OCHRONA DANYCH OSOBOWYCH w służbach mundurowych

JANUSZ BECKER

W książce omówiono zagadnienia dotyczące ochrony danych osobowych w różnych służbach mundurowych. Pozycja skierowana jest do wykładowców i studentów szkół wyższych o kierunku bezpieczeństwo wewnętrzne. Będzie również przydatna dla wszystkich osób zainteresowanych tematyką ochrony danych osobowych.

Janusz Becker jest doktorem nauk humanistycznych w dziedzinie historii najnowszej, absolwentem Uniwersytetu Humanistyczno-Przyrodniczego w Siedlcach, Akademii Humanistycznej w Pułtusku, Wyższej Szkoły Policji w Szczytnie, Polskiej Akademii Nauk, wieloletnim funkcjonariuszem służb mundurowych, m.in. CBA, oficerem Policji w stanie spoczynku, wykładowcą akademickim (Akademia Obrony Narodowej, Wyższa Szkoła Bezpieczeństwa i Ochrony), autorem publikacji z dziedziny bezpieczeństwa wewnętrznego, historii policji i ochrony danych osobowych.

Janusz Becker

Ochrona danych osobowych w służbach mundurowych

Sorus

Redaktor prowadzący
Wojciech Nowakowski

Redakcja
Aleksandra Zok-Smoła

Projekt okładki
Emilia Dajnowicz

Wydanie I, Poznań 2023

ISBN 978-83-67139-11-3 e-book

Wydawnictwo Sorus
Księgarnia internetowa: www.sorus.pl

Przygotowanie, druk i dystrybucja
DM Sorus sp. z o.o.
ul. Bóżnicza 15/6, 61-751 Poznań tel.
+48 61 653 01 43
sorus@sorus.pl

Spis treści

Rozdział I

Ochrona danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości

W dniu uchwalenia RODO, czyli 27 kwietnia 2016 roku[1], został w rzeczywistości przyjęty cały pakiet legislacyjny związany z ochroną danych osobowych. Oprócz ogólnego rozporządzenia o ochronie danych osobowych została również przyjęta Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW[2]. Celem dyrektywy 2016/680 jest zapewnienie lepszej ochrony danych osobowych obywateli Unii Europejskiej w związku z zapobieganiem i zwalczaniem przestępczości. Prawodawca unijny zwrócił uwagę na to, że szybki postęp techniczny i cywilizacyjny powoduje wyzwania dla prawnej ochrony danych osobowych. Współcześnie dane osobowe mogą być przetwarzane na niespotykaną dotąd skalę, np. w celu zapobiegania przestępczości.

---

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

[2] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW.

Dwudziestego piątego maja 2018 r. w Unii Europejskiej zaczęły obowiązywać przepisy ogólnego rozporządzenia o ochronie danych osobowych (RODO). Dyrektywa policyjna jest aktem prawnym, który dotyczy tylko przetwarzania danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości. Jej stosowanie w porządkach prawnych państw członkowskich wymagało implementacji, czyli wdrożenia przepisów na podstawie dyrektywy na mocy krajowego aktu prawnego. W Polsce implementacja następuje przez uchwalenie ustawy po przejściu całego procesu legislacyjnego. Dyrektywa policyjna jest aktem prawnym, który dotyczy tylko przetwarzania danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości. Jej stosowanie, jak już wspomniano, w porządkach prawnych państw członkowskich wymaga implementacji, czyli wdrożenia przepisów na podstawie dyrektywy na mocy krajowego aktu prawnego.

Wspomniane dyrektywa unijna obejmuje przetwarzanie danych osobowych w określonych celach. Ma być ono związane z rozpoznawaniem, zapobieganiem, wykrywaniem i zwalczaniem czynów zabronionych. Dyrektywa reguluje przypadki przetwarzania informacji o osobach, m.in. w celu minimalizowania zagrożeń dla bezpieczeństwa oraz ochrony porządku publicznego. Obejmuje także prowadzenie postępowań w sprawach dotyczących tych czynów oraz wykonywanie wydanych w nich orzeczeń, kar porządkowych i środków przymusu.

