Białostockie Studia Prawnicze
2020 vol. 25 nr 2

DOI: 10.15290/bsp.2020.25.02.13

Received: 17.03.2020
Accepted: 16.06.2020

Katarzyna Konopka
Uniwersytet w Białymstoku, Polska
katarzynakonopka@opoczta.pl
ORCID ID: https://orcid.org/0000-0003-1758-2185

Ochrona tajemnicy medycznej w e-zdrowiu

Protection of Medical Privilege in eHealth

Abstract: This article exposes legal and moral concerns regarding medical privilege and safety of patients' medical data in association with the area of eHealth. Digital technology in modern society provides unbelievable opportunities for patients, but also challenges for their privacy. The availability and incorporation of digital technology in almost every aspect of life provides not only opportunities, but also challenges. The security of medical information in the context of medical privilege seems to be at risk, especially in the mHealth area.

This article focuses on the emerging privacy issues regarding medical privilege in eHealth. The article analyzes the framework for eHealth in the Polish legal system, with consideration of current legal acts, in relation to medical privilege and security of patients' data, especially in mHealth and the Internet of Things. Due to the delicate nature of information about patients in medicine, it is strongly needed to balance the safeguarding of data and privacy with the development of eHealth.

Keywords: eHealth, medical privilege, data protection
Słowa kluczowe: e-zdrowie, przywilej medyczny, ochrona danych

Wprowadzenie

W sformułowanej przez Ruth Gavison[1] koncepcji prywatności jej podstawowym elementem, obok kwestii gwarancji uprawnień do poszanowania samotności i anonimowości jednostki, jest tajemnica. Podstawową cechą informacji stanowiących tajemnicę powinna być według tej tezy poufność, czyli zachowanie w dyskrecji uzyskanych wiadomości.

Termin ten został także zdefiniowany w przepisach z zakresu ochrony danych osobowych oraz informatyzacji podmiotów publicznych – według § 2 pkt 14 roz-

1 R. Gavison, Privacy and the limits of law, "The Yale Law Journal" 1980, vol. 89, nr 3, s. 423.

porządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[2] poufność to właściwość zapewniająca, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym podmiotom.

Tajemnica lekarska jest jedną z najstarszych oraz najważniejszych tajemnic, należących do kategorii zawodowych. Stanowi ona podstawową gwarancję ochrony prywatności pacjenta w związku z udzielaniem świadczeń zdrowotnych. Zachowanie jako poufnych wiadomości związanych z pacjentem i jego stanem zdrowia jest nie tylko istotne, jeśli chodzi o poszanowanie prawa do prywatności i intymności, ale też przyczynia się do utrzymania zaufania między stronami stosunku medycznego. Stanowi jasny sygnał dla pacjent, że jego autonomia i podmiotowość jest szanowana i chroniona.

Zachowanie tajemnicy zawodów medycznych gwarantują przepisy prawa krajowego i międzynarodowego. Podstawowe regulacje w prawie polskim są zawarte w rozdziale IV ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta[3]. Mają one porządkujący charakter, definiują najważniejsze elementy przedmiotowe i podmiotowe, powiązane z tajemnicami zawodów medycznych. Tajemnica medyczna swoim zakresem obejmuje również ochronę danych medycznych, zbieranych w trakcie udzielania świadczenia leczniczego.

W związku z rozwojem społeczeństwa cyfrowego kwestia ochrony zdrowia również przeniosła się na grunt cyberprzestrzeni, co sprawiło, iż zachodzą poważne obawy co do bezpieczeństwa danych medycznych i gwarancji ich ochrony. Bezsprzeczne jest, iż na przestrzeni ostatnich lat Internet zrewolucjonizował społeczeństwo we wszystkich sferach życia. Popularyzację użycia sieci łączności na odległość przyrównać można do rewolucji przemysłowej wieku XIX w. Algorytmy i zbiory danych wypełniają współczesny sen o życiu, które jest łatwe, sprawne, wydajne i zoptymalizowane. Należy jednak tu zadać pytanie, czy powierzenie danych tak wrażliwych, jak informacje dotyczące stanu zdrowia, jest rozwiązaniem, które rzeczywiście służy człowiekowi.

2 Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2012 r. poz. 526 ze zm.).

3 Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (tekst jedn. Dz.U. 2009 r. Nr 52, poz. 417 ze zm., dalej jako: u.p.p.)

1. Definicja i pozycja e-zdrowia w systemie prawa polskiego

Termin „e-zdrowie" oznacza wykorzystanie technologii służących medycynie w sektorze zdrowia[4]. Telemedycyna natomiast odnosi się do wykorzystania technologii medycznych przy udzielaniu świadczeń medycznych. Wydaje się, że wprowadzenie technologii komunikacji na odległość wobec istniejących problemów będzie ruchem naturalnym i nieuniknionym. Wprowadzanie i przepływ informacji o zdrowiu oraz sytuacji medycznej pacjenta przy użyciu danych elektronicznych i łączności na odległość jest główną częścią składową usług e-zdrowia. Z uwagi na charakter tych czynności występują tu liczne zagrożenia ochrony dobra osobistego, jakim jest prywatność każdej jednostki.

