„Polityka i Społeczeństwo" 3(18) / 2020
DOI: 10.15584/polispol.2020.3.8

ARTYKUŁY

Robert Zapart*

TEORIA I PRAKTYKA OCHRONY INFORMACJI NIEJAWNYCH – WYBRANE ZAGADNIENIA DOTYCZĄCE BEZPIECZEŃSTWA INFORMACJI

THEORY AND PRACTICE OF CLASSIFIED INFORMATION PROTECTION – SELECTED ISSUES RELATED TO SECURITY OF INFORMATION

Abstract

A key issue for every state is the protection of information about its resources that should not be made public for various reasons, including national security reasons in particular. The article discusses the problem of its lawful protection against unauthorised disclosure in relation to emergency situations. The author claims that the discrepancies in this area result from both the provisions of the Act on the Protection of Classified Information, which allows for excessive arbitrariness, and the shortages caused by the actions of persons working in the public administration sector. A slight amendment to the current legislation, combined with training on the marking of materials that require actual protection, may ensure the systemic enhancement of the protection of classified information and thus, national security, without excessively limiting the transparency of public life.

Keywords: public administration, politics, democratic rule of law, classified information, security

Wstęp

Bezpieczeństwo państwa jest kwestią, której nie sposób rozważać z pominięciem szeregu procesów informacyjnych związanych z decydowaniem w sprawach publicznych, a także instrumentów identyfikujących, a następnie chroniących jego interesy w zmieniających się warunkach współczesnego świata. Uzasadnione jest zatem postrzeganie bezpieczeństwa informacyjnego jako składowej większego systemu narodowej obrony opartego na wartościach wypływających z pojęcia racji

* Instytut Nauk o Polityce, Uniwersytet Rzeszowski, al. mjr. W. Kopisto 2a, 35-959 Rzeszów, e-mail: robert.zapart@onet.poczta.pl, ORCID ID: 0000-0002-3590-1189.

stanu. W następstwie tak przyjętego stanowiska pojawia się potrzeba przyjęcia norm i metod wspierających jego skuteczną ochronę, co odbywa się kosztem jawności życia publicznego. Towarzyszą temu dylematy związane z próbami pogodzenia praw wspólnoty do życia bez zagrożeń z prawami jednostek do wiedzy o działaniach władz odpowiedzialnych za realizację tych uprawnień, co oddaje skalę wyzwań związanych z odpowiedzialną realizacją krajowej polityki bezpieczeństwa (Zalewski, 2013, s. 13). Prewencyjne działania w tym zakresie polegają między innymi na ukrywaniu informacji, kontroli dostępu, ocenie oraz likwidowaniu słabych punktów związanych z ich przetwarzaniem (Żebrowski, Żmigrodzki, 2017, s. 505). W międzynarodowym i polskim ustawodawstwie dopuszcza się wyjątki od zasady jawności życia publicznego, przy czym muszą one być określone w ustawie i dotyczyć fundamentów bezpieczeństwa państwa lub innych prawnie chronionych interesów osób i podmiotów. Głównym aktem prawnym wspierającym to pierwsze odstępstwo jest ustawa o ochronie informacji niejawnych (Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji…). Jej znowelizowanie w 2010 r. pozwoliło między innymi na odejście od obowiązującego od 1999 r. dwustopniowego podziału na informacje stanowiące tajemnicę służbową oraz państwową, a także rezygnację z praktycznego załącznika wspierającego ich oznaczanie adekwatnymi do poziomu zagrożenia klauzulami ochrony (Smykla, 2011, s. 118–120).

Celem poniższych rozważań naukowych będzie próba zbadania efektów wprowadzonych dekadę wcześniej w systemie ochrony informacji niejawnych zmian z perspektywy bezpieczeństwa państwa, przy czym ich wiodącą częścią będzie wskazanie rozbieżności pomiędzy opartą na przepisach prawa teorią a praktyką oraz sposobów ich eliminacji. W ocenie autora nadmierna dowolność w oznaczaniu klauzulami niejawności informacji oraz spadający poziom świadomości osób zajmujących się powyższymi zadaniami, a także niewielka skala prowadzonych w tym obszarze zewnętrznych kontroli może ułatwiać wrogim podmiotom uzyskiwanie wiedzy o stanie bezpieczeństwa państwa. Pomocne w uzasadnieniu powyższej tezy będą analiza systemowa oraz metody, eksplanacyjna i porównawcza, a także wykorzystana w artykule literatura przedmiotu.