Na podstawie nowych przepisów organy państwowe mogą korzystać z danych osobowych wyłącznie w ściśle określonych celach oraz pod kontrolą niezależnego od rządu organu ochrony danych osobowych, np. w Polsce jest nim Prezes Urzędu Ochrony Danych Osobowych.

Nowa regulacja ustawowa zakłada przede wszystkim konieczność zachowania równowagi pomiędzy prawem osób do prywatności, w tym do ochrony danych osobowych, a koniecznością przetwarzania tych danych przez takie służby, jak policja czy Straż Graniczna w zakresie prowadzonych przez nie postępowań. Takie użycie danych osobowych powinno cechować się zachowaniem szczególnej poufności.

Jak już wspomniano, nadzór nad zgodnym z prawem przetwarzaniem danych osobowych w związku z zapobieganiem i zwalczaniem

przestępczości sprawuje Prezes Urzędu Ochrony Danych Osobowych. Może on w szczególności monitorować stosowanie przepisów ustawy, przeprowadzać kontrole przetwarzania danych osobowych i rozpatrywać zażalenia osób, których prawa zostały naruszone.

Biorąc pod uwagę powyższe ustalenia, w grudniu 2018 r. Sejm RP uchwalił ustawę o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[3]. Ustawa określa prawa osób, których dane będą przetwarzane, współpracę z UE oraz kary za naruszenie przepisów ustawy. Założenia ustawy wpisują się w ogólne zasady dotyczące przetwarzania danych osobowych wynikające z RODO. Zgodnie z przepisami administratorzy danych osobowych będą mieli obowiązek przeprowadzania analizy przetwarzanych danych pod kątem tego, czy nie upłynął czas niezbędny do ich posiadania. Jeżeli dane nie są już niezbędne do celu, w jakim je zebrano, powinny zostać przez administratora usunięte. Wiąże się to także z zasadą celowości przetwarzania danych osobowych oraz koniecznością ich aktualizowania. Co więcej, administratorzy, którzy przetwarzają dane wskazane w ustawie, są zobowiązani do opracowania polityki ochrony danych.

Przepisy dyrektywy policyjnej miały zostać transponowane do krajowego porządku prawnego do 6.05.2018 r., tak się jednak nie stało. W związku z tym, aby nie powstała luka w zakresie podstawy prawnej przetwarzania danych osobowych, częściowo pozostawiono jako obowiązującą Ustawę z dnia 29.08.1997 r. o ochronie danych osobowych[4]. Część przepisów dawnej ustawy zachowała moc w odniesieniu do przetwarzania danych osobowych w celu rozpoznawania, zapobiegania, wykrywania i zwalczania czynów zabronionych, prowadzenia postępowań w sprawach dotyczących tych czynów oraz wykonywania orzeczeń w nich wydanych, kar porządkowych i środków przymusu w zakresie określonym w przepisach stanowiących podstawę działania służb i organów uprawnionych do realizacji zadań w tym zakresie.

[3] Dz.U. 2019, poz. 125.

[4] Dz.U. 1997, nr 133, poz. 883.

Niestety akt prawny, czyli ustawa wdrażająca przedmiotową dyrektywę, budzi liczne kontrowersje, ponieważ nie ma zastosowania do służb specjalnych, tj. Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego i Centralnego Biura Antykorupcyjnego, w zakresie zapewnienia bezpieczeństwa narodowego.

Na podstawie dyrektywy państwa członkowskie zobowiązane są przyjąć przepisy, zgodnie z którymi policja i inne podmioty zajmujące się przeciwdziałaniem przestępczości mogą pobierać tylko te dane, które są niezbędne do realizacji ich zadań. Żadnych danych na zapas, dla wygody i na wszelki wypadek. Prawo unijne pozostawia jednak furtkę w postaci „bezpieczeństwa narodowego" – ci, którzy się nim zajmują, nie podlegają ograniczeniom wynikającym z dyrektywy. Zgodnie z definicją bezpieczeństwo narodowe to nie tylko praca kontrwywiadowcza prowadzona przez kontrwywiad wojskowy czy zapobieganie terroryzmowi przez Agencję Bezpieczeństwa Wewnętrznego, ale nawet przeciwdziałanie korupcji w sporcie. Efektem tego jest fakt, iż pięć typów służb specjalnych zostało wyjętych spod zakresu obowiązywania nowych przepisów i w konsekwencji nie ma żadnych ograniczeń związanych z pozyskiwaniem danych osobowych.

