

BEZPIECZEŃSTWO INFORMACJI W ADMINISTRACJI PUBLICZNEJ



pod redakcją
Doroty Fleszer

BEZPIECZEŃSTWO INFORMACJI
W ADMINISTRACJI PUBLICZNEJ

pod redakcją
Doroty Fleszer

BEZPIECZEŃSTWO INFORMACJI W ADMINISTRACJI PUBLICZNEJ

pod redakcją
Doroty Fleszer



Sosnowiec 2017

Recenzent

prof. dr hab. Lidia Zacharko

Redaktor Oficyny Wydawniczej „Humanitas”

Danuta Dziewięcka

Projekt okładki

Bartłomiej Dudek

Copyright by

Oficina Wydawnicza „Humanitas”

ul. Kilińskiego 43

41-200 Sosnowiec

tel.: 32 363 12 25

e-mail: wydawnictwo@humanitas.edu.pl

dystribucja@humanitas.edu.pl

ISBN: 978-83-65682-63-5

Sosnowiec 2017

Spis treści

Wstęp	7
--------------------	---

Rozdział I

Zakres przetwarzania informacji w administracji publicznej

Grzegorz Krawiec

Działalność Rzecznika Praw Obywatelskich w zakresie ochrony prywatności	13
---	----

Wojciech Papis

Autonomia informacyjna jednostki w kontekście gromadzenia danych osobowych w postępowaniu karnym	27
---	----

Tomasz Miłkowski

Uprawnienie do gromadzenia informacji w ramach działań antyterrorystycznych	51
---	----

Mariusz Korobłowski

Przepadek pojazdu w świetle art. 130a ust. 10 ustawy z dnia 20 czerwca 1997 r. Prawo o ruchu drogowym – przyczynek do dyskusji	67
---	----

Rozdział II

Organizacja zabezpieczenia informacji w administracji publicznej

Dorota Fleszer

Zabezpieczenie danych osobowych – zakres obowiązku i sankcje za jego naruszenie.....	83
--	----

Anna Rogacka-Łukasik

Ochrona informacji w jednostkach samorządu terytorialnego poprzez stosowanie polityki bezpieczeństwa informacji	97
--	----

Katarzyna Płonka-Bielenin

Programy ochrony infrastruktury krytycznej jako dokumenty podlegające przepisom ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych	113
--	-----

Rozdział III

Sposób i metody przetwarzania informacji w administracji publicznej

Adrianna Paroń

Chmura obliczeniowa a administracja publiczna	129
---	-----

Wstęp

Niezbędnym elementem sprawnego i rzetelnego wykonywania zadań publicznych jest posiadanie odpowiednich pod względem zakresu i treści informacji. Tylko działanie w warunkach pełnej wiedzy o okolicznościach istotnych dla realizacji konkretnego zadania pozwala na eliminację lub zminimalizowanie możliwości powstania nieprawidłowości. Nie bez znaczenia są także wyraźnie artykułowane oczekiwania społeczeństwa dotyczące poziomu i sposobu realizacji usług publicznych. Standardy ich świadczenia mają być takie same jak w sferze komercyjnej. Poza tym nie ma przyzwolenia na podejmowanie błędnych decyzji lub działanie w warunkach niewiedzy lub braku pełnego rozeznania w realizowanej sprawie. Nie oznacza to jednak akceptacji dowolności, szerokiego i nieograniczonego pod względem zakresu zbierania informacji. Trzeba przyjąć bowiem założenie, że dobrem, które ponad wszelką wątpliwość wymaga szczególnej ochrony, jest godność i prywatność osoby. W ten sposób dochodzi do powstania swoistego konfliktu pomiędzy limitowaniem ingerencji w prywatność osoby poprzez ograniczanie przetwarzania informacji o charakterze osobowym a koniecznością szybkiego i skutecznego reagowania na zagrożenia, szczególnie te w sferze bezpieczeństwa zarówno wewnętrznego, jak i zewnętrznego.