Polski system prawny nie zawiera definicji legalnej telemedycyny, stąd w zależności od indywidualnych preferencji może być ona poczytywana jako alternatywna dla standardowej, obejmującej kontakt fizyczny, procedury udzielania świadczenia zdrowotnego w tym samym miejscu geograficznym, dla formy wymiany informacji między lekarzem a pacjentem[5] bądź też jako kategoria zbiorcza dla nowych procedur medycznych, które wykorzystują informatykę i telekomunikację w medycynie[6].

Rozwój technologii oraz potrzeba szybkich konsultacji specjalistycznych, skonfrontowana z niewystarczającymi zasobami ludzkimi i finansowymi, od lat wymusza w praktyce medycznej sięganie po nowe rozwiązania, nieprzewidziane w prawodawstwie aktualnie obowiązującym lub przez nie wykluczonym; prowadzi to do konkluzji, iż rozwój telemedycyny następował pomimo obowiązujących przepisów, a nie z ich pomocą. Ustawodawca dopuścił orzekanie przez lekarza o stanie zdrowia pacjenta po zbadaniu go za pomocą systemów teleinformatycznych lub systemów łączności w 2015 r. Przepisy ustawy z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty[7] nie wprowadzają ograniczeń co do rodzaju konsultacji, uzależniając ją od specjalności lekarza, wieku osoby konsultowanej czy przyczyny konsultacji – wyjątkiem są tutaj regulacje ustawy z dnia 19 sierpnia 1994 r. o ochronie zdrowia psychicznego[8] oraz ustawa z dnia 15 czerwca 2007 r. o lekarzu sądowym (tekst jedn. Dz.U. Nr 123, poz. 849)[9], gdzie zastrzeżono obowiązek uprzedniego osobistego zbadania pacjenta, przy określeniu uprawnień lekarza, przysługujących w ramach tychże regu-

4 E. Sarnacka, Telemedycyna i eRecepta – nowe wyzwania legislacyjne, (w:) J. Sobczak, M. Reshef (red.), Nowe procedury medyczne a prawo, Toruń 2016, s. 268.

5 G. Glanowski, Telemedycyna w świetle ustawy o zawodach lekarza i lekarza dentysty, „Monitor Prawniczy" 2015, nr 18, s. 978.

6 *Ibidem*.

7 Ustawa z dnia 5 grudnia 1996 r. o zawodzie lekarza i lekarza dentysty(tekst jedn. Dz.U. z 1997 r. Nr 28, poz. 152 ze zm., dalej jako: u.z.l.).

8 Ustawa z dnia 19 sierpnia 1994 r. o ochronie zdrowia psychicznego (tekst jedn. Dz.U. Nr 111, poz. 535 ze zm., dalej jako: u.o.z.p.).

9 Ustawa z dnia 15 czerwca 2007 r. o lekarzu sądowym (tekst jedn. Dz.U. Nr 123, poz. 849).

lacji – jest to jednak uzasadnione, zważywszy na specyfikę wykonywanych przez lekarza psychiatrę i lekarza sądowego czynności.

Prawo do prywatności, jeżeli chodzi o kwestie związane ze zdrowiem człowieka i informacjami tego dotyczącymi, to nie tylko problematyka polegająca na potrzebie intymności czy wyboru faktów, które chcemy ujawnić; informacje o naszym zdrowiu to też problematyka kwestii biznesowej, komercyjnej. Dzięki posiadaniu odpowiednich danych dotyczących stanu zdrowia można tworzyć profilowane pod danego pacjenta treści oferowane w marketingu wobec konsumentów, szczególnie w sieci internetowej, w formie wyświetlanych reklam, pozycjonowania stron oraz proponowania produktów; to również ważne informacje dla ubezpieczyciela oraz potencjalnego pracodawcy. W końcu też informacje te mogą stać się elementem czynu zabronionego, mającego na celu wymuszenie określonych zachowań przy pomocy szantażu.

W związku z powyższym dane sensytywne, jakimi są dane medyczne, powinny być również obwarowane dostatecznymi środkami technicznymi i organizacyjnymi, które uwzględniać będą specyfikę zagrożeń, związaną z przetwarzaniem danych o zdrowiu za pomocą technologii informacyjno-komunikacyjnych.

2. Ochrona danych medycznych w prawie polskim i europejskim

Szczegółowo ochronę danych reguluje ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych. Ustawa została przyjęta w celu implementacji unijnego Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 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 (rozporządzenie ogólne o ochronie danych, dalej jako: RODO)[10].

Z treści RODO wynika zakaz przetwarzania danych osobowych, które ujawniają pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby (art. 9 ust. 1 RODO). RODO danym tego rzędu przypisuje charakter wcześniej wspomnianych danych sensytywnych, ze względu na to, że ich przetwarzanie niesie za sobą zagrożenie prywatności pacjenta w stopniu większym niż w przypadku tzw. danych zwykłych[11].

