Łukasz Wojciechowski

Bezpieczeństwo informacji i ochrona danych osobowych jako polityka publiczna – analiza wprowadzania mechanizmów i uregulowań prawnych

Polityka i Społeczeństwo nr 4 (14), 82-93

2016

ARTYKUŁY

„Polityka i Społeczeństwo" 4(14) / 2016
DOI: 10.15584/polispol.2016.4.6

Łukasz Wojciechowski*

BEZPIECZEŃSTWO INFORMACJI I OCHRONA DANYCH OSOBOWYCH JAKO POLITYKA PUBLICZNA – ANALIZA WPROWADZANIA MECHANIZMÓW I UREGULOWAŃ PRAWNYCH

INFORMATION SECURITY AND THE PROTECTION OF PERSONAL DATA AS A PUBLIC POLICY – AN ANALYSIS OF THE INTRODUCTION OF LEGAL REGULATIONS AND MECHANISMS

Abstract

The article aims to provide a comprehensive account of the legal regulations and mechanisms for the protection of personal data in Poland. In the last few years, considerable attention has been paid to this subject, which results in the wide-ranging character of the issues examined. The author classifies, based on sectors, the protection of personal data as a public policy and justifies such classification through the use of, among other tools, an institutional and legal method and factor analysis. The conclusions of the article are based on the analysis of the Polish legislation on the protection of personal data as well as on the analysis of the practical implementation of the solutions in companies, government and self-government institutions. Based on the results, it can be concluded that the protection of personal data falls within the scope of the public policy. However, it is necessary to take into account that some of its elements must be assigned to the policy of a party.

Key words: Public Policy, personal data protection, Information Security Policy

Wstęp

Wprowadzanie mechanizmów ochrony danych osobowych w Polsce, związane nieodłącznie z przemianami społeczno-gospodarczymi będącymi konsekwencją transformacji ustrojowej, stanowiło jedno z największych wyzwań legislacyjno-organizacyjnych w historii III Rze-

* Wyższa Szkoła Ekonomii i Innowacji w Lublinie, ul. Projektowa 4, 20-209 Lublin, e-mail: lukasz.wojciechowski@wsei.lublin.pl

czypospolitej. Przyjmując a priori, że działania te miały charakter polityki publicznej, już we wstępie warto podkreślić specyficzną sytuację aktorów tejże polityki. Oprócz polityków, którzy na poszczególnych etapach brali udział w tworzeniu i uchwalaniu aktów prawnych regulujących przedmiotową materię, aktorami byli także urzędnicy wszystkich szczebli administracji rządowej (zespolonej i niezespolonej) oraz samorządowej. Osobliwy charakter omawianej polityki publicznej wynika jednak z faktu, iż wraz z wdrażaniem mechanizmów ochrony danych osobowych, aktorami stawali się de facto wszyscy obywatele.

Celem niniejszego opracowania jest weryfikacja hipotezy badawczej, iż ochronę danych osobowych i politykę bezpieczeństwa informacji zaliczyć należy w poczet polityk publicznych w ujęciu sektorowym. Takie ujęcie problemu wymaga także zbadania, w jakim stopniu działania wybranych aktorów, ze szczególnym uwzględnieniem polityków, miały charakter polityki partyjnej. Do weryfikacji przedmiotowej hipotezy autor wykorzystał następujące metody badawcze: metodę instytucjonalno-prawną, która umożliwiła analizę aktów prawnych regulujących materię ochrony danych osobowych w Rzeczypospolitej Polskiej, oraz metodę decyzyjną i analizę czynnikową, co umożliwiło zbadanie interakcji w poszczególnych ogniwach łańcucha wprowadzanych mechanizmów. Materiał źródłowy stanowi przegląd aktów prawnych odnoszących się do ochrony danych osobowych, jak również publikacji traktujących o ochronie danych osobowych oraz politykach publicznych. Duże znaczenie przy powstawaniu pracy miały też doświadczenia empiryczne autora we współpracy z instytucjami samorządowymi.

Artykuł obejmuje swym zakresem chronologicznym okres obowiązywania Konstytucji Rzeczypospolitej Polskiej z 2 kwietnia 1997 r. Cezura początkowa to dzień uchwalenia ustawy zasadniczej przez Zgromadzenie Narodowe. Warto zwrócić uwagę, iż to właśnie ten akt prawny zawiera normy odnoszące się bezpośrednio do bezpieczeństwa informacyjnego obywateli, co w roku 1997 było zjawiskiem innowacyjnym. Cezura końcowa to 31 grudnia 2015 r.

