Damina Wąsik

Bezprawne udostępnianie i umożliwianie dostępu do jednostkowych danych medycznych w świetle odpowiedzialności karnej art. 51 u.o.d.o.

Studia Prawnoustrojowe nr 28, 259-272

2015

Damian Wąsik
Collegium Medicum
Uniwersytet Mikołaja Kopernika w Toruniu

Bezprawne udostępnianie i umożliwianie dostępu do jednostkowych danych medycznych w świetle odpowiedzialności karnej art. 51 u.o.d.o.

Wprowadzenie

W prawie międzynarodowym od lat wskazuje się na potrzebę wzmożonej ochrony danych dotyczących stanu zdrowia pacjentów jako szczególnej kategorii danych osobowych – danych wrażliwych, przykładem czego są m.in. rekomendacja nr 818 (1977) Zgromadzenia Parlamentarnego Rady Europy, rekomendacje Komitetu Ministrów Rady Europy nr R (81)1 i R (97)5 oraz art. 8 ust. 1 dyrektywy Parlamentu Europejskiego i Rady Unii Europejskiej 95/46/WE z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych[1]. Prawu do zabezpieczenia danych osobowych przed ich nieuprawnionym pozyskiwaniem nadaje się rangę jednego z podstawowych praw obywatelskich. Prawo do prywatności i autonomia informacyjna są gwarantowane m.in. przez Konstytucję Rzeczypospolitej Polskiej z 1997 r. W swoim dotychczasowym orzecznictwie Trybunał Konstytucyjny wielokrotnie podkreślał, że art. 47 Konstytucji wyraża prawo każdej osoby do „ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym", a ujęte w ten sposób prawo do prywatności odnosi się m.in. do informacji o stanie zdrowia[2]. Autonomia informacyjna oznacza natomiast prawo do samodzielnego decydowania o ujawnianiu innym informacji dotyczących swojej osoby, a także prawo do sprawowania kontroli nad takimi informacjami, jeśli znajdują się w posiadaniu innych podmiotów[3]. Przepis art. 51 Konstytucji RP wyraża

[1] Dz. Urz. WE L 281 z 23 listopada 1995 r., s. 31.

[2] Zob. wyrok TK z dnia 19 maja 1998 r., U 5/97, OTK ZU 1998, nr 4, poz. 46.

[3] Zob. wyroki TK z dnia: 19 lutego 2002 r., U 3/01, OTK ZU 2002, nr 1/A, poz. 3 oraz 20 listopada 2002 r., K 41/02, LEX nr 57092.

prawo jednostki do ochrony danych osobowych, w zakres którego wchodzi m.in. wymaganie ustawowej podstawy nałożenia obowiązku ujawnienia przez daną osobę informacji jej dotyczących (ust. 1), zakaz pozyskiwania, gromadzenia i udostępniania innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym (ust. 2), prawo dostępu jednostki do dokumentów i zbiorów danych oraz prawo żądania sprostowania bądź usunięcia danych nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą (ust. 3 i 4). Warto również zauważyć, że zgodnie z art. 51 ust. 5 Konstytucji RP zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa.

Naruszanie unormowań dotyczących ochrony danych osobowych jest w Polsce problemem aktualnym, którego skala co roku wzrasta. Dowodzi tego chociażby systematycznie zwiększająca się liczba skarg obywateli kierowanych do Generalnego Inspektora Ochrony Danych Osobowych (dalej: GIODO) na nadużycia w przedmiocie pozyskiwania, przetwarzania i udostępniania ich danych osobowych[4]. Sektor służby zdrowia jest zaś jednym z najbardziej newralgicznych obszarów oddziaływania negatywnych skutków bezprawnego udostępnienia danych osobowych.

Zasadniczym celem publikacji jest kompleksowe omówienie częstokroć bagatelizowanego w służbie zdrowia problemu ochrony danych pacjentów przed ich bezprawnym udostępnianiem i przetwarzaniem, ze szczególnym uwzględnieniem jednostkowych danych medycznych. Postępujący proces informatyzacji w ochronie zdrowia wymusza konieczność zabezpieczenia prawidłowej realizacji obowiązku przetwarzania danych pod rygorem m.in. sankcji karnych za wszelkie uchybienia w tym zakresie. Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia[5] (dalej: u.s.i.o.z.) nie zawiera jednak właściwych sobie przepisów prawnokarnych i odsyła w tym przedmiocie do odpowiedniego stosowania unormowań ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[6] (dalej: u.o.d.o.). Niezbędna w tej sytuacji staje się ocena, czy nieprawidłowości dotyczące udostępniania i przetwarzania danych pacjentów mogą być bez problemów karane na podstawie art. 51 u.o.d.o. W tym celu omówię kolejno kwestię zakresu pojęciowego jednostkowych danych medycznych i problemów interpretacyjnych w tym obszarze, przeprowadzę analizę znamion przestępstwa bezprawnego udostępniania i przetwarzania danych osobowych w odniesieniu do jednostkowych danych medycznych oraz przykładów czynów zabronionych wypełniających znamiona art. 51 u.o.d.o.

[4] *GIODO dostaje coraz więcej skarg*, [online] <www.lex.pl/czytaj/-/artykul/giodo-dostaje-coraz-wiecej-skarg> (dostęp: 20.07.2014).

[5] Dz. U. nr 113, poz. 657 z późn. zm.

[6] Tekst jedn. Dz. U. z 2014, poz. 1183 z późn. zm.

Pojęcie jednostkowych danych medycznych

Sprecyzowanie zakresu przedmiotowego danych pacjentów, które podlegają ochronie prawnej, może budzić pewne problemy praktyczne z uwagi na unormowanie tego zagadnienia w dwóch odrębnych aktach prawnych.

