ISSN 1640-9280

POLICJA

KWARTALNIK KADRY KIEROWNICZEJ POLICJI

Volume 18, Issue 2

9 771640 928702 06

Year 2017

Policjanci o outsourcingu

Szkolenie oficerskie w Policji

Służba pełniona przez policjanta w ramach dyżuru domowego

Zagrożenia oraz podmioty ochrony danych osobowych i informacji niejawnych

WYŻSZA SZKOŁA POLICJI W SZCZYTNIE

NOWOŚCI WYDAWNICZE
WYDAWNICTWA WYŻSZEJ SZKOŁY POLICJI

Monika Porwisz

Sprzedajność funkcjonariusza Policji. Aspekty normatywne i kryminologiczne

ISBN 978-83-7462-554-8

oprawa twarda,
format B5,
ss. 452

Kuba Jałoszyński,
Waldemar Zubrzycki,
Jarosław Jabłoński

Kontrterroryzm. Siły specjalne. Działania. Wydarzenia w 2016 roku

ISBN 978-83-7462-576-0

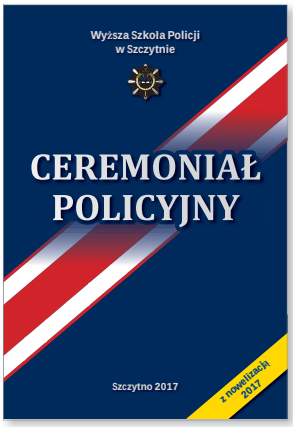
oprawa twarda,
format B5,
ss. 286

Zarządzanie instytucjami publicznymi i prywatnymi w kontekście niepewności zagrożeń kryzysów i ryzyka

Pod redakcją naukową
Jarosława Prońko,
Bernarda Wiśniewskiego

ISBN 978-83-7462-578-4

oprawa twarda,
format B5,
ss. 376



Ceremoniał policyjny

ISBN 978-83-7462-588-3

oprawa miękka,
format B5,
ss. 80

POLICJA
KWARTALNIK KADRY KIEROWNICZEJ POLICJI

Komitet redakcyjny: przewodniczący — Marek Fałdowski; członkowie: Jarosław Szymczyk, Irmina Gołębiewska, Małgorzata Borowik, Krzysztof Pobuta, Iwona Klonowska, Waldemar Zubrzycki, Magdalena Zubańska

Zespół redakcyjny: Zbigniew Mikołajczyk (redaktor naczelny), Krzysztof Łojek (zastępca redaktora naczelnego), Aleksander Babiński (sekretarz redakcji), Mariola Bil (redaktor językowy)

Redakcja wydawcy: Małgorzata Bukowska, Iwona Pac, Anika Pogorzelska (redakcja językowa), Adam Rogala (redakcja techniczna)

Wydawca: Wydawnictwo Wyższej Szkoły Policji w Szczytnie, 12-100 Szczytno, ul. Marsz. J. Piłsudskiego 111, **e-mail:** wwip@wspol.edu.pl, telefony kontaktowe: 89 621 51 50 (red. nacz.), 89 621 59 21 (zast. red. nacz.), 89 621 51 02 (sekretarz red.), fax 89 621 54 48

ISSN 1640-9280

Wersją referencyjną tytułu jest wersja drukowana

Zgodnie z komunikatem Ministerstwa Nauki i Szkolnictwa Wyższego z 12 grudnia 2016 r., za publikację w naszym periodyku „Policja. Kwartalnik Kadry Kierowniczej Policji" uzyskuje 6 punktów w kategorii czasopism naukowych nieposiadających współczynnika wpływu Impact Factor (IF).

SPIS TREŚCI

MATERIAŁY

Andrzej Warmiński[1]

Zagrożenia oraz podmioty ochrony danych osobowych i informacji niejawnych

Streszczenie: *Artykuł poświęcony jest zagrożeniom i podmiotom bezpieczeństwa w zakresie ochrony danych osobowych i informacji niejawnych. Już na samym wstępie opisuje podstawowe regulacje prawne w tym przedmiocie, a więc ustawowe główne założenia wynikające z ochrony danych osobowych i ustawy o ochronie informacji niejawnych. Następnie odnosi się do potencjalnych zagrożeń bezpieczeństwa danych osobowych i informacji niejawnych. W dalszej części przedstawia podmioty odpowiedzialne za ochronę danych i informacji, przede wszystkim generalnego inspektora ochrony danych osobowych, administratorów danych osobowych i administratorów bezpieczeństwa informacji, podkreślając znaczenie rolę i zadania Agencji Bezpieczeństwa Wewnętrznego oraz jej zadania wykonywane za pośrednictwem Służby Kontrwywiadu Wojskowego. Następnie analizuje działania ABW w przedmiocie ochrony i kontroli informacji niejawnych, kończąc na współpracy z organami partnerskimi w kraju i za granicą, akcentując rangę zawartych umów i porozumień.*

Słowa kluczowe: *regulacje prawne, zagrożenia, dane osobowe, informacje niejawne, podmioty, administratorzy ochrony danych osobowych i informacji niejawnych, Agencja Bezpieczeństwa Wewnętrznego, współpraca*

Abstract: *This article describes issues related to threats and security entities in the field of protection of personal data and classified information. At the very begiining, it describes the fundamental legal regulations in this regard, statutory main assumptions stemming from the protection of personal data and the law on the protection of classified information. Then it refers to potential threats to the security of personal data and classified information. This is followed by the entities responsible for data and information protection such as the Inspector General for Personal Data Protection, personal data administrators and information security administrators (ADO and ABI). The role and tasks of the Internal Security Agency (ABW), accomplished through the Military Counterintelligence Service (SKW) are underlined. The article presents also deepened analysis of the work of the Internal Security Agency on the protection and control of classified information and the problem of its cooperation with partner institutions in Poland and abroad, emphasizing the importance of concluded agreements*.

Keywords: *legal regulations, threats, personal data, classified information, entities, administrators of the protection of personal data and classified information, Internal Security Agency, cooperation*

Celem artykułu jest przedstawienie potencjalnych zagrożeń bezpieczeństwa danych osobowych i informacji niejawnych. Ponadto — zdiagnozowanie aktualnego stanu ochrony w tym przedmiocie, opis podmiotów odpowiedzialne za ochronę danych i informacji oraz wskazanie mankamentów występujących w systemie i błędnych zachowań (postępowań) w tym zakresie.

Podjęcie tej problematyki wynika z tego, że ochrona danych i informacji już od dawna stanowi tajemnicę, towarzysząc człowiekowi na przestrzeni dziejów i na różnych etapach rozwoju społecznego państwa, a przede wszystkim różnym formom jego działalności oraz życia. Także i w chwili obecnej kwestie związane z ochroną i bezpieczeństwem nie straciły swojego znaczenia i nadal pozostają w obrębie szczególnego zainteresowania współczesnego państwa i powołanych w tym celu organów bezpieczeństwa kraju.

Można więc zauważyć, że aktualnie zadaniem państwa jest zagwarantowanie każdemu obywatelowi szczególnej ochrony przed wszelkimi możliwymi zagrożeniami oraz należytych warunków zabezpieczenia jego danych i informacji ważnych z uwagi na bezpieczeństwo państwa. Wobec tego organy państwa nie mogą wykazywać jakichkolwiek dylematów w tej materii, natomiast powinny dysponować wiedzą i dużym doświadczeniem praktycznym, by móc sprostać obowiązkom w omawianej dziedzinie.

Państwo jest tym podmiotem, którego podstawowym zadaniem jest stworzenie jednolitego systemu, form

[1] Dr Andrzej Warmiński — absolwent wydziału dziennikarstwa i nauk politycznych Uniwersytetu Warszawskiego. Posiada tytuł doktora nauk humanistycznych w zakresie nauk o polityce. Aktualnie wykładowca PWSZ w Ciechanowie na kierunku Bezpieczeństwo Wewnętrzne oraz wykładowca Państwowej Wyższej Szkoły Informatyki i Przedsiębiorczości w Łomży. Specjalizuje się w problematyce bezpieczeństwa państwa. Autor książek: *Cywilne służby specjalne RP, Administracja bezpieczeństwa i porządku publicznego w Polsce* oraz *Zadania i środki działania rządowych organów administracji ochrony bezpieczeństwa państwa i porządku publicznego w okresie transformacji ustrojowej*. Wydawca innych publikacji m.in. *Bezpieczeństwo obrotu towarami o znaczeniu strategicznym*, *Bezpieczeństwo przewozu materiałów niebezpiecznych*, *Konstytucyjne regulacje stanów nadzwyczajnych w Polsce*, *Przedmiot Międzynarodowego Prawa Humanitarnego*, *Planowanie strategiczne w zarządzaniu jednostkami organizacyjnymi Policji*, *Czynności ratownicze policjanta na miejscu wypadku lotniczego*, *Postępowanie skargowe — obowiązujące regulacje prawne*, *Uwarunkowania, podstawy prawne i podmioty Międzynarodowej Współpracy Euroregionalnej*, *Regulacje Unii Europejskiej w kontekście bezpieczeństwa RP*, *Założenia koncepcji funkcjonowania i rozwoju lotnictwa Policji w systemie bezpieczeństwa wewnętrznego państwa do 2020 r.*

Kontakt z autorem za pośrednictwem redakcji.

i sposobów instytucjonalnego zabezpieczenia ochrony interesów państwa i człowieka[2]. Tym samym powstaje obowiązek państwa do przeciwdziałania wszelkim zagrożeniom naruszającym jego podstawowe interesy i cele. Ważną rolę odgrywa tutaj niełatwy proces zadbania o utrzymanie w tajemnicy działań i czynności powołanych do tego służb, które — funkcjonując — muszą z jednej strony zwracać uwagę na prawa i wolności, a z drugiej realizować ustawowe zadania w omawianym zakresie.