Bezpieczeństwo informacji i ochrona danych osobowych jako polityka publiczna

Andrzej Zybała, dokonując przeglądu definicji polityk publicznych, definiuje zjawisko jako „zracjonalizowane działania i programy publiczne, które oparte są na zgromadzonej, względnie zobiektywizowanej wiedzy i usystematyzowanym procesie projektowania i wykonywania tych

działań" (Zybała 2012: 24). Badacz zwraca też uwagę, iż w Polsce dyscyplina „polityki publiczne" jest obecnie w trakcie wyłaniania się z innych nauk, które wciąż pozostają głównym narzędziem opisu działań państwa (Zybała 2012: 8). Nie oznacza to jednak, że przed podjęciem przedmiotowej problematyki przez środowisko akademickie w Polsce nie prowadzono (grup) działań, które spełniają kryteria polityk publicznych. Takie działania miały miejsce, a ich aktorzy często nie zdawali sobie sprawy, że ich aktywność może zostać opisana w analizowanym nurcie badawczym.

Niniejszy artykuł odnosi się do wprowadzania mechanizmów ochrony danych osobowych, co jest często utożsamiane z polityką bezpieczeństwa informacji. Wyjaśnienia wymaga, iż polityka bezpieczeństwa informacji jest pojęciem o bardzo szerokim zakresie i trudno w tym przypadku dokonać klasyfikacji zjawiska jako polityka publiczna. Ponadto, dla mniej zaawansowanych odbiorców, bezpieczeństwo informacyjne będzie rodziło skojarzenia z zawężeniem działań tylko do tych związanych z sieciami teleinformatycznymi (Namieśnik, Wesołowski 2007: 15). Natomiast ochrona danych osobowych to zbiór uregulowań prawnych i czynności prowadzących do właściwego zabezpieczenia interesów obywateli poprzez ochronę ich danych (m.in. nr PESEL, adres, telefon), dotyczących ich informacji wrażliwych (m.in. informacji o stanie zdrowia, życiu seksualnym, sporach sądowych), jak również ich wizerunku w formie fotografii lub filmu. Dane przetwarzane w systemach informatycznych podłączonych do sieci publicznej są ważnym obszarem ochrony, biorąc pod uwagę fakt, iż liczba urządzeń łączących się z Internetem w 2015 r. wynosiła na całym świecie 14 mld i systematycznie wzrasta (Pawlak 2015: 205). Równie ważne są jednak dane przetwarzane w sposób tradycyjny, tj. w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych (Ustawa o ochronie danych…, art. 2).

Kwestią dyskusyjną pozostaje przyporządkowanie ochrony danych osobowych do polityk publicznych w ujęciu sektorowym. Skala zjawiska wskazuje bowiem na horyzontalny charakter polityki. Warto jednak zwrócić uwagę na specyficzny charakter przedmiotowej materii, która wymaga od części aktorów specjalistycznej wiedzy, a od wszystkich ścisłego przestrzegania narzuconych procedur w celu zmniejszenia ryzyka utraty (części) chronionego zasobu. Polityka ochrony danych osobowych stopniowo wyodrębnia się także z obszernej dziedziny wiedzy, jaką jest polityka bezpieczeństwa informacji, stając się osobnym obiektem badań naukowych z coraz obszerniejszą literaturą przedmiotu.

Instrumenty wprowadzania polityki ochrony danych osobowych można podzielić na cztery grupy. Pierwsza z nich to wprowadzanie ure-

gulowań prawnych. Szczególnie w początkowej fazie procesu można było zaobserwować niedostosowanie wymogów zawartych w aktach prawnych w stosunku do stanu faktycznego w instytucjach i przedsiębiorstwach, na co składały się przede wszystkim: niedostateczne dostosowanie infrastruktury oraz brak właściwego przygotowania merytorycznego pracowników odpowiedzialnych za wdrażanie nowych rozwiązań. Podobnie jak w przypadku wprowadzania uregulowań prawnych odnoszących się do wielu innych obszarów, również na ochronę danych osobowych nie zabezpieczono wystarczających środków finansowych w budżecie państwa, przez co restrykcyjne przepisy przełożyły się na duży popyt na szkolenia pracowników, które to zapotrzebowanie nie mogło zostać zaspokojone z powodu braku funduszy.