W pierwszej kolejności wskazać należy na szeroką definicję danych osobowych, zawartą w art. 6 ust. 1 dalej: u.o.d.o., zgodnie z którym za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. W myśl ust. 2 cytowanego przepisu osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Tym samym pojęcie „informacja" w tym kontekście oznacza komunikaty (wiadomości, wypowiedzi, prezentacje) wyrażone w jakikolwiek sposób: znakami graficznymi, symbolami, w języku komputerowym czy też na fotografii, np. na zdjęciu RTG lub wyniku badań USG. Dla kwalifikacji określonej informacji do kategorii danych osobowych nie ma znaczenia również ich prawdziwość[7]. Zdaniem części doktryny informacje wystarczające do ustalenia tożsamości osoby to nie tylko samo imię i nazwisko, ale – koniecznie – dodatkowe informacje pozwalające na określenie (bezpośrednio lub pośrednio) tożsamości osoby fizycznej (np. data i miejsce urodzenia, cechy zewnętrzne, numer PESEL, struktura DNA)[8].

Z drugiej strony, w odniesieniu do gromadzenia i przetwarzania danych w systemach teleinformatycznych i rejestrach medycznych, art. 37 u.s.i.o.z. stanowi, że podmioty prowadzące bazy danych w zakresie ochrony zdrowia są obowiązane do stworzenia warunków organizacyjnych i technicznych zapewniających ochronę przetwarzanych danych, w szczególności ich zabezpieczenia przed nieuprawnionym dostępem, nielegalnym ujawnieniem lub pozyskaniem, a także ich modyfikacją, uszkodzeniem, zniszczeniem lub utratą. Mówiąc w tym przypadku o „danych", należy mieć na względzie przede wszystkim jednostkowe dane medyczne, którymi zgodnie z art. 2 pkt 7 u.s.i.o.z. są dane osobowe oraz inne dane osób fizycznych dotyczące uprawnień do udzielonych, udzielanych i planowanych świadczeń opieki zdrowotnej, stanu zdrowia, jak też inne dane przetwarzane w związku z planowanymi, udzielanymi i udzielonymi świadczeniami opieki zdrowotnej oraz profilaktyką

[7] Zob. wyrok Wojewódzkiego Sądu Administracyjnego w Krakowie z dnia 11 października 2013 r., II SA/Kr 682/13, LEX nr 1384885; wyrok Wojewódzkiego Sądu Administracyjnego w Poznaniu z dnia 5 czerwca 2013 r., IV SA/Po 23/13, LEX nr 1333700; postanowienie Sądu Apelacyjnego w Warszawie z dnia 29 grudnia 2011 r., VI ACz 2212/11; wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 9 kwietnia 2013 r., II SA/Wa 211/13, LEX nr 1317030.

[8] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Warszawa 2011, s. 345; P. Pochopień, *Dokumentacja medyczna jako zbiór danych zawierający tzw. wrażliwe dane osobowe*, [w:] idem (red.), *Dokumentacja medyczna*, Warszawa 2012, s. 82.

zdrowotną i realizacją programów zdrowotnych. Jednostkowe dane medyczne to np. stwierdzenie jednostki chorobowej, zdarzenia medyczne kwalifikujące pacjenta do świadczeń zdrowotnych określonego typu, zaordynowane leki, wyniki badań radiologicznych i laboratoryjnych. Podstawowym repozytorium jednostkowych danych medycznych są dokumenty zawierające informacje o poszczególnych etapach realizowania procesu leczniczego: począwszy od rejestracji pacjentów i planowanych wizytach poprzez wystawianie skierowań, zleceń badań specjalistycznych i zwolnień lekarskich aż po dane o hospitalizacji pacjenta (np. historia choroby)[9].

W kontekście zakresu pojęciowego jednostkowych danych medycznych wskazać trzeba, że ustawodawca zdefiniował je w sposób niekonsekwentny, przez co wykładnia tego pojęcia stwarza pewne problemy praktyczne. Z jednej bowiem strony w art. 2 pkt 7 u.s.i.o.z. stwierdza się, iż jednostkowymi danymi medycznymi są m.in. dane osobowe, z drugiej np. w art. 4 ust. 3 u.s.i.o.z. dane osobowe i jednostkowe dane medyczne zostały rozgraniczone. Literalna wykładnia art. 2 pkt 7 u.s.i.o.z. prowadzi do wniosku, że wszystkie dane osobowe pacjenta będą jednostkowymi danymi medycznymi, ale nie wszystkie jednostkowe dane medyczne będą stanowiły dane osobowe. Przedstawiony problem komplikuje się jeszcze bardziej, gdy wziąć pod uwagę legalną definicję danych osobowych, obejmującą każdą informację pozwalającą na zidentyfikowanie osoby fizycznej i zestawić tę okoliczność z faktem, że proces udzielania świadczeń zdrowotnych jest każdorazowo zindywidualizowany i związany ściśle ze stanem zdrowia konkretnego pacjenta. W praktyce zatem może okazać się, że zakresy pojęciowe jednostkowych danych medycznych i danych osobowych w odniesieniu do pacjentów dość często będą zanikać[10].

Wobec powyższego problemu i specyfiki działalności leczniczej przyjąć należy szczególny charakter obowiązku ochrony danych pacjentów przez personel medyczny i jego rozszerzenie przedmiotowe w stosunku do danych zawartych np. w dokumentacji medycznej. Wydaje się, że koncepcja ta pozwoli uniknąć problemów interpretacyjnych podczas analizowania okoliczności ujawnienia określonych danych pacjentów, przy czym uwzględnia zakres tajemnicy lekarskiej, pielęgniarskiej i położniczej, która obejmuje nie tylko dane o stanie zdrowia, ale także informacje uzyskane w związku z wykonywaniem zawodu, dotyczące np. stanu majątkowego czy stopnia inteligencji pacjenta, nałogów i trybu życia[11].