W tym kontekście pozwala to na wyciągnięcie wniosku, że Agencja Bezpieczeństwa Wewnętrznego (dalej jako ABW), Służba Kontrwywiadu Wojskowego (dalej jako SKW), główny inspektor ochrony danych osobowych i pozostałe odgrywają wyjątkową rolę w przedmiocie ochrony danych osobowych i informacji niejawnych. Niezbicie świadczy to o tym okoliczność, że w świetle obowiązujących w Polsce przepisów prawnych, to informacje i obywatel znajdują się w szczególnym centrum ochrony, jakie stworzyło demokratyczne państwo, przykładając dużą wagę do tych spraw.

Szczególne reulacje prawne

Rozważania należy rozpocząć od ukazania podstawowych regulacji prawnych. W szczególności należy mieć tu na uwadze dwie ustawy. Pierwsza z nich to ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych[3]. Wynika z niej, że każdy ma prawo do ochrony dotyczących go danych osobowych. Ustawę stosuje się tylko do danych osób fizycznych. Zatem zgodnie z dyspozycją art. 6 ust. 1 tejże ustawy za dane osobowe należy uznawać wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

Oznacza to, że osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny, albo jeden lub kilka specyficznych czynników, określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Natomiast nie uważa się informacji za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu i działań.

Wyraźnie można zauważyć, że przepisy ustawy stosuje się wyłącznie do danych osobowych każdej osoby fizycznej. Bowiem zgodnie z powszechnie obowiązującym prawem, w szczególności stosując wykładnię przepisów prawa, osobą fizyczną jest tylko taka osoba fizyczna, każdy człowiek mogący być uczestnikiem stosunków prawnych. Liczy się więc tylko posiadanie zdolności do bycia podmiotem praw i obowiązków oraz podejmowania czynności prawnych, która ustaje zawsze w chwili śmierci każdego człowieka[4].

Stosownie do tego danymi osobowymi są tylko takie dane, które dotyczą wyłącznie konkretnie sprecyzowanej osoby, umożliwiające niepodważalnie i natychmiastowo określić jej tożsamość i w ten sposób ją zidentyfikować. Należy mieć tu na uwadze wszelkie informacje, których zdobycie nie wymaga poniesienia dużych nakładów i kosztów — odbywa się za pomocą wprost osiągalnych i powszechnie dostępnych źródeł. Przy czym pozyskiwanie to musi odbywać się w sposób racjonalny i proporcjonalny.

Takim typowym przykładem informacji stanowiących dane osobowe może być numer PESEL, który na podstawie ustawy z 24 września 2010 r. o ewidencji ludności i dowodach osobistych[5], pozostaje stałym i niezmiennym jedenastocyfrowym symbolem–numerem identyfikacyjnym, stanowiąc jednoznacznie o danej osobie fizycznej. W nim pierwsze sześć cyfr odpowiada dacie urodzenia — rok, miesiąc i dzień, następne cztery to liczba porządkowa i płeć danej osoby, zaś ostatnia jest komputerową cyfrą kontrolną numeru ewidencyjnego. Jest to więc numer identyfikujący konkretną osobę, definitywnie podlegający ochronie i rygorom, przewidzianym w ustawie o ochronie danych osobowych.

Tak jak za dane osobowe uważa się informacje dotyczące osoby fizycznej, tak analogicznie tożsamość osoby można zidentyfikować dzięki IP komputera. Opinię w tej sprawie podjęła grupa robocza ds. ochrony danych Parlamentu Europejskiego i Rady Europejskiej[6], która literalnie przyjęła adres IP komputera za dane dotyczące osoby możliwej do zidentyfikowania, stwierdzając, że dostawcy usług internetowych, jak również menedżerowie lokalnych sieci, stosując rozsądne środki, mogą zidentyfikować wszystkich użytkowników Internetu, którym przypisali adresy IP, gdyż systematycznie i regularnie zapisują oni w plikach daty, czas trwania i korzystania, jaki odpowiada i został przypisany danej osobie.

Na tej zasadzie można stwierdzić, że także numer identyfikacyjny pojazdu VIN stanowi dane osobowe w rozumieniu ustawy o ochronie danych osobowych. Jednakże co do zasady sam numer VIN nie stanowi informacji, pozwalającej zidentyfikować konkretną osobę. Nie można więc uznać go za dane osobowe. Aczkolwiek dla administratora danych, jakim jest minister właściwy do spraw wewnętrznych i administracji, gdy jest on powiązany z innymi informacjami identyfikującymi właściciela pojazdu, stanowi dla niego dane osobowe.

Podobnie będzie z danymi osobowymi zgromadzonymi w formie akt, które są w rozumieniu ustawy o ochronie danych osobowych zbiorem danych osobowych. Również w wypadku, gdy klient banku nie wyraził zgody na przetwarzanie jego danych osobowych innemu podmiotowi, bez wyrażenia wyraźnej zgody przez niego, chociażby w celach marketingowych spółce, zajmującej się badaniem rynku.

Jak widać każde dane osobowe są gromadzone i mogą być przetwarzane. Wymienione dane stosuje się do prze-

[2] S. Zalewski, *Dylematy ochrony informacji niejawnych*, Katowice 2009, s. 7–10.

[3] Tekst jedn. z 2016 r., poz. 922.

[4] Wynika z tego, że osoba zmarła nie może być podmiotem praw i obowiązków we wszelkich stosunkach prawnych i nie może zostać uznana za osobę fizyczną.

[5] Tekst jedn. z 2016 r., poz. 722.

[6] Mówi o tym rozdział III, pkt 3, przykład piętnasty dyrektywy 95/46/WE Parlamentu Europejskiego i Rady Europejskiej z 24 października 1995 r. (Dz. Urz. Z 23 listopada 1995 r., L 281, P. 0031-0050).

twarzania danych osobowych w: kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych oraz w systemach informatycznych, także w wypadku przetwarzania danych poza zbiorem danych. Można zauważyć, że chodzi tu o każdy zbiór danych posiadający swoją strukturę, zestaw danych o charakterze osobowym, zebrany według ściśle określonych i sformułowanych kryteriów, bez względu (niezależnie), czy ma on charakter rozproszony lub jest on podzielony z punktu widzenia funkcjonalnego. Za zbiór danych należy uważać więc wszelkie różnorodne materiały zebrane i gromadzone w formie akt, przede wszystkim o charakterze policyjnym i prokuratorsko-sądowym[7].

Druga z regulacji to ustawa z 5 sierpnia 2010 r. o ochronie informacji niejawnych[8]. Ustawa ta określa: zasady ochrony informacji niejawnych, klasyfikację informacji niejawnych, zasady przetwarzania informacji niejawnych, tryb postępowania sprawdzającego, zasady przeprowadzania szkolenia w zakresie ochrony informacji niejawnych, zasady bezpieczeństwa osobowego, zasady działania kancelarii tajnych oraz zasady bezpieczeństwa teleinformatycznego i przemysłowego.

Na początku należy wyjaśnić, czym jest informacja niejawna. Tak więc ustawa dokładnie precyzuje, że chodzi o informację, której nieuprawnione ujawnienie, nawet w trakcie jej opracowywania oraz niezależnie od formy i sposobu jej wyrażania, spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej, albo byłoby z punktu widzenia jej interesów niekorzystne.