Drugą grupę stanowią działania służb i organów państwowych podejmowane w celu wprowadzania, implementowania, jak również egzekwowania mechanizmów ochrony danych osobowych. W tym przypadku warto podkreślić, iż organ państwowy do spraw ochrony danych osobowych, którym na mocy ustawy jest Generalny Inspektor Ochrony Danych Osobowych (Ustawa o ochronie danych…, art. 8), nie jest w stanie samodzielnie kontrolować procedur określonych przepisami prawa w skali całego kraju. W związku z tym rolę instytucji kontrolujących muszą przyjmować też organy samorządowe, kierownicy jednostek oraz przedsiębiorcy, natomiast GIODO często ogranicza się do roli arbitra w najbardziej skomplikowanych kwestiach na gruncie przedmiotowej materii. Taka kontrola odbywa się sektorowo w ramach kompetencji danego organu bądź też kierownika jednostki, a do jej przeprowadzenia skłania wymienione podmioty konieczność zapewnienia właściwego funkcjonowania jednostek im podległych. Jednocześnie kontrola i dbałość o przestrzeganie procedur w przypadku przedsiębiorców jest ściśle związana z trzecią grupą instrumentów wprowadzania polityki ochrony – naturalnych procesów wolnego rynku. W tym przypadku warto skonstatować fakt, iż wraz z rozbudowywaniem mechanizmów gospodarki rynkowej w Polsce można było odnotować systematyczny wzrost świadomości przedsiębiorców w kwestii korzyści dla firm w przypadku właściwej polityki ochrony danych osobowych. Owe korzyści związane są m.in. ze wzrostem zaufania i poczucia bezpieczeństwa u klientów, adaptacją właściwego typu kultury w przedsiębiorstwie, jak również względami związanymi z prestiżem i wizerunkiem.

Ostatnią grupę instrumentów wprowadzania polityki ochrony danych osobowych w Polsce stanowią działania związane z edukacją. Obszar ten ma kluczowe znaczenie z punktu widzenia wprowadzania uregulowań prawnych i mechanizmów w praktyce. Nie jest możliwe właściwe funkcjonowanie ochrony danych osobowych jako polityki publicznej

jedynie poprzez stosowanie nawet najbardziej adekwatnych i zaawansowanych uregulowań prawnych. Warto zwrócić uwagę, iż największym mankamentem funkcjonowania nowego ładu po transformacji ustrojowej nie była niewłaściwa legislacja, lecz trudności z efektywną implementacją rozwiązań do poszczególnych instytucji i przedsiębiorstw. To właśnie bariery implementacyjne były wykładnią deficytu w przygotowaniu merytorycznym kadr. Szkolenia z zakresu polityki ochrony danych osobowych odbywają się na dwóch płaszczyznach. Pierwszą z nich jest działalność edukacyjna GIODO. Odbywa się ona m.in. poprzez wydawanie publikacji odnoszących się do przedmiotowej materii, organizację klasycznych szkoleń, e-learning skierowany do różnych grup docelowych, jak również organizację konferencji naukowych. Biuro GIODO prowadzi też działalność edukacyjną poprzez organizację konkursów dla uczniów różnych typów szkół, z uwzględnieniem zainteresowań związanych z przedmiotami humanistycznymi i przedmiotami ścisłymi. Podobnie jak w przypadku działań kontrolnych Biuro GIODO nie jest w stanie zapewnić właściwej podaży szkoleń z punktu widzenia bardzo dużego zapotrzebowania. W związku z tym przygotowywanie merytoryczne pracowników staje się często zadaniem własnym instytucji i przedsiębiorstw. Jako drugą płaszczyznę wskazać więc należy szkolenia organizowane przez kierowników jednostek lub przedsiębiorców, które mogą przybierać formę wewnętrzną lub zewnętrzną. W początkowym etapie wprowadzania nowych rozwiązań konieczne było systematyczne korzystanie z usług szkoleniowców zewnętrznych, co uwarunkowane było znacznym deficytem wiedzy w tym zakresie w skali makrostrukturalnej. Obecnie w zasobach kadrowych wielu instytucji i firm znajdują się pracownicy, którzy pełnią rolę szkoleniowców wewnętrznych.

