

Milena Gniewaszewska

Akademia Humanistyczno-Ekonomiczna w Łodzi

Bezpieczeństwo państwa w aspekcie ochrony informacji¹

Zarządzanie aktualną, pewną i szybko dostępną informacją jest warunkiem skutecznego działania, decyduje często o powodzeniu lub porażce w osiągnięciu wytyczonego celu. Postęp gospodarczy oraz rozkwit nowatorskich technologii, zwłaszcza informacyjnych, spotęgowały zagrożenie dla sfery prywatności człowieka. Informacja o danych osobowych to kategoria danych o intratnym znaczeniu, dlatego też wymagają one szczególnej kontroli. Bazy danych o instytucjach, firmach i społeczeństwie oraz plany marketingowe i inne stają się drogim produktem, o który bez względu na koszty toczą się zaciekle walki. Zagwarantowanie bezpieczeństwa państwa, a tym samym jego obywateli jest konstytucyjnym obowiązkiem każdego rządu, bez względu na jego stronnictwo polityczne². Dlatego wszystkie państwa tworzą określony system ochrony i zdobywania informacji, na machinę tą składają się zarówno przepisy prawne, jak i odpowiednie przedsięwzięcia organizacyjno-techniczne.

Poczucie bezpieczeństwa to fundamentalna wartość każdego człowieka. „W najbardziej dosłownym znaczeniu bezpieczeństwo jest właściwie identyczne z pewnością i oznacza brak zagrożenia fizycznego albo ochronę przed nim”³. Zagrożeniami dla bezpieczeństwa państwa i jego obywateli mogą być m.in.: rosnąca przestępczość z zakresu terroryzmu, konfliktów militarnych, politycznych, narkomanii, katastrof ekologicznych, nacjonalizmu, konfliktów religijnych i społecznych, jak i cyberprzestępczość. Zapobieganie zagrożeniom to rola państwa przy aktywnym udziale społeczeństwa. Przypuszczalnie każdy z nas choć raz zadał sobie pytanie o rzeczywiste ograniczenia w dostępie do informacji, rozważając,

¹ Fragmenty pracy magisterskiej napisanej pod kierunkiem dr hab. Edyty Pietrzak, prof. AHE w Łodzi na kierunku politologia na Wydziale Humanistycznym Akademii Humanistyczno-Ekonomicznej w Łodzi.

² Art. 146 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz. U. 1997, nr 78, poz. 483.

³ R. Zięba, *Instytucjonalizacja bezpieczeństwa europejskiego: koncepcje – struktury – funkcjonowanie*, Scholar, Warszawa 1999, s. 27.

czy nasz lekarz, a może i spowiednik nie przekazał dalej naszych tajemnic i zwierzeń. Problem ochrony informacji staje się zasadniczy, gdy dotyczy elementów istotnych z punktu widzenia nie tylko obywatela, ale także z pozycji funkcjonowania państwa w promieniu działań wojskowo-obronnych, wywiadowczych, ekonomicznych i gospodarczych.

Celem niniejszej pracy jest przedstawienie podstawowych zasad, czynności, a także procedur postępowania w zakresie ochrony informacji niejawnych, jak i ochrony danych osobowych w aspekcie bezpieczeństwa państwa i jego obywateli. Wiedza specjalistyczna pozyskana poprzez analityczne przyswajanie aktów jurystycznych powoduje umiejętność postrzegania różnorodnych sytuacji przez pryzmat otaczającego nas zagrożenia. Świadomość niebezpieczeństwa, jakie niesie ze sobą ujawnienie chronionych informacji, zapewni bezpieczeństwo naszemu państwu w kontekście jego suwerennej gospodarki, jak i bezpieczeństwa obywateli. W całym systemie zabezpieczeń fizyczno-technicznych zawsze najsłabszym ogniwem jest człowiek.

Wyzwaniem w realizacji badań jest precyzyjne określenie przedmiotu – rozpoznawane w nim zjawiska powinny być porównywalne⁴. Podążając za literaturą przedmiotu, postawiono następującą hipotezę dla badanego obszaru: bezpieczeństwo państwa w aspekcie ochrony informacji jest strategicznym elementem ochrony kraju, ponieważ zarządzanie informacją jest warunkiem skutecznego działania decydującego o powodzeniu lub porażce w dążeniu do wytyczonego celu.