Przetwarzanie informacji w administracji publicznej wymaga podjęcia przez nią także skutecznych działań w zakresie stworzenia organizacyjnych i technicznych warunków jej przetwarzania. Problematyka bezpieczeństwa informacji kojarzona jest przede wszystkim z ochroną danych osobowych i ochroną prywatności, ponieważ nieuprawnione ujawnienie informacji o charakterze osobowym godzi bezpośrednio w prawa i wolności człowieka, zwłaszcza zaś w jego godność. A przecież nie mniej istotna jest kwestia ochrony informacji z uwagi na ich szczególną rolę w funkcjonowaniu państwa. Mowa tu oczywiście o ochronie informacji niejawnych. W dyskursie na temat bezpieczeństwa informacji niezmiennie rzadko porusza się kwestie ich autorsko prawnej ochrony, zwłaszcza w działaniach o charakterze promocyjnym, wizerunkowym czy też tajemnicy przedsiębiorstwa. Warto w tym miejscu podkreślić, że problematyka zabezpieczenia przetwarzanych informacji nie jest przez ustawodawcę w sposób precyzyjny określana. Przepisy o ochronie danych osobowych a także regulacje o charakterze wykonawczym w sprawie dokumentacji i warunków technicznych przetwarzania danych osobowych nie zawierają wyraźnie określonych rozwiązań organizacyjnych w zakresie ochrony fizycznej i informacyjnej, do stosowania których zobowiązany byłby administrator danych. Raczej wskazywane są metody, sfery wymagające zainteresowania organu administracji publicznej pod kątem ich właściwego zorganizowania, tak aby uzyskać właściwy poziom zabezpieczeń. Brak dokładnej specyfikacji technicznej należy ocenić pozy-

tywnie, ponieważ jej przydatność byłaby niewielka. Każdy bowiem administrator danych ma wypracować własny system zabezpieczeń, dostosowany do jego potrzeb i warunków przetwarzania danych osobowych.

Nie mniej istotnym elementem przetwarzania informacji, który ma też bezpośredni wpływ na przyjęty sposób i poziom stosowanych zabezpieczeń, jest metoda, sposób wykonywania operacji na informacji. Rozwój technik informatycznych i możliwości, jakie daje informatyka, czynią niezbędnym nie tylko zainteresowanie się nowymi formami przetwarzania i zabezpieczania informacji, ale też ich stosowanie. Przykładem jest choćby korzystanie z chmury obliczeniowej, czyli z modelu organizacji pracy polegającego na korzystaniu z usług dostarczonych przez wybranego, zewnętrznego dostawcę w ramach opłaty licencyjnej. Daje ona możliwość zwiększenia efektywności całej gospodarki i poszczególnych organizacji dzięki osiągnięciu większej optymalizacji funkcjonowania infrastruktury informatycznej. To właśnie konieczność zapewnienia odpowiedniego poziomu zabezpieczeń czyni niezwykle aktualną dyskusję nad możliwością korzystania także przez administrację z nowych technologii i wykorzystywania nowych proponowanych rozwiązań w zakresie informatyki.

Prezentowana monografia zbiorowa wiąże się z realizowanym w latach 2016-2017 r. w Instytucie Administracji i Prawa Wyższej Szkoły Humanitas projektem badawczym pt. „Bezpieczeństwo informacji w administracji publicznej”, finansowanego z dotacji Ministerstwa Nauki i Szkolnictwa Wyższego na podtrzymanie i rozwój potencjału badawczego. Zaproszenie do współpracy przy jej tworzeniu przyjęli naukowcy specjalizujący się nie tylko w zakresie prawa administracyjnego, ale także niezwiązani bezpośrednio z tym obszarem badań naukowych. Z pewnością tak złożone zagadnienie, jakim jest bezpieczeństwo informacji przetwarzanych w administracji publicznej, nie zostało wyczerpane, tym niemniej Autorzy wywodzący się z różnych ośrodków akademickich podjęli się przedstawienia istotnych pod względem prawnym zagadnień dotyczących sfery informacyjnej funkcjonowania administracji publicznej. Wyniki przeprowadzonych badań złożyły się na niniejszą monografię. Podejmowane w niej zagadnienia zostały podzielone na trzy tematyczne rozdziały.

