Uniwersytet Warszawski
Wydział Prawa i Administracji

Katarzyna Łakomiec

Prawo do ochrony prywatności

w kontekście informacji o stanie zdrowia

Autoreferat rozprawy doktorskiej, napisanej pod kierunkiem
prof. dr. hab. Marka Zubika

Warszawa 2018

1. Temat pracy i uzasadnienie jego wyboru

Kwestie ochrony prywatności i autonomii informacyjnej jednostki są przedmiotem zainteresowania polskiej nauki prawa. Należy przy tym zauważyć, że najwięcej opracowań na ten temat powstało w literaturze prawa administracyjnego i europejskiego. Jest to zjawisko łatwo wytłumaczalne, ponieważ wiąże się z jednoczesnym kształtowaniem się europejskiego i polskiego systemu ochrony danych osobowych oraz zobowiązaniem Polski do transpozycji unijnych przepisów w tym zakresie. Prywatność jako dobro osobiste była także przedmiotem analiz doktryny prawa cywilnego. Ochrona informacji o stanie zdrowia jest również tematem opracowań odnoszących się do prawa medycznego. Kwestie zachowania poufności przy wykonywaniu zawodów medycznych należą do szeroko komentowanych zagadnień z zakresu bioetyki. Prace dotyczące prawa do ochrony prywatności i autonomii informacyjnej jednostki analizowanych z perspektywy dogmatyki prawa konstytucyjnego nie należą do rzadkości, jednak w mojej ocenie brakuje kompleksowego opracowania dotyczącego konstytucyjnej ochrony danych o stanie zdrowia.

Wielopoziomowość ochrony prawnej prywatności i autonomii informacyjnej jednostki wpływa na to, że w opracowaniach dotyczących tych tematów przenikają różne dogmatyki prawa. W efekcie, pogłębiona refleksja konstytucyjna jest zastępowana uzupełnianiem wywodów instytucjami prawa europejskiego. Problematyka ochrony prywatności jest powszechna i dotyczy podmiotów znajdujących się w różnych sytuacjach prawnych. Przy tym wiele poziomów ochrony pozostaje współzależnych oraz jednocześnie hierarchicznie podporządkowanych Konstytucji. Niewątpliwie ochrona prywatności jest związana z wieloma zróżnicowanymi roszczeniami z zakresu prawa publicznego i prywatnego, a w konsekwencji analizowana jest z różnych perspektyw przy użyciu różnej siatki pojęciowej oraz koncepcji dogmatycznych. W doktrynie pojawiają się nawet głosy – pozostaje kwestią sporną czy zasadne – że prawo ochrony danych osobowych powinno zostać uznane za odrębną dziedzinę prawa.

Z powyższych zjawisk wynika również pewien nadmiar definicji, ponieważ w zarówno w doktrynie, jak i w orzecznictwie używa się co najmniej kilku określeń odnoszących się do prawnej ochrony prywatności. I tak mówi się o: prawie do prywatności, prywatności jako wolności, autonomii informacyjnej jednostki, prywatności informacyjnej oraz prawie

do tożsamości informacyjnej, a także prawie do ochrony danych osobowych. Najszerszym pojęciem jest oczywiście prawo do ochrony prywatności, które jest uregulowane w art. 47 Konstytucji i zgodnie z poglądami Trybunału Konstytucyjnego obejmuje ochroną wielopoziomową sieć dóbr osobistych. Z kolei autonomia informacyjna jest przez TK utożsamiana z regulacją art. 51 Konstytucji i rozumiana jako pozostawienie każdej osobie swobody w określeniu sfery dostępności dla innych wiedzy o sobie. Należy przy tym zaznaczyć, że wbrew literalnemu brzmieniu, w tak rozumianej autonomii nie zawiera się jedynie aspekt kontroli nad danymi, ale również ograniczenia dostępu do danych. Prywatność informacyjna jest z kolei identyfikowana jako aspekty dotyczące informacji z art. 47, a także art. 51 Konstytucji. Tożsamość informacyjna dotyczy kontroli nad informacjami istotnymi dla odrębności osoby. Zaś prawo ochrony danych osobowych wywodzi się z prawa Unii Europejskiej.

Celem mojej rozprawy była analiza kształtu regulacji konstytucyjnej ochrony prywatności i odniesienie jej do kontekstu przetwarzania informacji o stanie zdrowia, co znajduje wyraz w wybranym przeze mnie tytule pracy. „Prawo do ochrony prywatności" odnosi się do norm konstytucyjnych, natomiast „kontekst informacji o stanie zdrowia" przesądza o zawężeniu tematu pracy do kwestii przetwarzania danych osobowych w kontekstach związanych z medycyną.

Wybór takiego tematu jest zasadny również dlatego, że obecnie kształt ochrony prywatności ulega przemianom na skutek dynamicznego rozwoju nowych technologii. Ponownie analizowane są zarówno założenia systemów ochrony prywatności, jak i skuteczność poszczególnych rozwiązań przyjętych przez ustawodawcę. Inicjatorem tych zmian jest między innymi Unia Europejska, która w ostatnich latach dokonała reformy swojego systemu ochrony danych osobowych. Zasadniczej ewolucji podlega również prawo medyczne, a w szczególności wykorzystanie informacji o stanie zdrowia. System prawa medycznego opiera się na chronionych konstytucyjnie wartościach takich jak godność, zdrowie czy życie, co również było istotne z perspektywy wyboru tematu.

