STUDIA I ARTYKUŁY

Marek Zubik

Ochrona prywatności informacji o zdrowiu w nowym prawodawstwie Unii Europejskiej*

Wraz z rozwojem i upowszechnieniem się nowych metod komunikowania się coraz bardziej współczesny człowiek funkcjonuje w cyberrzeczywistości. Nie jest jednak jednoznaczne, czy rozwojowi technicznemu towarzyszy proporcjonalny wzrost świadomości potrzeby ochrony własnej prywatności. Władza publiczna musi przyjść tu obywatelom z pomocą. Tworzone przez nią prawo poprawnie działa wszakże tylko w odniesieniu do tych, którzy roztropnie dbają o własne prawa, jak przypomina starodawna paremia rzymska: *ius vigilantibus scriptum est*. Prawo też, ze swojej natury, jest wytworem ludzkim, obarczonym swoimi ograniczeniami, będącym mechanizmem reaktywnym. Prawodawca najczęściej odpowiada na problemy powstające już w praktyce; rzadziej jest w stanie je przewidzieć i prognozować.

Chciałbym zatem, z prawniczego punktu widzenia, przedstawić kilka ogólnych uwag, które powinno się postrzegać w perspektywie ochrony prywatności w systemie ochrony zdrowia. Być może pozwoli to nieco lepiej zrozumieć aktualnego prawodawcę. Jest to konieczne chociażby ze względu na proces zmian rozwiązań prawnych dotyczących ochrony prywatności – także w medycynie – zachodzący we wszystkich państwach

* Tekst stanowi zmodyfikowaną wersję referatu wygłoszonego podczas konferencji „Tajemnica medyczna. Praktyczne dylematy ochrony danych pacjentów" dn. 5 marca 2018 r., zorganizowanej przez Okręgową Izbę Lekarską w Warszawie.

członkowskich Unii Europejskiej. Jest też i inna motywacja. Niezależnie od ról społecznych, które pełnimy, bywamy także pacjentami. Natomiast prawo dotyczące ochrony prywatności dopadnie nas także po okresie ludzkiej egzystencji, choć naturalnie w zmodyfikowanym już zakresie, i tylko w doczesności.

1. Kwestia zachowania poufności informacji odnoszącej się do pacjenta i jego stanu zdrowia jest immanentnie związana z zawodami medycznymi. Stanowi niezbędny element, który pozwala wytworzyć konieczne zaufanie między pacjentem a lekarzem, innymi osobami świadczącymi usługi medyczne czy całym systemem ochrony zdrowia, nie wyłączając nawet systemu zabezpieczenia społecznego. Tak szeroko rozumiana tajemnica medyczna nie wyczerpuje wszakże problematyki ochrony danych osobowych w interesującej nas sferze. Dotyczy bowiem także danych osobowych personelu medycznego i technicznego pracującego w systemie ochrony zdrowia. Ochrona informacji niebędących informacją publiczną odnosi się do wszystkich osób, które funkcjonują w obrębie systemu ochrony zdrowia, również tych wykonujących zawody medyczne, chociaż niewątpliwie w innym zakresie niż w przypadku pacjentów. Zachowanie tajemnicy zawodowej jest niezwykle istotnym elementem, jednakże stanowi tylko część systemu ochrony prywatności. Nie da się zatem zagadnienia ochrony danych osobowych sprowadzić tylko do kwestii relacji lekarz–pacjent ani do sfery: tajemnica zawodowa a dane osobowe. Pamiętać wszakże należy o tym szerokim kontekście doniosłości prawnej ochrony prywatności w całym kontekście funkcjonowania systemu ochrony zdrowia.

2. Wszystkie wolności prawnie chronione w cywilizowanych społeczeństwach swój rodowód czerpią z godności człowieka. Prawodawca może i powinien je odtworzyć oraz ma obowiązek je chronić. Nie przyznaje ich jednak według własnego uznania. Nie ma tutaj istotnej swobody regulacyjnej, o ile nie chce się narazić na to, że ustrój, jaki stworzy, zostanie uznany za niegodziwy. Niewątpliwie natomiast od działalności prawodawcy zależy efektywność poszczególnych wolności człowieka. Realizacja praw człowieka wiąże się bowiem zarówno z profesjonalizmem przy tworzeniu norm prawnych, jak i z odpowiednim stosowaniem przepisów

przez organy wykonawcze, nie wyłączając ochrony poszczególnych osób, realizowanej przez sądy.

