*, Komentarz do artykułu 5, [w:] *E. Bielak-Jomaa*, *D. Lubasz* (red.), RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, Warszawa 2018, s. 323–324.

[31] *M.J. Bietz*, *C.S. Bloss*, *S. Calvert*, *J.G. Godino*, *J. Gregory*, *M.P. Claffey*, et al, Opportunities and challenges in the use of personal health data for health research, Journal of the American Medical Informatics Association 2016, Nr 23(e1), s. 42–48; *K. Denecke*, *P. Bamidis*, *C. Bond*, *E. Gabarron*, *M. Househ, A.Y.S. Lau*, et al, Ethical issues of social media usage in healthcare, IMIA Yearbook of Medical Informatics 2015, Nr 10(1), s. 137–47.

[32] *B. Mittelstadt*, Ethics of the health-related internet…, s. 165.

[33] *Ibidem*, s. 165.

[34] *Y.A. de Montjoye*, *A.C. Hidalgo*, *M. Verleysena* i *V.D. Blondela*, Unique in the Crowd: The privacy bounds of human mobility, Nature 2013, s. 1376.

danych zależy od umów dotyczących korzystania z H-IoT. Najczęściej przybierają one formę licencji dla użytkownika końcowego i obejmują określony zestaw informacji dotyczący bezpośrednio stanu zdrowia pacjenta. Pomijane są więc metadane i inne informacje, które nie mają bezpośredniego związku z leczeniem. Trzecią grupą są pacjenci, którzy mogą otrzymywać uproszczony zestaw podstawowych informacji wraz z ich interpretacją lub otrzymywać zinterpretowane informacje wyłącznie od lekarza.

Na tym tle pojawia się kilka wątpliwości. Po pierwsze, zebrane dane mają wartość finansową, której beneficjentem jest producent urządzenia. Podmiot ten nie dzieli się przy tym zyskami z pacjentami. Podobnie jak w przypadku badań w przemyśle farmaceutycznym, podmioty badań mogą dysponować roszczeniem do udziału w zysku z produktów i usług powstałych dzięki przekazaniu danych. Źródła takiego roszczenia należy upatrywać w normach etycznych, a nie prawnych[35].

Po drugie, podmioty prywatne nie mają żadnego obowiązku dzielenia się uzyskanymi informacjami. Dysponowanie danymi w zakresie ich sprzedaży, licencjonowania czy tworzenia baz danych regulowane są przez prawo cywilne. Głównym podmiotem zainteresowanym dostępem do danych są naukowcy, dla których jest to otwarcie nowych możliwości w badaniach. Dotyczy to zarówno obszaru medycyny, jak i nauk społecznych czy humanistyki. Trzeba pamiętać, że w przypadku podmiotów publicznych istnieją normy kształtujące zasady ponownego wykorzystania danych. W UE wynikają one z dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/1024 z 20.6.2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego[36]. Jednocześnie wskazuje się, że normy praw człowieka, w szczególności w zakresie prawa do najwyższego osiągalnego standardu zdrowia, jak też wolności akademickiej, mogą ograniczać prawa własności intelektualnej, jednakże w praktyce ma to znikome znaczenie[37].

Kolejnym problemem jest obawa, że nieograniczony dostęp do surowych danych może zaszkodzić pacjentowi ze względu na możliwe problemy z ich interpretacją wynikającą z braku odpowiedniej wiedzy i doświadczenia[38]. Jak się wskazuje, przyjęcie założenia, że takie osoby zdobędą odpowiednie zasoby do interpretacji, jest nieracjonalne[39]. Jednocześnie udostępnienie nieprzetworzonych informacji może mieć zasadnicze znaczenie dla postawienia alternatywnej diagnozy przez innego lekarza. Należy zauważyć, że art. 20 RODO zawiera prawo do przeniesienia danych zgromadzonych przez administratora. Należy jednak zauważyć, że dotyczy ono tylko danych osobowych, a więc poza zakresem normowania mogą być informacje niemające takiego charakteru, a cenne z perspektywy diagnostycznej, jak np. czas zażywania leku. Ponadto prawo to dotyczy wyłącznie danych przetwarzanych na podstawie zgody (art. 6 ust. 1 lit. a RODO lub art. 9 ust. 2 lit. a RODO) lub na podstawie umowy (art. 6 ust. 1 lit. b RODO). Wyłącza to zatem informacje o stanie zdrowia, które przetwarzane są na podstawie art. 9 ust. 1 lit. h RODO będącego podstawą najczęściej wykorzystywaną w trakcie świadczenia usług medycznych.