Wspomniane wyżej przemiany inspirują do ponownej analizy konstytucyjnych standardów dotyczących ochrony prywatności i autonomii informacyjnej jednostki i oceny, czy są one aktualne i efektywnie chronią wartość, jaką jest prywatność. Szczególnie wobec najnowszego orzecznictwa Trybunału Konstytucyjnego związanego z ochroną danych o stanie zdrowia podjęcie tego tematu wydaje się uzasadnione.

2. Wpływ nowych technologii na prawną ochronę prywatności

Analiza literatury przedmiotu wskazuje, że znalezienie jednolitej definicji prywatności jest bardzo trudne. Początkowo prywatność była postrzegana jako prawo do bycia pozostawionym w spokoju. Ewolucja poglądów dotyczących prywatności doprowadziła do sformułowania różnych teorii, wśród których wiodące znaczenie mają teorie dostępu oraz kontroli. Pierwsza z nich odnosi się do prywatności jako sytuacji, w której podmioty są pozbawione: możliwości zapoznania się z informacjami o jednostce, śledzenia działań jednostki czy też wkroczenia w sferę jej fizyczności. Teorie kontroli odnoszą się do prywatności jako stanu, w którym jednostka może samodzielnie określać, kiedy, jak i w jakim stopniu informacja na ich temat jest udostępniana innym. Obie teorie, występujące często w różnych wariantach, spotkały się z krytyką.

Współcześnie proponowane jest spojrzenie na prywatność, które zakłada, że kontrola przez jednostkę informacji jej dotyczących jest istotnym aspektem prywatności. Jest nim również wymiar dostępu do tych informacji, jaki posiadają inne osoby, niezależnie od tego, kto sprawuje nad nią kontrolę. We współczesnych teoriach odchodzi się od poszukiwania jednolitego pojęcia prywatności, skupiając się raczej na wyodrębnieniu różnych jej form oraz kontekstów, w których prywatność jest zagrożona i analizie powiązań między tymi formami oraz kontekstami.

Prawo do ochrony prywatności, w zależności od przyjętych założeń, chroni różne interesy jednostki, takie jak jej indywidualny rozwój, integralność cielesna, życie rodzinne, seksualne oraz wybory reprodukcyjne czy niezakłócone korzystanie przez nią z przysługujących jej wolności i praw.

Analiza okoliczności w których konieczna jest ochrona prywatności, nabrała znaczenia w związku z dynamicznym rozwojem nowych technologii informacyjnych, który wpływa na zacieranie się podziału między sferą prywatną a sferą publiczną. Informacje o stanie zdrowia, których przetwarzanie odbywało się głównie w podmiotach leczniczych, są obecnie przetwarzane w coraz to nowszych okolicznościach.

Odnosząc się do rozwoju nowych technologii informacyjnych, zwraca się uwagę przede wszystkim na demokratyzację dostępu do narzędzi umożliwiających przetwarzanie danych. Sprzęt i oprogramowanie konieczne do prowadzenia operacji na danych na dużą skalę

posiadają obecnie nie tylko podmioty państwowe i duże przedsiębiorstwa, ale praktycznie każdy zainteresowany podmiot. Nie zawsze jednak tworzone są właściwe uregulowania co do możliwości wykorzystywania tych zasobów. Co więcej, na rynku dostępne jest coraz więcej przystępnych narzędzi informatycznych, pozwalających na przetwarzanie danych. Oznacza to, że dane dotyczące jednostki mogą być zbierane i przechowywane przez różne podmioty, również te nieposiadające wyspecjalizowanej wiedzy, przez nieokreśloną ilość czasu i łatwo przesyłane. Rozwój Internetu pozwala na natychmiastowe przesyłanie dużej ilości danych, ale także umożliwia dostęp dowolnego podmiotu do zbiorów danych z każdego miejsca i o każdej porze, dzięki rozwiązaniom opartym na chmurze obliczeniowej.

Demokratyzacja dostępu do technologii informacyjnych pozwalających na gromadzenie danych idzie w parze z rozwojem technik analizy danych. Po pierwsze, dane są agregowane na niespotykaną dotąd skalę, głównie poprzez łączenie baz danych uprzednio służących różnym celom. Agregacja może się przy tym odbywać zarówno w ramach baz danych stanowiących kompletne i zorganizowane zbiory, jak i może być dokonywana w ramach różnych sieci przy użyciu narzędzi wyszukiwania i pozyskiwania danych. Nowe sposoby agregacji i analizy danych są obecnie powiązywane z określeniem *big data*. Analiza *big data* jest wykorzystywana do odkrywania generalnych trendów i powiązań, ale może też być używana w celu wywierania bezpośredniego wpływu na jednostkę. Dane te mogą pochodzić z różnych źródeł, są zebrane, cyfrowo utrwalone i sformatowane w sposób pozwalający na ich analizę. Dane w tych zbiorach są analizowane przy użyciu algorytmów. Źródłem fenomenu *big data* jest wzrastająca dostępność narzędzi automatycznego przetwarzania informacji.