10 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 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 (tekst jedn. Dz. Urz. UE.L Nr 119).

11 P. Durbajło, A. Piskorz-Ryń, Problemy cyberbezpieczeństwa w telemedycynie, (w:) I. Lipowicz, G. Szpor, M. Świerczyński (red.), Telemedycyna i e-Zdrowie. Prawo i informatyka, Warszawa

Wyjątki od powyżej opisanego zakazu zostały ujęte dyspozycją art. 9 ust. 2 lit. h RODO. Na jego mocy przetwarzać dane sensytywne można w sytuacji, gdy „przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem warunków i zabezpieczeń, o których mowa w ust. 3". W tym miejscu należy od razu odwołać się do powoływanego ust. 3 art. 9 RODO – na jego podstawie dopuszczalne jest przetwarzanie danych wrażliwych, jeżeli są przetwarzane przez – lub na odpowiedzialność – pracownika podlegającego obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe lub przez inną osobę również podlegającą obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe. Ponadto na mocy art. 9 ust. 4 państwa członkowskie mogą zachować lub wprowadzić dalsze warunki, w tym ograniczenia w odniesieniu do przetwarzania danych genetycznych, danych biometrycznych lub danych dotyczących zdrowia.

Nie sposób tutaj nie zauważyć, iż zachowanie tajemnicy medycznej oraz dopuszczenie przetwarzania danych medycznych pod pewnymi warunkami jest ze sobą ściśle związane na gruncie faktycznym, jednak pod względem legislacyjnym zauważalna jest tu pewna niekompletność w stosunku do regulacji ustawowej polskiego systemu prawnego, w związku z czym nie można przepisów art. 9 ust. 2 lit. h w zw. z art. 9 ust. 3 traktować rozszerzająco, takaby nie dopuścić do ewentualnych naruszeń praw pacjentów[12], przede wszystkim poprzez nieodpowiednie zabezpieczenie przetwarzanych danych pacjentów, co narusza podstawy stosunku profesjonalisty medycznego i pacjenta, który z natury winien być otoczony gwarancją poufności, tak aby osoba leczona miała poczucie bezpieczeństwa i komfortu.

3. Gwarancje bezpieczeństwa przetwarzanych danych medycznych

Zabezpieczenie danych przetwarzanych w systemie informatycznym to przede wszystkim wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych, które zapewnią ochronę danych przed ich nieuprawnionym przetwarzaniem – jest to obowiązek organizacyjny administratora danych[13]. Przetwarzanie danych w systemach teleinformatycznych, szczególnie w chmurze obliczeniowej, sprawia, że

2019, s. 285–286.

12 *Ibidem*, s. 287.

13 A. Drozd, Ustawa o ochronie danych, Warszawa 2008, s. 247.

zabezpieczenia powinny mieć bardziej rozbudowany charakter, ze środkami ochrony dostosowanymi do kategorii danych i możliwych zagrożeń. Należy tu przypomnieć, iż zgodnie z art. 35 ust. 1a ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia[14] jednostkowe dane medyczne z Systemu Informacji Medycznej mogą być udostępnione wyłącznie w takim zakresie, jaki wynika ze zgody, która została udzielona przez usługobiorcę[15] na dokonanie czynności z zakresu świadczenia usług medycznych, powiązanej z wprowadzaniem danych do elektronicznej dokumentacji medycznej, oraz przez autoryzację opisanej czynności przez pacjenta, aczkolwiek warto jednocześnie odnotować, iż od tej zasady istnieje szereg wyjątków w przepisach – w art. 12 ust. 3–10 u.s.i.o.z. określono krąg podmiotów, które mogą uzyskać dostęp do danych pacjenta przetwarzanych w SIM w zakresie, który określają przepisy ustawy i akty prawne z nią powiązane. Ponadto, na podstawie treści art. 35 ust. 1 u.s.i.o.z. zezwala się na dostęp do danych medycznych członkom personelu medycznego, takim jak lekarz, pielęgniarka, położna, oraz podmiotom określanym szeroko jako zbiór pracowników medycznych usługodawcy[16], a także podmiotom takim jak wojewoda i minister właściwy do spraw zdrowia[17]. Wprawdzie to do pacjenta jako podmiotu danych wrażliwych, które są gromadzone w bazach, należy decyzja o tym, czy i w jakim zakresie udostępniane będą zasoby zawierające informacje dotyczące jego zdrowia, zawarte w elektronicznej dokumentacji medycznej i przetwarzanej w SIM, jednakże nie sposób nie zauważyć, że bez udostępnienia tych danych udzielenie świadczenia leczniczego jest praktycznie niewykonalne oraz że szeroki i rozproszony między różne akty prawne katalog wyjątków od zasad generalnych znacząco wpływa na gwarancję i ochronę uprawnień związanych z ochroną danych medycznych[18]. System Informacji Medycznej i rejestry z nim powiązane dopiero rozpoczynają swoje działanie[19]. Dodatkowo ciągłe korygowanie przepisów prawnych,

14 Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowie (tekst jedn. Dz.U. Nr 113, poz. 657 ze zm., dalej jako: u.s.i.o.z.).