Ustawa z dnia 14.12.2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[5], określa:

– zasady i warunki ochrony danych osobowych przetwarzanych przez właściwe organy w celu rozpoznawania, zapobiegania, wykrywania i zwalczania czynów zabronionych, w tym zagrożeń dla bezpieczeństwa i porządku publicznego, a także wykonywania tymczasowego aresztowania, kar, kar porządkowych i środków przymusu skutkujących pozbawieniem wolności;

– prawa osób, których dane osobowe są przetwarzane przez właściwe organy, oraz środki ochrony prawnej przysługujące tym osobom;

– sposób prowadzenia nadzoru nad ochroną danych osobowych przetwarzanych przez właściwe organy, z wyłączeniem danych osobowych przetwarzanych przez prokuraturę i sądy;

[5] Dz.U. 2019, poz. 125.

– zadania organu nadzorczego oraz formy i sposób ich wykonania;

– obowiązki administratora i podmiotu przetwarzającego oraz inspektora ochrony danych, a także tryb jego wyznaczania;

– sposób zabezpieczenia danych osobowych;

– tryb współpracy z organami nadzorczymi w innych państwach Unii Europejskiej;

– odpowiedzialność karną za naruszenie przepisów niniejszej ustawy.

Głównym celem nowych przepisów ma być zapewnienie skutecznej współpracy wymiaru sprawiedliwości w sprawach karnych oraz policji z innymi partnerami/ organami z państw członkowskich. Ustawa reguluje zasady ochrony danych osobowych, m.in. w odniesieniu do czynności operacyjno-rozpoznawczych, dochodzeniowo-śledczych i administracyjno-porządkowych, które są związane z zapobieganiem i zwalczaniem przestępczości. Dzięki tej ustawie zostały wzmocnione przede wszystkim prawa osób w zakresie ochrony ich danych osobowych.

Osoby, których dane są przetwarzane w związku z zapobieganiem i zwalczaniem przestępczości, tak jak w RODO, mają m.in. prawo dostępu do swoich danych osobowych, ich uzupełnienia, uaktualnienia lub sprostowania, a także prawo do ich usunięcia w przypadku, gdy zostały zebrane lub są przetwarzane z naruszeniem przepisów ustawy. Zgodnie z art. 16 ustawy administrator dokonuje weryfikacji danych osobowych w terminach określonych przez przepisy szczególne, regulujące działania właściwego organu, a jeżeli przepisy te nie określają terminu – nie rzadziej niż co 10 lat od dnia zebrania, uzyskania, pobrania lub aktualizacji danych. Weryfikacja jest dokonywana w celu ustalenia, czy istnieją dane, których dalsze przechowywanie jest zbędne. Zbędne dane będą usuwane.

Warto zaznaczyć, że organem nadzorczym kontrolującym przetwarzanie danych jest Prezes Urzędu Ochrony Danych Osobowych. Przepisów ustawy nie stosuje sie jednakże w odniesieniu do danych osobowych znajdujących się w aktach spraw lub czynności w urządzeniach ewidencyjnych, w tym tworzonych i przetwarzanych z wykorzystaniem technik informatycznych, prowadzonych na podstawie ustawy o postę-

powaniu w sprawach nieletnich[6], ustawy Kodeks karny wykonawczy[7], ustawy Kodeks postępowania karnego[8], ustawy Kodeks karny skarbowy[9], ustawy Kodeks postępowania w sprawach o wykroczenia[10], ustawy o postępowaniu wobec osób z zaburzeniami psychicznymi stwarzających zagrożenie życia, zdrowia lub wolności seksualnej innych osób[11], ustawy Prawo o prokuraturze[12]. W praktyce oznacza to, że w tych przypadkach ustawa nie ma zastosowania, a tym samym nadzór Prezesa Urzędu Ochrony Danych Osobowych nad przetwarzaniem danych co do zasady jest wyłączony w ramach prowadzonego konkretnego postępowania – co jest niezgodne z dyrektywą 2016/680[13].

Ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i przeciwdziałaniem przestępczości nakłada nowe obowiązki na administratorów danych. Są oni zobligowani m.in. do opracowania polityki ochrony danych oraz dokonywania w określonych terminach oceny, które z posiadanych danych są zbędne i należy je usunąć. Zgodnie z przepisami ustawy dane będą mogły być przetwarzane wyłącznie w uzasadnionych celach.

Ustawa umożliwia dostęp do informacji o przetwarzanych danych przez służby publiczne osobom, których dane dotyczą, a także możliwość wniesienia ich aktualizacji, sprostowania lub usunięcia. Administrator danych (właściwy organ, który samodzielnie lub wspólnie z innym organem ustala cele i sposoby przetwarzania danych osobowych, albo podmiot wskazany przez ustawę jako administrator danych oso-

[6] Dz.U. 1982, nr 35, poz. 228.

[7] Dz.U. 1997, nr 90, poz. 557.

[8] Dz.U. 1997, nr 89, poz. 555.

[9] Dz.U. 1999, nr 83, poz. 930.

[10] Dz.U. 2001, nr 106, poz. 1148.

[11] Dz.U. 2014, poz. 24.

[12] Dz.U. 2016, poz. 177.

[13] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW.

bowych) będzie mógł jednak odmówić m.in. poinformowania o fakcie przetwarzania danych czy usunięcia danych, jeśli utrudni lub uniemożliwi to zwalczanie przestępstw i wykroczeń lub prowadzenie postępowań czy zagrażać będzie bezpieczeństwu państwa[14].

Nie przekazuje się informacji oraz nie udostępnia się danych osobowych, jeżeli mogłoby to powodować:

– ujawnienie informacji uzyskanych w wyniku czynności operacyjno-rozpoznawczych,

– utrudnienie lub uniemożliwienie rozpoznawania, zapobiegania, wykrywania lub zwalczania czynów zabronionych,

– utrudnienie prowadzenia postępowania karnego, karnego wykonawczego, karnego skarbowego lub w sprawach o wykroczenia lub wykroczenia skarbowe,

– zagrożenie życia, zdrowia ludzkiego lub bezpieczeństwa i porządku publicznego,

– zagrożenie bezpieczeństwa narodowego, w tym obronności lub bezpieczeństwa oraz ekonomicznych podstaw funkcjonowania państwa,

– istotne naruszenie dóbr osobistych innych osób[15].

Rzecznik Praw Obywatelskich negatywnie ocenił wyłączenia spod ustawy danych osobowych przetwarzanych w ramach realizacji zadań służb specjalnych, tj. Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego i Centralnego Biura Antykorupcyjnego.

Zdaniem RPO nie wszystkie bowiem zadania tych służb mieszczą się w zakresie pojęcia „bezpieczeństwo narodowe", co uzasadniałoby wyłączenie uznane za dopuszczalne przez tzw. dyrektywę policyjną. Według RPO z punktu widzenia prawa UE pojęcie „bezpieczeństwo narodowe" nie może być utożsamiane z pojęciem „bezpieczeństwa narodowego". Działalność CBA nie ma według niego na przykład bezpośredniego związku z „bezpieczeństwem narodowym".

---

[14] Dz.U. 2019, poz. 125.

[15] Tamże.

Dlatego, zdaniem byłego RPO Adama Bodnara, nie można się zgodzić z pozostawieniem poza obowiązkiem stosowania przepisów o ochronie danych osobowych co najmniej pięciu służb specjalnych. Może to oznaczać, przynajmniej w części, nie tylko sprzeczność z postanowieniami dyrektywy, ale przede wszystkim z art. 51 Konstytucji RP[16] (mowa w nim m.in. o tym, że władze nie mogą gromadzić innych informacji o obywatelach niż te niezbędne do funkcjonowania demokratycznego państwa prawnego).

Liczne zastrzeżenia do przedmiotowego aktu prawnego jeszcze na etapie projektu ustawy zgłosiła również Fundacja Panoptykon.