Zakres pojęciowy jednostkowych danych medycznych, w tym danych osobowych, jak też metody i cele ich pozyskiwania oraz przetwarzania niewątpliwie uzasadniają ich szeroką ochronę prawną. Jednocześnie zabezpieczenie przed bezprawną ingerencją w autonomię informacyjną pacjentów i przyjęte ustawowo zasady przetwarzania danych słusznie znajduje swoje odzwierciedlenie na płaszczyźnie prawa karnego. Jak wcześniej wspomniano, ustawa o systemie informacji w ochronie zdro-

[9] Zob. D. Wąsik, *Ustawa o systemie informacji w ochronie zdrowia. Komentarz*, Warszawa 2015, s. 34.

[10] Ibidem.

[11] Zob. A. Huk, *Tajemnica zawodowa lekarza*, „Prokuratura i Prawo" 2001, nr 6, s. 69–85.

wia co prawda nie zawiera przepisów karnych, niemniej jednak w uzasadnieniu do projektu tegoż aktu prawnego wskazuje sie, że „ze względu na przepisy karne zawarte w ustawie o ochronie danych osobowych w ustawie o systemie informacji w ochronie zdrowia nie było potrzeby zamieszczania dodatkowych regulacji w tym zakresie"[12].

Ustawa o ochronie danych osobowych penalizuje m.in. takie przestępstwa, jak przetwarzanie danych osobowych w sposób nieuprawniony lub przez osobę do tego nieupoważnioną (art. 49 u.o.d.o.), bezprawne udostępnianie lub umożliwianie dostępu do danych osobowych (art. 51 u.o.d.o.), naruszenie obowiązku zabezpieczenia danych osobowych przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem (art. 52 u.o.d.o.), zaniechanie obowiązku zgłoszenia rejestracji zbioru danych (art. 53 u.o.d.o.), niedopełnienie obowiązku poinformowania osoby, której dane dotyczą, o jej prawach wynikających z przepisów o ochronie danych osobowych (art. 54 u.o.d.o.), a także udaremnianie lub utrudnianie czynności kontrolnych inspektorom GIODO (art. 54a u.o.d.o.)[13].

Z racji pozyskiwania przez personel medyczny jednostkowych danych medycznych, w tym danych osobowych pacjentów, niemalże przez cały okres udzielania świadczeń opieki zdrowotnej, a także konieczność ich ciągłego przetwarzania istnieje ryzyko związane z bezprawnymi działaniami w ww. obszarze personelu medycznego i osób zatrudnionych lub współpracujących z zakładami opieki zdrowotnej. Znajduje to swój wyraz nie tylko w orzecznictwie sądowym, ale i w licznych skargach pacjentów kierowanych do GIODO i Rzecznika Praw Pacjentów. Przy stosowaniu art. 51 u.o.d.o. również mogą pojawić się problemy interpretacyjne, stąd też konieczne wydaje się omówienie znamion określonego w nim czynu zabronionego w odniesieniu do jednostkowych danych medycznych pozyskiwanych i przetwarzanych w warunkach działalności leczniczej i udzielania świadczeń opieki zdrowotnej.

Bezprawne udostępnianie lub umożliwianie dostępu do jednostkowych danych medycznych w świetle art. 51 u.o.d.o.

Zgodnie z art. 51 ust. 1 u.o.d.o., kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. Stosownie do ust. 2 cytowanego przepisu, jeżeli sprawca działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku. Przedmiotem ochrony art. 51 u.o.d.o. jest zatem bezpieczeństwo danych osobowych, a w zakresie systemu informacji w ochronie zdrowia – bezpieczeństwo jednostkowych danych medycznych.

---

[12] *Uzasadnienie projektu ustawy o systemie informacji w ochronie zdrowia*, Sejm IV kadencji, druk 3485, [online] <www.sejm.gov.pl>.

[13] Zob. D. Wąsik, op. cit., s. 203.

Przestępstwo z art. 51 ust. 1 u.o.d.o. jest przestępstwem indywidualnym, albowiem może być ono popełnione wyłącznie przez osobę, której powierzono obowiązki dotyczące administrowania zbiorem danych osobowych lub która zobligowana jest na podstawie przepisów lub polecenia służbowego wydanego *lege artis* do ochrony tych danych. Nie należy mylić pojęć „administrujący danymi" i „administrator danych", na co słusznie wskazywał Sąd Najwyższy w postanowieniu z dnia 11 grudnia 2000 r.[14] Na gruncie ustawy o ochronie danych osobowych administratorem danych osobowych jest jedynie ten podmiot, który decyduje o celach i środkach przetwarzania tych danych (por. art. 7 pkt 4 u.o.d.o.), natomiast administrującym także taki podmiot, który zarządza, zawiaduje zbiorem danych lub danymi w procesie ich przetwarzania, przy czym odpowiedzialność karna administrującego niebędącego administratorem danych wchodzi w rachubę wówczas, gdy jego zachowanie – uznane za karalne przez ustawę – wynika z powierzonych mu czynności przetwarzania danych. Takie okoliczności będą często spotykane w przypadku podmiotów leczniczych i osób wykonujących zawody medyczne, na co wskazuje chociażby definicja rejestru medycznego, określona w art. 2 pkt 12 u.s.i.o.z., zgodnie z którym rejestrem medycznym jest tworzony zgodnie z prawem rejestr, ewidencja, lista, spis albo inny uporządkowany zbiór danych osobowych lub jednostkowych danych medycznych. Jeżeli więc poszczególnym podmiotom leczniczym, a w ich strukturach – właściwym członkom personelu medycznego powierzone zostaną obowiązki prowadzenia określonego rejestru medycznego, tudzież przekazywania danych do takiego rejestru (por. 19 ust. 1 u.s.i.o.z.), krąg osób, które mogą być pociągnięte do odpowiedzialności karnej na podstawie art. 51 u.o.d.o., staje się bardzo obszerny[15].