15 Usługobiorca to osoba fizyczna korzystająca lub uprawniona do korzystania ze świadczeń opieki zdrowotnej, w tym świadczeniobiorca w rozumieniu art. 2 ust. 1 ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych oraz osoba, o której mowa w art. 2 ust. 2 i art. 13 tej ustawy (art. 2 pkt 16 u.s.i.o.z.).

16 Przez usługodawcę należy rozumieć świadczeniodawcę, o którym mowa w art. 5 pkt 41 ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych – czyli podmioty profesjonalnie udzielające świadczeń z zakresu leczenia oraz zaopatrujące w wyroby medyczne, a także apteki (art. 2 pkt 15 u.s.i.o.z.).

17 Art. 12 ust. 1 pkt 5 w zw. z art. 10 i art. 11 ust. 1 ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowych ze środków publicznych (tekst jedn. Dz.U. Nr 210, poz. 2135 ze zm.).

18 Świtała K., Pacjent jako beneficjent ograniczeń jawności elektronicznej dokumentacji medycznej, Warszawa 2018, s. 88.

19 Wejście w życie systemu wystawiania e-recept było kilkakrotnie odsuwane w czasie, ostatecznie zaczął on obowiązywać od 8 stycznia 2020 r.; por. w tym zakresie – Stanowisko Naczelnej Rady

niejasne i niespójne regulacje zawierające niejednoznaczne pojęcia oddziałują negatywnie na funkcjonujący system przetwarzania danych medycznych w systemach teleinformatycznych.

Dane medyczne nie bez powodu zaliczane są do kategorii danych wrażliwych – dzieje się tak dlatego, że ich bezprawne ujawnienie naraża podmiot tych danych na poważną szkodę. Według przepisów placówki medyczne są ustawowo zobowiązane do zapewnienia odpowiednich poziomów gwarancji pod względem technologicznym, jednak polska służba zdrowia jest w niewystarczającym stopniu dofinansowana, co powoduje, że istnieją poważne braki w zapewnieniu zaplecza technologiczno-komunikacyjnego, a dodatkowo często nie ma kompatybilności przepływu danych między poszczególnymi placówkami. Wprawdzie nawet najlepsze zabezpieczenia nie zapewnią stuprocentowego bezpieczeństwa, gdyż pewne spektrum zagrożeń występuje stale, jeśli chodzi o przetwarzanie danych w cyberprzestrzeni, jednak dane medyczne powinny być chronione przede wszystkim z uwagi na bezpieczeństwo pacjenta, jeśli chodzi o nieautoryzowany dostęp do ich treści i modyfikację, co wiąże się z możliwością ujawnienia danych medycznych. Dane medyczne przetwarzane w sieci telekomunikacyjnej mogą być bowiem narażone na ataki prowadzące do niedostępności usługi lub na ryzyko związane z ransomware, czy przyłączaniem urządzeń wykorzystywanych w eHeath do botnetów[20].

Należyta realizacja gwarancji zachowania prawa pacjenta do prywatności to przede wszystkim konieczność wdrożenia specjalistycznych rozwiązań w zakresie zabezpieczeń systemów teleinformatycznych, obsługujących system informacji w ochronie zdrowia. Dostęp do danych sensytywnych w nich przetwarzanych jest ograniczony poprzez stosowanie mechanizmów uwierzytelniania i autoryzacji. Poufność tych zasobów gwarantuje użytkowanie odpowiednio silnych algorytmów kryptograficznych[21].

4. Tajemnica medyczna w obliczu rzeczywistości e-zdrowia

Nadrzędną rolę, jeśli chodzi o gwarancje zachowania prywatności świadczeniobiorcy i ochrony danych medycznych w e-zdrowiu, pełni stworzenie środowiska prawnego, w którym ta ochrona będzie miała charakter nadrzędny. Tradycyjnie poglądy na temat poufności w stosunku medycznym skupiają się na tajemnicy me-

Lekarskiej z dnia 22 listopada 2019 r. w sprawie wprowadzania e-recept, https://gazetalekarska.pl/?p=51842 (24.02.2020).

20 K.M. Mazur, Zagrożenia cybernetyczne związane z rozwojem eHealth, (w:) M. Jackowski (red.), Ochrona danych medycznych. RODO w ochronie zdrowia, Warszawa 2018, system informacji prawnej Lex.

21 K. Świtała, Pacjent…, *op. cit.*, s. 336.

dycznej relacji lekarz – pacjent, ale należy to zmienić – w związku z nowoczesną rzeczywistością.