W literaturze zwraca się uwagę, że wpływ nowych technologii informacyjnych, w tym *big data*, na medycynę polega na popularyzowaniu długoterminowego przechowywania, agregacji i dzielenia przez różne podmioty wrażliwych danych dotyczących zdrowia jednostki. Raz zebrane dane mogą być wykorzystywane i łączone z innymi danymi w ramach nieograniczonej liczby projektów badawczych. Może to oznaczać odejście od związania pierwotnym celem pozyskania danych, wprowadzając zasadnicze zmiany paradygmatu w odniesieniu do mechanizmu ochrony danych o stanie zdrowia. Wiąże się to z odejściem od ochrony danych w konkretnym zbiorze, a wymusza wprowadzenie instrumentów ochrony adekwatnych w sytuacji stałego przepływu danych osobowych.

Do zmiany zasad przetwarzania danych doprowadziło również umożliwienie profilowania jednostki. W procesie profilowania bowiem, na podstawie analizy matematycznej, uzyskuje się nowe informacje o jednostce, co poszerza zakres wkroczenia w sferę autonomii informacyjnej. Profilowanie umożliwia klasyfikację jednostki. Klasyfikacja ta może mieć przełożenie na status jednostki i możliwość korzystania przez nią z jej wolności i praw. Identyfikacja, klasyfikacja i monitorowanie umożliwiają koordynację działań zarówno organów państwa, jak i prywatnych podmiotów w skali lokalnej, jak i globalnej. Procesy te wpisują się w opisywane w literaturze zjawisko „płynnej inwigilacji".

3. Cel i zakres rozprawy

Celem rozprawy jest analiza konstytucyjnych przepisów chroniących wartości, takie jak prywatność i autonomia informacyjna jednostki. Badania zostały skoncentrowane na ocenie standardu ochrony informacji o stanie zdrowia jednostki. Analiza prowadzona z uwzględnieniem przemian związanych z dynamicznym rozwojem technologii informacyjnych i powszechnym ich zastosowaniem w codziennej działalności podmiotów przetwarzających dane. Rozprawa ma odpowiedzieć na pytanie czy konstytucyjny zakres normowania dotyczący ochrony prywatności, jest adekwatny wobec zmiany obiegu informacji o jednostkach w społeczeństwie.

Przyjmując, że Konstytucja ma charakter spójny, kompleksowy oraz wyczerpujący materię normowania należało ocenić, jaka wykładnia norm konstytucyjnych jest adekwatna wobec wyzwań związanych z rozwojem nowych technologii. W mojej ocenie powszechność, złożoność i płynność procesów przetwarzania informacji o jednostce we współczesnym społeczeństwie będzie miała z pewnością przełożenie na sposób w jaki ustawodawca dokonuje oceny proporcjonalności wprowadzanych przez siebie ograniczeń ochrony prywatności informacyjnej i w jaki sposób sąd konstytucyjny bada prawidłowość tego procesu oraz jego rezultaty oceniając konstytucyjność regulacji. Jest to spójne z przyjmowanym w doktrynie i orzecznictwie założeniem uznania centralnego znaczenia zasady proporcjonalności w odniesieniu do poszczególnych typów wolności i praw. Celem mojej rozprawy było ukazanie treści konstytucyjnych norm dotyczących ochrony

prywatności jednostki w odniesieniu do stanu jej zdrowia i ewolucji ich wykładni pod wpływem zmian kontekstu przetwarzania danych.

Konieczność zachowania poufności w stosunku do wrażliwych danych o stanie zdrowia jednostki, nie dotyczy obecnie – jak to było kiedyś – jedynie lekarzy, ale także coraz szerszego kręgu osób wykonujących zawody medyczne oraz personelu pomocniczego. Dane o stanie zdrowia są przetwarzane w systemach informatycznych, które często łączą więcej niż jedną placówkę. Mogą być one przetwarzane również w sieciach, które łączą ośrodki badawcze lub szpitale znajdujące się w różnych państwach. Stąd też nastąpiło zwiększenie zagrożenia poufności danych o stanie zdrowia, a ich potencjalne nieautoryzowane ujawnienie może mieć głębokie konsekwencje. Dostęp do informacji o stanie zdrowia, dla podmiotów prowadzących działalność bankową lub ubezpieczeniową, jest pożądany w celu zastosowania systemów optymalizacji oceny ryzyka. Jednocześnie zbyt szerokie udostępnianie tego rodzaju wrażliwych informacji może doprowadzić np. do dyskryminacji w dostępie do usług.

Należy jednak zauważyć, że przetwarzanie danych o stanie zdrowia jest istotnym elementem badań naukowych prowadzonych przez wyspecjalizowane jednostki jakimi są biobanki populacyjne (naukowe). W biobankach takich – poza materiałem biologicznym – zbierane i przetwarzane są różne rodzaje danych dotyczących jednostki, w tym dane o stanie zdrowia, oraz dane genetyczne (stanowiące główny przedmiot biobankowania) oraz dodatkowo inne dane relewantne z perspektywy działalności biobanków (np. dane o uzależnieniach, warunkach środowiskowych, wieku), a także dane identyfikujące jednostkę. Funkcjonowanie biobanków naukowych jest istotne z perspektywy rozwoju medycyny i biotechnologii. Możliwość sięgania po dane genetyczne połączone z innymi relewantnymi informacjami ma poszerzyć możliwości badawcze i w konsekwencji wiedzę, m.in. o przyczynach chorób populacyjnych oraz pozwolić na znalezienie nowych i rozwijanie obecnych terapii stosowanych w opiece medycznej. Biorąc pod uwagę powyższe, należy stwierdzić, że przetwarzanie informacji o jednostkach będzie miało pozytywny wpływ zarówno na zdrowie publiczne, jak i zdrowie jednostek.