Identyfikacja i klasyfikacja informacji podlegających ochronie

We współczesnym świecie informacja jest jednym z wykorzystywanych przez państwo instrumentów w relacjach zewnętrznych i wewnętrznych wspierających ciągłość jego podmiotowego istnienia. Jest niematerialnym dobrem strategicznym rozpatrywanym w kategoriach jego bezpieczeństwa narażonym na zniszczenie, manipulację czy też

kradzież w ramach celowego działania przeciwnika (Żarkowski, 2018, s. 35; Zalewski, 2018, s. 5 i n.). Zdefiniowanie zasobów i interesów wymagających ochrony, jak również ocena, czy występuje ryzyko narażenia ich na uszczerbek, wiąże się z przyjętym przez państwo systemem aksjonormatywnym. Zatem zasady, a w szczególności zakres i skuteczność ochrony informacji niejawnych, są pochodną artykułowanych przez państwo interesów w sferze jego bezpieczeństwa i wiążą się zarówno z przyjętą przez nie strategią w tym zakresie, jak i zawartymi umowami międzynarodowymi wzmacniającymi relacje pod kątem udzielenia ewentualnej pomocy w przypadku zewnętrznego zagrożenia. Z uwagi na wynikające z tego tytułu negatywne następstwa dla jawności życia publicznego, wprowadzane ograniczenia powinny z odpowiednim uzasadnieniem nawiązywać do obrony fundamentów suwerenności wspólnoty. Mając na względzie podstawy funkcjonowania demokratycznego państwa prawa, musi to być synteza dwóch wartości, praw jednostek do wiedzy o aktywności władz publicznych oraz praw wspólnoty, która oczekuje od nich skutecznego przeciwdziałania zagrożeniom dla jej przetrwania, czasami kosztem tych pierwszych. Niestety może się także w tym miejscu pojawić niebezpieczeństwo nadużywania przez rządzących obywatelskiego zaufania w przypadku, gdy ograniczenia w dostępie do informacji są wprowadzone na bazie zmanipulowanych na ich użytek przesłanek. Tendencja do poszerzania przez nich własnych kompetencji, pod pozorem eliminacji potencjalnych lub występujących zagrożeń, jest niepożądanym zjawiskiem prowadzącym do regresu społecznego zainteresowania bezpieczeństwem państwa. Zatem zasięg i poziom skuteczności takich działań odzwierciedla w praktyce realność kontroli nad poczynaniami władzy i stopień jawności życia publicznego. W dojrzałych demokracjach powinniśmy obserwować odwoływanie się do racji stanu w przypadku ochrony informacji, którym przypisuje się fundamentalne znaczenie dla bezpieczeństwa państwa. Taki przekaz ma wtedy znamiona racjonalnego i wyważonego, a przede wszystkim wiarygodnego (Zapart, 2019, s. 194–195). W polskim systemie prawnym w podstawach definiują ten obszar Konstytucja RP oraz oparte na jej zapisach ustawy i niższe akty wykonawcze. Generalnie podkreśla się w nich znaczenie obywateli dla trwania Rzeczypospolitej Polskiej jako dobra wspólnego, natomiast w odniesieniu do władzy wykonawczej, wyznacza się zadania związane z ochroną całokształtu ich życiowych interesów (Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997, art. 1; Zalewski, 2009, s. 25; Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej z 17 maja 2020). Następstwem przyjmowanych w tym zakresie rozwiązań jest, dopuszczone przez ustawę zasadniczą, ograniczenie praw i wol-

ności jednostek do uzyskiwania oraz rozpowszechniania informacji o działalności organów władzy publicznej, któremu towarzyszy powoływanie się na bezpieczeństwo państwa i porządek publiczny, a także ochronę środowiska, zdrowia, moralności publicznej, albo wolności i praw innych osób (art. 54 i art. 61 Konstytucji RP). Konsekwencją powyższych zapisów jest między innymi nakaz ścisłej i restrykcyjnej wykładni przepisów stanowiących podstawę do zawężenia tych uprawnień (Dana, 2016, s. 77). Aktualnie powyższe zagadnienie reguluje ustawa o ochronie informacji niejawnych, która weszła w życie z dniem 2 stycznia 2011 r. (Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji…). Przesłanki jej funkcjonowania są powiązane z fundamentalnymi interesami bezpieczeństwa państwa, co bezpośrednio wpływa na zasady organizacji całego systemu ochrony (legalizm, obiektywizm, bezstronność, ograniczoność dostępu, hierarchiczność organów ochrony, kontrola, instancyjność, pierwszeństwo informacji niejawnych) oraz sposób ich klasyfikowania (Polok, 2006, s. 79–94). Wyróżnia ją także stabilność zakreślonego celu oraz wskazanie formalnych podstaw jego osiągnięcia i odpowiedzialnych za końcowy rezultat struktur (Topolewski, 2013, s. 27). Ponad dekadę temu, w ramach poprzednio obowiązującej ustawy o podobnej nazwie obowiązującej od 1999 r., stosowano podział na informacje stanowiące tajemnicę państwową (ściśle tajne oraz tajne) oraz tajemnicę służbową (poufne i zastrzeżone). Obecne definicje wiążą nieuprawnione ujawnienie z wielkością potencjalnej szkody dla państwa, i tak kolejno:

