aut. Fundacja Insytut Bezpieczeństwa i Strategii
15.08.2019

JAK UNIEMOŻLIWIĆ SŁUŻBOM ZAWŁASZCZENIE SYSTEMU OCHRONY TAJEMNIC PAŃSTWA?

"(...) służby specjalne mają wiele innych zadań i przy ich realizacji istnieje pokusa <<skorzystania>> z wiedzy, którą gromadzą w ramach nadzoru nad systemem ochrony informacji niejawnych" - pisze Czesław Rybak, ekspert Fundacji Instytut Bezpieczeństwa i Strategii.

W Polsce od 1990 roku (wcześniej zresztą też) system ochrony informacji niejawnych opiera się na służbach specjalnych: najpierw na UOP i WSI, później na ABW i SKW. Służby nadają uprawnienia osobom i firmom do dostępu do informacji niejawnych i je cofają, służby akredytują systemy teleinformatyczne i certyfikują sprzęt, służby prowadzą kontrole w zakresie przestrzegania przepisów oraz realizują postępowania karne w sytuacji rażącego naruszenia przepisów o ochronie informacji niejawnych. Służby samodzielnie decydują o tym komu dać uprawnienia a komu ich nie dać lub je cofnąć. Przy okazji gromadzą multum wiedzy dot. tysięcy osób i podmiotów.

Zasadniczy problem polega na tym, że praktycznie nikt nie kontroluje służb w tym zakresie i nie możemy mieć pewności, iż zgromadzona wiedza nie jest wykorzystywana do innych celów niż ochrona informacji niejawnych. Należy pamiętać, iż służby specjalne mają wiele innych zadań i przy ich realizacji istnieje pokusa "skorzystania" z wiedzy, którą gromadzą w ramach nadzoru nad systemem ochrony informacji niejawnych.

A jak wygląda system ochrony informacji niejawnych w innych krajach? Analizując poszczególne systemy w krajach europejskich zauważa się, iż w niektórych z nich za system ten odpowiadają zupełnie niezależne od służb specjalnych urzędy. I tak, przykładowo, są to:

1. Czechy: Narodowy Urząd Bezpieczeństwa (NBU) oraz Narodowy Urząd Bezpieczeństwa Cybernetycznego i Informatycznego (NÚKIB),
2. Słowacja: Narodowy Urząd Bezpieczeństwa (NBU),
3. Rumunia: Narodowy Rejestr Informacji Niejawnych (ORNISS),
4. Belgia: Narodowa Władza Bezpieczeństwa (ANS).

Kto i jak?

Przyglądając się bliżej modelowi funkcjonującemu u naszego południowego sąsiada stwierdzamy, iż zgodnie z § 5 ustawy nr 153/1994 o służbach wywiadowczych Republiki Czeskiej, działaniami zagrażającymi bezpieczeństwu informacji stanowiących tajemnicę państwową lub służbową zajmuje się Informacyjna Służba Bezpieczeństwa (Bezpečnostní informační služba – BIS). BIS nie prowadzi jednak postępowań w zakresie dostępu do informacji niejawnych, tak jak to jest w przypadku ABW (służba takie postępowania, zgodnie z § 9 ustawy nr 148/1998 o ochronie informacji niejawnych, może prowadzić jedynie wobec własnych funkcjonariuszy). Za kwestie bezpieczeństwa informacji niejawnych w Czechach odpowiada Narodowy Urząd Bezpieczeństwa (Národní bezpečnostní úřad – NBU) oraz Narodowy Urząd ds. Bezpieczeństwa Cybernetycznego i Informatycznego (Národní úřad pro

kybernetickou a informační bezpečnost – NÚKIB).