Czwartym problemem jest format danych. Pomimo że art. 20 ust. 1 RODO wprost wskazuje, że dane powinny być przekazane w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, to brak interoperacyjności urządzeń IoT jest powszechnie występującym problemem w praktyce[40].

Ostatnim zagadnieniem związanym z ograniczonym dostępem do danych zbieranych przez H-IoT jest niemożność oceny prawidłowości działania urządzenia przez osoby trzecie. W przypadku wyrobów medycznych kwestia ta jest przedmiotem regulacji prawnych określających zasady klasyfikowania i certyfikowania urządzeń pod kątem bezpieczeństwa, do których należy wspomniane powyżej rozporządzenie 2017/745. Jednocześnie wskazuje się, że system ten może mieć wady, szczególnie w przypadku nowoczesnych technologii. Problem ten dotyczy różnych technologii medycznych[41], ale można go zilustrować amerykańskim przykładem urządzenia do leczenia bezdechu sennego. Urządzenie to było skonfigurowane w taki sposób, że jego działanie nie przynosiło korzyści terapeutycznych pacjentom odbiegającym od założonej przez producenta średniej[42]. Jednocześnie pacjent nie miał możliwości ani konfiguracji urządzenia pod kątem swoich potrzeb, ani dostępu do informacji, które urządzenie zbierało, co mogłoby potwierdzić brak zysków terapeutycznych z jego używania. Dowody dotyczące skuteczności terapii uzyskano, zmieniając oprogramowanie sterujące urządzeniem, co było naruszeniem warunków licencji i spotkało się z prawną reakcją producenta urządzenia, który zażądał zwrotu urządzeń

[35] *S. Chapman*, *E. Reeve*, *G. Rajaratnam*, *R. Neary*, Setting up an outcomes guarantee for pharmaceuticals: new approach to risk sharing in primary care, British Medical Journal 2003, Nr 326(7391), s. 707; *A. Petryna*, *A. Lakoff*, *A. Kleinman*, Global pharmaceuticals: Ethics, markets, practices, Durham 2006, s. 301.

[36] Dz.Urz. UE L Nr 172, s. 56; dalej jako: dyrektywa 2019/1024.

[37] *J. Greser*, Prawa autorskie a prawa człowieka, [w:] *J. Kępiński*, *K. Klafkowska-Wiśniowska*, *R. Sikorski* (red.), Granice prawa autorskiego, Warszawa 2010, s. s. 202–206.

[38] *D. Boyd*, *K. Crawford*, Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon, Information Communication & Society 2012, Nr 15(5), s. 662–679.

[39] *M. Andrejevic*, Big data, big questions, the big data divide, International Journal of Communication 2014, Nr 8(0), s. 17.

[40] Problem ten jest przedmiotem badań Komisji Europejskiej pod kątem naruszania reguł konkurencji. Zob. Antitrust: Commission launches sector inquiry into the consumer Internet of Things (IoT), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1326 (dostęp z 24.7.2020 r.).

[41] *S. Hanselman*, The Promising State of Diabetes Technology in 2016, https://www.hanselman.com/blog/ThePromisingStateOfDiabetesTechnologyIn2016.aspx (dostęp z 24.7.2020 r.).