Przestępstwo bezprawnego udostępniania lub umożliwiania dostępu do jednostkowych danych medycznych (w tym danych osobowych pacjentów) jest przestępstwem formalnym, przy czym nie jest konieczne wystąpienie skutku w postaci zapoznania się z danymi przez osobę trzecią. Skoro bowiem przedmiotem ochrony art. 51 u.o.d.o. jest bezpieczeństwo danych, wydaje się oczywiste, iż bezpieczeństwo to jest zagrożone już z chwilą, gdy przestają działać jakiekolwiek ograniczenia w możliwości wglądu do tych danych. Stanowisko takie aprobuje m.in. Andrzej Adamski[16]. Innego zdania są natomiast Janusz Barta, Paweł Fajgielski oraz Ryszard Markiewicz, którzy w odniesieniu do udostępnienia danych wskazują, że w tym przypadku przestępstwo nabiera charakteru materialnego, gdyż „dla realizacji tego znamienia niezbędne jest zapoznanie się z danymi osobowymi przez co najmniej

[14] II KKN 438/00, LEX nr 45466.

[15] W literaturze przyjmuje się, że określenie „osoba obowiązana do ochrony danych osobowych" obejmuje wszystkie osoby fizyczne przetwarzające dane osobowe na podstawie upoważnienia administratora danych osobowych, względnie zawartej z nim umowy, o ile zostały one zobowiązane do ochrony takich danych. J. Barta, P. Fajgielski, R. Markiewicz, op. cit., 694–695; P. Pochopień, *Odpowiedzialność prawna związana z prowadzeniem dokumentacji medycznej*, [w:] idem (red.), *Dokumentacja medyczna*, Warszawa 2012, s. 197.

[16] Por. A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s. 51.

jednego nieupoważnionego odbiorcę"[17]. Wniosek ten wydaje się być jednak chybiony, bowiem pojęcia „udostępnianie" i „umożliwianie", biorąc pod uwagę literalne znaczenie tych słów, nie warunkują karalności czynu od przekazywania danych czy wglądu do nich przez osobę nieupoważnioną, ale od ułatwiania kontaktu osoby nieupoważnionej z danymi poprzez usunięcie barier – zabezpieczeń fizycznych, technicznych lub formalnych.

W świetle ww. wniosku bezprzedmiotowe wydają się jakiekolwiek rozważania, czy w przypadku udostępnienia danych osobowych tylko jednej osobie nieupoważnionej można uznać, że już doszło do zrealizowania znamion przestępstwa z art. 51 u.o.d.o. (z racji użycia przez ustawodawcę sformułowania „udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym"). Jedynie na marginesie trzeba zauważyć, że wedle krytykowanej w piśmiennictwie tezy postanowienia Sądu Najwyższego z dnia 21 listopada 2007 r.[18] „udostępnienie danych lub umożliwienie do nich dostępu jednej osobie nie wyczerpuje znamion omawianego przestępstwa"[19]. Z racji formalnego charakteru przestępstwa określonego w art. 51 u.o.d.o. istotne jest bowiem utrzymywanie się stanu zagrożenia bezpieczeństwa danych bez względu na to, ile osób pozyska te dane w sposób nieupoważniony, tudzież czy w ogóle ktokolwiek będzie zainteresowany ich pozyskaniem. Co prawda, w praktyce śledczej dokładne ustalenie kręgu osób, które w danym czasie miały dostęp np. do niezabezpieczonego komputera z rejestrem medycznym, bardzo często będzie w ogóle niemożliwe.

Przestępstwo bezprawnego udostępniania lub umożliwiania dostępu do jednostkowych danych medycznych i danych osobowych pacjentów może być popełnione zarówno umyślnie (art. 51 ust. 1 u.o.d.o.), jak i nieumyślnie (art. 51 ust. 2 u.o.d.o.). Sprawca przestępstwa określonego w art. 51 u.o.d.o. może popełnić je tak w postaci działania, jak zaniechania, chociaż i w tej kwestii w doktrynie występują rozbieżności stanowisk. Zdaniem J. Barty, P. Fajgielskiego i R. Markiewicza tak „udostępnienie", jak „umożliwienie dostępu" może nastąpić w postaci działania oraz zaniechania[20]. Według A. Adamskiego „umożliwianie dostępu" do danych może nastąpić tylko przez zaniechanie[21], natomiast Bolesław Kurzępa[22] zdaje się akceptować założenie o „umożliwianiu dostępu" w formie zarówno działania, jak i zaniechania (tj. nie tylko jako dopuszczenie osoby nieupoważnionej do urządzeń zawierających dane, ale także jako pozostawienie tych urządzeń bez żadnego realnego zabezpieczenia uniemożliwiającego dostęp do nich). Zasadne wydaje się zaaprobowanie sta-

[17] Por. J. Barta, P. Fajgielski, R. Markiewicz, op. cit., s. 696.

[18] IV KK 376/07, LEX nr 351219.

[19] Zob. A. Herzog, *Glosa do postanowienia SN z dnia 21 listopada 2007 r., IV KK 376/07*, „Prokuratura i Prawo" 2008, nr 11, s. 163–168.

[20] Zob. J. Barta, P. Fajgielski, R. Markiewicz, op. cit., s. 697.

[21] Por. A. Adamski, op. cit., s. 164.