W prawie polskim najszerszą gwarancję ochrony pacjenta zapewnia ustawodawstwo dotyczące praw pacjenta oraz tajemnicy zawodów medycznych. Na mocy postanowień u.p.p. w art. 13 stanowi się, iż pacjent ma prawo do zachowania w tajemnicy przez osoby wykonujące zawód medyczny, w tym udzielające mu świadczeń zdrowotnych, informacji z nim związanych, a uzyskanych w związku z wykonywaniem tego zawodu. Na mocy art. 13 u.p.p. osoby, które wykonują zawód medyczny, są obowiązane do zachowania w tajemnicy informacji powiązanych z pacjentem, szczególnie tych dotyczących jego stanu zdrowia; tajemnica pacjenta obejmuje swoim zakresem wszystkie informacje, z którymi osoba wykonująca zawód medyczny miała styczność podczas wykonywania czynności zawodowych. Należy się tu zatrzymać nad ustawową definicją osoby wykonującej zawód medyczny – zgodnie z art. 2 ust. 1 pkt 2 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej[22] osoba wykonująca zawód medyczny to osoba uprawniona na podstawie odrębnych przepisów do udzielania świadczeń zdrowotnych oraz osoba legitymująca się nabyciem uprawnień zawodowych pod względem medycznym. Będą to oczywiście profesje takie jak: lekarz, pielęgniarka, położna, fizjoterapeuta, ale także osoby, które w powszechnej percepcji jednoznacznie są kojarzone z dziedziną medycyny, lecz nie mają swojej oddzielnej regulacji ustawowej, jak na przykład dietetyk (rozumiany jako samodzielny zawód specjalisty ds. żywienia i chorób dietozależnych) czy psychoterapeuta.

Nie istnieje jednakże ustawowa definicja zawodu medycznego, a także nie ma sporządzonego katalogu tychże zawodów[23]. Brak jasnych i przejrzystych reguł klasyfikacji zawodów medycznych utrudnia zdefiniowanie, kto jest zobowiązany przepisami do dochowania tajemnicy pacjenta. Na przykład bezsprzecznie kontakt z danymi medycznymi będzie miała osoba wykonująca zawód rejestratora medycznego, jednak to, czy osoba taka będzie objęta obowiązkiem wynikającym z tajemnicy medycznej, należy analizować indywidualnie, co do danego stanu faktycznego[24]. Ustawodawca wprawdzie w art. 22 u.p.p. określa, iż do zachowania tajemnicy są obowiązane także osoby, które uczestniczą w udzielaniu świadczeń medycznych, ale nie wykonują zawodu medycznego; również w art. 24 u.p.p. ustawodawca ustanawia uprawnienie do przetwarzania danych zawartych w dokumentacji medycznej w celu

22 Ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej (tekst jedn. Dz.U. Nr 112, poz. 654 ze zm., dalej jako: u.d.l.).

23 Za wyjątek można tu uznać rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 7 sierpnia 2014 r. w sprawie klasyfikacji zawodów i specjalności na potrzeby rynku pracy oraz zakresu jej stosowania (tekst jedn. Dz. U. z 2018 r., poz. 227), zawierające wyszczególnioną kategorię „specjalistów do spraw zdrowia", ale nie traktuje się zamieszczonej tam klasyfikacji zawodów jako katalogu obowiązującego.

24 Z. Banaszczyk, Formy prowadzenia działalności leczniczej, „Studia Prawa Prywatnego" 2016, nr 3, s. 26.

ochrony zdrowia, udzielania oraz zarządzania udzielaniem świadczeń zdrowotnych, utrzymania systemu teleinformatycznego, w którym przetwarzana jest dokumentacja medyczna, i zapewnienia bezpieczeństwa tego systemu – dla osób wykonujących czynności pomocnicze przy udzielaniu świadczeń zdrowotnych, a także czynności związane z utrzymaniem systemu teleinformatycznego, w którym przetwarzana jest dokumentacja medyczna, i zapewnieniem bezpieczeństwa tego systemu, na podstawie upoważnienia administratora danych, i równocześnie zastrzega, że osoby takie zobowiązane są do zachowania w tajemnicy informacji, które uzyskały w związku z wykonywaniem zadań przy udzielaniu świadczenia zdrowotnego[25]. Jednak nasuwa się tu pytanie, czy na pewno te regulacje ustawowe pokrywają w sposób pełny gwarancje bezpieczeństwa przetwarzanych danych, zwłaszcza w świetle braku katalogu zawodów medycznych oraz faktu, iż poza tymi przepisami w prawie polskim generalnie pracownicy szeroko pojętej administracji nie są objęci obowiązkiem dochowania dyskrecji, oprócz, oczywiście, jurysdykcji z zakresu prawa pracy[26].

5. Kwestia tajemnicy medycznej w pryzmacie mHealth

W tym miejscu warto omówić kwestię obszaru, w którym znacząco wzrósł odsetek świadczonych usług w ostatnich latach, a którym jest mHealth – usługi medyczne świadczone za pomocą aplikacji mobilnych. Dotyczy to nie tylko aplikacji oferowanych przez samodzielnych deweloperów, również przedsiębiorstwa zajmujące się świadczeniem usług leczniczych w formie „tradycyjnej", to jest w ramach placówek medycznych, wypuszczają swoje autorskie aplikacje z zakresu mHealth, aby usprawnić świadczenie usług dla pacjentów danej przychodni leczniczej czy laboratorium diagnostycznego. Aplikacje medyczne działają także w ramach tzw. Wearbles, czyli urządzeń noszalnych, takich jak na przykład *smartwatch*, pozwalających na kontrolowanie kondycji, aktywności oraz parametrów zdrowotnych.