[42] *A. Wesołowska*, Hakowanie warunkiem przeżycia – o łamaniu zabezpieczeń, które ratuje pacjentów, Zaufana Trzecia Strona, https://zaufanatrzeciastrona.pl/post/hakowanie-warunkiem-przezycia-o-lamaniu-zabezpieczen-ktore-ratuje-pacjentow/ (dostęp z 24.7.2020 r.).

i groził wszczęciem postępowań karnych. Trzeba zwrócić uwagę, że w tym przypadku pojawia się również zagadnienie udostępnienia danych osobom, które mogą mieć problem z ich właściwą interpretacją. Natomiast z perspektywy etycznej zachowanie przedsiębiorstwa nie może być uznane za zgodne z tymi normami.

Problemy etyczne a zapewnienie cyberbezpieczeństwa H-IoT

Cyberbezpieczeństwo nie jest rozważane jako osobna kwestia etyczna, ale wskazuje się na bardzo silny związek tego zagadnienia z prywatnością[43]. Należy podzielić ten pogląd, jednocześnie zwracając uwagę, że cele działań na rzecz bezpieczeństwa i prywatności są różne. W pierwszym przypadku będzie to zapewnienie „poufności, integralności i dostępności"[44] informacji, co pozwala osobie, której dane dotyczą, zachować prywatność w rozumieniu sprawowania kontroli nad tym, jak są one wykorzystywane[45]. Tym samym cele te są współzależne, a więc nie sposób zrealizować jednego bez realizacji drugiego.

Problematyka cyberbezpieczeństwa jest w pewnym zakresie regulowana przez normy prawne[46]. Poza tymi przepisami pozostaje część obszarów wykorzystania H-IoT, co wynika zarówno z celowych działań prawodawcy – jak w przypadku braku narzucania określonych standardów zabezpieczeń – jak i niewprowadzania takich regulacji z powodu opóźnień w reakcji organów państwa na zmiany technologiczne. W literaturze wskazuje się, że w takich przypadkach producent, tworząc standardy zabezpieczeń, powinien kierować się normami etyki biznesu[47].

Wśród zagadnień, które są przynajmniej częściowo regulowane normami etycznymi, można wskazać obowiązki producenta do dostarczania wsparcia dla urządzenia wycofanego ze sprzedaży. Należy zauważyć, że wyroby takie, nazywane *orphant devices*, stanowią istotne zagrożenie dla bezpieczeństwa osób z nich korzystających[48]. Problem ten został zauważony przez prawodawcę europejskiego i zaowocował wydaniem dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/770 z 20.5.2019 r. w sprawie niektórych aspektów umów o dostarczanie treści cyfrowych i usług cyfrowych[49] oraz dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/771 z 20.5.2019 r. w sprawie niektórych aspektów umów sprzedaży towarów, zmieniająca rozporządzenie (UE) 2017/2394 oraz dyrektywę 2009/22/WE i uchylająca dyrektywę 1999/44/WE[50], które częściowo regulują tę kwestię. Należy jednak zwrócić uwagę, że termin transpozycji przepisów został wskazany na 1.7.2021 r., a nie mogą one wejść w życie później niż 1.1.2022 r. Do tego czasu na producentach nie ciążą zobowiązania wynikające z przepisów prawa. Nie zmienia to jednak faktu istnienia obowiązku etycznego, który obciąża producenta. W tym zakresie można wyróżnić co najmniej trzy sytuacje. Pierwsza, gdy producent jasno deklaruje użytkownikowi, jaki jest cykl życia produktu i kiedy zakończy dla niego wsparcie oraz jakie konsekwencje są z tym związane. Druga, gdy nie ma takiego komunikatu, a wycofanie się ze wsparcia zależy od decyzji biznesowej. Trzecia obejmuje przypadki, gdy wycofanie się ze wsparcia produktu wynika z czynników zewnętrznych takich jak ogłoszenie niewypłacalności producenta.