Generalnie w prawoznawstwie rozróżnia się wolności, prawa oraz obowiązki[1]. Dwa pierwsze pojęcia zbiorczo z czasem zaczęto ujmować jako prawa człowieka. Niekiedy oddzielnie konstruuje się kategorię środków ochrony wolności i praw, czyli takich uprawnień, głównie procesowych, które pozwalają na egzekwowanie praw człowieka. Kategorie te odnoszą się do jednostek, ściślej – poszczególnych osób. Brak jest jednak pełnej jednolitości w posługiwaniu się tymi pojęciami oraz jednoznacznych konstrukcji doktrynalnych. Niejednolitość języka prawnego (czyli tekstów normatywnych) i prawniczego (w którym formułowane są wypowiedzi o prawie) przeniosła się na język publicystyki. Brak ogólnej wizji, niestaranność, niższy stopień precyzji, chęć łatwego przekazu przeniosły się i utrwaliły w języku potocznym, z którego z kolei zaczął czerpać prawodawca, zamykając intelektualne koło.

Podmiotem wolności są niewątpliwie wszyscy ludzie, co wynika z samego faktu przynależności do gatunku *homo sapiens*[2]. Teza ta nie przekreśla możliwości odnoszenia wolności również do podmiotów zbiorowych, które niekiedy mają swoją własną osobowość prawną. Natomiast adresatem wolności są podmioty władzy publicznej. Na organach władzy ciążą obowiązki negatywne oraz pozytywne. Pierwsze polegają na zakazie utrudniania realizacji treści danej wolności (zob. art. 31 ust. 2 zd. 2 Konstytucji[3]); drugie – na nakazie stworzenia efektywnych mechanizmów pozwalających na ich prawną ochronę. Konstytucja podkreśla, że „Nikogo nie wolno zmuszać do czynienia tego, czego prawo mu nie nakazuje" (art. 31 ust. 2 zd. 2). Nie wolno również zapominać o prawnych konsekwencjach realizacji wolności jednych przez drugich (zob. art. 31 ust. 2 zd. 1); nie tylko o bezpośrednim oddziaływaniu organów państwa na prawa człowieka. Konstytucja jednoznacznie wskazuje, że „Każdy jest

1 Prawdą jest jednak, że coraz częściej trudno jest mówić, z różnych zresztą powodów, o „czystej postaci" tego podziału. Zob. np. zdanie odrębne sędziego P. Tulei do wyroku TK z 12 I 2012 r., Kp 10/09, OTK ZU 2012, seria A, nr 1, poz. 4.

2 Zob. np. M. Zubik, *„Wolność" a „prawo" (pięć hipotez o stosowaniu pojęć konstytucyjnych dotyczących praw człowieka)*, „Państwo i Prawo" 2015, z. 9, s. 3–19.

3 Konstytucja Rzeczypospolitej Polskiej z dn. 2 IV 1997 r., Dz.U. 1997, nr 78, poz. 483 ze zm., dalej: „Konstytucja".

obowiązany szanować wolności i prawa innych" (art. 31 ust. 2 zd. 1), nie tylko zatem władze publiczne.

3. Prywatność człowieka jest – w kontekście podziału na wolności i prawa – niewątpliwie wolnością. Zasadne jest mówienie o jej prawnej ochronie, o szczegółowych prawach, które służą zachowaniu prywatności, a także o obowiązkach ciążących w związku z tym na innych. W tym sensie wolność, jaką jest prywatność, stanowi konglomerat szczegółowych praw, chronionych przez prawo międzynarodowe czy Konstytucję, takich jak: prawo do ochrony życia prywatnego, decydowania o swoim życiu osobistym, tajemnica komunikowania się, nienaruszalność mieszkania, autonomia informacyjna, prawo dostępu do urzędowych zbiorów danych dotyczących danej osoby itd. Będąc ze swojej istoty wolnością, prywatność jest sferą swobodnego działania nas wszystkich dopóty, dopóki prawo opatrzone sankcją ze strony organów państwa nam czegoś nie nakazuje lub zakazuje, i to wyłącznie w granicach określonych zasadami pomocniczości i proporcjonalności. Gdyby była „tylko" prawem, musielibyśmy wówczas odnaleźć wyraźną regulację ustawową, która pozwalałaby nam wskazać, dlaczego domagamy się, by nikt, nie tyko państwo, nie ingerował, gdy decydujemy o swoim życiu osobistym – o tym, z kim i jak się komunikujemy, kogo wybieramy na partnerów życiowych, skąd mamy możliwość swobodnego wyboru, jakie informacje przekażemy innym na swój temat itd.

Zrozumienie tej różnicy w kategoriach prawnych ma doniosłe konsekwencje i znaczenie praktyczne. Muszę wszakże przyznać, że w języku prawnym, nie tylko polskim, utrwalił się inny związek frazeologiczny. Zapewne zwrot „prawo do prywatności" już pozostanie w powszechnym użyciu. Nie ma widoków, by miało się tu coś zmienić. O naturze i istocie prywatności jako wolności należy jednak pamiętać.