Ochrona danych osobowych to obszar, który w znikomym stopniu można określić jako politykę partyjną. Biorąc pod uwagę skalę i szeroki zakres wprowadzanych rozwiązań, taki stan rzeczy uznać należy za ewenement. Obszary, które należy zakwalifikować jako politykę partyjną, to przede wszystkim polityka kadrowa w instytucjach publicznych oraz dążenie podmiotów rywalizacji politycznej do systematycznego pozyskiwania poparcia elektoratu. Pierwszy obszar wzbudza liczne kontrowersje i dostarcza wielu trudności z punktu widzenia badań naukowych, jednak zależność pomiędzy przygotowaniem merytorycznym kadr a skutecznością mechanizmów ochrony danych osobowych nie wzbudza wątpliwości. Ponadto podkreślić należy, że prowadzona polityka kadrowa może utrudniać, ale nie uniemożliwia projektowania i wdrażania przedmiotowej polityki publicznej. W przypadku drugiego obszaru warto zwrócić uwagę na synergię pomiędzy celami ugrupowań politycznych

i kandydatów a priorytetami ochrony danych osobowych. Celem nadrzędnym w jednym i drugim przypadku jest zapewnienie bezpieczeństwa obywateli, co w przypadku rywalizacji wyborczej ma przełożyć się na korzystną z punktu widzenia podmiotów rywalizacji politycznej partycypację wyborczą obywateli. Takie podejście jest też spójne z jednym z podstawowych celów wdrażania polityk publicznych, jakim jest osiąganie wysokiej jakości życia obywateli (Osiński 2015: 14).

Uregulowania prawne

Warto zwrócić uwagę, iż postępujący proces transformacji ustrojowej wiązał się z koniecznością dostosowania polskiego prawodawstwa i mechanizmów funkcjonowania państwa na wzór demokracji zachodnich. Ewaluacja uregulowań prawnych lub wprowadzanie całkowicie nowych rozwiązań stała się udziałem niemal wszystkich obszarów, stąd też powstanie „legislacyjnej kolejki" i rozłożenie wprowadzania zmian niemalże na całe lata 90. XX w. Z punktu widzenia prawnych mechanizmów ochrony danych osobowych przełomowym wydarzeniem było uchwalenie przez Zgromadzenie Narodowe Konstytucji Rzeczypospolitej Polskiej 2 kwietnia 1997 r., a następnie jej zatwierdzenie przez obywateli w referendum 25 maja 1997 r. (Millard 2000: 42).

W Konstytucji RP została wyrażona zasada legalizmu, będąca fundamentem działań administracji publicznej (Konstytucja…, art. 7). Działanie organów administracji publicznej na podstawie przepisów prawa odzwierciedla również *Kodeks postępowania administracyjnego* (Ustawa kodeks…, art. 6). Zasada ta stanowi rozróżnienie pomiędzy działaniami (służbowymi) urzędników a czynnościami, jakie podejmują obywatele w codziennym życiu oraz prowadząc działalność gospodarczą. Obywatele mają zagwarantowaną wolność pozyskiwania i rozpowszechniania informacji (Konstytucja…, art. 54) oraz prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia, a także do decydowania o swoim życiu osobistym (Konstytucja…, art. 47). Warto zwrócić uwagę na związek pomiędzy przytoczoną regulacją a przepisami odnoszącymi się do ochrony danych osobowych, jednocześnie biorąc pod uwagę konieczność rozgraniczenia obydwu kwestii (Fajgielski 2007: 28). Ponadto, ustawa zasadnicza zawiera regulacje bezpośrednio odnoszące się do ochrony danych osobowych. Wśród nich wskazać należy m.in. następujące przepisy: „Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby"; „Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie praw-

nym"; „Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa"; „Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą" (Konstytucja…, art. 51).

Z punktu widzenia tworzenia uregulowań prawnych dotyczących ochrony danych osobowych szczególne znaczenie ma regulacja odnosząca się do przeniesienia określenia zasad i trybu gromadzenia oraz udostępniania informacji do ustawy (Konstytucja…, art. 51). Wynika to z faktu, iż konsekwencją stało się procedowanie i uchwalenie ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Warto podkreślić, iż z punktu widzenia niespełna dwudziestu lat funkcjonowania tego aktu prawnego, twórcom ustawy udało się stworzyć nowoczesny akt prawny, a wiele przyjętych rozwiązań funkcjonuje niezmiennie do dziś. Jest to osiągnięcie warte podkreślenia z uwagi na postępującą w ostatnich latach digitalizację i postęp technologiczny. Przedmiotem regulacji ustawy są m.in.: organ ochrony danych osobowych, zasady przetwarzania danych osobowych, prawa osoby, której dane dotyczą, zabezpieczenie danych osobowych, rejestracja zbiorów danych osobowych i administratorów bezpieczeństwa informacji oraz przekazywanie danych osobowych do państwa trzeciego.