Wspólny dla tych sytuacji jest wynikający z norm etycznych nakaz poinformowania użytkowników o zakończeniu wsparcia, związanych z tym konsekwencjach i potencjalnych ryzykach wynikających z dalszego korzystania z urządzenia. W przypadku H-IoT konieczne będzie również poinformowanie odpowiednich organów nadzorujących rynek wyrobów medycznych. Producent może również rozważyć uniemożliwienie korzystania z urządzenia poprzez jego programowe wyłączenie. Takie działanie musi być jednak poprzedzone staranną analizą, której wyniki wskażą, że ryzyko dalszego wykorzystania urządzenia znacznie przewyższa korzyści, które uzyskuje pacjent. Szczególnie należy wziąć pod uwagę możliwości wtórnego wykorzystania urządzenia przez pacjentów, którzy wcześniej nie mieli do niego dostępu ze względu na cenę.

Jednocześnie powinno się rozważyć udostępnienie plików źródłowych programów sterujących urządzeniem wraz z jego dokumentacją techniczną oraz objęcie ich wolną licencją. Taki zabieg pozwoli na rozwijanie oprogramowania przez grupy niezależnych programistów i dalsze utrzymywanie funkcjonalności urządzenia. Trzeba jednak zwrócić uwagę na liczne problemy, które mogą pojawić się w związku z takim działaniem zarówno w sferze prawnej, jak i praktycznej. W pierwszej z nich znaczącą rolę będą odgrywały regulacje

[43] *M. Chan*, *D. Estève*, *C. Escriba*, *E. Campo*, A review of smart homes: Present state and future challenges, Computer Methods and Programs in Biomedicine 2008, Nr 91, s. 55–81; *M. Mana*, *M. Feham*, *B.A. Bensaber*, Trust key management scheme for wireless body area networks, International Journal of Network Security 2011, Nr 12, s. 75–83; *H.F. Atlam*, *G.B. Wills*, IoT Security, Privacy, Safety and Ethics, [w:] *M. Farsi*, *A. Daneshkhah*, *A. Hosseinian-Far, H. Jahankhani* (red.), Digital Twin Technologies and Smart Cities, Internet of Things, Technology, Communications and Computing, Cham 2020, s. 140–141.

[44] *F. Giannotti*, *Y. Saygin*, Privacy and security in ubiquitous knowledge discovery, Lecture Notes in Computer Science, Berlin 2010, s. 75.

[45] *S.R. Peppet*, Regulating the internet of things: First steps toward managing discrimination, privacy, security and consent, Texas Law Review, 2014, 93, s. 85; *A. Greenfield*, Some guidelines for the ethical development of ubiquitous computing, Philosophical Transactions of the Royal Society A 2008, Nr 366(1881), s. 3823–3831.

[46] *C. Banasiński*, Prawne i pozaprawne źródła wymagań dla systemów cyberbezpieczeństwa, [w:] *C. Banasiński*, *M. Rojszczak* (red.), Cyberbezpieczeństwo, Warszawa 2020, s. 15.

[47] *M. Flyverbom*, *R. Deibert*, *D. Matten*, The Governance of Digital Technology, Big Data, and the Internet: New Roles and Responsibilities for Business, Business & Society 2019, Nr 58(1), s. 3–19.

[48] (Marvin 2017).

[49] Dz.Urz. UE L Nr 136, s. 1; dalej jako: dyrektywa 2019/770.

[50] Dz.Urz. UE L Nr 136, s. 28; dalej jako: dyrektywa 2019/771.

związane z własnością intelektualną. Chodzi tu w szczególności o licencje do określonych komponentów programu, takich jak biblioteki programistyczne lub bazy danych, które zostały udzielone producentowi urządzenia. W standardowej sytuacji uniemożliwiają one ich wykorzystanie przez podmioty inne niż strony umowy. Zatem nie będzie możliwości prawnej do rozszerzenia kręgu licencjobiorców. W sferze praktycznej natomiast publikacja kodu źródłowego może pogorszyć poziom cyberbezpieczeństwa urządzenia, ponieważ wgląd do niego będą miały osoby chcące wykorzystać jego podatności. Udostępnienie kodu w formie otwartej znacznie ułatwia jego analizę, a tym samym wykrycie luk w bezpieczeństwie.