4. Władze publiczne nie mogą arbitralnie naruszać prywatności obywateli, dowolnie zbierać o nich wszelkich informacji czy potem je przetwarzać. Mają obowiązek zapewnienia podmiotom prywatności efektywnych mechanizmów jej ochrony. Muszą chronić prywatność swoich obywateli, również przed naruszeniem prywatności ze strony innych podmiotów prawa prywatnego czy zagrożeniami płynącymi spoza terytorium

państwa. Także współobywatele nie mogą sobie dowolnie postępować z danymi osobowymi innych podmiotów. Chroniąc prywatność, mówimy zatem o złożoności relacji: władza–jednostka, jednostka–jednostka czy podmioty na zewnątrz kraju a obywatele.

Pamiętać jednak należy, że żadna z wolności – w tym prywatność – nie ma charakteru absolutnego. Istnieją w demokratycznym państwie prawa takie wartości, które mogą nakładać pewne obowiązki przełamujące ochronę płynącą z realizacji danej wolności. Niekiedy także taka interwencja ustawodawcza będzie konieczna ze względu na potrzebę zapewnienia jednoczesnej realizacji wolności i praw przez inne podmioty. Wówczas władze publiczne muszą dokonać starannego wyważenia ze sobą poszczególnych wolności i praw. Najczęściej ingerencja ta polegać będzie na stworzeniu prawnych, formalnych i organizacyjnych elementów systemu prawnego, regulującego daną sferę życia społecznego, w interesującym nas zakresie – żądaniu podania zakresu przekazywania danych osobowych, ich przetwarzania, ochrony, udostępniania, korygowania, niszczenia czy nawet zasad ponoszenia odpowiedzialności za naruszenie prywatności.

Nie inaczej rzecz się ma w przypadku tej części prywatności człowieka, która wiąże się z ochroną zdrowia. Tu bowiem w konkurencji pozostają ze sobą: zakaz zmuszania ludzi do ujawniania informacji o sobie samych (art. 51 ust. 1), zakaz gromadzenia i udostępniania przez władze publiczne informacji o obywatelach ponad to, co konieczne w demokratycznym państwie prawa (art. 51 ust. 2), zapewnienie prawa dostępu do urzędowych zbiorów dokumentów i danych (art. 51 ust. 3 zd. 1), prawo do sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych i pozyskanych w sposób niezgodny z prawem (art. 51 ust. 4) – z takimi wartościami jak: zapewnienie prawa do ochrony zdrowia (art. 68 ust. 1), prawo do równego dostępu do świadczeń opieki zdrowotnej finansowanej ze środków publicznych (art. 68 ust. 2 zd. 1), zapewnienie szczególnej opieki zdrowotnej dzieciom, kobietom ciężarnym, osobom niepełnosprawnym i w podeszłym wieku (art. 68 ust. 3) oraz zwalczanie chorób epidemicznych (art. 68 ust. 4). Pamiętać też warto, że zdrowie publiczne oraz realizacja wymienionych praw konstytucyjnych związanych z życiem i zdrowiem człowieka mogą uzasadniać ograniczenie w korzystaniu z konstytucyjnych wolności i praw jednych względem drugich (art. 31 ust. 3).

5. Znajdujemy się obecnie w szczególnym momencie rozwoju podejścia aktualnego prawodawcy unijnego do ochrony informacji i danych osobowych pozyskiwanych i przetwarzanych między innymi w związku z działalnością systemu ochrony zdrowia. Są co najmniej dwie doniosłe okoliczności, które należy uwzględnić. Pierwsza ma wymiar globalny i dotyczy zmian cywilizacyjnych i technologicznych, druga – ewolucji podejścia prawodawcy unijnego do ochrony danych osobowych. Te aspekty muszą być widziane łącznie, gdyż dopiero w tym świetle można dostrzec pełną gamę nowych zagrożeń, jak i bardziej realistyczne podejście prawodawcy do tych zagadnień.

6. Stoimy u progu – z jednej strony – rozpoczęcia obowiązywania od 25 maja 2018 r. nowych regulacji prawa unijnego bezpośrednio dotyczących ochrony prywatności. Chodzi przede wszystkim o dwa dokumenty: ogólne rozporządzenie o ochronie danych (2016/679)[4] oraz tzw. dyrektywę policyjną[5]. Dodać warto, że trwają, w różnym stopniu zaawansowane, prace legislacyjne nad jeszcze dwoma innymi aktami normatywnymi – rozporządzeniem w sprawie prywatności i łączności elektronicznej[6] oraz wnioskiem Komisji Europejskiej w sprawie przyjęcia dyrektywy Parlamentu Europejskiego i Rady (UE) wprowadzającej Europejski kodeks łączności elektronicznej, zawierający wiele definicji legalnych rzutujących na znaczenie pojęć ujętych w pozostałych aktach normatywnych.