[22] Por. B. Kurzępa, *Przestępstwa z ustawy o ochronie danych osobowych*, „Prokuratura i Prawo" 1999, nr 6, s. 51.

nowiska J. Barty, P. Fajgielskiego i R. Markiewicza w przedmiocie postaci czynności sprawczych przestępstwa określonego w art. 51 u.o.d.o. „Udostępnianie" i „umożliwianie dostępu" może nastąpić w formie działania i zaniechania. Czynności sprawcy mogą być wprost ukierunkowane na ułatwienie dostępu do danych (np. gdy lekarz lub pielęgniarka/ położna przekazują osobie postronnej swój login i hasło do rejestru medycznego – w tej sytuacji zacierają się nawet granice między „udostępnianiem" a „umożliwianiem dostępu"), a także poprzez odstąpienie od przyjętych w zakładzie opieki zdrowotnej reguł zapewnienia bezpieczeństwa informacji, gdyż stwarza to warunki do niekontrolowanego zapoznania się z danymi przez osoby nieupoważnione (np. gdy lekarz lub pielęgniarka/ położna po zakończeniu pracy z rejestrem medycznym pozostawia niezabezpieczony komputer bez uprzedniego wylogowania się z systemu/ rejestru).

Trzeba zgodzić się z poglądem J. Barty, P. Fajgielskiego i R. Markiewicza, że istnieje możliwość kumulatywnego zbiegu art. 51 ust. 1 u.o.d.o. oraz art. 266 § 1 k.k.[23], przy czym przypadki bezprawnego ujawnienia danych przetwarzanych w systemie informacji w ochronie zdrowia najczęściej będą dotyczyć tzw. tajemnic medycznych (lekarskiej, pielęgniarskiej itp.).

Przykłady bezprawnego udostępniania i umożliwiania dostępu do jednostkowych danych medycznych

Słusznie w literaturze podkreśla się, że na każdym etapie przetwarzania danych osobowych (zbierania informacji, ich przechowywania i wykorzystywania) informacja narażona jest na niebezpieczeństwo kradzieży lub nieautoryzowanej zmiany przypadkowej lub celowej. Coraz częściej też pacjenci, zdając sobie sprawę z wymienionych niebezpieczeństw, wyrażają zastrzeżenia co do celowości udostępniania niektórych danych medycznych gromadzonych i przetwarzanych w zakładach opieki zdrowotnej[24].

Najbardziej jaskrawym przykładem popełnienia czynu zabronionego określonego w art. 51 ust. 1 u.o.d.o. jest sprawa rozpatrywana przed Sądem Okręgowym w O.[25] W stanie faktycznym przedmiotowej sprawy pokrzywdzona X była pacjentką oskarżonej Y, wykonującej zawód lekarza psychiatry. X wraz z mężem odbywali wizyty w gabinecie oskarżonej w ramach prowadzonej terapii małżeńskiej. Po upływie około 1,5 roku od ostatniej konsultacji lekarskiej asystentka oskarżonej Y odebrała telefon od osoby, która żądając wydania zaświadczenia lekarskiego, przedstawiła się jako pokrzywdzona X. Aby potwierdzić tę informację, asystentka oskarżonej Y

[23] Zob. J. Barta, P. Fajgielski, R. Markiewicz, op. cit., s. 699.

[24] E. Strzesak, *Aspekty praktyczne przetwarzania danych osobowych w zakładach opieki zdrowotnej*, „Prawo i Medycyna" 2000, nr 2, s. 145.

[25] Sygn. akt VII Ka 855/13. Szczegółowe informacje dotyczące przedmiotowego rozstrzygnięcia sądowego w posiadaniu autora.

poprosiła rozmówczynię o podanie imienia, nazwiska, adresu, nazwy leków, które przyjmuje, oraz numeru telefonu. Po uzyskaniu odpowiedzi na ww. pytania i zapewnieniu „podjęcia próby załatwienia sprawy" asystentka zdała oskarżonej Y relację z przebiegu rozmowy. Oskarżona Y wystawiła żądane zaświadczenie lekarskie i zgodnie ze wskazówką osoby telefonującej do gabinetu przesłała je mężowi pokrzywdzonej X, z którym ta pozostawała w konflikcie małżeńskim i z którym ostatecznie się rozwiodł. W związku z powyższym oskarżonej Y postawiono zarzut popełnienia przestępstwa z art. 51 ust. 1 u.o.d.o. w zb. z art. 266 § 1 k.k., wskazując, że będąc zobowiązaną do ochrony danych osobowych pacjentów gabinetu psychiatrycznego, udostępniła osobie nieuprawnionej informacje o zdrowiu pacjentki X w ten sposób, że przekazała (byłemu) mężowi pacjentki X zaświadczenie lekarskie zawierające dane osobowe wymienionej, czym wbrew przepisom ustawy oraz przyjętemu na siebie zobowiązaniu ujawniła informacje o zdrowiu psychicznym pokrzywdzonej, które uzyskała w związku z wykonywaną pracą lekarza psychiatry. Sąd I instancji uznał oskarżoną Y za winną popełnienia zarzucanych jej czynów i wydał wyrok skazujący[26].