1. ściśle tajne – może spowodować wyjątkowo poważne szkody dla Rzeczypospolitej Polskiej;
2. tajne – poważne szkody dla Rzeczypospolitej Polskiej;
3. poufne – szkody dla Rzeczypospolitej Polskiej;
4. zastrzeżone – może szkodliwie wpłynąć na wykonywanie przez organy władzy publicznej zadań w zakresie obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczypospolitej Polskiej (Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji…, art. 5; Hoc, 2012, s. 27–33; Stankowska, 2014, s. 32–38).

Najwyższe klauzule ochrony informacji zostały zarezerwowane dla obronności, polityki międzynarodowej, podstawowych interesów gospodarczych Rzeczypospolitej Polskiej czy też czynności operacyjno-rozpoznawczych uprawnionych służb, natomiast najniższe dla mniej istotnych z perspektywy bezpieczeństwa aspektów jej funkcjonowania. Zatem kryterium, jakim powinien się kierować ich wytwórca, jest rodzaj potencjalnie poniesionej szkody związany z oceną ryzyka jej zaistnienia. Powyższe rozwiązanie miało służyć uproszczeniu całego systemu ochro-

ny, a tym samym zmniejszyć liczbę oznaczonych najwyższymi klauzulami materiałów i obniżyć koszty ich technicznego i osobowego zabezpieczenia (głównie w postaci rozbudowanych kancelarii tajnych), a także przenieść prawnie chronione wcześniej przez poprzednią ustawę interesy obywateli do odrębnych unormowań obejmujących informacje prawnie chronione (np. tajemnica bankowa, adwokacka, dziennikarska, itd.). Użycie w nich jednak nieostrych sformułowań, by wymienić „poważne szkody", „szkodliwy wpływ", „duży uszczerbek", doprowadziło do sytuacji, że te same informacje mogą mieć w różnych podmiotach inne klauzule niejawności, a w skrajnych i nieodosobnionych przypadkach, część z nich może być w jednych chroniona, natomiast w drugich pozostawać jawna. Spory w tym zakresie miały rozstrzygać posiadające uprawnienia nadzoru – Agencja Bezpieczeństwa Wewnętrznego, natomiast w odniesieniu do jednostek podległych Ministerstwu Obrony Narodowej – Służba Kontrwywiadu Wojskowego. Nie zawsze jednak są one w stanie odpowiednio szybko zareagować z uwagi na pierwotną samodzielność wielu cywilnych i wojskowych podmiotów w oznaczaniu materiałów klauzulami niejawności. Krótko po wprowadzeniu obecnej ustawy podnoszono już problem zbyt szybkiego wyeliminowania z praktycznego stosowania obowiązującego w poprzednich unormowaniach załącznika wspomagającego ten proces, przywołując na przykład potencjalnie negatywne następstwa związane z ochroną obiektów infrastruktury krytycznej wpisanych do rejestrów wojewodów (Ryszkowski, Ryszkowska, Ryszkowska, 2011, s. 245–246). Szereg innych wątpliwości w tym zakresie zgłaszano jeszcze na etapie legislacji, jednakże nie zostały one uwzględnione i pozostają przyczyną obecnych problemów (Stankowska, 2014, s. 32–38).

Zarządzanie ochroną informacji niejawnych

Przepisy Ustawy o ochronie informacji niejawnych mają zastosowanie do organów władzy publicznej, jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych, Narodowego Banku Polskiego, państwowych osób prawnych i państwowych jednostek organizacyjnych, jednostek organizacyjnych podległych organom władzy publicznej lub nadzorowanych przez te organy, przedsiębiorców zamierzających ubiegać się albo ubiegających się o zawarcie umów związanych z dostępem do informacji niejawnych lub wykonujących takie umowy albo wykonujących na podstawie przepisów prawa zadania związane z dostępem do informacji niejawnych i nie naruszają, z pewnymi zastrzeżeniami, przepisów innych ustaw o ochronie