Nowe rozwiązania wymagają interwencji prawodawcy krajowego[7], a następnie przyswojenia praktycznego. Ważne jest, by je zauważyć, gdyż

4 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dn. 27 IV 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, Dz.U. UE L 119/1 z 2016 r.

5 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dn. 27 IV 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW, Dz.U. UE L 119/89 z 2016 r.

6 Rozporządzenie Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylające dyrektywę 2002/58/WE.

7 Ustawa wprowadzająca nowe prawodawstwo unijne w perspektywie zapewnienia odpowiedniego okresu dostosowawczego została przyjęta bardzo późno. Zob. ustawa z dn. 10 V 2018 r. o ochronie danych osobowych, Dz.U. 2018, poz. 1000. Opublikowaną ją w Dzienniku Ustaw z dn. 24 maja 2018 r., czyli w przeddzień wejścia w życie nowych rozwiązań prawnych Unii Europejskiej.

zarówno jako całość, jak i ich poszczególne, specyficzne rozwiązania odnoszą się do tych danych osobowych, o generalnie niezwykłej doniosłości dla prywatności każdego człowieka, które pozyskiwane, przetwarzane i przechowywane są w związku z realizacją prawa do ochrony zdrowia.

Obecnie działalność prawodawcza nie dokonuje się jednak na legislacyjnym „ugorze". W ostatnich dziesięcioleciach widać coraz większą świadomość demokratycznego prawodawcy, którego zadaniem jest konstruowanie efektywnych mechanizmów zapewniających ochronę prywatności każdego człowieka, a szczególnie w sferze informacji medycznych. Jednocześnie świadomość zagrożeń przełożyła się na samoświadomość jednostek, a to pociągnęło za sobą wzrost orzecznictwa sądowego. Nie chodzi tylko o orzeczenia sądów polskich[8], lecz głównie Europejskiego Trybunału Praw Człowieka[9] oraz Trybunału Sprawiedliwości Unii Europejskiej. Warto przypomnieć, że Trybunał w 2014 r. uznał nieważność całej dyrektywy 2006/24/WE w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej[10]. Działalność obu tych sądowych organów międzynarodowych, chociaż ich kognicja terytorialnie i przedmiotowo nie w pełni się pokrywa, zdecydowanie przyczyniła się do zmiany podejścia do ochrony prywatności w ogóle, a także wymusiła zmiany w prawie państw należących do Rady Europy oraz – co bezpośrednio wiąże się z przywołanymi aktami normatywnymi – państw członkowskich Unii Europejskiej.

7. Jest jeszcze co najmniej jeden ważny aspekt nowych regulacji dotyczących ochrony danych osobowych, i to najbardziej globalny. Znajdujemy się na progu kolejnej rewolucji technologicznej, której znaczenia nie można zignorować, analizując zagadnienia ochrony prywatności i tajemnic zawodowych, w tym lekarskiej. Od niepamiętnych czasów gromadzono

8 Zob. np. wyrok TK z 11 X 2016 r., SK 28/15, OTK ZU 2016, seria A, poz. 79; wyrok TK z 18 XII 2014 r., K 33/13, OTK ZU 2014, seria A, nr 11, poz. 120.

9 Zob. np. orzeczenie ETPC z 29 IV 2014 r. w sprawie L.H. p. Łotwie, skarga nr 52019/07, w którym Trybunał jednoznacznie uznał, że zbieranie medycznych danych osobowych wkracza w sferę życia prywatnego, a dokonywanie tego bez uprzedniej zgody tej osoby narusza art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności (Dz.U. 1993, nr 61, poz. 284).

10 Chodzi tu o orzeczenie z 8 IV 2014 r. w połączonych sprawach C-293/12 i C-594/12 Digital Rights Ireland i Seitlinger i inni. Istotne znaczenie miało też orzeczenie z 21 XII 2016 r. w sprawie C-203/15 i C-698/15 Tele2 Sverige AB i Secretary of State for the Home Department.