W kolejnych odsłonach pracy poczyniono weryfikację przesłanek zawartych w hipotezie, wykorzystując odpowiednie metody badawcze. W definicyjnym rozumieniu przyjęto, że „przez metodę rozumie się na ogół system założeń i reguł pozwalających na takie uporządkowanie praktycznej lub teoretycznej działalności, aby można było osiągnąć cel, do jakiego się świadomie zmierza”⁵. Zatem konieczne jest poznanie instytucjonalnego środowiska odpowiedzialnego za właściwe funkcjonowanie informacji niejawnych oraz danych osobowych. Wachlarz tychże informacji ujęto w pięciu rozdziałach procesu badawczego.

Problematyka rozdziału pierwszego zajmuje się płaszczyzną formalno-prawną ochrony informacji niejawnych. Pełne zrozumienie pojęć ustawowych umożliwi wytwórcy dokumentu poprawne klasyfikowanie wiadomości, wpływając tym samym na umiejętność w wyborze klauzuli ich nadawania, znoszenia oraz zmiany. Nie bez znaczenia dla bezpieczeństwa przedmiotowej kwestii jest biegłość oceny i wyrażania wątpliwości oraz zastrzeżeń wobec stopnia tajności otrzymanych dokumentów. Należy pamiętać, że zawyżanie i zaniżanie klauzul tajności jest sprzeczne z zapisami przepisu.

Organizacji ochrony i roli służb ochrony państwa, jak i szkoleniom w przedmiotowym zakresie poświęcony jest rozdział drugi. Przedstawiono w nim zasady funkcjonowania kancelarii tajnych i jej zadania oraz postępowanie w sytuacjach zagrożenia dla informacji niejawnych. W tym studium ujęto także zagadnienia związane z rzeczywistymi środkami

⁴ A. Chodubski, *Metodologia jako szczególna wartość badań politologicznych*, „Studia Gdańskie”, t. VI, s. 95, <http://www.studiagdanskieda.pl/tom6/studia%20VI%20chodubski.pdf> [dostęp: 24.04.2016].

⁵ J. Sztumski, *Wstęp do metod badawczych*, Wydawnictwo Śląsk, Katowice 1995, s. 60.

ochrony fizycznej – to ważne przedsięwzięcie, bez którego nie jest możliwe przetwarzanie informacji niejawnych. Dalsza odsłona zawiera materię „bezpieczeństwa osobowego”, która dotyczy rekrutacji osób uprawnionych oraz poszanowania zasad dostępu do informacji niejawnych.

Trzeci rozdział prezentuje serwis wiadomości w ujęciu ustawy o danych osobowych. Ochrona danych osobowych zajmuje się nadzorowaniem wszystkich operacji stosowanych podczas przetwarzania tych danych. Warto zaznaczyć, że z literalnego punktu widzenia za przetwarzanie rozumie się: jakiegokolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie⁶. Nie sposób pracować „na” danych osobowych, jednocześnie ich nie syntetyzując.

Organizacja ochrony danych osobowych to temat rozdziału czwartego. To kwintesencja zakresu ochrony danych osobowych w wymowie zabezpieczenia zarówno osobowego, jak i fizycznego. Każdej osobie, której dane są przetwarzane, przysługują konstytucyjne gwarancje bezpieczeństwa. Nienaruszalnością tychże norm zajmuje się Generalny Inspektor Danych Osobowych, u którego możemy złożyć skargę, aby uruchomić procedury kontrolne w stosunku do wskazanego domniemanego winowajcy.

Piąty rozdział pracy omawia tematykę odpowiedzialności karnej i administracyjnej przewidzianej dla osób, które pozyskały wiedzę w związku z wykonywaniem swoich funkcji czy też obowiązków służbowych, lecz nie tylko, oraz dokonały jej rozpowszechnienia umyślnie bądź nieumyślnie. Wskazano prawne możliwości ścigania i karania sprawców przestępstw przeciwko ochronie informacji niejawnych, jak również przeciw ustawie o danych osobowych. Prawidła kodeksowe normalizują zasady postępowania dla obywatela oraz instytucji, jakim jest polskie demokratyczne państwo prawa.