tajemnicy zawodowej lub innych tajemnic prawnie chronionych (Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji…, art. 1). Nadanie klauzul niejawności przetwarzanym w nich materiałom leży w kompetencjach osób uprawnionych do ich oznaczenia (Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji…, art. 6). Mogą one zatem fakultatywnie określić termin zniesienia lub zmiany poziomu ich ochrony. Służy temu przeprowadzona odpowiednią metodą ocena wystąpienia ryzyka szkodliwych dla państwa następstw nieuprawnionego ujawnienia tych informacji. Obecna ustawa definiuje przywoływane ryzyko jako „kombinację wystąpienia zdarzenia niepożądanego i jego konsekwencji", szacowanie określa jako „całościowy proces analizy i oceny ryzyka", zarządzanie nim jako „skoordynowane działania w zakresie zarządzania bezpieczeństwem informacji z uwzględnieniem ryzyka" (Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji…, art. 2). W przeszłości podejmowano polemikę z autorami wspomnianych ustawowych terminów, wskazując na ich niepotrzebne zawężenie w porównaniu do wzorca, którym była, bazująca na brytyjskich rozwiązaniach systemowych opisanych na przykład w BS 25999, norma PN-ISO/IEC 27005:2010. Zarzuty ogniskowały się wokół braku w definicji ryzyka zapisów o istnieniu zagrożeń i podatności na nie, sposobów jego pomiaru (iloraz prawdopodobieństwa zdarzenia i jego następstw), nieobecności przywołania w jego szacowaniu identyfikacji zagrożeń, czyli formalnego wymogu sporządzenia kompletnej i wyczerpującej dla informacji niejawnych listy z nimi związanej, co może rodzić problemy z właściwym przygotowaniem ich zabezpieczeń, a także w odniesieniu do zarządzania ryzykiem, wskazówki, że powinien to być proces systematyczny i ciągły, obejmujący planowanie, organizowanie i kontrolowanie zasobów, którego celem winno być przekonanie, że ryzyko pozostaje w dopuszczalnych, przez świadome następstw swoich decyzji kompetentne do jego oceny osoby, granicach (Iwaszko, 2012, s. 29, 86–87). Powyższe działania przypisano w ustawie pełnomocnikom ochrony informacji niejawnych, którzy po pozytywnym zakończeniu realizowanych przez ABW lub SKW szkoleń zarządzają ryzykiem bezpieczeństwa informacji, w tym jego szacowaniem. Kierownicy jednostek organizacyjnych zostali natomiast zobligowani do zatwierdzenia przedłożonej im przez tych wyżej wymienionych dokumentacji określającej poziom zagrożeń związanych z nieuprawnionym dostępem lub potencjalną utratą chronionych informacji (Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji…, art. 15). W jej przygotowaniu pomocne mogą być normy: PN-ISO/IEC 27005:2018 Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji (Information technology – Security techniques –

Information security risk management) oraz PN-ISO/IEC 27001: 2017-06 System Zarządzania Bezpieczeństwem Informacji (Information Security Management System, w skrócie ISMS), a także CRAAM – Metoda analizy i zarządzania ryzykiem CCTA (Crisis Risk Analysis and Management Method CCTT) wykorzystującą wcześniej przywoływane i przygotowane tabele z macierzami. Wymagania związane z bezpieczeństwem informacji obejmują w procesie zarządzania ryzykiem nieuprawnionego ujawnienia informacji zachowanie:

a) poufności – informacja nie jest udostępniania nieuprawnionym osobom lub podmiotom;
b) integralności – zapewnienie dokładności i kompletności chronionych aktywów;
c) dostępności – użyteczność dla upoważnionych do przetwarzania (Anzel, 2011, s. 8).

Najważniejsze w całym procesie jest zidentyfikowanie celów jednostki organizacyjnej jako całości i wyznaczenie jej komórkom odpowiednich zadań z zakresu ochrony informacji, a następnie zidentyfikowanie możliwych zagrożeń wynikających z jej aktywności. Powyższe działania muszą prowadzić do oszacowania prawdopodobieństwa wystąpienia niepożądanego zdarzenia i ustalenia wartości skutków jego wystąpienia. Strata może mieć wymiar finansowy, prawny, militarny lub wizerunkowy i stanowić przyczynę poważnych problemów danego podmiotu, a w następstwie także bezpieczeństwa państwa. Każdorazowo winna być ona określana w ramach analizy dostępnych z różnych źródeł informacji lub innych planowanych zewnętrznych projekcji z podziałem na ryzyka istotne i nieistotne. Poprzedza ją:

a) rozpoznanie i opis środowiska;
b) identyfikacja i oszacowanie wartości posiadanych informacji związanych z bezpieczeństwem państwa, pod kątem ich ochrony;
c) identyfikacja zagrożeń (środowisko globalne i lokalne) i określenie poziomu ich występowania (losowych i celowych);
d) określenie podatności na ryzyka ewentualnego ujawnienia i zweryfikowania ich poziomu;
e) identyfikacja i szacowanie ryzyka wystąpienia zagrożenia na poufność, integralność i dostępność.