informacje o ludziach. Robiły to organy władzy, jak i podmioty prywatne. Władza publiczna zawsze była zainteresowana zbieraniem informacji o obywatelach; wspomnę tu chociażby tylko o tych bardziej godziwych celach, jak zapewnienie źródeł podatkowych, pozyskiwanie rekruta, zapobieganie spiskom i przestępstwom czy ze względu na rozwój statystyki. Z czasem informacje o ludziach stały się też ważnym elementem wiedzy handlowej. Zatem nie tyle sam fakt zbierania informacji o jednostkach jest zjawiskiem nowym. W obecnym pokoleniu mogliśmy dojrzeć, jak zdobycze techniczne poszerzyły zdolność do gromadzenia i przetwarzania informacji na niespotykaną dotąd skalę. Początkowo umiejętność pozyskiwania tych informacji jeszcze nie była aż tak groźna, gdyż wzrostowi ilości informacji nie towarzyszyły zwiększone możliwości ich przetwarzania – ale ten czas już bezpowrotnie minął. Dzisiaj nie tylko państwa mają dostęp do technologii, która pozwala na łączenie wielkich baz danych, tworzenie konglomeratów baz danych (megakartoteki), personalizowanie złożonych informacji i profilowanie ich w odniesieniu do konkretnych osób. Wreszcie wydaje się, że jesteśmy w przededniu realności odgrywania istotnej roli przez sztuczną inteligencję, co do tej pory wydawało się domeną tworów z dziedziny fantastyki naukowej. Teraz już samodzielnie, bez jednostkowej interwencji człowieka, sztuczna inteligencja będzie zdolna nie tylko do automatycznego przetwarzania danych, ale i „kreowania" wytworów. Wraz z nowymi możliwościami technologicznymi pojawiły się też nowe zagrożenia, dotyczące zarówno bezpieczeństwa publicznego, jak i naruszania praw człowieka, w tym dyskryminacji, płynące z uwarunkowań technologicznych, a także wytworów sztucznej inteligencji. Nowe możliwości komunikacyjne coraz częściej stanowią narzędzia wykorzystywane przez osoby fizyczne, państwa oraz podmioty niepaństwowe do wpływania poprzez cyberoperacje na życie demokratycznych wspólnot; są wykorzystywane do cyberszpiegostwa czy cyberprzestępczości itp.

Nowe technologie przekroczyły granice możliwości ingerencji człowieka w sfery uchodzące do tej pory za pewne tabu cywilizacyjne. W sferze medycznej dość wspomnieć o kwestii pewności macierzyństwa w perspektywie sztucznego zapłodnienia czy praktyk surogacji, wymagania zgody na eksperyment medyczny na poziomie badań na zarodkach itd. Cyberrzeczywistość przekształciła także nasze postrzeganie „zastanych" pojęć, na przykład rozumienie miejsca dokonania czynności, szczególnie

gdy wykorzystujemy maszyny cyfrowe (czy jest to miejsce położenia użytkownika, jednostki centralnej, serwera, odbiorcy), a co za tym idzie – ustalenia wiążącego reżimu prawnego, dostępności, ochrony i bezpieczeństwa przechowywania w chmurze cyfrowej danych, w tym wyników badań medycznych; czy nawet takiej sprawy, jak ocena zdolności zrozumienia zagrożeń i ryzyka, co pozostaje nie bez znaczenia dla oceny wyrażenia zgody na zabieg medyczny. Pozostaje pytanie o faktyczne rozpoznanie tego, w jaki sposób i gdzie pozyskiwana jest wiedza na temat nas samych oraz kto ma dostateczne zasoby, by z tego korzystać. Czy aby nie stajemy się coraz bardziej uzależnieni od wiedzy specjalistów informatyków? Musimy zdawać sobie sprawę, że przetwarzanie wielkich danych uzależnione jest od wysublimowanej wiedzy technicznej, nad którą coraz trudniej będzie nam zapanować – nie tylko nam jako poszczególnym jednostkom, ale także jako społeczności. Wiadomo, kto sprawuje oficjalne władztwo publiczne. Jednakże poszukiwanie odpowiedzi na pytanie, kto jest jednak w stanie, ze względu na posiadane zasoby – wiedzę, umiejętności oraz możliwości techniczne – mieć do tych informacji faktyczny dostęp, prowadzić może niekiedy do nieoczekiwanych ustaleń.

8. Niewątpliwie wykonywanie pozytywnego obowiązku realizacji prawa do ochrony zdrowia przez władze publiczne wymaga dostępu, przetwarzania i przechowywania danych osobowych o szczególnej wrażliwości. Prawodawca unijny z jednej strony musiał uwzględnić ten kontekst; z drugiej starał się zapobiec temu, aby potrzeba ochrony zdrowia nie spowodowała zbyt szerokiego wyłomu w ogólnej ochronie prywatności i wykorzystywania danych osobowych do celów handlowych przez administratorów czy operatorów komunikacji elektronicznej. Prawodawca wyraźnie zauważa, że dziedzina zdrowia może stać się „otwartą bramą" dla gromadzenia ogromnych ilości danych osobowych. Problem ten wymaga zatem zwrócenia szczególnej uwagi przez prawodawcę krajowego, również w kontekście ochrony danych o stanie zdrowia w łączności elektronicznej. Ich ujawnienie może bowiem powodować istotną szkodę[11].

11 Zob. np. uwagi 1.3.7 i 5.1.2 Opinii Europejskiego Komitetu Ekonomiczno-Społecznego „Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylającego dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej)" z 5 VII 2017 r., Dz.U. UE C 345/23 z 2017 r.