Dlatego z uwagi na jej zawartość, skład, treść, w świetle ustawy informacjom niejawnym nadaje się klauzulę: „ściśle tajne", jeśli ich nieuprawnione ujawnienie spowoduje wyjątkowo poważną szkodę dla Rzeczypospolitej Polskiej przez to, że: zagrozi niepodległości, suwerenności lub integralności terytorialnej Rzeczypospolitej Polskiej, „tajne", jeśli ich nieuprawnione ujawnienie spowoduje poważną szkodę dla Rzeczypospolitej Polskiej przez to, że: uniemożliwi realizację zadań związanych z ochroną suwerenności, lub porządku konstytucyjnego Rzeczypospolitej Polskiej, „poufne", jeśli ich nieuprawnione ujawnienie spowoduje szkodę dla Rzeczypospolitej Polskiej przez to, że: utrudni prowadzenie bieżącej polityki zagranicznej Rzeczypospolitej Polskiej, „zastrzeżone", jeśli nie nadano im wyższej klauzuli tajności, a ich nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań w zakresie obrony narodowej Rzeczypospolitej Polskiej.

Kontrolę ochrony informacji niejawnych prowadzą ABW[9] i SKW[10] w zakresie opisanym w ustawie, dlatego za jej nieprzestrzeganie grozi odpowiedzialność karna. Zgodnie z polską ustawą z 6 czerwca 1997 r. — kodeks karny[11] za ujawnienie informacji o klauzuli „ściśle tajne", albo „tajne" przewiduje się karę pozbawienia wolności od 3 miesięcy do 5 lat. Zaś za ujawnienie informacji o klauzuli „poufne" lub „zastrzeżone" przez funkcjonariusza publicznego grozi kara pozbawienia wolności do 3 lat[12].

W związku z tym każda osoba ubiegająca się o dostęp do informacji niejawnych na danym stanowisku służbowym podlega postępowaniu sprawdzającemu. Realizowane czynności i sprawdzenia mają na celu ustalenie, czy osoba sprawdzana daje rękojmię zachowania tajemnicy; postępowanie rozpoczyna się od wypełnienia przez osobę ankiety bezpieczeństwa osobowego. W zależności więc od stanowiska lub zleconej pracy, o które ubiega się dana osoba, przeprowadza się postępowanie sprawdzające: zwykłe — przy stanowiskach i pracach związanych z dostępem do informacji niejawnych oznaczonych klauzulą „poufne" oraz poszerzone — przy stanowiskach i pracach związanych z dostępem do informacji niejawnych oznaczonych klauzulą „tajne" lub „ściśle tajne". Z tym, że takie postępowanie sprawdzające może zakończyć się wydaniem poświadczenia bezpieczeństwa, umorzeniem lub odmową wydania takiego poświadczenia. Należy więc zakres stosowania środków bezpieczeństwa fizycznego uzależniać od poziomu zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą, uwzględniając przy określaniu poziomu zagrożeń w szczególności występujące rodzaje zagrożeń, klauzule tajności i liczbę informacji niejawnych.

Zagrożenia bezpieczeństwa ochrony danych osobowych i informacji niejawnych

Jeżeli chodzi o zagrożenia, to z dużym niezadowoleniem i smutkiem trzeba przyznać, że w wielu sytuacjach dochodzi do bagatelizowania i lekceważenia zasad i reguł postępowania związanych z ochroną danych osobowych i informacji niejawnych. W wielu wypadkach ludzie wyrzucają wiele dokumentów lub udostępniają je innym, nie zdając sobie sprawy z powagi sytuacji oraz uznając takie postępowanie za coś zwykłego i normalnego.

Na podstawie badań i przeprowadzonych analiz przez Annę Wilk[13] można dobitnie stwierdzić, że duża liczba dokumentów jest wyrzucana, lądując w śmietnikach lub w innych nieodpowiednich miejscach. Badania prowadzone przez wspomnianą socjolog były dwustronne — z jednej strony

[7] Ochrona danych osobowych, *Dane osobowe w pytaniach i odpowiedziach*, „Ochrona Informacji" 2015, sierpień (02), s. 28–32.

[8] Tekst jedn. z 2016 r., poz. 1167, z późn. zm.

[9] Została powołana na podstawie ustawy z 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (DzU z 2015 r., poz. 1929 z późn. zm.).

[10] Powstała na podstawie ustawy z 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (DzU z 2014 r., poz. 253 z późn. zm.).

[11] Tekst jedn. DzU z 2016 r., poz. 1137 z późn. zm.

[12] Jednakże Agencja Bezpieczeństwa Wewnętrznego, Biuro Ochrony Rządu, Agencja Wywiadu, Służba Kontrwywiadu Wojskowego, Służba Wywiadu Wojskowego, Centralne Biuro Antykorupcyjne oraz Policja, Żandarmeria Wojskowa, Straż Graniczna i Służba Więzienna przeprowadzają samodzielne postępowania sprawdzające wobec osób ubiegających się o przyjęcie do służby lub pracy w tych organach oraz pełniących służbę lub zatrudnionych w tych organach i służbach.

[13] Polska socjolog, doktor nauk humanistycznych w zakresie nauk socjologii. Badaczka, analityczka oraz konsultantka wielu projektów, również z zakresu ochrony danych osobowych i informacji niejawnych.

miały ukazać stopień przekonania o konieczności zabezpieczenia dokumentów zawierających istotne dane, analizując przy okazji — jak są zabezpieczane w praktyce, natomiast z drugiej strony, sprawdzając, jakie dokumenty trafiają do śmietnika. Najczęściej okazywało się, że to przeważnie z domów prywatnych wyrzuca się najwięcej ważnych dokumentów. Ponadto podczas badań ustalono, że większość osób zdaje sobie sprawę z tego, co to jest kradzież tożsamości, oraz że zwykle nie wyrażamy zgody na pobieranie naszych danych do celów marketingowych, zabezpieczamy posiadane dane komputerowe hasłami tak, aby osoby drugie nie posiadały do niego dostępu. Jednak, jak się okazało, nie przywiązujemy zbytniej wagi do pewnych danych, którymi posługujemy się i zarządzamy na bieżąco, na co dzień[14].

Prowadząc badania, zauważono, że w śmietnikach było bardzo dużo niezniszczonych dokumentów. Stwierdzono że na stacji przeładunkowej w Warszawie, gdzie ankieterzy przejrzeli cztery tony papieru zgromadzonego z całej stolicy, w ciągu dwóch tygodni w całości odnaleziono ponad półtorej tony różnych dokumentów. Dostrzegając, iż część z nich była tylko przedarta na połowę, co pozwalało na ich pełne odtworzenie. W dodatku niektóre z nich były zbindowane, zapakowane w teczkę lub folię. Łącznie około 85% z nich nadawała się do identyfikacji, a około 65% zawierała ważne i istotne dane. Można było odnaleźć listy płac pracowników, umowy z kontrahentami, z kwotami i terminami wpłat, informacje o przejęciu majątków konkretnych osób, listy i wykazy uczestników wyjazdów z ich adresami domowymi, co gorsze z numerami PESEL, dowodami wpłat, ponadto akty notarialne nabycia nieruchomości, raporty medyczne dotyczące stanu zdrowia osób, projekty budowlane, rachunki zysków i strat podmiotów gospodarczych, przedsiębiorców, opinie bankowe firm, świadectwa ślubów, dokumenty skarbowo-podatkowe — PIT-y z pełnymi informacjami, w tym nazwisko, imię, adres zamieszkania, z nazwą pracodawcy z wielkością i rozmiarami obrotów, faktury, akty notarialne itd. Zatem były to niebywale istotne rzeczy i niesamowicie trudne do wyobrażenia i pojęcia jest to, że znalazły się w takim miejscu.

Oprócz tego znaleziono raport z kontroli w sprawie braku zabezpieczenia dokumentów związanych ze sprzedażą, zbindowany w całości; plik dokumentów konwoju pomiędzy bankami — kiedy i jaką trasą pieniądze będą przewożone, ze zdjęciami konwojentów i godziną wyjazdu. Znaleziono również dużo kopii dowodów osobistych i praw jazdy oraz dokumentacji medycznej. Takie odkrycie jest dużym zaskoczeniem i zastanawia fakt, jak można postępować w taki niepoważny sposób z istotnymi dokumentami. Jest jeszcze jeden wniosek — że obecnie po sortowaniu śmieci dokumenty tego typy zapewne znajdują się w jednym miejscu.

Trochę inaczej wygląda sprawa, gdy dokumenty trafiają do zakładu sortowni śmieci. Tego typu miejsca są ochraniane przez system zabezpieczeń, przez ochraniarzy i jednak trudno jest się tam dostać. Należy podkreślić, że przez tak nieodpowiedzialny sposób postępowania z dokumentami można wiele stracić, gdyż wystarczy, że inne osoby wejdą w posiadanie którychś z tych dokumentów, poznając np. stan zdrowia, mogą wykorzystać znalezione informację i próbować chociażby przejąć majątek czy wpływać na testament. Są to nieciekawe scenariusze, ale jak najbardziej realne.