Pierwszy rozdział zatytułowany „Zakres przetwarzania informacji w administracji publicznej” grupuje teksty związane z procesem przetwarzania informacji w administracji publicznej, ze szczególnym uwzględnieniem ich gromadzenia, przechowywania i udostępniania. Grzegorz Krawiec („Działalność Rzecznika Praw Obywatelskich w zakresie ochrony prywatności”) ujmuje problematykę prywatności z perspektywy praw człowieka, co jest przedmiotem zainteresowania Rzecznika Praw Obywatelskich. Kontynuuje ten wątek Wojciech Papis („Autonomia informacyjna jednostki w kontekście gromadzenia danych osobowych w postępowaniu karnym”), poruszając kwestię autonomii informacyjnej jednostki w postępowaniu

karnym, czynnościach operacyjno-rozpoznawczych prowadzonych przez policję oraz w działaniach antyterrorystycznych. Z kolei Tomasz Miłkowski („Uprawnienie do gromadzenia informacji w ramach działań antyterrorystycznych”) koncentruje się na problematyce gromadzenia informacji (w szerokim ujęciu, a więc również narzędzi do tego służących) w ramach działań antyterrorystycznych, na przykładzie dwóch ustaw: o zarządzeniu kryzysowym i o działaniach antyterrorystycznych. Natomiast Mariusz Korobłowski („Przepadek pojazdu w świetle art. 130a ust. 10 ustawy z dnia 20 czerwca 1997 r. Prawo o ruchu drogowym – przyczynek do dyskusji”) podejmuje problematykę postępowania przed sądem cywilnym inicjowanym na wniosek starosty w sprawie wydania orzeczenia przypadku pojazdu w trybie art. 130a ust. 10 w związku z art. 130a ust. 1 i 2 ustawy z dnia 20 czerwca 1997 r. Prawo o ruchu drogowym. W toku postępowania sąd może napotkać na szereg rozmaitych trudności, np. w zakresie ustalenia danych osobowych właściciela pojazdu. Istotne znaczenie ma podanie przez wnioskodawcę prawidłowych oraz aktualnych danych adresowych uczestnika postępowania.

Rozdział drugi, traktujący o organizacji zabezpieczenia informacji w administracji publicznej, otwiera opracowanie Doroty Fleszer (Zabezpieczenie danych osobowych – zakres obowiązku i sankcje za jego naruszenie”) dotyczące elementów tworzonego przez administratora danych systemu zabezpieczeń przetwarzanych danych osobowych. Tę problematykę uzupełnia Anna Rogacka-Łukasik („Ochrona informacji w jednostkach samorządu terytorialnego poprzez stosowanie polityki bezpieczeństwa informacji”), analizując jeden z dokumentów, którego opracowanie jest wymagane dla właściwie funkcjonującego systemu zabezpieczeń, a mianowicie politykę bezpieczeństwa informacji. Inny aspekt bezpieczeństwa informacji analizuje Katarzyna Płonka-Bielenin („Programy ochrony infrastruktury krytycznej jako dokumenty podlegające przepisom ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych”). Na płaszczyźnie zarządzania kryzysowego ochrona informacji niejawnych dotyczy infrastruktury krytycznej oraz jej ochrony. Potrzeba objęcia wskazanych powyżej dokumentów i informacji ochroną informacji niejawnych podyktowana jest faktem, że zawierają one szczególnie istotne informacje dotyczące bezpieczeństwa państwa i jego obywateli.