Każda z jednostek organizacyjnych ma prawo tworzyć dostosowaną do potrzeb i specyfiki działalności własną metodologię zarządzania ryzykiem, biorąc odpowiedzialność za następstwa popełnionych błędów w tym zakresie (Anzel, 2011, s. 11). Dodajmy, że kierownicy jednostek organizacyjnych są zobowiązani do przeprowadzania, nie rzadziej niż raz na pięć lat, przeglądu wszystkich materiałów niejawnych pod kątem

ich dalszej ochrony. Ewentualny nadzór w tym zakresie należy do ABW lub SKW, przy czym w kontekście możliwych błędów będzie się on odnosił do neutralizacji następstw występującej szkody i korekty procedur na przyszłość, a nie bieżącej analizy prawidłowości ujawnień materiałów. Kompetencjami kontrolnymi w wybranych obszarach ochrony informacji niejawnych dysponuje również Najwyższa Izba Kontroli.

Pomiędzy teorią a praktyką

Przyjęte dekadę temu rozwiązania niewątpliwie wpłynęły na zakres ograniczeń jawności życia publicznego, zmniejszyły koszty ochrony informacji, jednakże równocześnie ujawniły problemy z praktycznym stosowaniem przepisów, które mogą negatywnie w niektórych przypadkach wpływać na bezpieczeństwo państwa. Stosunkowo nietrudno, przeszukując media, znaleźć przykłady niekonsekwencji w oznakowaniu informacji z pokrewnych sobie obszarów bezpieczeństwa. Porównajmy dla przykładu zasady ochrony informacji dotyczące poziomu wyszkolenia naszych żołnierzy pochodzące z dwóch różnych źródeł. Najwyższa Izba Kontroli opublikowała na swoich stronach internetowych informację o wynikach kontroli „Szkolenie podoficerów i szeregowych zawodowych w jednostkach szkoleniowych" w Siłach Zbrojnych Rzeczypospolitej Polskiej. Analizie poddano wskazanych enumeratywnie dziewięć centrów szkoleniowych realizujących swoje zadania w latach 2016–2018. W syntezie wyników kontroli wskazano na niski, od 63% do 66%, wskaźnik zaspokojenia potrzeb szkoleniowych, niepełne ukompletowanie w sprzęt etatowy, „przypadki nierzetelnego prowadzenia dokumentacji szkoleniowej" oraz „problemy z zapewnieniem podstawowych materiałów i środków technicznych służących szkoleniu, takich jak amunicja strzelecka ślepa, lont prochowy, petardy, ręczne granaty dymne i inne środki pozoracji pola walki, niezbędnych do prawidłowej realizacji programów szkoleń (co ograniczało zakres umiejętności nabywanych w ich trakcie przez żołnierzy)" (*Szkolenie podoficerów i szeregowych*…, 2018). W ocenie NIK spośród czterech programów wojskowych poddanych analizie, ten obejmujący kształcenie ogólne kandydatów na podoficerów zawodowych w ograniczonym stopniu zapewniał słuchaczom możliwości wykazania się przygotowaniem do dowodzenia w czasie pokoju, kryzysu i wojny oraz nie zapewniał im możliwości wykazania się umiejętnościami szkolenia i wychowawczego oddziaływania na podwładnych. Pozostałe również nie pozwalały kadetom w pełni przygotować się do sprawowania obowiązków na stanowisku dowódcy wraz z opanowaniem przez nich umiejętności bojowych. Zarzucono także

podmiotom odpowiedzialnym za ich aktualizację brak „analiz i badań skuteczności szkolenia żołnierzy w jednostkach szkolnictwa wojskowego z zastosowaniem badań ankietowych wśród przeszkolonych żołnierzy i ich przełożonych" (*Szkolenie podoficerów i szeregowych*…, 2018). Opublikowany raport Najwyższej Izby Kontroli, obligatoryjnie badającej działalność organów administracji rządowej, Narodowego Banku Polskiego, państwowych osób prawnych i innych jednostek organizacyjnych z punktu widzenia legalności, gospodarności, celowości i rzetelności (Bodio, Borkowski, Demendecki, 2013, s. 263; Serafin, Szmulik, 2007, s. 238) wskazywał na zaniedbania systemowe w Siłach Zbrojnych RP i nakazywał podjęcie skoordynowanych działań naprawczych „w procesie szkolenia żołnierzy zawodowych" (*Szkolenie podoficerów i szeregowych*…, 2018).