O tym, że poufne dane wyciekają z placówek medycznych wiadomo. Aż ¼ wszystkich wycieków poufnych danych w 2014 r. wypłynęła z sektora placówek ochrony zdrowia. Jednocześnie podwoiła się liczba tzw. leaków[15], czyli danych zgromadzonych w starym systemie w postaci wycieku, czy w inny sposób dostających się w niepowołane ręce w służbie zdrowia. Tymczasem w 2013 r., jak podają środki masowego przekazu, było ich zaledwie 7,6% z placówek medycznych. Oznacza to, że pracownicy służby zdrowia nie za bardzo skupiają się i koncentrują na zabezpieczeniu i ochronie danych osobowych, często nie zdając sobie do końca sprawy ze znaczenia i wagi danych i informacji, do jakich posiadają dostęp w swojej codziennej pracy[16].

Szczęście, że tego typu praktyki ulegają zmianie. Pracownicy firm zaczynają coraz bardziej dbać o bezpieczeństwo danych, ponieważ mają do tego niszczarki. Ponadto polskie prawo zobowiązuje do niszczenia dokumentów, pomimo że jeszcze niekiedy znajduje się różne rachunki, faktury, listy klientów hotelu, raporty i sprawozdania finansowe, to jednak jest ich już zdecydowanie mniej, niż kiedyś. Trzeba jednak pamiętać, że każdy z nas ma obowiązek dbania o własne dane osobowe i informacje na swój temat, zabezpieczając je w sposób jak najbardziej możliwy, ponieważ nikt inny za nas tego nie zrobi.

Aktualnie niebezpiecznym narzędziem staje się Internet, świat wirtualny, w którym bardzo dużo danych pojawia się i niestety w nim pozostaje, a także jest przekazywanych w inne miejsca. Przykładem mogą być konkursy internetowe, które cieszą się sporą popularnością. Biorąc w nich udział, podaje się wiele istotnych danych osobowych, nawet numer PESEL i nazwisko panieńskie matki.

Należy chronić portfel z dokumentami i kartami płatniczymi przed zagubieniem lub kradzieżą, gdyż dane w nich zawarte mogą zostać wykorzystane na naszą niekorzyść. W szczególności należy nie dopuścić, aby ktoś poznał kod PIN naszej karty. Bardzo często nie wiemy, kogo należy powiadomić w razie jej utraty; tudzież innego dokumentu. Badania wykazują, że w wypadku utraty dowodu osobistego, tylko 5% odpowiedziało poprawnie, wskazując miedzy innymi: generalnego inspektora ochrony danych osobowych, Policję.

W świetle badań tylko 3 osoby na 100 wyznały, że w przeszłości były ofiarami kradzieży tożsamości. W wielu takich sytuacjach udzielano na podstawie np. skradzionych dokumentów pożyczki — chwilówki. Okazuje się, że pożyczkobiorca nie jest sprawdzany w BIK, ani w innych bazach, a tym samym w kilka godzin, ze skradzionym dowodem,

[14] A. Wilk, *Dane na talerzu podane*, „Polityka" nr 10(2999), 4–10 marca 2015 r., s. 27–29.

[15] <http://pl.bab.la/slownik/angielski-polski/leak>, 15 marca 2017 r.

[16] *Aktualności*, „Ekspert Ochrony Informacji" 2015, nr 7, s. 4.

można obejść kilka placówek bankowych i otrzymać kilka kredytów. Badani wskazali, że ⅕ z nich była bezpośrednio narażona na kradzież danych osobowych, z kolei 12% odpowiedziało, iż dotknęło to ich najbliższych z rodziny.

Nasuwa się więc pytanie, czy w omawianej dziedzinie nasze prawo jest niewłaściwe i złe. Musimy zdawać sobie z sprawę, że — czy nam się to podoba, czy nie — zgodnie z obecnie obowiązującymi w Polsce przepisami, to na każdym z nas spoczywa obowiązek ochrony własnych danych, dlatego żal i pretensje można mieć jedynie do siebie.

Należy więc robić i czynić wszystko, aby zabezpieczyć ważne dane — nie wyrzucać dokumentów pochodzących z pracy lub z własnego domu na śmietnik (należy je palić lub niszczyć w inny skuteczny sposób), pilnować, aby nie wpadły w niepowołane ręce, zabezpieczać, na ile to możliwe za pomocą kodów, szyfrów, tak aby nie mogły zostać złamane. Ściśle rzecz biorąc, starać się i wystrzegać niefrasobliwego stosunku do własnych dokumentów, aby nie popaść w tarapaty i poważne kłopoty.

Podmioty odpowiedzialne za bezpieczeństwo danych osobowych i informacji niejawnych

Do podmiotów odpowiadających za ochronę danych osobowych i informacji niejawnych, w szczególności zalicza się: główny inspektor ochrony danych osobowych, administratorzy bezpieczeństwa danych osobowych i informacji niejawnych oraz ABW i SKW.

Generalny inspektor ochrony danych osobowych (dalej jako GIODO) to stanowisko powołane przede wszystkim, w celu kontroli zgodności procedur przetwarzania danych osobowych oraz prowadzenia ewidencji zarejestrowanych zbiorów tego rodzaju danych. Powoływany i odwoływany jest przez sejm, za zgodą senatu na czteroletnią kadencję. Do zadań, w ramach przyznanych kompetencji, GIODO, między innymi należy: kontrola zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych[17], wydawanie decyzji i rozpatrywanie skarg dotyczących wykonywania przepisów o ochronie danych osobowych, prowadzenie rejestru zbiorów danych osobowych oraz udzielenie informacji o zarejestrowanych zbiorach, opiniowanie projektów ustaw i rozporządzeń, dotyczących danych osobowych oraz inicjowanie i podejmowanie przedsięwzięć, w zakresie doskonalenia ochrony danych osobowych.

W zakresie kontroli zgodności przetwarzania danych osobowych z przepisami obejmuje ona przetwarzanie danych osobowych w zbiorach danych osobowych oraz zbiorach ewidencyjnych, niezależnie od tego, czy zbiory te są zarejestrowane w zbiorze danych prowadzonym przez GIODO. W tym celu, upoważnionym organom przysługuje między innymi prawo do: wstępu w godzinach między 6:00 a 22:00, za okazaniem ważnego upoważnienia i legitymacji służbowej, do pomieszczenia, w którym znajdują się zbiory danych osobowych i przeprowadzenia czynności kontrolnych celem ustalenia, czy przetwarzanie danych osobowych odbywa się zgodnie z ochroną danych osobowych, żądania złożenia pisemnych lub ustnych wyjaśnień, wzywania lub przesłuchiwania osób, dokonania wglądu do wszelkich dokumentów i danych, mających związek z kontrolą oraz przeprowadzania oględzin urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych[18].

W związku z powyższym w trakcie kontroli każdy kierownik kontrolowanej jednostki, bądź kontrolowana osoba fizyczna, mają obowiązek udostępnić organom kontroli niezbędne dokumenty oraz złożyć niezbędne wyjaśnienia. Nie wymaga się, aby kontrolowana osoba prawna, bądź inna jednostka organizacyjna była administratorem danych osobowych (wystarczy by dane przetwarzała), aby na kierownikach tych osób ciążył obowiązek udostępnienia organom niezbędnych danych i udzielenia wyjaśnień podczas kontroli. W przypadku kontroli osoby fizycznej sytuacja ta jest odmienna. Mianowicie kontrolowana osoba fizyczna musi być jednocześnie administratorem danych osobowych, by ciążył na niej obowiązek udostępnienia danych podczas kontroli[19].

W wypadku stwierdzenia podczas kontroli podejrzenia popełnienia przez kierownika danej jednostki, jej pracowników oraz inne osoby fizyczne przestępstwa w związku z zaniedbaniem obowiązków związanych z przetwarzaniem danych osobowych, podmioty te mają obowiązek zawiadomić organy ścigania o podejrzeniu popełnienia przestępstwa. Wśród przestępstw znaleźć można: przetwarzanie danych osobowych, których przetwarzanie jest niedopuszczalne, udostępnienie lub umożliwienie dostępu do danych osobowych osobie nieupoważnionej przez administratora tych danych bądź inną osobę obowiązaną do ochrony danych osobowych, naruszenie, również nieumyślne, przez administratora danych osobowych obowiązku odpowiedniego (zgodnego z przepisami) zabezpieczenia danych osobowych, niezgłoszenie zbioru danych osobowych do rejestracji[20], niedopełnienie obowiązku informacyjnego o prawach wobec osoby, której dane osobowe znajdu-

[17] To do GIODO należy wydawanie decyzji i rozpatrywanie skarg dotyczących wykonywania przepisów o ochronie danych osobowych. W sytuacjach stwierdzenia uchybień w toku kontroli GIODO wydaje decyzję zmierzającą do przywrócenia stanu zgodnego z prawem, w tym celu może nakazać: usunięcie uchybień, uzupełnienia, uaktualnienia, sprostowania, udostępnienia lub nieudostępnienia danych osobowych, zastosowania dodatkowych środków zabezpieczających zgromadzone dane osobowe, wstrzymania przekazywania danych osobowych do państwa trzeciego, zabezpieczenia danych lub przekazanie ich innym podmiotom, usunięcia danych osobowych. Adresatem decyzji nie musi być tylko kontrolowana jednostka — może nim być administrator danych osobowych, osoba przetwarzająca dane osobowe oraz inny podmiot, który dopuścił się naruszenia przepisów ustawy o ochronie danych osobowych. Każda wydana decyzja nie jest ostateczna — osobie zainteresowanej (np. osobie kontrolowanej, administratorowi danych, osobie przetwarzającej dane) przysługuje wniosek o ponowne rozpatrzenie sprawy do GIODO, a w dalszej kolejności skarga do wojewódzkiego sądu administracyjnego.