Mimo swej nazwy żaden z tych urzędów nie jest służbą specjalną. Urząd (NBU) został powołany w dniu 1 sierpnia 1998 roku na mocy ustawy nr 148/1998 o ochronie informacji niejawnych i jest centralnym organem administracji w zakresie ochrony informacji niejawnych oraz wydawania certyfikatów dostępu do tych informacji. Z kolei Narodowy Urząd ds. Bezpieczeństwa Cybernetycznego i Informatycznego (NÚKIB) został powołany 1 sierpnia 2017 roku na podstawie ustawy nr 205/2017 o bezpieczeństwie cybernetycznym. Urząd ten jest obecnie centralnym organem administracji ds. bezpieczeństwa cybernetycznego, w tym również w zakresie ochrony informacji niejawnych w systemach informatycznych i teleinformatycznych oraz w zakresie ochrony kryptograficznej. NÚKIB odpowiada np. za certyfikację systemów informatycznych, środków technicznych i kryptograficznych. Urzędy te funkcjonują poza systemem czeskich służb specjalnych.

Czytaj też: Kto pilnuje naszej prywatności? Podsłuchy bez kontroli

Ustawa o ochronie informacji niejawnych nr 412/2015 wprowadziła kontrolę NBU ze strony Izby Poselskiej. Izba ustanowiła specjalny organ kontrolny „Stałą komisję ds. kontroli działalności NBU". Komisja liczy siedmiu członków. W ustawie określono również dokumenty i informacje, które dyrektor NBU przedkłada komisji. Są to informacje o działalności NBU, informacje na temat poszczególnych postępowań oraz materiały dotyczące budżetu urzędu.

W starej ustawie w art. 9 (ustawy nr 148/1998 o ochronie informacji niejawnych) był zapis, że Wywiad Wojskowy (Vojenské zpravodajství) wydaje poświadczenia bezpieczeństwa w zakresie kompetencji Ministerstwa Obrony. Zmiana nastąpiła w roku 2003 na podstawie rozporządzenia Rządu RC nr 1251 z 10 grudnia 2003. Od tego roku MON utraciło możliwość przeprowadzania postępowań w zakresie dostępu do informacji niejawnych. Zgodnie z nową UOIN nr 412/2005 wszelkie postępowania w zakresie dostępu do informacji niejawnych niezależnie, czy jest to sfera cywilna czy wojskowa, prowadzi NBU i NÚKIB. Wyłączone są z tego tylko służby wywiadowcze i czeskie MSW (np. Policja).

NBU współpracuje ze wszystkimi służbami specjalnymi RC, Policją, MSW i innymi instytucjami w zakresie zwracania się do tych instytucji o przekazywanie informacji niezbędnych do przeprowadzenia postępowania sprawdzającego. Ankiety bezpieczeństwa osobowego są podobne do tych stosowanych w Polsce.

U drugiego z naszych południowych sąsiadów – Słowacji, tematem ochrony informacji niejawnych zajmuje się instytucja o tej samej nazwie co w Czechach – Narodowy Urząd Bezpieczeństwa (Národný bezpečnostný úrad). NBU jest centralnym organem ds. ochrony informacji niejawnych, szyfrów, bezpieczeństwa cybernetycznego i zaufanych usług (podpis elektroniczny). Urząd powstał w roku 2001, od 1 listopada 2001 r. przejął kompetencje Ministerstwa Spraw Wewnętrznych. Nie jest to służba specjalna. Ze służbami specjalnymi łączy go jedynie procedura sprawdzeniowa. Urząd zwraca się do służb i innych instytucji o wszelkie niezbędne informacje potrzebne do zakończenia danej procedury.

Czytaj też: Nowa era szpiegostwa, czyli czego uczy nas sprawa Marka W.

Urząd przedkłada informację roczną z działalności Specjalnej Komisji ds. Kontroli NBU Słowackiej Rady Narodowej. Komisja w przypadku stwierdzenia naruszenia przepisów ma obowiązek zawiadomić Radę Narodową, Prokuratora Generalnego i rząd RS.