3.1. Tezy rozprawy

Najważniejsza teza mojej pracy odnosi się bezpośrednio do dopuszczalnych konstytucyjnie ograniczeń w korzystaniu z wolności i praw. W mojej ocenie przy dokonywaniu oceny niezbędności i proporcjonalności *sensu stricto* ograniczeń prywatności informacyjnej konieczna jest analiza kontekstu przetwarzania informacji. Jest ona warunkiem prawidłowości wykładni w odniesieniu do prawa do prywatności informacyjnej. Badanie kontekstu ma przy tym na celu określenie zakresu ingerencji przyjętego przez ustawodawcę rozwiązania w prywatność informacyjną oraz stopnia dolegliwości takiego rozwiązania dla jednostki. W pracy przyjmuję, że kontekstem będzie zespół okoliczności mający przełożenie na ocenę specyfiki, w tym głębokości wpływu na prywatność informacyjną jednostki procesu przetwarzania danych. Przetwarzanie danych jest tu traktowane jako ograniczenie prawa do ochrony prywatności informacyjnej jednostki. Badanie kontekstu, konieczne dla zrozumienia wpływu na prywatność informacyjną, jest niezbędne dla oceny dopuszczalnych ograniczeń tego prawa. Ocena kontekstu w aspekcie prawnym będzie opierała się na analizie norm konstytucyjnych, ustawowych, podustawowych, a także zawartych w instrumentach prawa międzynarodowego, oraz będzie wymagała zastosowania reguł interpretacyjnych i inferencyjnych pozwalających na dokonanie wykładni tych norm. Subsydiarnie, analiza kontekstu w aspekcie faktycznym będzie się odnosiła do pozaprawnych okoliczności i warunków przetwarzania danych.

Do elementów analizy kontekstu będzie należała ocena m.in.: podmiotów przetwarzających dane, charakteru przetwarzanych danych, struktury ich przetwarzania, technologii, jakie będą stosowane do przetwarzania danych, okresu przetwarzania danych i mechanizmów usuwania danych po spełnieniu przez nie celu, dla którego zostały zebrane. Badanie kontekstu musi uwzględniać także analizę prawnych i pozaprawnych możliwości niwelowania wpływu wprowadzanych ograniczeń na prywatność informacyjną jednostki. Przetwarzanie danych podlega zmianom pod wpływem ewolucji rozwiązań technologicznych. W moim przekonaniu, oceniając kontekst przetwarzania informacji o jednostce, należy zwrócić uwagę na to, że skutki przetwarzania można zaobserwować zarówno w odniesieniu do sytuacji jednostki (skutki mikro), jak i w odniesieniu do

procesów społecznych (skutki makro). Oba rodzaje skutków są istotne z punktu widzenia analizy dopuszczalności ograniczeń prawa do prywatności jednostki.

Należy wskazać, że ważnym zjawiskiem, które doprowadziło do zmiany paradygmatu w odniesieniu do ochrony danych osobowych, jest odejście od systemów ochrony opartych w przeważającej mierze na koncepcji autonomii jednostki na rzecz tworzenia systemu ochrony o silnych gwarancjach odnoszących się do przetwarzania danych. Zjawisko to jest powiązane ze wspomnianą przeze mnie masowością obecnie występujących procesów przetwarzania danych oraz rozwojem narzędzi ich agregacji i analizy. Istotnym aspektem jest również demokratyzacja dostępu do technologii przetwarzania danych. Wobec powyższych procesów, proste rozwiązania oparte na wykluczeniu dostępu do danych lub przyznaniu jednostce autonomii w podejmowaniu decyzji co do przetwarzania jej danych nie są już wystarczające. Coraz więcej procesów zachodzących w społeczeństwie oparte jest bowiem na przetwarzaniu danych, co nie łączy się z zainteresowaniem jednostek warunkami przetwarzania tych danych.

Stawiam w mojej rozprawie tezę, że ustrojodawca wprowadza konstytucyjny nakaz zaprojektowania przez państwo normatywnego systemu regulującego na poziomie ustawowym obieg informacji o jednostce. W ramach tej architektury ustawodawca musi zapewnić realizację autonomii informacyjnej jednostki.

3.2. Metodologia

Rozprawa ma charakter studium z polskiego prawa konstytucyjnego. Badania były prowadzone metodą prawno-dogmatyczną.

W rozprawie nie zostały natomiast uwzględnione rozważania o charakterze prawnoporównawczym. Komparatystyka konstytucyjna stanowi odrębną dziedzinę badań w zakresie nauki prawa konstytucyjnego, posiadającą odrębną metodologię i przedmiot. Rozprawa przygotowana tą metodą prowadzenia badań musiałaby mieć zatem odmienny przedmiot. Podobnie praca nie zawiera wyczerpującej analizy orzecznictwa międzynarodowego. W zakresie opisywanym przeze mnie istotne są elementy analizy prawa międzynarodowego i ponadnarodowego, które umożliwiają kompleksową analizę zasad ochrony prywatności w Polsce. W rozprawie nie rozważam również w sposób

wyczerpujący problematyki prokonstytucyjnej wykładni ustaw oraz problematyki oceny ich zgodności z konstytucją.