Rozporządzenie 2016/679 zawiera kilka specyficznych rozwiązań odnośnie do ochrony danych osobowych dotyczących zdrowia. Nie wszystkie stanowią nowość regulacyjną w perspektywie dotychczasowych rozwiązań.

Już w ramach określenia definicji rozporządzenie przynosi trzy kategorie, które dotyczą bezpośrednio sfery zdrowia człowieka: dane dotyczące zdrowia, dane genetyczne i dane biometryczne (art. 4 pkt 13–15). Wszystkie zaliczone są do kategorii danych o szczególnym reżimie prawnym ich przetwarzania (art. 9). W motywach do rozporządzenia wyraźnie wskazano, że do danych dotyczących zdrowia należy zaliczyć wszystkie informacje o przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego zdrowia osoby, której dane dotyczą. Do danych takich należą informacje o danej osobie fizycznej zbierane podczas jej rejestracji do usług opieki zdrowotnej lub podczas ich świadczenia; numer, symbol lub oznaczenie przypisane danej osobie fizycznej w celu jednoznacznego zidentyfikowania tej osoby do celów zdrowotnych; informacje pochodzące z badań – laboratoryjnych lub lekarskich – części ciała, płynów ustrojowych, danych genetycznych i próbek biologicznych; oraz wszelkie informacje na przykład o chorobie, niepełnosprawności, ryzyku choroby, historii medycznej, leczeniu klinicznym, stanie fizjologicznym lub biomedycznym tej osoby, niezależnie od ich źródła, którym może być na przykład lekarz lub inny pracownik służby zdrowia, szpital, urządzenie medyczne lub badanie diagnostyczne *in vitro* (motyw 35).

Jednocześnie prawodawca unijny wprost przewiduje możliwość odstępstwa w prawie krajowym od zakazu przetwarzania szczególnych kategorii danych osobowych do celów monitorowania i ostrzegania zdrowotnego, zapobiegania chorobom zakaźnym i innym poważnym zagrożeniom zdrowotnym. Taki wyjątek może być przewidziany ze względu na cele zdrowotne, w tym związane ze zdrowiem publicznym oraz zarządzaniem usługami opieki zdrowotnej, w szczególności zapewnianiem jakości i ekonomiczności procedur stosowanych do rozstrzygania roszczeń w sprawie świadczeń i usług w ramach systemu ubezpieczeń zdrowotnych lub ze względu na prowadzone w interesie publicznym cele archiwalne, badań naukowych, historyczne lub statystyczne (motyw 52).

Rozporządzenie podkreśla znaczenie zasady proporcjonalności w przypadku określenia warunków odstępstwa od ogólnego zakazu

przetwarzania danych o stanie zdrowia osób. Szczególne kategorie danych osobowych zasługujące na większą ochronę powinny być przetwarzane do celów zdrowotnych wyłącznie w przypadkach, gdy jest to niezbędne do zarządzania systemem opieki zdrowotnej lub zabezpieczenia społecznego, w tym przetwarzania takich danych przez organy władzy publicznej do celów zarządzania, kontroli jakości oraz nadzoru nad systemem opieki zdrowotnej i zabezpieczenia społecznego, zapewniania ciągłości świadczenia takich usług, opieki zdrowotnej poza terytorium państwa członkowskiego, bezpieczeństwa, monitorowania i ostrzegania zdrowotnego, celów archiwalnych, badań naukowych, historycznych, statystycznych lub analiz prowadzonych w interesie publicznym w dziedzinie zdrowia publicznego. Państwa członkowskie mogą przewidzieć dalej idące ograniczenia w przetwarzaniu danych genetycznych, biometrycznych lub dotyczących zdrowia, z zachowaniem jednak swobodnego przepływu danych osobowych w ramach Unii (motyw 53).

Dopuszczono także, z uwagi na interes publiczny w dziedzinie zdrowia publicznego, przetwarzanie szczególnych kategorii danych osobowych nawet bez zgody osoby, której dane dotyczą. Przetwarzanie danych dotyczących zdrowia przez takie podmioty jak pracodawcy, zakłady ubezpieczeń lub banki nie powinno jednak skutkować w późniejszym czasie przetwarzaniem tych danych do innych celów (motyw 54). W rozporządzeniu podkreślono prawo każdego do dostępu do własnych danych, żądania ich sprostowania oraz żądania „bycia zapomnianym". Dotyczyć to ma danych o zdrowiu zawartych w dokumentacji medycznej zawierającej takie informacje jak diagnoza, wyniki badań, oceny dokonywane przez lekarzy prowadzących, stosowane terapie czy przeprowadzone zabiegi (motyw 63 i 64). Niemniej dalsze zatrzymywanie danych osobowych powinno być uznane za zgodne z prawem, jeżeli jest niezbędne do korzystania z wolności wypowiedzi i informacji, a także między innymi z uwagi na interes publiczny w dziedzinie zdrowia publicznego (motyw 65). Ograniczenie w przepisach krajowych prawa dostępu do własnych danych, ich sprostowania lub usunięcia dopuszczalne jest jednak ze względu na szereg doniosłych celów publicznych, w tym między innymi zapobieganie naruszeniom zasad etyki w zawodach regulowanych lub prowadzenie rejestrów publicznych w dziedzinie pomocy socjalnej i ochrony zdrowia publicznego (motyw 73).