Rozważając sytuację, w której brak wsparcia wynika z niewypłacalności producenta, należy zauważyć, że dochodzi do naruszenia jego deklaracji dotyczących cyklu życia produktu, ale wynika ono z przyczyn od niego niezależnych. W tym przypadku zasadnicze znaczenie będzie miała forma upadłości. W sytuacji gdy prowadzi ona do likwidacji przedsiębiorstwa i nie ma podmiotu, który wchodzi w jego prawa i obowiązki, wydaje się, że konieczne jest przeprowadzenie procedury informacyjnej opisanej powyżej. Dobrą praktyką będzie też wskazanie producentów lub urządzeń komplementarnych, które mogą zastąpić produkowane rozwiązanie. Natomiast jeżeli prawa do urządzenia zostaną przejęte przez inny podmiot, to nabywa on również obowiązki etyczne związane z urządzeniem. Tym samym wsparcie dla użytkowników powinno być świadczone na zasadach ustalonych przez pierwotnego producenta.

Wśród innych problemów etycznych związanych z korzystaniem z H-IoT można wskazać zakres podejmowanych działań, w przypadku gdy luka w zabezpieczeniach urządzenia wynika z błędu podwykonawcy, oraz kwestie związane ze standaryzacją rozwiązań. Objętość niniejszego opracowania uniemożliwia ich rozwinięcie, jednak warto zasygnalizować, że w pierwszym przypadku konieczne będzie ustalenie, jakie są obowiązki producenta w zależności od tego, czy oprogramowanie było tworzone na zamówienie, czy jest częścią istniejącego programu. W drugim natomiast trzeba zwrócić uwagę na zagadnienie interoperacyjności urządzeń i protokołów, którą wskazuje się jako kluczową dla bezpieczeństwa[51], oraz zestawić je z polityką sprzedażową preferującą tworzenie odrębnych standardów, nad którymi tylko producent sprawuje kontrolę.

Podsumowanie

Korzyści wynikające z wdrażania rozwiązań H-IoT zarówno dla pacjentów, jak i podmiotów systemu ochrony zdrowia, prowadzą do coraz szerszego stosowania tej technologii. W przypadku UE normy prawne będą w różnym stopniu regulowały zasady korzystania w nich w zależności od tego, czy będziemy mieli do czynienia z wyrobem medycznym czy z produktem zbierającym informacje o stanie zdrowia. Jednocześnie do obu typów urządzeń mogą znaleźć zastosowanie przepisy dotyczące ochrony danych osobowych czy cyberbezpieczeństwa. Mimo tego, jak wskazywałem powyżej, brakuje norm prawnych regulujących niektóre, ważne aspekty związane z korzystaniem z tej technologii. W literaturze wskazuje się, że w przypadku urządzeń H-IoT oczekuje się wyjścia administratorów poza wyłącznie wymagania prawne[52]. Ten pogląd należy podzielić, zaznaczając jednak, że etyka biznesu będzie formułować wyłącznie metacele, które będą konkretyzowane na poziomie samoregulacji branżowych takich jak kodeksy postępowania. Takie działanie likwiduje mankament norm etycznych polegający na zróżnicowaniu ich treści, która prowadzi do możliwości arbitralnego ich rozumienia. Jednocześnie przedsiębiorstwo przystępujące do kodeksu nie będzie mogło twierdzić, że norma w nim zawarta nie obowiązuje go, co rozwiązuje problem ustalenia obowiązywania normy etycznej. Ponadto naruszanie postanowień kodeksu postępowania może prowadzić do odpowiedzialności prawnej. Artykuł 6 ust. 2 lit. b dyrektywy Parlamentu Europejskiego i Rady (UE) 2005/29/WE z 11.5.2005 r. dotyczącej nieuczciwych praktyk handlowych stosowanych przez przedsiębiorstwa wobec konsumentów na rynku wewnętrznym oraz zmieniającej dyrektywę Rady (UE) 84/450/EWG, dyrektywy 97/7/WE, 98/27/WE, 2002/65/WE Parlamentu Europejskiego i Rady (UE) oraz rozporządzenia (WE) Nr 2006/2004 Parlamentu Europejskiego i Rady (UE)[53] wskazuje, że takie działanie jest nieuczciwą praktyką rynkową, których stosowanie w zależności od wyboru państwa członkowskiego naraża na odpowiedzialność cywilną lub administracyjną.