W rozdziale trzecim „Sposób i metody przetwarzania informacji w administracji publicznej” Adrianna Paroń („Chmura obliczeniowa a administracja publiczna”) podejmuje zagadnienie wykorzystania w administracji publicznej nowej usługi informatycznej, jaką jest chmura obliczeniowa.

Rozległość zagadnienia bezpieczeństwa w administracji informacji publicznej, znaczna ilość aktów normatywnych ją regulujących powoduje, że swobodne poruszanie w tej materii jest trudne. W związku z tym wydaje się uzasadnione szersze i głębsze zainteresowanie tą problematyką. Niewątpliwie wyniki badań służyć będą rozwojowi nauki prawa administracyjnego. Podjęta problematyka ma bowiem

przede wszystkim wymiar praktyczny, stąd też wyniki badań kierowane są przede wszystkim do urzędników przetwarzających w ramach realizacji swoich zadań informacje o różnym charakterze. Niewątpliwie skorzystają z nich również studenci, poszerzając i ugruntowując swoją wiedzę w obszarze funkcjonowania administracji publicznej.

Jako reaktor naukowy pragnę serdecznie podziękować wszystkim Autorom tekstów za wkład naukowy, dzięki któremu niniejsza monografia mogła powstać. Serdeczne podziękowania kieruję również do prof. dr hab. Lidii Zacharko za podjęcie wysiłku sprawnego zrecenzowania tekstów zawartych w monografii. Dziękuję również Uczelni, a przede wszystkim Oficynie Wydawniczej „Humanitas” i Pani Redaktor Danucie Dziewięckiej za pomoc w opracowaniu tej publikacji.

Dorota Fleszer

Rozdział I

Zakres przetwarzania informacji w administracji publicznej

Działalność Rzecznika Praw Obywatelskich w zakresie ochrony prywatności

I

Zgodnie z art. 47 Konstytucji RP „każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym”. Przepis ten umieszczony jest w rozdziale II ustawy zasadniczej „Wolności, prawa i obowiązki człowieka i obywatela” w części dotyczącej wolności i praw osobistych. Prawo do prywatności ujmować zatem należy w perspektywie praw człowieka. W literaturze podaje się jednak, że „struktura tego przepisu zdaje się świadczyć, że poszczególne interesy w nim wskazane, tj. »prawo do ochrony prawnej życia prywatnego«, »prawo do ochrony prawnej życia rodzinnego«, »prawo do ochrony prawnej czci i dobrego imienia« wyrażają samodzielne treści normatywne. Każda ze wskazanych gwarancji posiada tym samym – przynajmniej w założeniu – pewien przedmiot, który nie podlega ochronie w ramach innych praw wyrażonych w art. 47 (...). Należy uznać za bardziej przekonujące poszukiwanie normy ogólnej w gwarancji autonomii jednostki niż w trudnym do zdefiniowania »prawie do prywatności«”. Ponadto, niezależnie od rozwiązania, należy odrębnie analizować każdą z gwarancji, podobnie jak odrębnie od gwarancji samostanowienia omawiane są poszczególne przepisy konstytucyjne. Niezależnie od wątpliwości terminologicznych związanych z „prawem do prywatności”, zgodzić się można z tym, że „funkcją prawa do prywatności jest regulowanie przez jednostkę dostępności swojej osoby dla innych. Chodzi o dostępność zarówno w sensie fizycznym (nietykalność cielesna, mir domowy, osobista przestrzeń), jak i dostępność sfery świata wewnętrznego jednostki – jej przeżyć, uczuć i myśli”².