Prawodawca unijny zdaje sobie sprawę, że ma do czynienia z różnym stopniem ryzyka zagrożeń i prawdopodobieństwem ich wystąpienia. Szczególnie zwraca uwagę na ryzyko związane z przetwarzaniem danych genetycznych, danych dotyczących stanu zdrowia lub seksualności (motyw 75). Administrator jest zobowiązany do takiego zabezpieczenia danych osobowych, aby zapobiec dyskryminacji osób fizycznych z uwagi między innymi na stan genetyczny lub zdrowotny (motyw 71).

Nowe rozporządzenie znosi ogólny obowiązek zawiadamiania organów nadzorczych o przetwarzaniu danych osobowych przez administratorów. Koncentruje się natomiast na tych rodzajach operacji przetwarzania danych, które ze względu na swój charakter, zakres, kontekst i cele mogą powodować wysokie ryzyko naruszenia wolności lub praw (motyw 89). W takim przypadku administrator powinien ocenić konkretne prawdopodobieństwo i realność tego wysokiego ryzyka (motyw 90). Za wysokie ryzyko rozporządzenie nakazuje uznać w szczególności operacje przetwarzania danych osobowych o dużej skali. Jednocześnie zastrzega, że za przetwarzanie danych osobowych na dużą skalę nie powinno być uznawane przetwarzanie danych osobowych pacjentów dokonywane przez pojedynczego lekarza, innego pracownika służby zdrowia lub prawnika. Wówczas dokonywanie oceny indywidualnych skutków dla ochrony danych nie powinno być obowiązkowe (motyw 91). Prawodawca unijny przewiduje też okoliczności wyjątkowo dopuszczające przekazywanie danych niezbędnych z uwagi na ważne względy interesu publicznego. Chodzi na przykład o międzynarodową wymianę danych między służbami odpowiedzialnymi za sprawy zabezpieczenia społecznego lub za zdrowie publiczne, zwalczanie chorób zakaźnych lub eliminowanie dopingu w sporcie (motyw 112).

Rozporządzenie ma zastosowanie także do przetwarzania danych osobowych do celów badań naukowych, obejmujących także badania nad zdrowiem publicznym (motyw 159).

9. Świadomość prawna to nie to samo co kultura prawna – chociaż ta pierwsza jest elementem koniecznym dla zbudowania wysokiej kultury prawnej. Sama świadomość istnienia mechanizmów prawnych nie ma takiej mocy sprawczej, aby dzięki niej mechanizmy prawne były wykorzystywane w sposób właściwy – a zatem zgodnie z tym, do czego

zostały przewidziane, służąc ochronie niezbywalnej i przyrodzonej godności każdego człowieka.

Porządek społeczny wspierany czy kreowany przez działanie prawodawcy powinien być godziwy. Jest bowiem ustanowiony dla i ze względu na każdego człowieka. Demokratyczne państwo prawa to nie idea wszechwładnego, a zatem i z natury rzeczy odhumanizowanego normatywizmu. Nie należy go też sprowadzać do tępego legalizmu, polegającego na scholastycznym aplikowaniu reguł, w oderwaniu od założenia, które legło u podstaw nadania im wiążącego charakteru. System obowiązujących norm musi też wyrażać odpowiednie wartości, aby mógł być uznany za demokratyczny. W tym ostatnim słowie nie chodzi bowiem tylko, czy nawet przede wszystkim, o kwestię rozstrzygania spraw publicznych w głosowaniu, według woli wszechwładnej większości. Demokratyczność ma odnosić się do pewnej wizji ładu politycznego, czyli metod ubiegania się o władzę oraz sprawowania jej w imieniu całej wspólnoty. Wreszcie warto pamiętać, że przewidziana w naszym kręgu kulturowym idea demokratycznego państwa prawnego powiązana jest z ideą sprawiedliwości społecznej. Ta ostatnia domaga się, by system społeczny był wykreowany na miarę godności człowieka.