4. Struktura pracy

Rozprawa jest podzielona na pięć rozdziałów. W pierwszym rozdziale przedstawione zostały różne definicje prywatności oraz różne koncepcje jej ochrony. Opisane teorie prywatności można podzielić na klasyczne (do których należą między innymi teorie dostępu i kontroli) oraz współczesne (teoria powiązań i teoria kontekstów). W rozdziale wykazano, jak na ewolucję teorii prywatności wpłynął rozwój nowoczesnych technologii informacyjnych (w tym demokratyzacja dostępu do technologii umożliwiających przetwarzanie danych, zwiększenie mobilności i możliwości agregacji danych). Zasygnalizowane zostały również takie zjawiska jak: *big data*, zasada ostrożności oraz płynna inwigilacja i ich wpływ na prywatność. W ostatniej części rozdziału przedstawione zostały relacje medycyny, bioetyki oraz praw człowieka.

Rozdział drugi odnosi się do ochrony prywatności informacyjnej w polskim prawie konstytucyjnym. Rozważania opierają się na analizie norm konstytucyjnych oraz poglądów doktryny. Analiza dotyczy prawa do ochrony prywatności jako zasady prawa, publicznego prawa podmiotowego oraz prywatności jako wartości. Szczególna uwaga została poświęcona dopuszczalnym konstytucyjnie ograniczeniom prawa do ochrony prywatności i autonomii informacyjnej jednostki. Co istotne, zaproponowane zostało zastosowanie teorii kontekstów w ocenie proporcjonalności ograniczeń. Badanie kontekstu ma przyczynić się do określenia zakresu ingerencji przyjętego przez ustawodawcę rozwiązania w prywatność informacyjną oraz stopnia dolegliwości takiego rozwiązania dla jednostki. Taka ocena dotyczy m.in. podmiotów, które przetwarzają dane, charakteru przetwarzanych danych, struktury ich przetwarzania, a także podstawy prawnej oraz gwarancji proceduralnych i technicznych przetwarzania danych.

Jeśli chodzi o rozdział trzeci, to odnosi się on do rozwiązań, jakie polski ustawodawca przyjął dokonując operacjonalizacji norm konstytucyjnych. Analiza tych rozwiązań jest prowadzona z perspektywy opisanych w rozdziale drugim kryteriów przyjętych w odniesieniu do testu proporcjonalności ograniczeń. Rozdział zawiera więc charakterystykę kontekstów, w jakich są przetwarzane dane osobowe w ujęciu przyjętym przez

ustawodawcę. W rozdziale przedstawione zostały ogólne zasady przetwarzania danych osobowych przyjęte w polskim ustawodawstwie przed 2018 r. oraz szczegółowe konteksty przetwarzania danych o stanie zdrowia. Scharakteryzowane zostały rodzaje danych o stanie zdrowia z uwzględnieniem informacji genetycznej. Zaprezentowana zostały zasady funkcjonowania rejestrów danych o stanie zdrowia. Odniesiono się również do podmiotów przetwarzających dane o stanie zdrowia, przy czym szczególna uwaga została poświęcona instytucji tajemnicy lekarskiej. Scharakteryzowane zostały również podstawy normatywne przetwarzania danych o stanie zdrowia. Wreszcie, ostatnie części rozdziału zostały poświęcone odpowiednio gwarancjom proceduralnym i technicznym przetwarzania danych. Zostały tu również uwzględnione rozwiązania europejskie, które zastąpiły zasady ogólne przetwarzania danych funkcjonujące do 2018 r. w polskim ustawodawstwie.

Celem czwartego rozdziału było wzbogacenie rozważań ujętych w poprzednich rozdziałach o analizę orzecznictwa Trybunału Konstytucyjnego, odnoszącego się do ochrony prywatności i autonomii informacyjnej jednostki. W rozdziale zostało przedstawione, jak opisane w rozdziale pierwszym teorie dostępu i kontroli, a także nowoczesne teorie prywatności są stosowane przez sąd konstytucyjny. Wskazano, jak TK dokonuje oceny dopuszczalności ograniczeń w korzystaniu z prawa do ochrony prywatności oraz autonomii informacyjnej jednostki.

W piątym rozdziale została przedstawiona niezwykle istotna z perspektywy polskiego systemu, ewolucja regulacji europejskich. Rozdział rozpoczyna się od analizy miejsca prawa międzynarodowego i ponadnarodowego w konstytucyjnym systemie źródeł prawa. Następnie analizowany jest system ochrony danych osobowych w Unii Europejskiej ze szczególnym uwzględnieniem zmian wynikające z unijnej reformy ochrony danych osobowych. W rozdziale zostały poruszone zagadnienia związane z wprowadzeniem na unijnym poziomie zasad ochrony danych w rozporządzeniu i konsekwencjami dla konstytucyjnego standardu ochrony prywatności. Po pierwsze jest to relacja między deficytem demokracji w Unii Europejskiej, a konstytucyjnym wymogiem ustanawiania ograniczeń prawa do ochrony prywatności i autonomii informacyjnej w formie ustawy, co ma zapewnić jawny i deliberatywny charakter tworzenia norm ingerujących w sferę prywatności jednostki. Po drugie, wpływ marginalizacji ustawy w systemie ochrony danych osobowych na architekturę tego systemu. Po trzecie, standard poprawnej legislacji w Konstytucji i orzecznictwie TK, a przepisy rozporządzenia. Po czwarte, problem zgodności

materialnej, między konstytucyjnym standardem ochrony prywatności i autonomii informacyjnej jednostki, a przepisami RODO, w tym dopuszczalność wyznaczonego przez UE celu RODO, czyli swobodnego przepływu danych osobowych w Unii jako przesłanki ograniczeń konstytucyjnych praw i wolności. Po piąte, problem badania zgodności RODO z Konstytucją. Rozdział zamyka charakterystyka przetwarzania danych o stanie zdrowia na podstawie RODO.