Ze względu na to, że prywatność ujmowana jest z perspektywy praw człowieka, pozostaje ona przedmiotem zainteresowania Rzecznika Praw Obywatelskich. Jest to bowiem organ stojący na straży wolności i praw człowieka i obywatela określonych w konstytucji oraz w innych aktach normatywnych (art. 208 Konstytucji RP). Zgodnie zaś z art. 1 ust. 2 ustawy z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich³ Rzecznik „stoi na straży wolności i praw człowieka i obywatela określonych w Konstytucji Rzeczypospolitej Polskiej oraz w innych aktach normatywnych,

¹ dr; Uniwersytet Pedagogiczny im. KEN w Krakowie, Biuro Rzecznika Praw Obywatelskich.

² A. Mednis, *Prawo do prywatności a interes publiczny*, Wolters Kluwer, Warszawa 2006, s. 93.

³ Tekst jedn. Dz.U. z 2014 r., poz. 1648, ze zm., dalej jako: u.r.p.o.

w tym również na straży realizacji zasady równego traktowania”. Redakcja tych przepisów wskazuje zaś na to, że „zadaniem Rzecznika jest ochrona całokształtu praw i wolności człowieka i obywatela, niezależnie od tego czy są one gwarantowane konstytucyjnie czy też wynikają z innych aktów prawotwórczych”⁴.

Jednym z takich praw jest właśnie prawo do prywatności. Analiza informacji rocznych Rzecznika Praw Obywatelskich potwierdza tezę, że sprawy dotyczące prywatności stanowią istotną część działalności tego organu ochrony prawa⁵. Wskazać należy również, że prawo do prywatności jest uznawane przez Rzecznika za kluczowe w obecnej kadencji⁶.

II

W zakresie ochrony prywatności, tak jak i w każdej innej, Rzecznik Praw Obywatelskich podejmuje działania na wniosek osób lub ich organizacji. Wniosek taki inicjuje postępowanie wyjaśniające w sprawie, w której Rzecznik może podjąć środki przewidziane w art. 11 i nast. u.r.p.o. Jednak istotną rolę odgrywają także tzw. wystąpienia generalne, które mogą być sporządzone w postępowaniu wszczętym przez Rzecznika z urzędu. W tej grupie wyróżnić można wystąpienia dotyczące ochrony prywatności: 1) w obowiązujących przepisach prawnych – Rzecznik postuluje tutaj zmianę przepisów; w tym obszarze Rzecznik wysuwać może również propozycje unormowania pewnych kwestii dotychczas nieuregulowanych przez prawo; 2) w wymiarze prewencyjnym – chodzi tu o „wychwycenie” naruszeń prawo do prywatności w projektach aktów prawnych, nad którymi pracuje parlament.

Podejmowane jednak przez Rzecznika Praw Obywatelskich sprawy z urzędu dotyczą nie tylko projektowanych lub obowiązujących przepisów prawa, ale także są reakcją na zachodzące w sferze publicznej zdarzenia (lub na głośne medialne doniesienia).

Poniżej zaprezentowane zostaną wybrane sprawy dotyczące problemów z prawem do prywatności, podejmowane z urzędu przez Rzecznika Praw Obywatelskich.

⁴ S. Trociuk, *Komentarz do ustawy o Rzeczniku Praw Obywatelskich*, Biuro Rzecznika Praw Obywatelskich, Warszawa 2014, s. 7-8.

⁵ Por. *Informacja o działalności Rzecznika Praw Obywatelskich w roku 2015 oraz o stanie przestrzegania wolności i praw człowieka i obywatela*, Biuletyn Rzecznika Praw Obywatelskich 2016, nr 1, Źródła, s. 73-84; *Informacja o działalności Rzecznika Praw Obywatelskich w roku 2014 oraz o stanie przestrzegania wolności i praw człowieka i obywatela*, Biuletyn Rzecznika Praw Obywatelskich 2015, nr 1, Źródła, s. 77-86; *Informacja o działalności Rzecznika Praw Obywatelskich w roku 2013 oraz o stanie przestrzegania wolności i praw człowieka i obywatela*, Biuletyn Rzecznika Praw Obywatelskich 2014, nr 1, Źródła, s. 70-77.