Odnosząc się do szczegółowych problemów, należy podkreślić, że prywatność ma węższą definicję w prawie niż etyce. W pierwszym przypadku, mimo licznych dyskusji, koncentruje się wokół koncepcji *right to be alone* sformułowanej pod koniec XIX w. przez *S. Warrena* i *L. Brandeisa*, a więc skupia się na ochronie przed zewnętrzną ingerencją w prywatność. W drugim wymiarze obejmuje ono również aspekty wewnętrzne życia jednostki. Przywołany przykład urządzeń monitorujących znajdujących się w ciele pacjenta pokazuje, jak istotną rolę odgrywa zbadanie potrzeb pacjentów w kontekście projektu zewnętrznego urządzenia i jego funkcjonalności. O ile wymóg bezpieczeństwa ma źródło w przepisach prawa, o tyle dbałość o dobrostan użytkownika należy do zobowiązań etycznych.

[51] *S.R. Peppet*, Regulating the internet of things…, s. 85; *A. Greenfield*, Some guidelines for the ethical development…, s. 3823–3831.

[52] *S. Wachter*, *B. Mittelstadt*, *L. Floridi*, Why a right to explanation of automated decision-making does not exist in the general data protection regulation, International Data Privacy Law, Social Science Research Network 2017, s. 76–99, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903469 (dostęp z 24.7.2020 r.); *B. Mittelstadt*, Ethics of the health-related internet…, s. 166.

[53] Dz.Urz. UE L Nr 149, s. 22; dalej jako: dyrektywa 2005/29/WE.

Na prywatność rzutuje też kwestia monitorowania zachowań użytkowników H-IoT. Kwestia ta podlega regulacjom prawnym i, co do zasady, prowadzenie takiego monitoringu jest dopuszczalne. Rozważając tę kwestię z perspektywy RODO, trzeba zauważyć, że zachowanie standardu prawnego – to jest znalezienie podstawy przetwarzania i zrealizowanie obowiązku informacyjnego – może być niewystarczające z perspektywy oczekiwań użytkownika. W tym względzie należy postulować ponawianie wykonania tego obowiązku, szczególnie w sytuacji gdy monitoring prowadzony jest za pomocą urządzeń niewidocznych dla użytkownika. Wydaje się, że w celu wypełnienia zobowiązań etycznych taka informacja powinna być przekazana osobiście pacjentowi przez osobę, która ułatwi zrozumienie treści komunikatu i wyjaśni ewentualne wątpliwości pojawiające się w związku z jego treścią. Ma to szczególne znaczenie, w sytuacji gdy komunikat kierowany jest do osób o ograniczonych funkcjach poznawczych.