5. Podstawowe ustalenia

5.1. Charakter normatywny prawa do ochrony prywatności

Regulację prawa do ochrony prywatności i autonomii informacyjnej jednostki wprowadza Konstytucja z 1997 r. Jednak już wcześniej Trybunał Konstytucyjny uznał ochronę prywatności za konieczną z perspektywy ochrony zasady demokratycznego państwa prawnego. Konstytucyjną ochroną objęta została zarówno prywatność (art. 47 Konstytucji), jak i autonomia informacyjna jednostki (art. 51 Konstytucji). Konstytucja w zakresie odnoszącym się do ochrony prywatności jest aktem nowoczesnym. Po pierwsze wprowadza ona odrębną ochronę informacji dotyczących jednostki, co nie jest powszechne w europejskich systemach prawnych. Po drugie ustanawia w art. 51 ust. 3 i ust. 4 prawa dostępu i korekty. Potrzeba realnego wykonania tych praw było przyczyną rewolucji w unijnej ochronie danych osobowych. Tymczasem w polskim systemie prawnym od dawna są to prawa rangi konstytucyjnej.

Prawo do ochrony prywatności należy do szczególnych zasad konstytucyjnych, dotyczących wolności i praw, które tworzą określony system i pozostają ze sobą we współzależności opierającej się na ich związkach z godnością jednostki oraz specyficznych, charakterystycznych dla tej grupy zasad norm kolizyjnych. Prawo do ochrony prywatności informacyjnej jako publiczne prawo podmiotowe stanowi agregat norm (instytucję), na który ze względu na więź funkcjonalną składają się normy kształtujące prawa podmiotowe jednostki i nakładające na państwo określone obowiązki skorelowane z tymi prawami. Ogólnie rzecz ujmując, celem tych norm jest zaprojektowanie relacji między jednostką a państwem oraz innymi podmiotami przetwarzającymi informacje o jednostce, z

uwzględnieniem określonych standardów ochrony prywatności. Proces ten opiera się na tworzeniu zasad przetwarzania danych w różnych kontekstach.

5.2. Dopuszczalne konstytucyjnie ograniczenia prawa do ochrony prywatności. Analiza kontekstu przetwarzania informacji

Istotnym problemem badawczym jest analiza dopuszczalnych ograniczeń prawa do ochrony prywatności. W wypadku prawa do ochrony prywatności informacyjnej źródłem klauzul ograniczających jest zarówno art. 31 ust. 3 Konstytucji, który zawiera ogólne standardy ograniczeń praw opierające się na klasycznej formule oraz art. 51, który po pierwsze podkreśla konieczność ustawowej regulacji przetwarzania informacji o jednostce, a po drugie wprowadza warunek niezbędności w demokratycznym państwie prawnym. Na postawie tych przepisów oraz orzecznictwa TK, zostały zrekonstruowane etapy oceny dopuszczalności ograniczeń, czyli, badanie spełnienia wymogów: ustawowej formy ograniczeń, zakazu naruszenia istoty wolności lub prawa, dopuszczalnego konstytucyjnie celu oraz trójetapowego testu proporcjonalności (przydatność, niezbędność i proporcjonalność *sensu stricto*).

Normy Konstytucji z 1997 r. odnoszące się do ochrony prywatności, przy założeniu dynamicznej wykładni jej przepisów są jak najbardziej adekwatne. Wytrzymują próbę w zderzeniu ze wspomnianymi procesami zmian cywilizacyjnych. Przepisy te zakładają stworzenie przez ustawodawcę odpowiedniego normatywnego systemu regulującego obiegu informacji, opartego na konstytucyjnym standardzie. W świetle norm konstytucyjnych, w szczególności w związku z koniecznością oceny proporcjonalności ograniczeń w korzystaniu z konstytucyjnych wolności i praw, bardzo istotnym elementem – zarówno tworzenia prawa, jak i kontroli konstytucyjności norm – jest analiza kontekstu przetwarzania danych.

W te tendencje, w odniesieniu do przyjmowanych koncepcji prywatności, wpisuje się Trybunał Konstytucyjny. Stosuje on w swoim orzecznictwie elementy teorii kontroli i teorii dostępu. Trybunał stwierdza, że z jednej strony prawo do ochrony prywatności gwarantuje jednostce prawa do życia własnym życiem układanym według własnej woli z ograniczeniem do niezbędnego minimum wszelkiej ingerencji zewnętrznej, z drugiej uznaje prywatność za pewien stan niezależności, w ramach którego jednostka może decydować o

zakresie i zasięgu udostępniania i komunikowania innym osobom informacji o swoim życiu.