Innymi występującymi i mogącymi wystąpić w praktyce przykładami bezprawnego udostępniania i umożliwiania dostępu do jednostkowych danych medycznych i danych osobowych pacjentów są[27]:

1) udostępnienie danych osobowych pacjentów przedsiębiorcom prowadzącym działalność ubezpieczeniową (chodzi tu w szczególności o udzielanie informacji

[26] W uzasadnieniu wyroku Sąd Okręgowy w O. zauważył m.in., że zakres informacji osobistych, o które wypytywała asystentka oskarżonej Y podczas rozmowy telefonicznej, nie był tego rodzaju, aby można była w sposób wyłączający jakąkolwiek omyłkę zidentyfikować osobę dzwoniącą jako uprawnioną do uzyskania żądanej dokumentacji. Dane personalne, o których podanie rozmówczyni gabinetu została poproszona, były *de facto* ogólnie dostępne dla osób trzecich (imię, nazwisko, adres, nazwy leków, numer telefonu). Jakkolwiek bardziej poufne było pytanie o przyjmowane leki, niemniej uzyskana odpowiedź nie mogła zadecydować o bezsprzecznym rozpoznaniu osoby dzwoniącej. Zdaniem Sądu Okręgowego w O. asystentka oskarżonej Y nie mogła wykluczyć, że dysponentem tych informacji mogą być również osoby z kręgu rodziny czy inne osoby bliskie dla pokrzywdzonej, które nie były uprawnione do otrzymania zaświadczenia. Rozpoznanie pokrzywdzonej X na podstawie głosu (ton lub tembr głosu) też budziło zasadnicze wątpliwości w kontekście okoliczności uprzednich jej wizyt. Z zeznań asystentki oskarżonej Y wynikało bowiem, że miała z pokrzywdzoną X kontakt sporadyczny, ograniczający się do rejestracji daty wizyty czy założenia karty choroby. Decyzja oskarżonej Y o wydaniu żądanej informacji bazowała jedynie na subiektywnych w tym zakresie wrażeniach asystentki, niepopartych żadnymi racjonalnymi przesłankami. Oskarżona Y nie podjęła żadnej próby dodatkowej weryfikacji osoby dzwoniącej, poprzestając jedynie na „rozpoznaniu" jej przez asystentkę, która miała sporadyczny, a przy tym bardzo wybiórczy kontakt z pokrzywdzoną X. Zdaniem Sądu Okręgowego w O., na oskarżonej Y z racji wykonywanego zawodu ciążył szczególny obowiązek zachowania pozyskiwanych informacji w tajemnicy. Wyjątkowość tego obowiązku wynikała z faktu, że oskarżona Y wykonywała zawód zaufania publicznego, a tego rodzaju działalność wiąże się z uzyskiwaniem ważnych, a przy tym często intymnych informacji dotyczących życia osobistego poszczególnych osób. Oskarżona Y wykonywała od wielu lat zawód lekarza psychiatry i z tej racji istnienie tego obowiązku w realiach omawianej sprawy nie było dla niej zaskoczeniem, a okolicznością standardową wynikającą z zawodowej rutyny.

[27] W przedmiocie powołanych przykładów por. D. Wąsik, op. cit., s. 204–205.

firmom ubezpieczeniowym o pacjentach poszkodowanych w wyniku wypadku komunikacyjnego celem skierowania do nich oferty uzyskania odszkodowania od sprawcy zdarzenia; firmy ubezpieczeniowe mogą być również zainteresowane w pozyskaniu danych o stanie zdrowia konkretnych pacjentów celem zweryfikowania prawdziwości informacji przekazanych im przy podpisaniu umowy o ubezpieczenie na życie i dochodzeniu wypłaty środków pieniężnych z polisy);

2) udostępnianie danych osobowych pacjentów podmiotom zajmującym się dystrybucją leków i wyrobów medycznych (celem skierowania oferty zakupu określonych wyrobów medycznych, np. wózków inwalidzkich);

3) udostępnianie danych osobowych pacjentów kancelariom świadczącym usługi prawne (np. udzielanie informacji o podejrzeniu popełnieniu błędu w procesie leczenia określonych pacjentów celem skierowania oferty prowadzenia procesów sądowych o odszkodowanie);

4) wywieszanie listy pacjentów na drzwiach gabinetów lekarskich celem uniknięcia nieporozumień wśród pacjentów co do kolejności odbywania konsultacji;

5) odczytywanie imienia i nazwiska pacjenta wchodzącego do gabinetu lekarskiego w obecności innych pacjentów oczekujących na wizytę;

6) udostępnianie danych pacjentów w trakcie rozmów towarzyskich prowadzonych pomiędzy przedstawicielami personelu medycznego na tematy związane z procesem leczenia lub zaobserwowane w dokumentacji medycznej, względnie udostępnianie danych osobowych w trakcie rozmowy telefonicznej lekarza z pacjentem, prowadzonej przy osobach trzecich, jeżeli ten udziela telefonicznych porad co do procesu leczenia lub odczytuje pacjentowi wyniki badań;

7) umożliwienie dostępu osób trzecich do danych pacjentów w wyniku niewłaściwego przechowywania dokumentacji medycznej lub wręcz braku jakiegokolwiek zabezpieczenia tej dokumentacji (np. gdy dokumentacja przechowywana jest w pomieszczeniach ogólnodostępnych i otwartych).

8) udostępnianie osobom nieuprawnionym danych (w postaci elektronicznej lub tradycyjnej – papierowej) kluczowych informacji o systemie, bazie (np. haseł) lub procedur przetwarzania danych;

9) nienależyte utrzymanie stanu infrastruktury telekomunikacyjnej, prowadzące do możliwości zainfekowania systemu wirusem komputerowym lub niekontrolowanego kopiowania i pobierania danych gromadzonych w systemie lub rejestrze;

10) rażące naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (np. pozostawienie pomieszczenia lub terminala bez odpowiedniego nadzoru).