Za materiał porównawczy w obszarze szkolenia wojskowego posłużą tezy z napisanej i przedstawionej do obrony w Akademii Wojsk Lądowych we Wrocławiu pracy doktorskiej. Według doniesień jednego z portali internetowych z 2019 r., niski poziom kształcenia wojskowego na wspomnianej uczelni miały potwierdzać przeprowadzone przez doktorantkę, a od 2014 r. wykładowczynię, badania ankietowe wśród jej elewów. Okazało się, że o ile do AWL trafiają aktywni, zmotywowani młodzi ludzie, to po kilku latach nauki ich kompetencje przywódcze drastycznie maleją. Zaufanie do przełożonego spada o 41%, szacunek do symboli narodowych o 35%, a lojalność wobec przełożonego o 25%. Władze uczelni, dostrzegając negatywne konsekwencje opublikowania wyników badań, zamierzały według doniesień medialnych zmusić autorkę do korekty pracy doktorskiej, a gdy postanowiła wycofać dysertację i otworzyć przewód na uczelni cywilnej, podjęły kroki zmierzające do oznaczenia jej klauzulą niejawności, powołując się na bezpieczeństwo państwa (Interpelacja nr 31501…, 2020; *Jeśli pani to ujawni*…, 2019).

Interesująco pod kątem omawianych problemów wyglądała niedawna polemika pomiędzy pracownikami Głównego Inspektoratu Sanitarnego w związku w wykryciem w Polsce pierwszego przypadku zachorowania na COVID-19. Szefowej słubickiego sanepidu, według jej słów, zarzucono między innymi naruszenie ustawy o ochronie informacji niejawnej, a w następstwie miano zażądać odwołania. Dla dotkniętej zarzutami osoby było to całkowicie niezrozumiałe, natomiast w oficjalnych wypowiedziach wskazano na naruszenie „pragmatyki służbowej" oraz unijnego rozporządzenia o ochronie danych osobowych (*Dyrektor sanepidu w Słubicach…*, 2020; Piegza, 2020). Mamy zatem do czynienia z pewnym dwugłosem w tej sprawie, który trudno jednoznacznie rozstrzy-

gnąć, aczkolwiek rzeczona informacja o pojawieniu się w kraju koronawirusa mogła w świetle ustawy o ochronie informacji niejawnych, z powołaniem się na jedną z niższych klauzul czasowo, pozostawać poza sferą dostępności publicznej.

Porównując tak stosunkowo sobie bliskie tematycznie przykłady, dostrzegamy pewne niespójności w zasadach ochrony. Dotyczy to głównie właściwej identyfikacji wartości posiadanych informacji, w następstwie czego pojawiają się błędy w szacowaniu ryzyka, które winno być powiązane z oceną stanu zagrożenia państwa. Przywołany jako pierwszy raport NIK ma status jawny, natomiast drugi materiał miał zostać objęty klauzulami niejawności przez uczelnię wojskową. Dodajmy, że w świetle wcześniej obowiązujących rozwiązań prawnych obydwie informacje mogłyby wypełniać wymogi ochrony w świetle wykazu rodzaju informacji oznaczonych klauzulą „ściśle tajne" (Ustawa z dnia 22 stycznia 1999 o ochronie informacji niejawnych. Załącznik nr 1). Nietrudno znaleźć kolejne przykłady podobnych rozbieżności w oznaczeniu materiałów. Generalnie ich przyczyn należy doszukiwać się, w dopuszczalnej ustawą, nadmiernej elastyczności w oznaczaniu dokumentów i brakach w szkoleniu osób ją stosujących. Zawiodły mechanizmy właściwej identyfikacji informacji i oszacowania ich wartości, które prawdopodobnie nie poddano odpowiednio wnikliwej kontroli. Nie można także wykluczyć pozamerytorycznych decyzji w tym względzie związanych z partykularnymi interesami lub polityką. Nieco więcej światła na niedomaganie całego systemu ochrony informacji niejawnych rzuca fakt, że od momentu wejścia w życie w 2011 r. nowej ustawy Najwyższa Izba Kontroli nie przeprowadziła kompleksowej weryfikacji prawidłowości działań administracji publicznej w tym obszarze bezpieczeństwa państwa. Ostatnia tego rodzaju systemowa kontrola miała miejsce w latach 2003–2004 i obejmowała urzędy wojewódzkie oraz marszałkowskie w zakresie prawidłowości przestrzegania przepisów dotyczących ochrony informacji niejawnych stanowiących tajemnicę służbową (Informacja o wynikach kontroli…, 2005).