Szczegółowe wytyczne dotyczące kształtu funkcjonowania mechanizmów ochrony danych osobowych w wymiarze prowadzonej dokumentacji, jak również praktycznego zastosowania zabezpieczeń reguluje rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Rozporządzenie reguluje sposób prowadzenia i zakres dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń i kategorii danych objętych ochroną; podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych; wymagania w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzania danych osobowych (Rozporządzenie…, par. 1). Minister określił trzy poziomy bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym. To właśnie w tym obszarze regulacje są najbardziej restrykcyjne i trudne do wprowadzenia, szczególnie w przypadku podmiotów dysponujących najmniejszymi zasobami.

Warto zwrócić uwagę, iż katalog aktów prawnych odnoszących się do ochrony danych osobowych w sposób pośredni jest znacznie bardziej szeroki niż przytoczone ustawy i rozporządzenie. Wśród nich priorytetowe znaczenie ma ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych oraz ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne. Akty prawne odnoszą się jedynie do wybranych, wyspecjalizowanych sektorów ochrony danych osobowych, co nie umniejsza ich rangi.

Mechanizmy ochrony danych

Normy prawne regulujące materię ochrony danych osobowych w Rzeczypospolitej Polskiej stanowią uniwersalne źródło wiedzy i wytycznych zarówno dla kierowników instytucji rządowych i samorządowych, jak również przedsiębiorców. W rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. został określony zakres dokumentacji, jaką powinni opracować kierownicy poszczególnych jednostek. Ponadto przyjęto rozwiązania, które mają zapewnić zapoznawanie się pracowników z przepisami wewnętrznymi, a przez to zwiększenie prawdopodobieństwa ich stosowania. Dla wielu osób jest to pierwsze zetknięcie się z zagadnieniem ochrony danych osobowych, będące jednocześnie pierwszym etapem edukacji w tym zakresie. Zdobyta wiedza w naturalny sposób może, a nawet powinna być wykorzystywana również poza zakładałem pracy i podczas wykonywania codziennych czynności związanych z przetwarzaniem danych osobowych. Samą świadomość odpowiedzialności za działania w tym zakresie przede wszystkim w wymiarze służbowym warto rozpatrywać także jako czynnik motywujący do poszerzania wiedzy w zakresie przedmiotowej materii, ze szczególnym uwzględnieniem kursów e-learningowych zaproponowanych przez GIODO.

Zgodnie z rozporządzeniem, na dokumentację składa się polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych (Rozporządzenie…, par. 3). Polityka bezpieczeństwa (ochrony danych osobowych) to dokument, który powinien być unikatowym zbiorem norm wewnętrznych opracowanych na potrzeby danej instytucji lub firmy. Taki charakter dokumentu wynika z różnorodności celów, infrastruktury oraz innych zasobów i wymaga indywidualnego podejścia. Znane są przypadki, w których kontrole i audyty wewnętrzne wykazują istnienie dokumentów w jednostkach samorządu terytorialnego, które zostały skopiowane ze stron internetowych innych jednostek bądź też zakupione od przedsiębiorstw, które sprzedają gotowe,

rzekomo uniwersalne rozwiązania. W akcie wykonawczym do ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych znajdują się precyzyjne wytyczne co do zawartości merytorycznej dokumentu. Zgodnie z nimi, polityka powinna zawierać: wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe; wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych; opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi; sposób przepływu danych pomiędzy poszczególnymi systemami oraz określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych (Rozporządzenie..., par. 4).

Kluczowe znaczenie z punktu widzenia bezpieczeństwa informacji ma precyzyjne określenie zasobów informacyjnych w postaci zbiorów danych i przyporządkowanie do tych zasobów pracowników, przy jednoczesnym wykluczeniu pracowników, którzy nie zostali upoważnieni do przetwarzania danego zbioru. Dlatego polityka bezpieczeństwa ochrony danych osobowych powinna zawierać wzory upoważnień dla pracowników do przetwarzania konkretnych, wcześniej zdefiniowanych zbiorów danych, jak również wzór oświadczenia pracownika o zapoznaniu się z przedmiotową dokumentacją.