⁶ Chodzi o kadencję Rzecznika Praw Obywatelskich rozpoczętą w 2015 r., o czym świadczy m.in. dokument A. Bodnara, *Rzecznik Praw Obywatelskich w Polsce – nowa energia na nowe czasy*, dostępny na stronie: naszrzecznik.pl, w którym A. Bodnar wskazał na swoje priorytety. W dokumencie tym wskazano m.in., że problemem jest rzeczywista dostępność środków ochrony prawa do prywatności (s. 9).

III

Jako przykład sprawy dotyczącej ochrony prywatności w obowiązujących przepisach prawnych można podać sprawę dotyczącą ustawy o obywatelstwie polskim⁷. W wystąpieniu do Ministra Spraw Wewnętrznych⁸ wskazano, że zgodnie z art. 56 ust. 1 u.o.p. „wniosek o potwierdzenie posiadania lub utraty obywatelstwa polskiego zawiera dane osoby, której potwierdzenie dotyczy, i jej wstępnych do drugiego stopnia oraz informacje o istotnych okolicznościach niezbędnych do ustalenia stanu faktycznego i prawnego”. Natomiast ustęp 2 tego artykułu zobowiązuje osobę i podmiot występujący z wnioskiem o potwierdzenie posiadania lub utraty obywatelstwa polskiego do dołączenia dokumentów potwierdzających dane i informacje zawarte we wniosku, chyba że uzyskanie tych dokumentów napotyka trudne do przewyciężenia przeszkody. Natomiast wzór wniosku został wprowadzony rozporządzeniem Ministra Spraw Wewnętrznych z dnia 7 sierpnia 2012 r. w sprawie wzoru formularza wniosku o potwierdzenie posiadania lub utraty obywatelstwa polskiego (Dz.U. z 2012 r., poz. 925). To właśnie we wniosku udzielić należy wielu – często nawet bardzo szczegółowych informacji, o których generalnie mowa w art. 56 ust. 1 u.o.p.

W swoim wystąpieniu Rzecznik wskazał, że konstrukcja art. 56 ust. 1 u.o.p. wskazuje, że umieszczone tam dane są wymagane w każdym postępowaniu – w przedmiocie potwierdzenia posiadania lub utraty obywatelstwa polskiego – chodzi więc o każdą sprawę, zarówno prostą i nieskomplikowaną (np. gdy dana osoba z jakichkolwiek powodów nie posiada dokumentu stwierdzającego obywatelstwo polskie, jak dowód osobisty czy dokument paszportowy), jak i w sprawach skomplikowanych (np. potwierdzenie posiadania lub utraty obywatelstwa polskiego dla osób starających się o uzyskanie rekompensaty za tzw. mienie zabużańskie).

Dane konieczne do rozstrzygnięcia dla większości prostych spraw o potwierdzenie posiadania lub utratę obywatelstwa polskiego zawiera część I formularza wniosku w pozycji od A do E, w części II. A życiorys osoby, której wniosek dotyczy i pkt B części III pkt D.

Jak wynika z informacji pozyskanych przez Rzecznika Praw Obywatelskich, dotychczasowa praktyka dotycząca przyjmowania wniosków wykazała, że duże problemy stwarza wypełnienie formularza o potwierdzenie posiadania lub utraty obywatelstwa polskiego, w szczególności dane zawarte w części I, dane F od I do IV (dane dotyczące danych osobowych dziadka i babki ze strony matki i ze strony ojca); dotyczy to zwłaszcza sytuacji, gdy osobie sporządzającej wniosek znane są tylko niektóre dane, np. imię i nazwisko dziadka lub babki. W praktyce wąt-

⁷ Ustawa z dnia 2 kwietnia 2009 r. o obywatelstwie polskim (Dz.U. z 2012 r., poz. 161), dalej jako: u.o.p.

⁸ Wystąpienie z dnia 16 stycznia 2015 r., nr BPK.533.2.2014.GK.