Problematycznym zagadnieniem przy stosowaniu art. 51 ust. 1 u.o.d.o. może być kwalifikowanie jako występek określonych sytuacji, gdy pacjent jest podmiotem faktycznie udostępniającym dane osobowe. Jako przykład wskazuje się tutaj np. zbieranie informacji o stanie cywilnym kobiety niezamężnej przyjmowanej do porodu, co naraża ją na przeżywanie kłopotliwej sytuacji, natomiast informacja ta (zmienna w czasie) nie ma żadnego znaczenia dla postępowania me-

dycznego[28]. Inne przykłady to konieczność ustnego przekazywania przez pacjenta danych osobowych w obecności innych osób, np. w rejestracji placówki, podczas sporządzania zaświadczenia o czasowej niezdolności do pracy lub innego typu dokumentacji medycznej, a także podczas obchodu lekarskiego w salach wieloosobowych. Co prawda, można próbować kwalifikować takie zdarzenia jako umożliwienie dostępu do danych osobowych przez osoby nieuprawnione, jednakże zawsze kwestią wątpliwą będzie zgoda pacjenta na ujawnienie jego danych osobowych, zwłaszcza wtedy, jeżeli nie zgłaszał on zastrzeżeń co do warunków (obecności osób trzecich), w jakich udzielał informacji personelowi medycznemu. Nadmienić należy, że ustalenie *post factum* takiej zgody może być znacznie utrudnione lub wręcz niemożliwe, np. w przypadku znacznego pogorszenia stanu zdrowia pacjenta (np. postęp i rozwój choroby Alzheimera oraz problemy z pamięcią, afazja, rozwój chorób psychicznych, zakłócenia czynności psychicznych innego typu etc.) lub jego śmierci[29].

Mając na względzie powyższe wątpliwości, należy zastanowić się nad zasadnością nowelizacji art. 51 ust. 1 u.o.d.o. i rozszerzenia strony przedmiotowej występku o przesłankę gromadzenia danych osobowych w warunkach umożliwiających dostęp do nich osobom nieuprawnionym. W takiej sytuacji brzmienie przepisu art. 51 ust. 1 u.o.d.o. mogłoby być następujące: „Kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je, umożliwia dostęp do nich osobom nieupoważnionym lub gromadzi je w warunkach umożliwiających zapoznanie się z nimi przez osoby nieupoważnione, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2”[30]. Zgoda zainteresowanego na zbieranie danych osobowych w warunkach wyłączających poufność przekazywanych informacji nie byłaby okolicznością wyłączającą winę sprawcy.

Wnioski

1. Najczęściej wśród mankamentów infrastruktury informacyjnej w ochronie zdrowia wymienia się:

a) brak strategicznego modelu infrastruktury informacyjnej;

b) autonomizację systemów i zasobów informacyjnych sektora publicznego (tworzenie wielu autonomicznych, niewspółpracujących ze sobą systemów teleinformatycznych, których funkcje ograniczone były do obsługi kompetencji zazwyczaj jednej jednostki organizacyjnej lub wybranego segmentu systemu ochrony zdrowia);

---

[28] E. Strzesak, op. cit., s. 145–146. Z drugiej strony autor wskazuje, że gromadzenie danych dotyczących wykształcenia, zawodu lub stanu cywilnego też ma ograniczone zastosowanie w procesie leczenia, ale może służyć do analiz epidemiologicznych.

[29] Zob. D. Wąsik, op. cit., s. 205–206.

[30] Ibidem, s. 206.

c) nagminne powielanie schematu „nowe technologie – stare procedury – jeszcze starsze metody projektowania systemów";

d) dezintegrację i brak interoperacyjności systemów informacyjnych;

e) dominację gestorów systemów nad ich użytkownikami[31].

Należy pamiętać, że obok mankamentów występują jeszcze zagrożenia, w tym przestępczość związana z nieprawidłowym udostępnianiem i przetwarzaniem danych medycznych. Motywacja sprawców, metody popełnienia czynów, jak również postacie występków bywają różne, niemniej jednak dotyczą one nie tylko danych pacjentów przetwarzanych w systemach informatycznych, ale również gromadzonych w tradycyjny sposób, w ramach kontaktów personelu medycznego z pacjentem przy udzielaniu mu świadczeń zdrowotnych.

2. Dokładne określenie zakresu przedmiotowego danych pacjentów, które podlegają ochronie prawnej, może budzić pewne problemy praktyczne z uwagi na „rozbicie" tego zagadnienia i jego umiejscowienie w ustawie o ochronie danych osobowych i ustawie o informacji w ochronie zdrowia. Sytuację komplikuje fakt, że jednostkowe dane medyczne zdefiniowane zostały w sposób niekonsekwentny, a wykładnia tego pojęcia stwarza pewne problemy praktyczne. Dzieje się tak dlatego, że zakresy pojęciowe jednostkowych danych medycznych i danych osobowych w odniesieniu do pacjentów dość często zanikają. Na gruncie przepisów ustaw zasadne wydaje się stwierdzenie, że wszystkie dane osobowe pacjenta są jednostkowymi danymi medycznymi, ale nie wszystkie jednostkowe dane medyczne będą stanowiły dane osobowe. Z tego względu podnieść należy postulat o rozszerzenie ochrony prawnej na wszelkie dane zawarte w dokumentacji medycznej. Koncepcja ta uwzględni zakres tajemnicy lekarskiej, pielęgniarskiej i położniczej, która obejmuje nie tylko dane dotyczące stanu zdrowia, ale także informacje uzyskane w związku z wykonywaniem zawodu medycznego.