[18] <http://osobowedane.pl/generalny-inspektor-ochrony-danych-osobowych-giodo/> 10 marca 2017 r.

[19] Potwierdza to wyrok NSA z 30 stycznia 2002 r., sygn. II SA 1098/01, „Wokanda" 2002, nr 7–8, s. 20.

[20] Właśnie to do kompetencji GIDO należy prowadzenie rejestru zbiorów danych osobowych. Wypływa to z przepisów ustawy o ochronie danych osobowych mówiącej, że każdy ADO ma obowiązek zgłosze-

ją się w zbiorze danych osobowych, udaremnianie lub utrudnianie przeprowadzenia kontroli przez inspektora.

Innymi podmiotami mającymi zadanie ochrony bezpieczeństwa danych i informacji są administrator ochrony danych i informacji niejawnych oraz administrator bezpieczeństwa informacji (ADO, ABI). Zgodnie z ustawą administratorzy danych są zobowiązani do zastosowania właściwych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednich do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinni zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. W tym przedmiocie powinni prowadzić stosowną dokumentację opisującą sposób przetwarzania danych oraz ich ochrony i zabezpieczania.

Administratorzy danych mogą powołać administratora bezpieczeństwa informacji, do którego należy: zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych, nadzorowanie opracowania i aktualizowania dokumentacji, zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych, prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów oraz rejestrów. Z uwagi na tak ważne zadania administrator bezpieczeństwa informacji podlega bezpośrednio kierownikowi jednostki organizacyjnej lub osobie fizycznej, będącej administratorem danych.

Możemy wyróżnić dwa podstawowe obowiązki administratorów: 1) obowiązek informacyjny, z którego wynika poinformowanie osoby, której dane dotyczą o adresie swojej siedziby i pełnej nazwie, w celu zbierania danych, w tym o odbiorcach lub kategoriach odbiorców danych, prawie dostępu do swoich danych oraz ich poprawiania, a także o nakazie podania swoich danych; 2) obowiązek zabezpieczenia danych osobowych przez zastosowanie odpowiednich środków technicznych i organizacyjnych zgodnych z ustawą w drodze postępowania w myśl przyjętej polityki bezpieczeństwa[21] i instrukcji zarządzania systemem informatycznym[22]. Jak wynika, rola administratora stanowi jedno z podstawowych, fundamentalnych, centralnych pojęć całego systemu ochrony danych i informacji osobowych — zarówno na szczeblu krajowym, jak i w Unii Europejskiej[23].

Kolejnym ważnym podmiotem pełniącym funkcję krajowej władzy bezpieczeństwa jest szef ABW[24], za pomocą (pośrednictwem) szefa SKW[25]. Dlatego, jak twierdzi Sławomir Zalewski[26], służby te spełniają funkcję ochronno-kontrolną w tej materii w sprawach: kontroli informacji niejawnych oraz kontroli przestrzegania ustawowych przepisów, realizacji zadań bezpieczeństwa systemów i sieci teleinformatycznych, prowadzenia postępowania sprawdzającego, ochrony informacji wymienianych przez Rzeczpospolitą Polską z innymi państwami i organizacjami międzynarodowymi oraz szkolenia i doradztwa w dziedzinie ochrony informacji niejawnych.

Mając na uwadze powyższe zadania, ABW, chcąc zapewnić prawidłowe działanie systemu ochrony informacji niejawnych, ściśle współpracuje z pionami ochrony w poszczególnych podmiotach państwa, prowadząc szkolenia zaadresowane do pełnomocników ochrony (np. w urzędach administracji publicznej) oraz szkolenia w ramach tzw. profilaktyki kontrwywiadowczej skierowane do osób pracujących w instytucjach istotnych z punktu widzenia interesów RP (Urzędzie Rady Ministrów, Kancelarii Sejmu, w poszczególnych ministerstwach itd.). Natomiast w ramach współpracy międzynarodowej Polska musi zapewnić jednolity stopień bezpieczeństwa informacji klasyfikowanych, które są wymieniane z zagranicznymi partnerami. Taką gwarancję dają umowy dwustronne oraz regulacje organizacji międzynarodowych, których Polska jest członkiem[27].

Jak już wspomniano, aby móc realizować powyżej nadmienione zadania, przeprowadza się i stosuje dwa rodzaje

nia prowadzonego przez siebie zbioru danych osobowych do rejestru prowadzonego przez GIODO.

[21] Polityka bezpieczeństwa jako dokument powinien zawierać: definicję bezpieczeństwa danych osobowych, główne cele i zakres, znaczenie, mechanizmy współużytkowania informacji, oświadczenie o intencjach kierownictwa, potwierdzenie celów i zasad bezpieczeństwa, wyjaśnienie polityki bezpieczeństwa, zasad, standardów, wymagań zgodności z prawem i wymaganiami wynikającymi z zawartych umów, wymagania dotyczące kształcenia w dziedzinie bezpieczeństwa, informacje na temat zapobiegania i wykrywania wirusów oraz złośliwego oprogramowania, sposoby zarządzania ciągłością działania, konsekwencje w razie naruszenia polityki bezpieczeństwa oraz tryb zgłaszania wymienionych naruszeń.

[22] Instrukcja określa: procedury nadawania i rejestrowania w systemie informatycznym uprawnień do przetwarzania danych oraz wskazanie osób odpowiedzialnych za realizację tych czynności, stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i stosowaniem, procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu, procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania, sposób, miejsce i czas przechowywania: elektronicznych nośników informacji zawierających dane osobowe, kopii zapasowych, sposób zabezpieczenia systemu informatycznego przed działalnością złośliwego oprogramowania tzw. wirusów oraz procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

[23] P. Pruszyński, *Rola i znaczenie ochrony danych osobowych*, „Ochrona danych osobowych, Ochrona Informacji Niejawnych" 2015, listopad, s. 34–37.

[24] Jest to ABW, która realizuje działania analityczno-informacyjne, operacyjno-rozpoznawcze i procesowe, a także uczestniczy w procedurach opiniodawczych oraz prowadzi czynności w ramach systemu ochrony informacji niejawnych.

[25] Szef Służby Kontrwywiadu Wojskowego dokonuje sprawdzeń, wydając je w formie dokumentu poświadczenia bezpieczeństwa we wszystkich jednostkach podległych Ministerstwu Obrony Narodowej w stosunku do żołnierzy i zatrudnionych osób cywilnych, natomiast szef ABW o wobec innych podmiotów.

[26] S. Zalewski, *Służby specjalne w państwie demokratycznym*, Warszawa 2002, s. 75.

[27] A. Warmiński, *Cywilne służby specjalne Rzeczypospolitej Polskiej*, Piotrków Trybunalski 2016, s. 64–65.

postępowań sprawdzających: zwykłe i poszerzone[28]. Postępowania zwykłe przeprowadzają pełnomocnicy do spraw ochrony informacji niejawnych, w stosunku do osób ubiegających się o dostęp do informacji niejawnych o klauzuli „poufne", na pisemny wniosek lub polecenie kierownika danej jednostki organizacyjnej. Natomiast postępowanie poszerzone jest wykonywane przez ABW i SKW. Zatem ABW i SKW prowadzą postępowanie sprawdzające w stosunku do: osób wykonujących zadania związane z dostępem do informacji niejawnych o klauzuli „tajne" lub „ściśle tajne", pełnomocników ochrony, ich zastępców oraz kandydatów na te stanowiska, kierowników jednostek organizacyjnych, w których przetwarzane są informacje poufne, tajne lub ściśle tajne, a także osób ubiegających się o dostęp do informacji niejawnych międzynarodowych. Z kolei zgodę na dostęp do informacji niejawnych oznaczonych klauzulą „zastrzeżone" wydaje kierownik jednostki organizacyjnej.