Należy jednak zauważyć, że żadna z tych teorii nie może zostać zastosowana w czystej postaci. Teoria kontroli przyznając jednostce wyłączne prawo do podejmowania decyzji o przetwarzaniu jej danych zapewnia najpełniejszą ochronę autonomii jako wartości konstytucyjnej. Wadą podejścia jest po pierwsze, że jeśli przyjęte zostaje założenie, że wymiana informacji o jednostce jest elementem życia społecznego, to każdorazowe uzależnianie tego przetwarzania od decyzji jednostki jest nierealistyczne. Po drugie, w rzeczywistości, w której dane są przetwarzane w bardzo wielu kontekstach, obciążenie jednostki odpowiedzialnością za podejmowanie świadomych decyzji we wszystkich tych sytuacjach może nie być skorelowane z zainteresowaniem jednostki ochroną swoich danych. Konsekwencją zastosowania teorii dostępu musiałoby być wyznaczenie stałego katalogu danych, które nie będą ujawniane. Biorąc pod uwagę różnorodność kontekstów przetwarzania danych, nie jest to rozwiązanie optymalne. Biorąc przykład danych o stanie zdrowia, jednostka zazwyczaj ujawnia je w kontekście interwencji medycznych, ale nie chce, żeby posiadał je pracodawca. Z tego powodu stała klasyfikacja nie jest optymalna. Należy więc uznać, że w orzecznictwie TK mogą zostać zastosowane jedynie elementy teorii kontroli i teorii dostępu. Co jest zresztą spójne z współczesnymi teoriami, które zakładają komplementarność pewnych aspektów teorii dostępu i kontroli. Zakładam przy tym, że teoria dostępu będzie dominowała w sprawach w których badane są akty normatywne regulujące relację między obywatelem a państwem, a nawet szerzej sprawy w których przetwarzanie danych odbywa się na podstawie ustawy, nie uwzględniając przesłanki jaką jest zgoda jednostki. Teoria kontroli będzie zaś przeważała w sprawach, które dotyczą relacji między podmiotami prywatnymi, w szczególności w wypadkach, kiedy przetwarzanie danych oparte są na zgodzie.

Dla oceny, w jakim zakresie istotne są elementy kontroli i elementy ograniczenia dostępu konieczna jest analiza kontekstu, która jest istotnym elementem rozważań TK. Trybunał skupia się przy tym na takich kwestiach, jak charakter danych oraz rodzaj podmiotów przetwarzających dane, podstawa przetwarzania danych, struktura przetwarzania danych oraz gwarancje proceduralne i techniczne przetwarzania danych. Przy pozytywnej ocenie dotychczasowej działalności orzeczniczej Trybunału w tym zakresie należy podkreślić, że wypracowanie przez TK uniwersalnego narzędzia badania

kontekstu przetwarzania danych, które mogłoby być zastosowane w sprawach dotyczących ochrony prywatności, byłoby korzystne przy obecnym skomplikowaniu procesów przetwarzania informacji o jednostkach w społeczeństwie informacyjnym.

Należy uznać, że sposoby badania kontekstu przetwarzania danych w orzecznictwie TK potwierdzają, że przepisy Konstytucji są aktualne nawet w dobie rozwoju nowych technologii. Wyznaczony konstytucyjnie standard ochrony prywatności jest zachowany, bardziej wyrafinowana i złożona staje się jednak ocena proporcjonalności procesów przetwarzania danych. Wymaga to większego wysiłku po stronie ustawodawcy w procesie tworzenia prawa. Ewolucja poglądów TK na temat zabezpieczeń technicznych danych (pseudonimizacji i anonimizacji) jest przykładem dostosowywania oceny wpływu na prywatność do zmieniających się kontekstów przetwarzania.

W mojej ocenie należy również podkreślić rolę analizy kontekstowej jako elementu procesu legislacyjnego. Pozwala ona ocenić różne rodzaje środków ochrony prywatności informacyjnej i wybrać najbardziej optymalne. Być może zasadne jest uznanie takiej analizy za wymóg formalny przy tworzeniu regulacji dotyczących prywatności jednostki. Potwierdzone odpowiednią dokumentacją dokonanie takich badań jest korzystne z perspektywy ewentualnej sądowej oceny konstytucyjności przyjętych rozwiązań legislacyjnych. Sprawia również, że rozwiązania te będą analizowane bardziej systemowo, adekwatnie do stopnia ich skomplikowania.

5.3. Wpływ charakteru danych o stanie zdrowia na kształt ich konstytucyjnej ochrony

Relacje między pacjentami a lekarzami oraz personelem medycznym są przedmiotem regulacji prawa medycznego. Jest to dziedzina prawa o silnych powiązaniach z prawem konstytucyjnym, szczególnie w aspekcie oparcia regulacji na wartościach takich jak m.in. godność, zdrowie, życie oraz równość. Prawo medyczne podlega ewolucji pod wpływem rozwoju nowych technologii, w tym także technologii informacyjnych opartych na profilowaniu i klasyfikacji danych. Przetwarzanie danych o stanie zdrowia jest immanentnym elementem zarówno terapii medycznych, jak i badań naukowych w dziedzinie biotechnologii i medycyny. Procesy przetwarzania informacji mogą się jednak wiązać z naruszeniem intymności jednostki. Dane o stanie zdrowia mają dużą wartość

ekonomiczną (są wykorzystywane w ocenie ryzyka), a ich nieprawidłowe przetwarzanie może prowadzić do działań o charakterze dyskryminacyjnym (klasyfikacja jednostki ze względu na jej cechy biologiczne). W ostatnich latach zmieniła się skala przetwarzania danych o stanie zdrowia. Informacje te są przechowywane przy użyciu nowoczesnych technologii informatycznych zwiększających mobilność danych i umożliwiających ich łączenie i analizowanie. Tworzone są również masowe rejestry danych, wykorzystywane m.in. do badań naukowych prowadzonych w celu realizacji zasady zdrowia publicznego.