Problematyka etyczna dzielenia się danymi sprowadza się do dylematu, w jaki sposób wyważyć dobro prywatne, jakim jest prawo własności danych i czerpanie związanych z nim przychodów oraz dobro publiczne, jakim jest dostęp do nich dla celów naukowych. Wydaje się, że rozwiązaniem może być taka implementacja dyrektywy 2019/1024, która w zakresie ponownego wykorzystania danych będzie obejmowała również podmioty prywatne. Należy zauważyć, że motyw 39 tego aktu prawnego wskazuje, że państwa członkowskie mogą również postanowić o stosowaniu jej wymogów do przedsiębiorstw prywatnych, w szczególności tych, które świadczą usługi w interesie ogólnym. Istotne w tym przypadku byłoby stworzenie minimalnego standardu na poziomie europejskim w celu zachowania takich samych reguł konkurencji.

W przypadku dostępu pacjenta do danych zgromadzonych przez urządzenie wydaje się, że z perspektywy etycznej prawo do uzyskania diagnozy przez innego specjalistę przeważa nad własnościowymi uprawnieniami producenta urządzenia. Obejmuje to informacje, co do których obowiązek przekazania nie wynika z art. 20 RODO lub innych przepisów prawnych. Jednocześnie po udostępnieniu danych producent urządzenia nie jest obarczony odpowiedzialnością, etyczną lub prawną, za ich dalsze wykorzystanie.

W obszarze cyberbezpieczeństwa problematyka etyczna stosowania H-IoT obejmuje między innymi zapewnienie wsparcia dla użytkownika polegającego na dostarczaniu aktualizacji oprogramowania. Problem jest tym istotniejszy, że ewentualny atak może mieć skutki bezpośrednio w sferze życia i zdrowia pacjenta. W przypadku wyrobów medycznych można przyjąć, że brak takiego wsparcia jest przesłanką do usunięciu produktu z rynku, ze względu na niespełnienie kryterium bezpieczeństwa użytkowania. W stosunku do innych H-IoT sytuacja wydaje się dużo bardziej złożona, a spełnienie wymogów etycznych będzie uzależnione od przyczyny zaprzestania wsparcia.

Poruszone w niniejszym artykule problemy są jedynie przykładami dylematów etycznych, które powstają w związku z korzystaniem z H-IoT. W kontekście dyskusji na ten temat pojawiają się zagadnienia dyskryminacji ze względu na błędy w algorytmach obsługujących H-IoT, interoperacyjności urządzeń, tworzenia na podstawie zebranych danych profili konsumenckich i sprzedawanie ich przedsiębiorstwom ubezpieczeniowym lub marketingowym czy izolacji społecznej związanej z mniejszą koniecznością interakcji z człowiekiem. Kolejne wyzwania będą się pojawiać wraz z rozwojem tej technologii. Bez wątpienia prawo nie powinno być jedynym źródłem normowania w tym zakresie, ale ze względu na swoje mankamenty, a w szczególności opóźnienie ustawodawcy wobec zmian społecznych, kwestie etyczne powinny być również ważną częścią tworzenia regulacji. Szczególnie należy postulować wsparcie dla tworzenia samoregulacji branżowych, które wydają się najefektywniejszą formą instytucjonalizacji etyki biznesu.

Słowa kluczowe: Internet rzeczy, wyrób medyczny, prywatność, cyberbezpieczeństwo, RODO.

Ethical problems of implementing the Internet of Medical Things

In the present article, the author brings up the issue connected with the implementation of the Internet of Medical Things. The literature emphasizes that there are ethical dilemmas regarding the use of H-IoT devices which are popular among researchers since the beginning of this technology and they are being analyzed from different perspectives, all of which raise different doubts. The author presents chosen ethical problems from the perspective of manufacturers of these devices which are located in the EU. The article is divided into four parts. The first one is an introduction to issues connected with business ethics – a specific set of rules of which the recipients are entrepreneurs. Secondly, there is an analysis of privacy in the area connected with stigmatization regarding the use of H-IoT devices and problems regarding ownership of data collected by these devices, and ensuring cybersecurity of their users.

Keywords: Internet of Medical Things, medical device, privacy, cybersecurity, GDPR.