Postępowanie sprawdzające zwykłe i poszerzone trwa odpowiednio każde trzy miesiące — jest to czas na wykonanie czynności. Nie jest to jednak termin zawity i może zostać wydłużony, ponieważ ustawodawca używa sformułowania powinny być zakończone, co umożliwia przekroczenie tego terminu, o ile uzasadnione jest to koniecznością zebrania materiału w celu wydania poprawnej decyzji, natomiast kolejne postępowanie powinno być zakończone przed upływem 6 miesięcy. Należy nadmienić, że nadal obowiązuje 10-letni okres ważności dostępu do informacji niejawnych o klauzuli „poufne", 7-letni do klauzuli „tajne" i 5-letni do klauzuli ściśle tajne[29].

Dla pełnego zobrazowania problemu w toku postępowania sprawdzającego (zwykłego i poszerzonego) ustala się wszelkie wątpliwości w sprawie, czyli: uczestnictwa, współpracy lub popierania przez osobę sprawdzaną działalności szpiegowskiej, terrorystycznej, sabotażowej lub innej wymierzonej przeciwko Rzeczypospolitej Polskiej; zagrożenia osoby sprawdzanej ze strony obcych służb specjalnych w postaci werbunku lub nawiązania z nią kontaktu; przestrzegania porządku konstytucyjnego RP; czy osoba nie uczestniczyła lub nie uczestniczy w działalności partii politycznych lub organizacjach, albo współpracowała lub współpracuje z takimi partiami lub organizacjami; ukrywania lub podawania świadomego, niezgodnego z prawdą przez osobę sprawdzaną w postępowaniu sprawdzającym informacji mających znaczenie dla ochrony informacji niejawnych; występowania związanych z osobą sprawdzaną okoliczności powodujących ryzyko jej podatności na szantaż lub wywieranie presji oraz niewłaściwego postępowania związanego z informacjami niejawnymi.

Z kolei osobno sprawdzeniu podlegają: czy istnieją wątpliwości dotyczące poziomu życia osoby sprawdzanej wyraźnie przewyższającego dochody przez nią osiągane, informacje o chorobie psychicznej lub innych zakłóceniach czynności psychicznych ograniczających sprawność umysłową i mogących negatywnie wpływać na zdolność osoby sprawdzanej do wykonywania i realizowania prac i czynności związanych z dostępem do informacji niejawnych, informacje o uzależnieniu od alkoholu, środków odurzających lub substancji psychotropowych.

Działania agencji bezpieczeństwa wewnętrznego w zakresie ochrony danych i informacji niejawnych

Wyraźnie można zauważyć, że ABW w kwestii nadzoru nad systemem ochrony informacji niejawnych, zgodnie ze swoją właściwością, dokonuje kontroli w dziedzinie bezpieczeństwa: osobowego — rozumianego jako procedury sprawdzeniowe służące weryfikacji wiarygodności osób ubiegających się o uzyskanie dostępu do informacji niejawnych i uniemożliwieniu takiego dostępu osobom, niedającym rękojmi zachowania tajemnicy oraz szkolenia osób przed udzieleniem im dostępu do informacji klauzulowanych; przemysłowego — pojmowanego jako procedury sprawdzeniowe wobec firm ubiegających się o wydanie świadectwa bezpieczeństwa przemysłowego; fizycznego — w tym określania standardów i zapewnianie fizycznych warunków do ochrony informacji niejawnych oraz kontrola ich przestrzegania; oraz teleinformatycznego — mającego na celu certyfikację urządzeń i akredytację systemów teleinformatycznych[30].

Ważną rolę w tym systemie odgrywa kontrola ochrony informacji niejawnych dokonywana na bazie obowiązujących przepisów. Jeśli chodzi o bezpieczeństwo osobowe, to ABW, prowadząc postępowania, kończy je wydaniem bezpieczeństwa lub decyzją o odmowie wydania poświadczenia bezpieczeństwa lub je umarza. Do najczęstszych okoliczności przemawiających za odmową wydania poświadczenia można wskazać: podatność na wywieranie presji, niewłaściwe postępowanie z informacjami niejawnymi, choroby lub zaburzenia psychiczne, zagrożenie ze strony obcych służb specjalnych w postaci prób werbunku lub nawiązania kontaktu, podawanie nieprawdziwych informacji, skazanie prawomocnym wyrokiem za przestępstwo umyślne, ścigane z oskarżenia publicznego, w tym również przestępstwo skarbowe.

Biorąc pod uwagę postępowania w przedmiocie bezpieczeństwa przemysłowego, należy powiedzieć, że jest ono prowadzone na wniosek przedsiębiorcy i obejmuje sprawdzenie przedsiębiorcy, kierownika oraz osób mających dostęp do informacji niejawnych, a więc osób zarządzających i kontrolnych. Dlatego przede wszystkim jego celem jest ustalenie, czy przedsiębiorca posiada zdolność do ochrony informacji niejawnych, w tym sprawdzenie m.in.: struktury kapitału oraz powiązań kapitałowych, źródła pochodzenia środków finansowych,

[28] Tymczasem poprzednie przepisy zakładały możliwość stosowanie jeszcze jednego rodzaju postępowania sprawdzającego — tzw. specjalnego.

[29] K. Krawczyk, *Poświadczenie bezpieczeństwa*, „Policja 997" 2011, nr 3(72), s. 40–42.

[30] Agencja Bezpieczeństwa Wewnętrznego, *Raport z działalności Agencji Bezpieczeństwa Wewnętrznego w 2014 r.*, Warszawa 2015, s. 7.

struktury organizacyjnej, systemu ochrony informacji niejawnych, wszystkich osób wchodzących w skład organów zarządzających i kontrolnych przedsiębiorcy. Sprawdzeń danych zawartych w kwestionariuszu oraz innych informacji uzyskanych w trakcie postępowania, dokonuje się w rejestrach, ewidencjach, kartotekach, a także w kartotekach niedostępnych powszechnie. Jednakże w tych postepowaniach bardzo rzadko wydaje się decyzje o odmowie wydania świadectwa albo o jego cofnięciu.

Jeżeli chodzi o certyfikację urządzeń i akredytację systemów teleinformatycznych, to w trakcie realizacji zadań wynikających z ustawy o ochronie informacji niejawnych ABW udziela akredytacji bezpieczeństwa teleinformatycznego dla systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych o klauzuli „poufne" lub wyżej, natomiast dokumentem potwierdzającym jest świadectwo akredytacji bezpieczeństwa systemu teleinformatycznego[31]. Ogólnie mówiąc, co roku ABW kilkanaście wystąpień pokontrolnych przesyła do kierowników jednostek kontrolowanych. Można zauważyć, że najczęstsze nieprawidłowości i uchybienia dotyczyły organizacji systemu ochrony informacji niejawnych i polegały na powoływaniu na stanowiska pełnomocnika ochrony lub zastępcy pełnomocnika ochrony osób niespełniających wymogów ustawowych oraz przeprowadzaniu przez pełnomocników ochrony kontroli w zakresie ochrony informacji niejawnych w jednostkach podległych, w których zatrudnieni byli pełnomocnicy.

W kwestii bezpieczeństwa systemów teleinformatycznych najwięcej nieprawidłowości wiązało się z brakiem specjalistycznego przeszkolenia osób realizujących obowiązki administratorów i inspektorów bezpieczeństwa teleinformatycznego oraz przetwarzaniem informacji niejawnych przy użyciu systemów nieakredytowanych. Z kolei w dziedzinie obiegu materiałów niejawnych nieprawidłowości związane były przede wszystkim z niewłaściwym ewidencjonowaniem materiałów niejawnych prowadzącym do niezgodności stanu ewidencyjnego z faktycznym, natomiast, jeśli chodzi o środki bezpieczeństwa fizycznego nieprawidłowości obejmowały obejmującego niewłaściwą organizację stref ochronnych i stosowania do ochrony informacji niejawnych urządzeń nieposiadających stosownych certyfikatów.

Współpraca międzynarodowa w przedmiocie ochrony danych osobowych i informacji niejawnych

W świetle potencjalnych zagrożeń w dziedzinie bezpieczeństwa i ochrony informacji niejawnych ABW między innymi utrzymuje kontakt i współpracuję na płaszczyźnie dwustronnej oraz wielostronnej ze służbami wywiadowczymi i odpowiednimi organami innych państw. Podtrzymywane kontakty z partnerami zagranicznymi pozwalają przede wszystkim na wspólną analizę zagrożeń, wymianę informacji i doświadczeń, negocjacje oraz zawieranie umów i porozumień[32]. Spora część współpracy i współdziałania poświęcona jest ochronie informacji niejawnych i zapewnieniu bezpieczeństwa ich obiegowi w relacjach międzynarodowych.

Wymienione relacje ze służbami partnerskimi mają ogromne znaczenie w kontekście walki z zagrożeniami o zasięgu międzynarodowym, takimi jak terroryzm, przestępczość zorganizowana czy proliferacja broni masowego rażenia. Dlatego tak ważnym zadaniem ABW, które wymaga współpracy międzynarodowej, staje się zabezpieczenie i ochrona sieci informatycznych instytucji państwowych przed cyberatakami.