Warto podkreślić, iż zawarte w rozporządzeniu wytyczne nie mają charakteru taksatywnego i określają jedynie najważniejsze i niezbędne składowe prawidłowej dokumentacji. Nadanie polityce bezpieczeństwa ochrony danych osobowych charakteru uniwersalnego wymaga zamieszczenia w dokumencie praktycznych informacji dotyczących właściwego posługiwania się danymi osobowymi. Autorzy opracowań powinni uwzględnić fakt, iż będą się z nimi zapoznawać pracownicy różnych szczebli, o zróżnicowanym przygotowaniu merytorycznym, stąd też właściwa jest rezygnacja ze skomplikowanej terminologii na rzecz języka powszechnie zrozumiałego. Celem nadrzędnym nie może być język dokumentu, lecz zapewnienie szerokiego spektrum odpowiednich zachowań i zastosowania procedur.

Drugi dokument, dotyczący zarządzania systemem informatycznym, również powinien mieć charakter unikatowy, uwzględniać infrastrukturę i zasoby danej jednostki oraz cechować się maksymalnym dopasowaniem do panujących tam realiów. Bardzo często instrukcja stanowi załącznik do polityki bezpieczeństwa ochrony danych osobowych, co jest zgodne ze stanem faktycznym, ponieważ jest de facto nieodłącznym elementem tejże polityki. W tym przypadku również określono wytyczne dotyczące zawartości opracowania. W rozporządzeniu wskazano, że instrukcja powinna zawierać m.in.: procedury nadawania uprawnień do przetwarzania danych

i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności; stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem; procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu oraz procedury tworzenia kopii zapasowych zbiorów danych, a także programów i narzędzi programowych służących do ich przetwarzania (Rozporządzenie…, par. 5).

Nawet najbardziej profesjonalne i adekwatne procedury nie wyeliminują sytuacji patologicznych, w których dochodzi z powodu cech charakterologicznych aktorów, najczęściej usytuowanych na niższych szczeblach hierarchii służbowej w danej instytucji lub przedsiębiorstwie. Czynnik ten jeszcze bardziej skłania do refleksji nad rolą edukacji oraz konieczności uświadamiania obywatelom wagi ochrony danych osobowych jako polityki publicznej. Jednym z przykładów zjawisk patologicznych jest tworzenie tzw. profili osobowych przez urzędników administracji rządowej i samorządowej. Zjawisko to polega na sprawdzaniu danych interesanta w kilku różnych bazach danych, chociaż do załatwienia sprawy wystarczą dane zawarte w jednej bazie. Decyzja wydawana jest na podstawie opinii o interesancie, jaka wytworzyła się w świadomości urzędnika, nie zaś na podstawie przesłanek merytorycznych. Takie zachowanie, abstrahując od wymiaru aksjologicznego, ma negatywny wpływ zarówno na prestiż danej jednostki, jak również może przynieść straty będące konsekwencją błędnej decyzji administracyjnej (Siwicki 2013: 254).

Podsumowanie

Głównym celem niniejszego artykułu było zbadanie uregulowań prawnych i mechanizmów ochrony danych osobowych w Polsce jako polityki publicznej. Przytoczone argumenty prowadzą do pozytywnej weryfikacji hipotezy zawartej we wstępie. Przedstawiona analiza zmierza do konkluzji, które można przyporządkować do kilku grup. W pierwszej z nich przytoczyć należy argumenty potwierdzające zasadność kwalifikacji przedmiotowej materii jako polityki publicznej. Do takich wniosków prowadzi możliwość wyłonienia aktorów, wśród których warto zwrócić szczególną uwagę na polityków jako kreatorów uregulowań prawnych, kierowników instytucji rządowych i samorządowych, jako konstruujących, wdrażających i kontrolujących politykę (w ramach swoich kompetencji), jak również przedsiębiorców, którzy w zależności od skali działalności pełnią podobną rolę jak kierownicy instytucji. Możliwe jest także odtworzenie procesu projektowania polityki poprzez syntezę kreacji prawnych aspektów polityki ochrony danych osobowych. W tym

przypadku podkreślenia wymaga korelacja pomiędzy wprowadzaniem norm prawnych a implementacją mechanizmów. Trudno wnioskować, czy ustawodawca, wprowadzając restrykcyjne wymagania, brał pod uwagę trudności implementacyjne, ze szczególnym uwzględnieniem okresu początkowego. Jednak biorąc pod uwagę ponad dziesięcioletnie funkcjonowanie aktu wykonawczego do ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, warto zwrócić uwagę na systematyczne przełamywanie barier implementacyjnych zarówno wśród instytucji publicznych, jak i przedsiębiorstw w skali mikro- i makrostrukturalnej.