Po tym okresie, pomimo że ta wcześniejsza przyniosła negatywne oceny dla wskazanych podmiotów, sporadycznie kontrolowano ten obszar bezpieczeństwa państwa, ostatnio w styczniu 2009 r. (Prawidłowość przestrzegania w Starostwie…, 2009). Przez kolejną dekadę, już w okresie obowiązywania nowej ustawy, NIK nie podjęła żadnych kompleksowych działań wobec administracji publicznej dotyczących właściwej ochrony informacji niejawnych. Miały one jedynie miejsce w odniesieniu do wybranych podmiotów najsilniej związanych z bezpieczeństwem państwa, a wnioski wypływające z ich kontroli muszą w całości lub w części pozostać niejawne (pełne wersje raportów zostały dostarczone najwyższym osobom w państwie). Powyższe ustalenia autora stawiają pod znakiem zapytania

efektywność kompleksowej ochrony informacji niejawnych w Polsce, co sprawia, że pojawiające się w tej przestrzeni błędy ułatwiają przeciwnikom zajęcie dogodniejszej pozycji w ramach bieżącej walki informacyjnej (Żebrowski, 2016, s. 277–280). Relatywizowanie przez rządzących tego typu zagrożeń i sposobów ich eliminowania może przynieść w przyszłości niepożądane konsekwencje dla bezpieczeństwa państwa.

Zakończenie

Fundamentalną zasadą demokratycznego państwa prawnego pozostaje prawo obywateli do uzyskiwania informacji o działalności jego organów. Towarzyszy jej zwrotny problem aktywności tych ostatnich zobowiązanych do ochrony żywotnych interesów całej wspólnoty kosztem uprawnień jednostki. Wypełnieniu powyższego zadania służy wyodrębnienie wartościowych dla bezpieczeństwa państwa zasobów informacji wymagających szczególnej ochrony przed szkodliwym dla niego ujawnieniem, które precyzuje ustawa o ochronie informacji niejawnych. Po dekadzie od jej przyjęcia warto się pochylić nad wnioskami płynącymi z nabytych doświadczeń wspartych analizą przykładów odzwierciedlających jej niedoskonałości. Z pewnością pożądane byłoby zmniejszenie stopnia ogólności zawartych w niej sformułowań, być może z jednoczesnym rozważeniem włączenia do systemu normatywnego praktycznych przewodników, jak to ma miejsce w kilku krajach europejskich (Bułgaria, Rosja, Ukraina, Węgry, Czechy, Słowacja), czy też w Stanach Zjednoczonych (tam określono 10 obszarów tematycznych), chociaż nie jest to też regułą, bowiem w wielu krajach Unii Europejskiej przepisy pozostają podobnie elastyczne i na zbliżonym poziomie ogólności (Hoc, 2010, s. 92–96). Dopuszczalną alternatywą może być promowanie innych rozwiązań, w tym dodatkowych szkoleń dla osób odpowiedzialnych za nadawanie klauzul niejawności, a także częstszych kontroli prowadzonych przez nadzorującą w kraju ochronę informacji niejawnych ABW oraz odpowiedzialną za właściwe wykonywanie przez administrację publiczną swoich zadań NIK, które wyeliminują lub przynajmniej ograniczą niepożądane dla systemu bezpieczeństwa informacyjnego państwa zjawiska, nie naruszając przy tym zasady jawności życia publicznego.

Bibliografia

Anzel, M. (2011). *Szacowanie ryzyka oraz zarządzanie ryzykiem w świetle nowej ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. Przykłady metody analizy ryzyka opartej na gotowych macierzach*, Poznań: ONE.

Bodio, J., Borkowski, G., Demendecki, T. (2013). *Ustrój organów ochrony prawnej, część szczegółowa*. Warszawa: Wolters Kluwer Polska.

Dana, A. (2016), System ochrony informacji niejawnych. W: S. Topolewski (red.), *Ochrona informacji niejawnych w XXI wieku*. Siedlce: UPH.

Gazeta.pl. (2020). MLZ: Dyrektor sanepidu w Słubicach: Nie przekazałam przecież tajnych danych obcemu wywiadowi. Pobrane z: https://wiadomosci.gazeta.pl/ wiadomosci/7,114883,25763857,dyrektor-sanepidu-w-slubicach-nie-przekazalam-przeciez-tajnych.html.

Hoc, S. (2010). *Ustawa o ochronie informacji niejawnych. Komentarz*, Warszawa: LexisNexis.

Hoc, S. (2012). *Karnoprawna ochrona informacji*. Opole: Wydawnictwo Uniwersytetu Opolskiego.

Informacja o wynikach kontroli prawidłowości przestrzegania w urzędach wojewódzkich i urzędach marszałkowskich przepisów dotyczących ochrony informacji niejawnych, stanowiących tajemnicę służbową. (2005). Pobrane z: www.nik.gov.pl › pobierz,px_2005158.pdf,typ,k.pdf .