Dobrze więc, że ABW współpracuje z wszystkimi organizacjami i państwami członkowskimi Unii Europejskiej oraz NATO w sferze ochrony informacji niejawnych przetwarzanych w akredytowanych systemach teleinformatycznych. Wspólnym celem współpracy jest wypracowanie nowych, wspólnych standardów ochrony w obszarze bezpieczeństwa osobowego, przemysłowego i obiegu dokumentów, wypracowanie i utrzymanie międzynarodowych standardów bezpieczeństwa systemów teleinformatycznych, utrzymanie porównywalnego poziomu bezpieczeństwa akredytowanych systemów TI, zapewnienie odpowiedniego poziomu bezpieczeństwa systemów łączności z organizacjami międzynarodowymi. Na kanwie takiej współpracy systematycznie wzrasta liczba obowiązujących dwustronnych umów o wzajemnej ochronie informacji, jakie ABW przez cały czas zawiera z właściwymi organami innych państw.

W zakresie ochrony informacji niejawnych ABW współpracuje również z różnymi gremiami europejskimi, np. Europejską Agencją Kosmiczną (*European Space Agency* — dalej jako ESA). Wspólnie z Ministerstwem Gospodarki i Polską Agencją Rozwoju Przedsiębiorczości ABW zorganizowała konferencję, na której przedstawiono przede wszystkim: zasady ubiegania się o kontrakty, system ochrony informacji niejawnych RP, podstawową wiedzę o wymianie takich danych na poziomie międzynarodowym oraz wymogi ESA i NATO w tym obszarze.

[31] Tylko w tym obszarze w 2014 r. ABW wystawiła 702 świadectwa akredytacji systemów TI. Obok tego ABW wydała 581 certyfikatów ochrony elektromagnetycznej, 6 certyfikatów ochrony kryptograficznej oraz 1443 certyfikaty zgodności.

[32] Dlatego w ostatnich latach podpisano umowę regulującą wzajemną ochronę informacji niejawnych z Węgrami, w listopadzie z Czarnogórą, a w grudniu z Algierią (dotyczy tylko informacji kwalifikowanych ze sfery obronności). Rozpoczęto negocjacje dotyczące projektów takich umów z Gruzją oraz Bośnią i Hercegowiną. Kontynuowano też rozpoczęte wcześniej prace nad porozumieniami z: Mongolią, Luksemburgiem, Ukrainą, Armenią, Wielką Brytanią, Cyprem, Szwajcarią, Holandią, Grecją, Chorwacją, Serbią, Turcją, Estonią oraz Zjednoczonymi Emiratami Arabskimi. Wszczęto również procedurę zmierzającą do zawarcia umowy z Etiopią. Trwają także prace nad projektem umowy o charakterze ogólnym z Organizacją ds. Współpracy w zakresie Uzbrojenia (OCCAR). Pozwoli ona na stworzenie jednolitych zasad ochrony wymienianych informacji oraz rozwój współpracy z OCCAR i państwami, które uczestniczą w różnych projektach tej organizacji.

Zakończenie

W demokratycznym kraju, jakim jest Rzeczypospolita Polska przepisy prawa dotyczące ochrony danych osobowych i informacji niejawnych stanowią ważny element życia państwa. Istotne jest, aby występowała równowaga między jawnością a tajnością, ponadto, by organy kontrolno-ochronne w tym przedmiocie działały zgodnie z prawem.

Szczególnie ważne są tu dwa akty prawne, które zostały wcześniej przytoczone: ustawa o ochronie danych osobowych i ustawa o ochronie informacji niejawnych. Wymienione ustawy stwarzają i zabezpieczają aktualny obraz bezpieczeństwa, odgrywając w nim podstawową rolę. W sumie tych dokumentów jest około dwustu. Widać, że owe przepisy wspólnie i jasno tworzą pewien system ochrony danych osobowych i informacji niejawnych.

We wspomnianym systemie ważną rolę ogrywa opracowana i przygotowana polityka bezpieczeństwa danych osobowych i informacji, której głównym celem jest wskazanie działań, jakie trzeba wykonać oraz ustanowienie jasnych zasad i reguł postępowania, których należy przestrzegać i stosować w praktyce, by móc w sposób prawidłowy realizować wyznaczone zadania, pozyskując na tej podstawie wzajemne zaufanie.

Na system ochrony informacji niejawnych w Polsce składają się: bezpieczeństwo osobowe, bezpieczeństwo fizyczne, bezpieczeństwo obiegu informacji, bezpieczeństwo przemysłowe i teleinformatyczne. Należy przywiązywać szczególną wagę do wymienionych spraw i zagadnień, gdyż one przesądzają o bezpieczeństwie państwa i jego obywateli, wydając jak ustalono stosowne poświadczenia bezpieczeństwa z dostępem do czterech klauzul oznaczonych jako: „zastrzeżone", „poufne", „tajne" i „ściśle tajne".

W świetle tego obowiązek zabezpieczenia danych osobowych i informacji niejawnych spoczywa na administratorach, którzy zobowiązani są stosować odpowiednie ustawowe środki i narzędzia (instrumenty) o charakterze technicznym i organizacyjnym, zapewniające im prawidłowe bezpieczeństwo. Należy mieć tu na uwadze między innymi ADO oraz ABI, pełnomocników oraz GIODO. Obok nich funkcjonuje jeszcze ABW, której szef, jako organ, sprawuje główną władzę, zapewniając bezpieczeństwo w tym zakresie za pośrednictwem szefa SKW.

Jeśli chodzi o działanie ABW, to nie można mieć tutaj uwag. Funkcjonariusze na bieżąco realizują wytyczone zadania zgodnie z przepisami, dbając o bezpieczeństwo osobowe i fizyczne, wykonując czynności w ramach prowadzonych postępowań bezpieczeństwa przemysłowego, udzielając akredytacji bezpieczeństwa teleinformatycznego dla systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych o klauzuli „poufne" oraz wyższych, przez cały czas dokonując kontroli ochrony informacji niejawnych. W sytuacji stwierdzenia występujących nieprawidłowości kierują oni zawiadomienie do prokuratury o możliwości popełnienia przestępstwa w rozumieniu kodeksu karnego, z wnioskiem o wszczęcie śledztwa. Z kolei w innych sytuacjach, kontrolując pod kątem prowadzonych postępowań sprawdzających przez pełnomocników ochrony, w razie stwierdzenia łamania zasad ochrony informacji niejawnych i nieprzestrzegania przepisów, sporządzają wystąpienia pokontrolne, po czym przekazują je kierownikom poszczególnych jednostek.

Niestety wyraźnie można również zauważyć, że powyższy system posiada wiele słabości i uchybień, że coś w nim zawodzi, czego dowodzą przedstawione w atykule występujące zagrożenia. Bardzo dużo informacji i wiadomości z niego wypływa wskutek błędnych ludzkich zachowań — osób, które postępują w sposób mało poważny i nieodpowiedzialny. Wobec tego wiele wskazuje na to, że prawidłowe i skuteczne zabezpieczenie istotnych i ważnych dla państwa i obywateli informacji wymaga bardziej rozsądniejszego myślenia i zwiększonego wysiłku umysłu, aniżeli zabezpieczenia fizycznego.

Oznacza to, że rozważenia wymaga, czy pomimo posiadanego certyfikatu (poświadczenia bezpieczeństwa, nie należałoby położyć jeszcze większy nacisk na szkolenie. Z powyższego wywodu wynika, że będzie to właściwe posunięcie, dzięki któremu zwiększymy pewność, że dany użytkownik pracuje w sposób merytoryczny, rzetelny, sumienny, odpowiedzialny, lojalny, ograniczający ewentualne ryzyko złamania zasad bezpieczeństwa ochrony danych osobowych i informacji niejawnych. Ponieważ, jak pokazują kontrole, nieprawidłowości przede wszystkim dotyczą niewłaściwego ewidencjonowania dokumentów, powoływania na stanowisko pełnomocników ochrony niezgodnie z ustawowymi wymaganiami, niewłaściwego ewidencjonowania dokumentów niejawnych, niewłaściwej organizacji stref ochronnych oraz stosowania do ochrony urządzeń, bez wymaganych certyfikatów.

Z analizowanego materiału również dobitnie wynika, że wśród wyciekających danych osób, pacjentów znajduje się bardzo dużo informacji tych wrażliwych, jak np. numer PESEL, NIP, historie chorób, dane dokumentów ubezpieczeniowych, adresy zamieszkania i zameldowania, rachunki, faktury, umowy, dokumenty osobowo-finansowe firm, spółek i przedsiębiorstw, dane Zakładu Ubezpieczeń Społecznych i szereg innych.