Dane medyczne zbierane podczas kontaktu pacjenta z przedstawicielem personelu medycznego obwarowane są gwarancjami tajemnicy medycznej oraz lekarskiej, kodeksami etyki tychże zawodów oraz przepisami ustaw dotyczących ochrony praw pacjentów; w przeciwieństwie do personelu medycznego deweloperzy aplikacji mHealth nie są nimi objęci. Stwarza to istotne zagrożenie dla prawa pacjenta do poufności ujawnianych danych, gdyż informacje, które zbierane są podczas używania aplikacji medycznych, mogą być zbierane, ujawniane i sprzedawane stronom spoza stosunku kreowanego podczas korzystania z tych narzędzi[27]. Deweloper aplikacji lub związany

25 P. Durbajło, A. Piskorz-Ryń, Problemy cyberbezpieczeństwa…, *op. cit.*, s. 284–285.

26 Art. 100 § 2 pkt 4 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (tekst jedn. Dz.U. Nr 24, poz. 141 ze zm., dalej jako: k.p.).

27 J. Hancock, Workplace Wellness Programs Put Employee Privacy at Risk, CNN, http://www.cnn.com/2015/09/28/health/workplace-wellness-privacy-risk-exclusive/index.html (18.04.2019).

z deweloperem agregator danych ma możliwość zbierania i sprzedawania informacji o użytkowniku aplikacji, a dane do aplikacji wprowadzane mogą być przedmiotem śledzenia przez ciasteczka (*cookies*), sygnał nawigacyjny sieci Web oraz boty pochodzące od innego rodzaju posiadanych przez użytkownika aplikacji, stron odwiedzanych przez niego albo od producenta danego urządzenia mobilnego. Upoważnienie do dostępu do wprowadzanych danych, udzielone przez użytkownika aplikacji, może również stanowić podstawę dla reklam oraz usług kierowanych do użytkownika.

Zwrócenie szczególnej uwagi na dziedzinę tajemnicy medycznej w obszarze mHealth jest konieczne ze względu na ogrom informacji, które są przetwarzane przez aplikacje o charakterze medycznym – zbierają bowiem one dane o ludzkim nastroju, wadze, aktywności fizycznej, przyjmowanej ilości kalorii, makroelementów, fazie cyklu menstruacyjnego, parametrach snu, przyjmowanych lekarstwach i suplementach, posiadanych schorzeniach, wskaźnikach zdrowotnych, takich jak wysokość ciśnienia krwi, seropozytywność, ilość wykonanych kroków i wiele innych[28]. Aplikacje, które używają w swoim funkcjonowaniu przyspieszeniomierza, aby mierzyć ilość kroków, oraz aparatu monitorowania mowy za pomocą używanego algorytmu potrafią dopasować zebrane objawy do diagnozy choroby Huntingtona, udaru czy nawet zwykłego przeziębienia, zanim pacjent odczuje wyraźne symptomy, pozwalające na rozpoznanie tych schorzeń za pomocą jego odczuć empirycznych.

Ta predyktywna cecha, właściwa obecnej generacji aplikacji medycznych, kreuje nowe wyzwania w dziedzinie ochrony prywatności pacjenta[29]. Zauważyć bowiem trzeba, że pacjenci mogą zachowywać swoje dane medyczne w tajemnicy, nie ujawniając ich nikomu, nawet lekarzowi, a tymczasem podczas używania aplikacji medycznych wiele pomiarów danych parametrów może być dokonywane bez wiedzy użytkownika[30]. Informacje te mogą być następnie dyskretnie udostępniane witrynom internetowym, które gromadzą i wyświetlają informacje pochodzące z różnych źródeł, a także sprzedawane osobom trzecim, co powoduje, że informacje o danych medycznych użytkownika, których on sam nawet nie zna, mogą być rozpowszechniane bez kontroli ich przepływu[31].

Obowiązek ochrony danych medycznych wynika z tego, że pacjenci mogą otrzymać odpowiednią opiekę zdrowotną tylko wówczas, jeśli będą szczerzy wobec osób, które udzielają im świadczeń, tak aby możliwe było postawienie pełnej i poprawnej diagnozy[32]. Jeśli pacjent nie będzie miał pewności co do poufności dotyczących go danych medycznych, to niewykluczone, że nie będzie szczery ani transparentny

28 L. Andrews, A New Privacy Paradigm in the Age of Apps, Wake Forest Law Review, t. 53, Winston-Salem 2018, s. 443.

29 *Ibidem*, s. 426.