Do drugiej grupy zaliczyć należy wnioski związane z brakiem kwalifikacji przedmiotowej polityki jako polityki partyjnej. Autor wskazuje elementy omawianej materii związane z rywalizacją podmiotów na rynku wyborczym. W obszarze tym wyłania się także paradoks korelacji właściwego funkcjonowania mechanizmów ochrony z satysfakcją i pozytywnym nastawieniem elektoratu przy jednoczesnym prawdopodobnym braku takich intencji po stronie uczestników politycznej areny. Partyjny charakter ma też dobór kadr uwzględniający kryteria posiadania legitymacji partyjnej lub innych form patologicznego spowinowacenia z ugrupowaniami politycznymi mającymi wpływ na procesy rekrutacyjne. Jednak poza przytoczonymi elementami partyjności procesy tworzenia uregulowań prawnych i wprowadzania mechanizmów ochrony danych osobowych stały się dobrem powszechnym i realizacją interesu obywateli niezwiązanych z rynkiem politycznym w zakresie ich bezpieczeństwa.

Trzeci obszar to konkluzje związane z nadaniem polityce charakteru sektorowego, pomimo występowania zasadnych argumentów prowadzących do przyporządkowania tej materii charakteru horyzontalnego. Wśród nich podkreślić należy specyficzny zakres ochrony danych osobowych jako polityki publicznej o bardzo szerokim wymiarze, która w zróżnicowanym stopniu odnosi się niemal do wszystkich obywateli Rzeczypospolitej Polskiej. Natomiast wykładnikiem sektorowego charakteru przedmiotowej materii jest przede wszystkim zakres badań naukowych, wyodrębnionych i szeroko opisanych, jak również polskie prawodawstwo i funkcjonowanie państwowego organu do spraw ochrony danych osobowych. Równolegle, do kanonu czynników sektorowych zaliczyć należy wąski charakter specjalizacyjny, co przejawia się m.in. w systematycznie zwiększającej się podaży dedykowanych usług w przedmiotowym sektorze.

Bibliografia

Fajgielski P. 2007, *Informacja w administracji publicznej. Prawne aspekty gromadzenia, udostępniania i ochrony*, Wrocław.

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (DzU nr 78, poz. 483).

Millard F. 2000, *Presidents and Democratization in Poland: The Roles of Lech Walesa and Aleksander Kwaśniewski in Building a New Polity*, „Journal of Communist Studies & Transition Politics", vol. 16, no. 3.

Osiński J. 2015, *Polityka publiczna w Polsce. Priorytety i wyzwania*, Warszawa.

Pawlak P. 2015, *Governance of Safety and Security in Cyberspace* [w:] *Global safety governance: Challenges and Solutions*, red. P. Dąbrowska-Kłosińska, Warszawa.

Romaniuk P. 2014, *Zarządzanie systemami bezpieczeństwa informacji w administracji publicznej z wykorzystaniem instytucji audytu wewnętrznego* [w:] W*ymiary ochrony informacji i polityki bezpieczeństwa*, red. M. Sitek, I. Niedziółka, A. Ukleja, Józefów.

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (DzU 2004, nr 100, poz. 1024).

Siwicki M. 2013, *Cyberprzestępczość*, Warszawa.

Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (tekst jednolity DzU z 2016 r., poz. 23).

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (DzU 2015. poz. 2135).

Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (DzU 2005, nr 64, poz. 565).

Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j. DzU z 2016 r., poz. 1167).

Wesołowski J., Namiestnik J. 2007, *Bezpieczeństwo i ochrona informacji*, Gdańsk.

Wojciechowski Ł. 2016, *Wykonywanie zadań ustawowych przez Generalnego Inspektora Ochrony Danych Osobowych – wybrane zagadnienia*, „Zeszyty Naukowe WSEI seria Administracja", nr 5 (1/2015).

Zybała A. 2012, *Polityki publiczne*, Warszawa.