I w tym miejscu należy zasygnalizować problem związany ze zmianami w prawodawstwie unijnym. Ochrona prywatności, w tym wrażliwych danych o pacjencie, nie może być tak interpretowana i stosowana, szczególnie w systemie zabezpieczenia zdrowotnego, by skutki ochrony prywatności przeważyły nad uzasadnionymi interesami wynikającymi z prawa do ochrony życia i zdrowia pacjenta. A nie są to jedyne doniosłe wolności i prawa, które mogą przeważyć nad ochroną prywatności.

Przywołane przeze mnie rozporządzenie kilkakrotnie odwołuje się do kategorii „żywotnych interesów osoby, której dane dotyczą" lub analogicznych (na przykład art. 6 ust. 1 lit. d; art. 9 ust. 2 lit. c; art. 23 ust. 1 lit. i). Rolą prawodawcy krajowego, organów nadzoru przestrzegania przepisów o ochronie danych osobowych, organów sądowych, a przede wszystkim osób stosujących te przepisy będzie ukształtowanie właściwej praktyki, by ochrona danych osobowych pacjenta nie skutkowała takim ich rozumieniem, które będzie szkodziło samemu pacjentowi. Pacjent jest podmiotem wolności, jaką jest prywatność. Przepisów o ochronie

prywatności nie należy zatem przeciwstawiać jej podmiotowi. Chodzi mi tu o to, by nie dochodziło do dehumanizacji zarówno pacjenta, który stałby się tylko jednostką statystyczną wobec administracyjnej części systemu ochrony zdrowia, jak i personelu medycznego, w tym osób, do których odnosi się tajemnica zawodowa. Podobnie rzecz się ma jednak i z bardziej praktycznymi kwestiami, jak chociażby podawanie leków. Nakaz anonimizacji danych nie może rodzić niepotrzebnego ryzyka pomyłki, szczególnie w odniesieniu do pacjenta nieprzytomnego bądź osoby o ograniczonej zdolności poznawczej.

Zapewne można byłoby mnożyć przykłady zderzania się różnych wartości w ramach funkcjonowania ochrony zdrowia. Jestem przekonany, że jako społeczność musimy zachować odpowiednią proporcję między dobrami prawnie chronionymi, możliwościami technicznymi, efektem ochrony danych osobowych a możliwymi zagrożeniami itd. To wszystko ostatecznie będzie lepiej służyło nam jako osobom niż pójście drogą co prawda łatwiejszego w praktyce, ale jednak nieludzkiego normatywizmu, przed którym trzeba się bronić szczególnie w systemie ochrony zdrowia.

10. Nie jestem przekonany, czy współczesny, nawet dobrze wykształcony i świadomy człowiek w pełni zdaje sobie sprawę z konsekwencji i zasad funkcjonowania cyberrzeczywistości. Prywatność jest dobrem, które chcą pozyskać nie tylko władze publiczne, ale i podmioty prywatne. Charakter tych podmiotów niekiedy trudno jest faktycznie rozpoznać, szczególnie gdy państwo wyzbywa się swoich obowiązków, przenosząc je na podmioty formalnie należące do sfery prawa prywatnego. Współczesny człowiek musi jednak zadawać sobie pytanie, czy nie nazbyt łatwo decydujemy się niekiedy na płacenie własną prywatnością za niewspółmierne dobra zamienne. W odniesieniu do ochrony zdrowia prawo musi przyjść ze szczególną pomocą pacjentowi. Dotykamy bowiem wówczas informacji, które są szczególnie delikatne i ważne. Dotyczą najbardziej intymnych sfer życia prywatnego. Czy zdołamy tu uzyskać, jako wspólnota, konieczną harmonię – to zależy nie tylko od prawodawcy oraz organów państwa, w tym sądów, ale też w nie mniejszym zakresie od wszystkich tych, którzy będą stosowali w praktyce dnia codziennego rozwiązania normatywne odnoszące się do ochrony prywatności w sferze ochrony zdrowia.

Protecting the privacy of health information in the new European Union legislation

As a starting point, the author takes considerations regarding the nature of privacy as a legal category. He acknowledges that it is a human freedom requiring effective legal mechanisms protected by public authorities. At the same time, he points out threats that civilization changes and technological development bring for human privacy. The author confronts these considerations with the problems of collecting and processing data in the health care system. The author, however, concentrates on solutions adopted by the current EU legislator in a new comprehensive set of normative acts on protecting privacy. In this context, the author presents new trends and specific legal solutions regarding health protection. He also indicates the danger of absolutizing the protection of privacy, especially where the need to protect the life and health of the patient demands a primacy over general legal solutions regarding the protection of personal data.

Keywords: privacy, health care, human rights, European Union

Marek Zubik – prof. dr hab., Katedra Prawa Konstytucyjnego Uniwersytetu Warszawskiego

Bibliografia

Zubik M., *„Wolność" a „prawo" (pięć hipotez o stosowaniu pojęć konstytucyjnych dotyczących praw człowieka)*, „Państwo i Prawo" 2015, z. 9.