30 L. Andrews, Future Perfect: Confronting Decisions About Genetics, Columbia 2002, s. 130–50.

31 L. Andrews, A New Privacy…, *op. cit.,* s. 427.

32 *Ibidem*, s. 443.

w ich ujawnianiu. Trzeba również odnotować, że takie obawy z pewnością zahamują rozwój usług telemedycznych, szczególnie w Polsce, gdzie nie są one jeszcze tak popularne jak na zachodzie Europy oraz w krajach Ameryki Północnej, a z pewnością mogłyby stanowić szansę na rozwiązanie wielu problemów, z którymi zmaga się krajowy system opieki zdrowotnej.

W podsumowaniu przedstawionych rozważań na temat tajemnicy medycznej w rzeczywistości e-zdrowia należy przede wszystkim zwrócić uwagę na problemy związane z brakiem jasnej, legalnej definicji terminu „zawód medyczny", przedstawiciele którego mają obowiązek dochowania tajemnicy medycznej, a także na problem ogólnej niespójności systemowej co do możliwego katalogu takiej grupy zawodowej. Ponadto należy podkreślić, iż ochrona danych medycznych w rzeczywistości udzielania świadczeń w cyberprzestrzeni dotyczy już nie tylko tradycyjnej relacji lekarz – pacjent, ale i innych stron, takich jak deweloperzy stron, aplikacji, informatycy, rejestratorzy medyczni. W związku z tym powstaje pytanie o treść art. 13 u.p.p. w kontekście tego, czy nie byłoby wskazane, aby szerzej ująć krąg podmiotów, co do których istnieje obowiązek zachowania tajemnicy medycznej, obejmując nim osoby, które weszły w posiadanie danych medycznych w związku z wykonywaniem zawodu (jak np. pracownik socjalny)[33] lub działalności gospodarczej (np. deweloper aplikacji medycznej). Takie ujęcie przyniosłoby korzyść w postaci likwidacji istniejących luk prawnych co do definicji zawodu medycznego i sprawiłoby, iż nie trzeba byłoby tworzyć sztywnego, zamkniętego katalogu tych zawodów i związanych z opisywanym w niniejszym artykule problemem – a w związku z rozwojem medycyny i możliwości wykorzystywania w niej rozwiązań z innych dziedzin tworzenie takiego katalogu nie jest ani celowe, ani konieczne.

Regulacje prawne dotyczące prawnym zasad ochrony informacji o zdrowiu pacjenta nie zostały jeszcze w pełni dostosowane do rzeczywistości e-zdrowia, w której poruszają się pacjenci, gdyż istniejąca ochrona nie jest kompleksowa i nie bierze pod uwagę większości możliwych zagrożeń, przede wszystkim w stosunku do kwestii podmiotowych. System Informacji Medycznej został zaprojektowany w sposób, który zakłada obecność dwóch stron stosunku świadczenia leczniczego – członka personelu medycznego i pacjenta, ale pomija kwestie związane z telemedycyną, elektroniczną dokumentacją medyczną oraz e-zdrowiem jako całością.

W e-zdrowiu dostęp do wprowadzanych danych medycznych uzyskiwany jest, jak wskazywano wcześniej, przez osoby, które nie wykonują zawodów medycznych, ale pełnią czynności techniczne w związku z obsługą systemów, na platformach, na których udzielane są usługi z zakresu e-zdrowia; ze względu na tworzenie coraz to bardziej zaawansowanych systemów z udziałem specjalistycznego sprzętu medycznego, w tym dotyczącego Internetu rzeczy, dane te będą nieustannie przetwarzane w przedmiotowych systemach teleinformatycznym. Z tego właśnie względu będzie

33 R. Kubiak, Tajemnica medyczna, Warszawa 2015, s. 32.

zwiększała się liczba osób, które zawodowo będą zapewniały utrzymanie i obsługę takich systemów i dlatego konieczne jest rozszerzenie katalogu osób zobowiązanych do tajemnicy medycznej – na osoby niewykonujące zawodu medycznego, ale związane z usługami zdrowotnymi lub prozdrowotnymi, oraz na jednostki, które dokonują czynności technicznych związane z funkcjonowaniem systemów e-zdrowia i urządzeń z zakresu Internetu rzeczy[34].