W ocenie Fundacji[17] Panoptykon[18], które to stanowisko zostało opracowane jeszcze na etapie projektu aktu prawnego, nie stanowi on właściwego wdrożenia tzw. dyrektywy policyjnej, będącej drugim – obok RODO – elementem reformy zasad ochrony danych osobowych. W opinii Fundacji celem dyrektywy policyjnej jest wzmocnienie ochrony praw jednostki w odniesieniu do relacji z podmiotami zajmującymi się przeciwdziałaniem przestępczości. Szybki postęp techniczny i globalizacja przyniosły nowe wyzwania w dziedzinie ochrony danych osobowych: „Aby ochrona danych osobowych w Unii Europejskiej była skuteczna, należy wzmocnić prawa osób, których dane dotyczą, oraz obowiązki podmiotów, które przetwarzają dane osobowe, jak i odpowiadające im uprawnienia w zakresie monitorowania i egzekwowania przepisów o ochronie danych osobowych w państwach członkowskich".

Oceniono, że w zaproponowanym kształcie projekt ma jedynie charakter fasadowy – nie wzmocni, ale wręcz osłabi ochronę prywatności osób będących w kręgu zainteresowania policji i służb specjalnych. Zwiększa w ten sposób ryzyko nadużyć w postaci nadmiernej ingerencji w prywatność Polek i Polaków. Jednocześnie brak mechanizmów

[16] Dz.U. 1997, nr 78, poz. 483.

[17] Celem fundacji jest działanie na rzecz wolności i ochrony praw człowieka w społeczeństwie nadzorowanym; por. https://panoptykon.org/organizacja [data dostępu: 15.01.2022].

[18] Stanowisko Fundacji Panoptykon w sprawie rządowego projektu ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (druk sejmowy 2989).

kontroli nad pozyskiwaniem przez służby specjalne danych osobowych może prowadzić do osłabienia bezpieczeństwa Rzeczpospolitej Polskiej. Zarówno osoby potencjalnie współpracujące ze służbami (np. w zakresie przeciwdziałania przestępczości terrorystycznej), jak i zagraniczne odpowiedniki polskich służb nie mogą mieć bowiem pewności, że przekazane polskim służbom dane zostaną wykorzystane w sposób zgodny z przeznaczeniem. Ponadto przedmiotowym przepisom zarzucono, że:

1. Służby specjalne będą pozostawały poza kontrolą, ponieważ przepisów nie stosuje się m.in. do ochrony danych osobowych przetwarzanych „w związku z zapewnieniem bezpieczeństwa narodowego, w tym w ramach realizacji zadań ustawowych ABW, AW, SKW, SWW oraz CBA". Zgodnie z dyrektywą, jej przepisy nie znajdują zastosowania w odniesieniu do przetwarzania danych osobowych w zakresie bezpieczeństwa narodowego. Pojęcie to nie jest jednak zdefiniowane. Jego wykładni należy zatem poszukiwać na gruncie art. 73 Traktatu o funkcjonowaniu Unii Europejskiej[19], zgodnie z którym państwa członkowskie mogą organizować współpracę między służbami odpowiedzialnymi właśnie za zapewnienie bezpieczeństwa narodowego. Jak zwracają uwagę autorzy komentarza do tego przepisu, „Bezpieczeństwo narodowe (ang. *national security*) najczęściej rozumiane jest jako jedna z podstawowych funkcji każdego państwa, która obejmuje problematykę przeciwstawienia się wszelkim zagrożeniom zewnętrznym oraz wewnętrznym dla istnienia oraz rozwoju narodu i państwa". Nie sposób zgodzić z zaproponowanym przez projektodawcę podejściem, że wszystkie działania podejmowane przez służby specjalne (ABW, AW, SKW, SWW i CBA) mieszczą się w zakresie tego pojęcia. Szczególnie jest to widoczne w kontekście zadań ustawowych Centralnego Biura Antykorupcyjnego, wśród których wymienić można np. rozpoznawanie, zapobieganie i wykrywanie przestępstw przeciwko zasadom rywalizacji sportowej. Należy przy tym zwrócić uwagę, że bez względu na zakres tzw. dyrektywy policyjnej konieczność ochrony danych osobowych w służbach specjalnych wynika

[19] Consolidated version of the *Treaty on the Functioning of the European Union* OJ C 326, 26.10.2012, p. 47–390 (BG, ES, CS, DA, DE, ET, EL, EN, FR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV) OJ C 326, 26.10.2012, p. 47–390 (GA).

także z zasad konstytucyjnych (por. art. 51 Konstytucji). Tymczasem w brzmieniu projektu aktu normatywnego nie sposób dopatrzyć się zasad, w oparciu o które przetwarzane i chronione będą dane osobowe, np. w ABW.