Należy stwierdzić, że zastosowanie analizy kontekstowej do ochrony informacji o stanie zdrowia powinno obejmować interdyscyplinarne podejście uwzględniające perspektywę nauk medycznych i bioetyki. Przetwarzanie danych o stanie zdrowia jest istotne z perspektywy ochrony konstytucyjnych wartości, takich jak zdrowie publiczne, zdrowie jednostki oraz prawo do życia. Jednocześnie Konstytucja nakazuje wprowadzenie takich mechanizmów ochrony, które zagwarantują zarówno bezpieczeństwo danych pacjentów poddających się terapii, jak i uczestników badań naukowych. Warto podkreślić, że zapewnienie prawidłowych procedur przetwarzania danych wpływa na budowanie relacji opartej na zaufaniu między pacjentem a lekarzem i ułatwia uzyskanie prawidłowej diagnozy.

Dane o stanie zdrowia z jednej strony mają wrażliwy charakter – ich niewłaściwe przetwarzanie może doprowadzić do naruszenia intymności i godności jednostki. Z drugiej strony, wykorzystanie tych informacji jest absolutnie niezbędne w procesie leczenia. Projektowanie zabezpieczeń technicznych przetwarzania danych o stanie zdrowia musi się więc odbywać w sposób uwzględniający efektywność pracy lekarzy i innego personelu medycznego. Proces leczenia nie może być bowiem paraliżowany. Trzeba wziąć pod uwagę specyfikę pracy specjalistów medycznych i zapewnić optymalizację zabezpieczeń przetwarzania danych właściwą dla procesu leczenia. Zagrożeniem bowiem jest, że w imię ochrony danych osobowych obniżymy realność ochrony zdrowia.

Nie można pominąć niewystarczających działań ustawodawcy w odniesieniu do ochrony danych o stanie zdrowia. Raport Najwyższej Izby Kontroli odnoszący się do ochrony danych genetycznych stwierdził zaniedbania w dziedzinie zachowania odpowiednich procedur dotyczących przetwarzania i niszczenia danych i wykazał podstawowe braki w regulacji ustawowej. Pozostaje mieć nadzieję, że trwające od lat prace legislacyjne w tym zakresie zostaną skonkludowane.

5.4. Wpływ unijnej reformy ochrony danych osobowych na konstytucyjny standard ochrony prywatności

Konstytucyjna regulacja ochrony prywatności informacyjnej powstawała i funkcjonuje w złożonym systemie charakteryzującym się wielością ośrodków tworzenia prawa. Ochrona prywatności i autonomii informacyjnej jednostki jest przedmiotem regulacji zarówno systemu prawa wewnętrznego (Konstytucji i aktów niższego rzędu), jak i normatywnych instrumentów Unii Europejskiej (również rozwijających hierarchiczny system) oraz Rady Europy. Poza tymi trzema fundamentalnymi dla ochrony prywatności informacyjnej systemami, znajdziemy szereg umów międzynarodowych, zarówno wielo-, jak i dwustronnych oraz dokumentów organizacji międzynarodowych, które będą miały przełożenie na ostateczny kształt pozycji prawnej jednostki w kontekście ochrony jej prywatności informacyjnej.

W najbliższych latach ogromny wpływ na polski system prawny ochrony informacji o jednostce będzie miała unijna reforma ochrony danych osobowych. Przepisy RODO zastąpiły już w części rozwiązania przyjęte przez polskiego ustawodawcę w ustawie o ochronie danych osobowych. Jest to niezwykle interesujące z perspektywy konstytucyjnych wymogów dotyczących systemu źródeł prawa, jak również tych odnoszących się do architektury obiegu informacji. Przy uwzględnieniu, że system ochrony danych osobowych w Polsce składa się z centralnego aktu zawierającego ogólne zasady ochrony danych osobowych, oraz przepisów szczegółowych zawartych w ustawach dotyczących sfer w których przetwarza się dane dotyczące jednostki, należy przyjąć, że RODO zastąpiło akt centralny. Rozporządzenie wprowadza harmonizację częściową, co oznacza, że pewne elementy systemu ochrony danych osobowych nadal będą regulowane przez państwa członkowskie w drodze ustawy. Oznacza to, że architektura polskiego systemu ochrony danych osobowych się nie zmienia, ale zostaje zmieniony centralny akt tego systemu, co z pewnością ma wpływ na złożoność procesów wykładni. Należy jednak zaznaczyć, że doktryna i orzecznictwo badało już różne kwestie stojące na przeszkodzie harmonijnego stosowania prawa pochodzącego z dwóch ośrodków. Również spójność standardów ochrony prywatności wynikających z Konstytucji i Karty praw podstawowych Unii Europejskiej jest korzystna z punktu widzenia procesu wykładni.