Na podstawie § 17 (3) ustawy o ochronie informacji niejawnych nr 215/2004, Wywiad Wojskowy (Vojenské spravodajstvo) przeprowadza postępowania sprawdzające II, III i IV stopnia (Poufne, Tajne i Ściśle tajne) wobec osób pozostających w stosunku służbowym lub stosunku pracy z Ministerstwem Obrony lub innymi organizacjami i instytucjami, których organem założycielskim jest MON. Zebrane przez Wywiad Wojskowy w trakcie postępowania materiały, z jego opinią i propozycją decyzji muszą zostać przekazane do Narodowego Urzędu Bezpieczeństwa. Spory pomiędzy tymi instytucjami rozstrzyga komisja Narodowej Rady Republiki. Również pracownicy słowackich służb specjalnych, wojskowych i cywilnych oraz policji, których postępowania prowadzą te instytucje, mogą się zwrócić z odwołaniem do tejże komisji parlamentu.

Z kolei w Rumunii systemem ochrony informacji niejawnych zajmuje się Narodowy Rejestr Informacji Niejawnych (ORNISS), który został utworzony rządowym rozporządzeniem wyjątkowym nr 153 z dnia 7 listopada 2002 roku, opublikowanym w Oficjalnym Dzienniku Rumunii nr 826 z dnia 15 listopada 2002 roku. Rozporządzenie wyjątkowe zostało zatwierdzone ustawą nr 101 z dnia 24 marca 2003 roku opublikowaną w Oficjalnym Dzienniku Rumunii, część I, nr 207 z dnia 31 marca 2003 roku.

ORNISS wykonuje zadania z zakresu regulacji, autoryzacji, kontroli oraz archiwizacji zgodnie z przepisami Ustawy nr 182/2002 o ochronie informacji niejawnych, Standardów Państwowych ochrony informacji niejawnych przyjętych przez Decyzję Rządową nr 585/2002 oraz Norm Organizacji Paktu Północnoatlantyckiego dot. ochrony informacji niejawnych w Rumunii przyjętych przez Decyzję Rządową nr 353/2002.

Czytaj też: "Przygoda życia" w CBA. Biuro szuka talentów

W celu wykonywania powierzonych zadań ORNISS posiada uprawnienia do żądania niezbędnych informacji od szefów służb i organów publicznych, podmiotów gospodarczych z wkładem państwowym oraz innych publicznych i prywatnych osób prawnych. Szefowie służb i organów publicznych, podmioty gospodarcze z wkładem państwowym oraz inne publiczne lub prywatne osoby prawne są obowiązane przekazać do dyspozycji ORNISS dane i informacje związane z ochroną informacji niejawnych na ich polu działalności, z wyjątkiem przypadków przewidzianych prawem.

Z kolei w Belgii, funkcję krajowej władzy bezpieczeństwa, zgodnie z dekretem wykonawczym do ustawy o ochronie informacji niejawnych i poświadczeniach bezpieczeństwa z 24 marca 2000 r., pełni organ o nazwie Autorité Nationale de Securité (Narodowa Władza Bezpieczeństwa). Jest to organ kolegialny, który odpowiada za wydawanie i odbieranie poświadczeń bezpieczeństwa oraz za sprawowanie nadzoru nad systemem ochrony informacji niejawnych. Na zasadzie wyjątku, funkcję Narodowej Władzy Bezpieczeństwa w stosunku do osób zatrudnionych w cywilnej Służbie Bezpieczeństwa (Sûreté de l'État/Veiligheid van den Staat – VSSE) i kandydatów do służby pełni dyrektor generalny VSSE.

Co z tą Polską?

Przedstawione wyżej cztery modele systemu ochrony informacji niejawnych, które opierają się na niezależności podmiotów odpowiedzialnych za system od służb specjalnych, stanowią rozwiązanie warte rozważenia i w Polsce. W państwach demokratycznych nie powinno się z zasady gromadzić zbyt wielu danych o obywatelu w jednym miejscu i tą drogą poszły te kraje, tworząc niezależne urzędy ds. ochrony informacji niejawnych. Były Generalny Inspektor Ochrony Danych Osobowych, dr Wojciech Wiewiórowski, w rozmowie z redaktorem Tomaszem Sekielskim przeprowadzonej w 2013 r. zwracał uwagę, że zarówno podmioty prywatne, jak i publiczne generalnie mają tendencję, by wiedzieć o nas jak najwięcej. Przypominał jednak, że *art. 51 ust. 2 Konstytucji RP wprost stanowi, że władza publiczna*