3. Z uwagi na odesłanie przez samego ustawodawcę przy projektowaniu ustawy o ochronie informacji do przepisów karnych ustawy o ochronie danych osobowych, zasadne jest przyjęcie, że każdy, kto udostępnia lub umożliwia dostęp do jednostkowych danych medycznych, będzie ponosił odpowiedzialność karną na podstawie art. 51 ust. 1 u.o.d.o. Zajmując stanowisko w przedmiocie dość burzliwych sporów co do możliwości zastosowania przepisu w konkretnych warunkach i określenia znamion tego czynu zabronionego, wskazać należy, że przestępstwo z art. 51 ust. 1 u.o.d.o. jest przestępstwem formalnym, albowiem skoro przedmiotem ochrony jest w tej sytuacji bezpieczeństwo danych, oczywiste wydaje się, iż bezpieczeństwo to jest zagrożone już z chwilą, gdy przestają działać jakiekolwiek ograniczenia w możliwości wglądu do tych danych. Pojęcia „udostępnianie" i „umożliwianie", biorąc pod uwagę literalne znaczenie tych słów, nie warunkują karalności czynu od przekazywania danych czy wglądu do nich osób nieupoważnionych, ale od ułatwiania kontaktu takich osób z danymi poprzez usunięcie barier – zabezpieczeń

[31] Por. uzasadnienie projektu ustawy o systemie informacji w ochronie zdrowia, Sejm VI kadencji, druk nr 3485.

fizycznych, technicznych lub formalnych. Co więcej, z racji formalnego charakteru przestępstwa określonego w art. 51 u.o.d.o. bez znaczenia jest, ile osób pozyska te dane w sposób nieupoważniony, tudzież czy w ogóle ktokolwiek będzie zainteresowany ich pozyskaniem.

4. Bezprawne udostępnianie lub umożliwianie dostępu do jednostkowych danych medycznych i innych danych pacjentów przybrać może różne postacie, wśród których szczególnie niebezpieczne to: udostępnienie danych osobowych pacjentów przedsiębiorcom prowadzącym działalność ubezpieczeniową, udostępnianie danych osobowych pacjentów podmiotom zajmującym się dystrybucją leków i wyrobów medycznych oraz udostępnianie danych osobowych pacjentów kancelariom świadczącym usługi prawne. W tych sytuacjach szczególna szkodliwość przestępstw przejawia się w fakcie, iż są one dokonywane na ogół z pobudek materialnych (udostępnianie danych za wynagrodzeniem lub w celu uzyskania konkretnych profitów), a z racji charakteru podmiotów zainteresowanych danymi, specyfiki ich działalności i celów dalszego przetwarzania, mogą być one wykorzystywane w sposób ciągły oraz przekazywane dalej nieograniczonej liczbie podmiotów (tzw. handel danymi osobowymi). Podmioty prowadzące bazy danych zobowiązane są zatem do zabezpieczenia przetwarzania danych poprzez stosowanie (wdrożenie i eksploatację) środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych i jednostkowych danych medycznych – odpowiednią do zagrożeń oraz kategorii danych objętych ochroną. Właściwe opracowanie i przestrzeganie procedur zaliczanych do tzw. polityki bezpieczeństwa systemów informatycznych może ograniczyć liczbę zjawisk zagrażających niekontrolowanym udostępnianiem danych osobowych podmiotom nieuprawnionym lub ich bezprawnym przetwarzaniem.

Wśród najważniejszych postanowień polityki bezpieczeństwa w pierwszej kolejności wymienić należy tzw. regułę czystego ekranu, która wymaga od pracownika podmiotu leczniczego po zakończeniu pracy z bazą danych (z systemem) zniszczenia w sposób uniemożliwiający zidentyfikowanie danych zbędnych dokumentów papierowych (wydruków) oraz dokumentów elektronicznych uzyskanych z systemów informatycznych (np. wygenerowanych uprzednio plików zapisanych na pulpicie ekranu), zawierających dane powstałe w trakcie przetwarzania. Istotną kwestią zaliczaną do polityki bezpieczeństwa jest też umieszczanie przez podmioty lecznicze w umowach zawieranych z podmiotami zewnętrznymi i bezpośrednimi wykonawcami (np. niepublicznymi zakładami opieki zdrowotnej lub lekarzami prowadzącymi prywatne praktyki zawodowe) klauzuli zobowiązującej do ochrony danych przetwarzanych przez ten podmiot. Ponadto istotne jest zwrócenie uwagi na potrzebę właściwego nadzoru nad przebywającymi w obiekcie podmiotu leczniczego po godzinach pracy przyjętych w regulaminie pracownikami personelu gospodarczego, ochrony itp. oraz pracownikami zatrudnionymi przez podmioty zewnętrzne, będące stronami umów cywilnoprawnych (dyżury)[32].

[32] D. Wąsik, op. cit., s. 198–199.

Innym elementem polityki bezpieczeństwa jest wyłączenie dostępności dla osób nieuprawnionych obszarów przetwarzania danych w obiektach i pomieszczeniach podmiotu leczniczego. W polityce bezpieczeństwa należy też uwzględnić zasadę proporcjonalności, przejawiającą się w konieczności stosowania środków technicznych i organizacyjnych adekwatnych do warunków użytkowania obiektów z określonymi obszarami przetwarzania danych[33].

Summary

Unauthorized sharing and providing access to individual medical data in terms of criminal responsibility (article 51 u.o.d.o.)

Key words: illegal sharing and processing of personal data, inidividual medical data, the information in health care.

The paper discusses the issue of the protection of patient data from unauthorized sharing and processing, with particular emphasis on individual medical data. Timeliness issues due to the ongoing process of informatization in health care will need to secure the proper implementation of the obligation to process data by means of, among others, criminal penalties for any failure in this regard. The publication discusses succession issues conceptual scope of individual medical data and interpretation problems in this area, the analysis of the offense of unlawful access and processing of personal data for individual medical data and examples of offenses specified in article 51 u.o.d.o.

[33] Więcej na temat założeń polityki bezpieczeństwa systemów informatycznych i baz danych w zakładach opieki zdrowotnej, a także zasad bezpiecznego zarządzania systemami informatycznymi i bazami danych zob. ibidem, s. 199–202.