Obecnie regulacja art. 24 u.p.p. obejmuje obowiązkiem zachowania tajemnicy osoby uprawnione do przetwarzania danych, które zawiera dokumentacja medyczna, w celu ochrony zdrowia, udzielania oraz zarządzania udzielaniem świadczeń zdrowotnych, utrzymania systemu teleinformatycznego, w którym przetwarzana jest dokumentacja medyczna, i zapewnienia bezpieczeństwa tego systemu, są uprawnione osoby wykonujące zawód medyczny oraz inne osoby wykonujące czynności pomocnicze przy udzielaniu świadczeń zdrowotnych, a także czynności związane z utrzymaniem systemu teleinformatycznego, w którym przetwarzana jest dokumentacja medyczna, i zapewnieniem bezpieczeństwa tego systemu, na podstawie upoważnienia administratora danych. Tymczasem w przypadku na przykład aplikacji medycznych czy Internetu rzeczy nie mamy do czynienia z dokumentacją medyczną, zatem w tym zakresie będą obowiązywały jedynie przepisy o ochronie danych, bez obostrzeń z zakresu tajemnicy medycznej określonej prawami pacjenta. Przepis ten w związku z powyższym może nie dawać wystarczających gwarancji ochrony prywatności pacjentów. Istniejące regulacje wydają się skonstruowane raczej pod tradycyjne relacje w ramach stosunku medycznego. Należy więc rozważyć, czy nie rozszerzyć tajemnicy medycznej na wszystkie podmioty, które w ramach swojej działalności zawodowej lub gospodarczej zapoznały się z danymi osobowymi z zakresu dotyczącego zdrowia człowieka[35], a także je przetwarzały – postulat ten również warto rozważyć w aspekcie coraz powszechniejszej obecności sztucznej inteligencji w codziennej rzeczywistości i tego jak pojmujemy jej podmiotowość.

Wnioski

Usługi z zakresu ochrony zdrowia realizowane za pomocą technologii informacyjno-komunikacyjnych nie powinny być postrzegane jako zagrożenie dla praw pacjentów oraz poufności innych danych, ale jako skutek rozwoju cywilizacji pod względem technologicznym i źródło czerpania korzyści z tego faktu. Prawo powinno być jednym z instrumentów kształtowania rzeczywistości, a więc musi również dostosowywać się do postępu i konsekwencji. Obecnie przepisy są już pewnością o wiele lepiej dostosowane do świadczenia usług telemedycznych, ale ciągle istnieją luki, które stawiają pod znakiem zapytania gwarancje ochrony praw pacjentów w nale-

34 P. Durbajło, A. Piskorz-Ryń, Problemy cyberbezpieczeństwa…, *op. cit*., s. 291.
35 *Ibidem*, s. 292.

żyty sposób. Polski ustawodawca musi uwzględnić to, że ekspansja świadczenia usług medycznych w sieciach łączności na odległość oraz z wykorzystaniem sztucznej inteligencji postępuje bardzo szybko, a jak pokazują liczne afery związane z wyciekiem danych[36], ta cenna i wrażliwa informacja może stać się łatwym towarem i to przy nieświadomości użytkownika, będącego pacjentem.

E-zdrowie nie zostało stworzone i rozwinięte dla inwigilacji czy naruszania praw, ale dla wyrównania szans wszystkich pacjentów, zwiększenia komfortu korzystania z usługi leczniczej oraz zapewnienia jak najlepszej i najwyższej jakości opieki medycznej. Jednak jeśli zignorowane zostaną możliwe zagrożenia prywatności pacjentów i ich danych medycznych, środowisko to może stać się miejscem „wycieku" danych medycznych, szczególnie przecież wrażliwych, bądź stać się usługą ekskluzywną, co byłoby krzywdzące dla wielu pacjentów. W związku z tym, ochrona prywatności winna być zapewniona na jak najwyższym poziomie.

BIBLIOGRAFIA

Andrews L., A New Privacy Paradigm in the Age of Apps, "Wake Forest L.Rev" 2018, t. 3.

Andrews L., Future Perfect: Confronting Decisions About Genetics, Columbia 2002.

Banaszczyk Z., Formy prowadzenia działalności leczniczej, „Studia Prawa Prywatnego" 2016, nr 3.

Drozd A., Ustawa o ochronie danych, Warszawa 2008.

Gavison R., Privacy and the limits of law, "The Yale Law Journal" 1980, vol. 89, nr 3.

Glanowski G., Telemedycyna w świetle ustawy o zawodach lekarza i lekarza dentysty, „Monitor Prawniczy" 2015, nr 18.

Jackowski M. (red.), Ochrona danych medycznych. RODO w ochronie zdrowia, Warszawa 2018.

Kubiak R., Tajemnica medyczna, Warszawa 2015.

Lipowicz I., Szpor G., Świerczyński M. (red.), Telemedycyna i e-Zdrowie. Prawo i informatyka, Warszawa 2019.

Sobczak J., Reshef M. (red.), Nowe procedury medyczne a prawo, Toruń 2016.

Świtała K., Pacjent jako beneficjent ograniczeń jawności elektronicznej dokumentacji medycznej, Warszawa 2018.

36 Najnowsza awaria Facebooka ze stycznia 2020 r. umożliwiała „podejrzenie", kto w ramach danego profilu ma przyznane uprawnienia administratora, w związku z czym może zamieszczać posty; zob. https://wyborcza.pl/7,156282,25584415,facebook-zdradza-kto-zarzadza-fanpagami-politycy-rzadko-pisza.html, https://polskatimes.pl/wielka-awaria-facebooka-kto-prowadzi-konta-morawieckiego-ziobry-holowni-kosiniakakamysza-macierewicza-i-innych-politykow/ar/c1-14708475 (02.03.2020).