może gromadzić o obywatelu tylko te informacje, które są niezbędne w demokratycznym państwie prawnym. Nie ma zatem prawa zbierać informacji, które mogą być jej „przydatne", „potrzebne", „logiczne" czy „ekonomicznie opłacalne", co postanowiono w 1997 roku, uchwalając polską Konstytucję i że była to reakcja na państwo totalitarne. Przestrzegał również, iż p*amięć państwa totalitarnego powinna wciąż tkwić w naszych głowach, ponieważ dane zebrane nawet do najbardziej cnotliwych celów, mogą być niecnie wykorzystane i przez instytucje prywatne, i przez instytucje państwowe.*

*System, w którym za ochronę informacji niejawnych odpowiadają służby specjalne, nie jest rozwiązaniem optymalnym. ABW, zgodnie z art. 5 ustawy o ABW oraz AW, realizuje cały szereg zadań, wśród których "*realizowanie, w granicach swojej właściwości, zadań związanych z ochroną informacji niejawnych oraz wykonywanie funkcji krajowej władzy bezpieczeństwa w zakresie ochrony informacji niejawnych w stosunkach międzynarodowych" jest jednym z wielu. Ponadto, zakres odpowiedzialności ABW stale się powiększa, np. o zapobieganie zdarzeniom o charakterze terrorystycznym (od 2016 r.) czy o CSIRT GOV – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym (od 2018 r.). ABW prowadzi też działalność operacyjną, dochodzeniowo-śledczą i analityczną a także – w zakresie ochrony informacji niejawnych – administracyjną (w oparciu o KPA). Zarządzanie tak wielkim podmiotem, z tak wieloma zadaniami i kompetencjami, jest niezwykle skomplikowane. Przy dużej "wadze" zadań zasadniczych (zwalczanie szpiegostwa, terroryzmu, ochrona ekonomicznych interesów państwa), temat ochrony informacji niejawnych nie jest przez ABW traktowany priorytetowo, choćby w zakresie kadrowym.

Czytaj też: Niejasne zasady przyznawania uposażeń w ABW

Może więc warto rozważyć, czy przedstawione wyżej rozwiązania nie powinny funkcjonować również w naszym kraju. Może warto zastanowić się, czy nie należałoby powołać odrębnej od służb specjalnych instytucji (urzędu) odpowiedzialnej za kreowanie polityki państwa w sferze informacji niejawnych, wydawanie certyfikatów (poświadczeń i świadectw) dostępu do tajemnic państwa osobom i firmom, nadzór i kontrolę nad instytucjami wydającymi takie certyfikaty swoim funkcjonariuszom, żołnierzom i pracownikom, wydawanie świadectw akredytacji systemów teleinformatycznych przetwarzających informacje niejawne, certyfikację środków ochrony elektromagnetycznej, nadzór i kontrolę nad instytucjami przetwarzającymi informacje niejawne (w tym służby wywiadowcze i policyjne), współpracę międzynarodową, prowadzenie negocjacji umów międzynarodowych w zakresie informacji niejawnych, tworzenie standardów dotyczących ochrony informacji niejawnych oraz szkolenia i działania prewencyjne. Instytucja ta musiałaby podlegać bezpośrednio Prezesowi Rady Ministrów.

Proponowane rozwiązanie uniemożliwi służbom specjalnym (głównie ABW) zawłaszczenie systemu ochrony tajemnic państwa i nadużywanie dominującej pozycji w tej sferze do limitowania dostępu do działalności związanej z możliwością przetwarzania informacji niejawnych arbitralnie wybranym osobom i podmiotom, według własnego uznania, często kierując się pozamerytorycznymi lub wręcz partykularnymi celami, w tym politycznymi. Uniemożliwi również służbom pozyskiwanie wrażliwej wiedzy o obywatelach, która to wiedza może być wykorzystywana do zupełnie innych celów niż ochrona informacji niejawnych.

Czesław Rybak, ekspert Fundacji Instytut Bezpieczeństwa i Strategii