Podsumowując, stwierdzić należy, że system ochrony informacji niejawnej oraz ochrony danych osobowych ma odpowiednią ochronę proceduralno-organizacyjną wynikającą z unormowań prawnych. Kreowanie efektywnego systemu ochrony dla badanego obszaru ma na celu zapewnienie bezpieczeństwa dla suwerenności, integralności, niepodległości kraju oraz prawnie chronionych interesów obywateli. Jest to niezbywalny obowiązek każdego państwa. Przeciętny obywatel nie jest świadomy zagrożeń, ale każdy chciałby żyć w poczuciu bezpieczeństwa i realizować własne życiowe cele w swoim kraju. Upowszechnienie wartościowych informacji, jakimi są dane niejawne oraz dane osobowe, może spowodować zagrożenie dla bezpieczeństwa państwa i jego obywateli. Służby wywiadowcze, grupy przestępcze i świat biznesu, chcąc zdobyć informacje o newralgicznym znaczeniu, bazują na słabościach i niepowodzeniach ludzi przetwarzających informacje prawnie chronione.

Informacje niejawne stanowią osobliwy rodzaj wiadomości nadzorowany i kontrolowany przez służby ochrony państwa. Dostęp do nich jest ściśle reglamentowany, następuje tylko w stosunku do osób dających rękojmię zachowania tajemnicy, stwierdzonej w ramach szczegółowego postępowania sprawdzającego i tylko w zakresie niezbędnym do wykonywania służby/pracy. Utrata poświadczenia bezpieczeństwa w przypadku naruszenia przepisów jest równoznaczna z wydaleniem ze służby lub z pracy.

⁶ Art. 7 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, tekst jedn. Dz. U. 2014, poz. 1182.

Dane osobowe to informacje własne każdego człowieka i jakiegokolwiek ich przetwarzanie musi być zgodne z intencją ich dysponenta. Nadzór nad całokształtem przedsięwzięcia ich ochrony pełni Główny Inspektor Ochrony Danych. Aby pozyskać legalnie informacje o danych osobowych, należy sprostać roszczeniom ustawy, a najważniejsze z nich to zgoda właściciela na ich przetwarzanie (poza wyjątkami wskazanymi w odrębnych ustawach) zwana zasadą legalności oraz zasadą celowości, jak i merytorycznej poprawności.

W jakimkolwiek systemie ograniczeń, zakazów i nakazów najważniejszym ogniwem jest zawsze człowiek. Warta podkreślenia jest konieczność właściwego kształtowania świadomości społecznej w zakresie tajemnicy chronionej informacji. Wcielenie zasad moralnych i etycznych w życie to element, nad którym warto pracować od najmłodszych lat. W zakresie ochrony informacji niejawnej oraz ochrony danych osobowych stosowane są właściwe normy prawodawstwa, środki fizyczne, techniczne, a zbiory tych elementów posiadają należne certyfikaty.

W tym miejscu można stwierdzić, że hipoteza badanego obszaru o treści: „Bezpieczeństwo państwa w aspekcie ochrony informacji jest strategicznym elementem ochrony kraju, ponieważ zarządzanie informacją jest warunkiem skutecznego działania decydującego o powodzeniu lub porażce w dążeniu do wytyczonego celu”, została zweryfikowana i jest prawdziwa. Wykazano w sposób uporządkowany następstwa zależności zachodzące między zmiennymi zależnymi dla ustalonej hipotezy. Udowodniono tym samym, że bezpieczeństwo państwa w aspekcie ochrony informacji to strategiczny element ochrony kraju. Zarządzanie informacją jest warunkiem skutecznego działania decydującego o powodzeniu lub porażce w dążeniu do wytyczonego celu. Jest to zdanie prawdziwe, a jego autentyczność poświadcza treść rzeczowego opracowania. Państwo jako instytucja dysponuje instrumentami jurystycznymi, które określają metody i formy ochrony dla wspólnego dobra, jakim jest „informacja”. Jak w każdej dziedzinie tak i w tej materii istnieją pewne nieścisłości oraz niedociągnięcia legislatury, które powinny zostać zniwelowane. Odcinkiem najbardziej zagrażającym bezpieczeństwu informacji jest czynnik ludzki, ten element jest kluczowy w aspekcie zabezpieczenia państwa i danych o jego obywatelach.

Bibliografia

Chodubski A., *Metodologia jako szczególna wartość badań politologicznych*, „Studia Gdańskie”, t. VI, <http://www.studiagdanskie.gwsh.gda.pl/tom6/studia%20VI%20chodubski.pdf> [dostęp: 24.04.2016].

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz. U. 1997, nr 78, poz. 483.

Sztumski J., *Wstęp do metod badawczych*, Wydawnictwo Śląsk, Katowice 1995.

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz. U. 2002, nr 101, poz. 926.

Zięba R., *Instytucjonalizacja bezpieczeństwa europejskiego: koncepcje – struktury – funkcjonowanie*, Scholar, Warszawa 1999.