Informacja o wynikach kontroli. Szkolenie podoficerów i szeregowych zawodowych w jednostkach szkoleniowych (2018), https://www.nik.gov.pl/kontrole/P/17/035/.

Interpelacja nr 31501 do ministra obrony narodowej w sprawie fali odejść studentów z Akademii Wojsk Lądowych we Wrocławiu oraz próby zafałszowania badań dotyczących spadku kompetencji przywódczych po kilku latach studiów w AWL, (2019), http://www.sejm.gov.pl/sejm8.nsf/InterpelacjaTresc.xsp?key=BCEHKR.

Iwaszko, I. (2012). *Ochrona informacji niejawnych w praktyce*. Wrocław: Presscom.

Jarosław Pinkas ostro o wypowiedzi inspektor w Słubicach: domagamy się odwołania, Szymon Piegza, (2020), onet.pl, https://wiadomosci.onet.pl/tylko-w-onecie/koronawirus-w-polsce-szef-gis-jaroslaw-pinkas-o-wypowiedzi-inspektor-w-slubicach/ dp8trrk.

„Jeśli pani to ujawni będzie katastrofa". Jak wojskowa uczelnia próbowała fałszować badania, (2019), https://wiadomosci.onet.pl/tylko-w-onecie/jesli-pani-to-ujawni-bedzie-katastrofa-jak-wojskowa-uczelnia-probowala-falszowac/58w1db9.

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. 1997 poz. 483 z późn. zm.).

Polok, M. (2006), *Ochrona tajemnicy państwowej i tajemnicy służbowej w polskim systemie prawnym.* Warszawa: LexisNexis.

Prawidłowość przestrzegania w Starostwie Powiatowym w Hajnówce przepisów dotyczących ochrony informacji niejawnych, stanowiących tajemnicę służbową, (2009), https://www.nik.gov.pl/kontrole/S/08/004/lbi/.

Ryszkowski, W.P., Ryszkowska, M.U., Ryszkowska, M.H. (2011). *O wybranych tajemnicach – bez tajemnic*. Katowice: Instytut Ochrony Informacji i Danych Osobowych.

Smykla, A. (2011), Zmiany w przepisach dotyczących ogólnych zasad systemu oraz klasyfikowania informacji niejawnych. W: Nawrocki (red.), *Ochrona informacji niejawnych. Poradnik praktyczny dla osób i instytucji przetwarzających informacje niejawne*. Emów: ABW.

Stankowska, I. (2014), *Ustawa o ochronie informacji niejawnych*. Warszawa: LexisNexis.

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej z 17 maja 2020 roku. Warszawa: Biuro Bezpieczeństwa Narodowego.

Serafin, S., Szmulik, B. (2007), *Organy ochrony prawnej*, Warszawa: C.H.Beck.
Topolewski, S. (2013). System ochrony informacji niejawnych. W: M. Kubiak, S. Topolewski (red.), *Ochrona informacji niejawnych. Teoria i praktyka*. Siedlce: UPH.
Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. 2010 nr 182, poz. 1228 z późniejszymi zmianami).
Zalewski, S. (2009). *Dylematy ochrony informacji niejawnych*. Katowice: Krajowe Stowarzyszenie Ochrony Informacji Niejawnych.
Zalewski, S. (2013). Informacje niejawne we współczesnym świecie. W: M. Kubiak, S. Topolewski (red.), *Ochrona informacji niejawnych. Teoria i praktyka*. Siedlce: UPH.
Zalewski, S. (2018). *Informacje niejawne we współczesnym państwie.* Warszawa: Editions Spotkania.
Zapart, R. (2019), Polityka a ochrona informacji niejawnych. W poszukiwaniu nadrzędnych wartości w państwie w obliczu zewnętrznego zagrożenia. W: S. Topolewski (red.), *Informacje prawnie chronione-wybrane zagadnienia*. Siedlce: UPH.
Żarkowski, P. (2018), Ochrona informacji niejawnych jako instrument zarządzania bezpieczeństwem państwa. W: M. Kubiak, S. Topolewski (red.), *Współczesne wyzwania i zagrożenia wobec ochrony informacji niejawnych i danych osobowych*, Siedlce-Warszawa: UPH.
Żebrowski, A. (2016), *Walka informacyjna w asymetrycznym środowisku bezpieczeństwa międzynarodowego. Wybrane problemy*, Kraków: UP.
Żebrowski, A., Żmigrodzki, R. (2017), *Informacja jednym z elementów bezpieczeństwa państwa. Wybrane aspekty*, Kraków–Warszawa: Sztafeta.

Data przekazania tekstu: 29.11.2020 r., data zaakceptowania: 10.12.2020 r.