Dlatego, chroniąc system, należy zwracać uwagę nie tylko na te zwykłe i tradycyjne źródła zagrożeń, ale i być przygotowanym na potencjalne działania ze strony terrorystów, szpiegów itd. Warto również dostrzec, że coraz częściej podejmując decyzje o udostępnieniu informacji niejawnych, trzeba będzie skuteczniej uzasadniać znaczenie niejawności informacji, natomiast — udzielając odmownej decyzji o dostępie do informacji — postępować zgodnie z ustawą, wydając szczegółowsze uzasadnienie, argumentujące, jakie czynniki i elementy za tym przemawiają.

Reasumując, można ogólnie powiedzieć, że są to rozwiązanie prawne na wzór tych już obowiązujących w większości państwach członkowskich Unii Europejskiej i NATO, a więc już znane i nieodosobnione, lecz oparte na pewnych i sprawdzonych standardach.

Ewa Pachura[1]
Beata Speichert-Zalewska[2]
Mariusz Wojtalewicz[3]

Procesowe wykorzystanie pułapki kryminalistycznej w kontrolowanym wręczeniu korzyści majątkowej

Streszczenie: *Artykuł przedstawia wybrane zagadnienia związane z wykorzystaniem przez policjantów w postępowaniu przygotowawczym pułapki kryminalistycznej w związku z realizacją kontrolowanego wręczenia korzyści majątkowej. Autorzy zaprezentowali możliwości wykorzystania niektórych czynności operacyjno-rozpoznawczych wprost do celów dowodowych. Opisano tu kwestie kryminalistycznego zabezpieczenia pieniędzy lub przedmiotów wartościowych użytych do kontrolowanego wręczenia korzyści majątkowej, co często ma kluczowe znaczenie w całym procesie dowodowym. W artykule podjęto próbę usystematyzowania działań Policji związanych z wykorzystaniem w procesie materiałów zdobytych dzięki zastosowaniu użytych środków technicznych.*

Słowa kluczowe: *pułapka kryminalistyczna, proces, kontrolowane wręczenie korzyści majątkowej*

Abstract: *The article presents selected issues related to the use of a trap by law enforcement in order to prepare for the controlled handover of funds. The authors list various possibilities of using some of the operational activities in order to collect the evidence. The article further describes how to secure the money or other valuables used in the events of controlled handover of funds which is often essential for the entire process of evidence collection. It has been attempted to systematize the activities taken up by law enforcement in relation to the use of evidence collected in the process.*

Keywords: *trap, process, controlled handover of funds*

Policja, wykonując swoje ustawowe zadania, zobowiązana jest m.in. do wykrywania przestępstw oraz ścigania ich sprawców[4]. W ustawie o Policji z 6 kwietnia 1990 r.[5] sprecyzowano, jakie czynności mogą zostać podjęte w celu rozpoznawania i wykrywania przestępstw oraz zapobiegania im. Są to czynności: operacyjno-rozpoznawcze, dochodzeniowo-śledcze oraz administarcyjno-porządkowe.

Czynności operacyjno-rozpoznawcze to system niejawnych działań organów policyjnych prowadzonych poza procesem karnym, ale zazwyczaj służących aktualnym bądź przyszłym celom tego procesu[6]. Aby osiągnąć poszczególne cele pracy operacyjnej, Policja posługuje się określonymi metodami[7].

Progresja zjawisk przestępczych w Polsce, cechujących się zwłaszcza zagrożeniami o charakterze zorganizowanym i korupcyjnym, stanowiła o zasadności decyzji wprowadzenia do systemu prawnego naszego kraju niekonwencjonalnych operacyjnych metod wykrywczych bazujących na swego rodzaju podstępie[8]. Opisana sytuacja spowodowała konieczność wykorzystania niektórych czynności operacyjno-rozpoznawczych wprost do celów dowodowych. Takimi działaniami jest m.in. kontrolowane wręczenie korzyści majątkowej. Mimo tego, że jest to metoda pracy operacyjnej realizowana w sposób niejawny, to jednak dla prawidłowego jej przeprowadzenia konieczny jest udział policjantów z dużym doświadczeniem zawodowym, znających przepisy prawne w tym zakresie, i to nie tylko związane z pracą operacyjną, ale również z wykorzystaniem dowodowym uzyskanego materiału. Nie bez znaczenia pozostaje również kwestia kryminalistycznego zabezpieczenia pieniędzy lub przedmiotów wartościowych użytych do kontrolowanego wręczenia korzyści majątkowej. Często założenie prawidłowej pułapki kryminalistycznej ma kluczowe znaczenie w całym procesie dowodowym.

---

[1] Insp. mgr Ewa Pachura — absolwentka prawa na Uniwersytecie Wrocławskim (2002); uzyskane nagrody i wyróżnienia: Złoty Krzyż Zasługi — 2016, Srebrna Odznaka: „Zasłużony Policjant" — 2010; obecnie uczestniczka seminarium doktoranckiego w Zakładzie Procesu Karnego Wydziału Prawa i Administracji Uniwersytetu Warmińsko-Mazurskiego w Olsztynie; obecnie zajmuje stanowisko zastępcy komendanta wojewódzkiego Policji w Gdańsku, wcześniej przez 6 lat była naczelnikiem Wydziału Dochodzeniowo-Śledczego KWP w Gdańsku; autorka artykułów w miesięczniku „Pomorska Policja" nr 10/2007, nr 6/2008, nr 12/2007; oraz artykułów w publikacjach zwartych, np.: *Praktyczne aspekty czynności Policji w postępowaniu w sprawach z oskarżenia prywatnego* [w:] *Czynności dochodzeniowo-śledcze i działania operacyjne Policji a rola sądu w postępowaniu przygotowawczym* (materiały pokonferencyjne) — pod redakcją S. Lelentala, J. Kudrelka, I. Nowickiej, Szczytno 2008; *Metody wykrywcze XXI wieku* [w:] *Edukacja dla bezpieczeństwa. Służby specjalne w systemie bezpieczeństwa państwa, Praktyczne aspekty bezpieczeństwa* — pod red. M. Ilnickiego, A. Piotrowskiego, Poznań 2012; *Zaginięcia osób jako problem społeczno-prawny XXI wieku* [w:] *Edukacja dla bezpieczeństwa. Wyzwania i zagrożenia w XXI wieku* — pod redakcją M. Borkowskiego, M. Stańczyk-Minkiewicz, I. Ziemkiewicz-Gawlicz, Poznań 2013; *Ewaluacja możliwości wykrywczych w kontekście przedawnienia przestępstw* [w:] *Bezpieczeństwo publiczne w wymiarze lokalnym — wyzwania XXI wieku* pod red. M. Darabasza, Elbląg 2013.
Kontakt z autorką za pośrednictwem redakcji.

[2] Mł. insp. mgr Beata Speichert-Zalewska — absolwentka biologii na Uniwersytecie Gdańskim o specjalności biologia molekularna. Od 1998 r. specjalista w Laboratorium Kryminalistycznym KWP w Gdańsku. Od 2001 r biegły z zakresu genetyki sądowej. Ukończyła specjalistyczny kurs analizy DNA Ministerstwa Sprawiedliwości USA i FBI. Autorka artykułu w kwartalniku „Policja" (4/2016) oraz szkoleń realizowanych w Szkole Policji w Pile w zakresie zwalczania przestępczości seksualnej. W 2015 r. została wyznaczona przez ministra spraw wewnętrznych i administracji na eksperta merytorycznego do prac w zespole NCBR, nadzorującym realizację projektu pn. *Genetyczny portret sprawcy oraz ofiary przestępstwa — opracowanie systemu do określania wyglądu człowieka i pochodzenia biogeograficznego poprzez analizę DNA z wykorzystaniem sekwencjonowania następnej generacji (NGS)*. Obecnie zajmuje stanowisko naczelnika Laboratorium Kryminalistycznego KWP w Gdańsku. Od lat zajmuje się tematyką przestępstw na tle seksualnym w aspekcie zabezpieczania śladów, a także psychologicznym portretem nieznanego sprawcy przestępstw, jak również możliwościami wykorzystania registratury bazy danych DNA.
Kontakt z autorką za pośrednictwem redakcji.

[3] Nadkom. mgr Mariusz Wojtalewicz — absolwent administracji na Wydziale Prawa i Administracji Uniwersytetu Gdańskiego (2005 r.), w 2015 r. ukończył studia podyplomowe w zakresie taktyki i techniki zwalczania współczesnych form przestępczości zorganizowane w WSPol w Szczytnie, od 2004 r. funkcjonariusz Wydziału dw. z Korupcją KWP w Gdańsku, od 2008 naczelnik Wydziału dw. z Korupcją KWP w Gdańsku.
Kontakt z autorem za pośrednictwem redakcji.