2. Osobom, których dotyczą dane, odbiera się prawa. Zgodnie z ustawą (art. 26 ust. 1) osobie, której dane dotyczą, nie przekazuje się informacji na ten temat m.in. wtedy, gdy mogłoby to spowodować ujawnienie informacji uzyskanych w wyniku czynności operacyjno-rozpoznawczych, a także jeśli mogłoby to utrudnić rozpoznawanie i zwalczanie czynów zabronionych.

Przesłanki umożliwiające ograniczenie praw informacyjnych jednostki wymienia art. 13 ust. 3 dyrektywy. Zdaniem fundacji projektodawca wykroczył poza przesłanki wskazane w dyrektywie, poprzez brak przesłanki niezbędności i proporcjonalności ograniczenia. Przede wszystkim dyrektywa umożliwia ograniczenie prawa do informacji wyłącznie w sytuacji, w której jest to konieczne i proporcjonalne w społeczeństwie demokratycznym. Projektodawca nie wprowadził analogicznego rozwiązania.

Przewidziane w dyrektywie dopuszczalne ograniczenia praw jednostki wiążą się z zagrożeniami, które mogą wywołać ujawnienie informacji (np. związanych z bezpieczeństwem publicznym czy narodowym) lub ze sprawnym przeprowadzeniem czynności urzędowych i zapobieganiem przestępczości. Tymczasem zgodnie z ustawą (art. 26 ust. 1 pkt 1) nie mogą być ujawniane informacje uzyskane w wyniku czynności operacyjno-rozpoznawczych. Oznacza to, że projektodawca przyjął źródło informacji jako kryterium umożliwiające odmowę realizacji prawa jednostki. Pozyskanie jednak informacji w ramach czynności operacyjno-rozpoznawczych nie zawsze będzie wiązać się z jedną z przesłanek przewidzianych w dyrektywie, zwłaszcza w obliczu upływu czasu od przeprowadzenia czynności operacyjno-rozpoznawczych. Tymczasem prawo do informacji na temat przetwarzania danych osobowych jest podstawowym i fundamentalnym uprawnieniem jednostki – bez wiedzy, że policja czy Straż Graniczna przetwarza dane osobowe, jednostka nie będzie mogła potencjalnie zakwestionować zgodności z prawem tego działania lub np. zażądać ich uzupełnienia czy sprostowania.

3. Wyłączenie ochrony danych osobowych na podstawie reżimu ochrony informacji niejawnych. Zgodnie z art. 84 ustawy, wprowadzającym zmiany do ustawy o ochronie informacji niejawnych[20], do danych osobowych stanowiących informacje niejawne nie stosuje się przepisów o ochronie danych osobowych. Tymczasem definicja informacji o charakterze niejawnym jest niezwykle pojemna, obejmuje bowiem wszystkie informacje, których ujawnienie „spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej".

Wśród informacji niejawnych o charakterze „poufne" ustawa wymienia informacje, których ujawnienie utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę bezpieczeństwa, z kolei informacje niejawne „zastrzeżone" to informacje, których ujawnienie może mieć szkodliwy wpływ na wykonywanie przez organy władzy publicznej ich zadań (m.in. w zakresie bezpieczeństwa publicznego). Jak zwrócili uwagę autorzy uzasadnienia projektu ustawy, pojęcia danych osobowych i informacji niejawnych częściowo się pokrywają. Ustawa o ochronie informacji niejawnych formułuje szereg warunków związanych z ochroną przed nieuprawnionym dostępem do tych informacji, w pewnym zakresie należy zatem zgodzić się z tezą projektodawcy, że „przepisy ustawy o ochronie informacji niejawnych zapewniają daleko idącą ochronę danych osobowych". Ustawodawca stracił jednak z pola widzenia fakt, że na ochronę danych osobowych składa się nie tylko ich zabezpieczenie przed nieuprawnionym dostępem, ale także szereg uprawnień osób, których dane dotyczą (m.in. prawo dostępu do danych), a także prawo do zakwestionowania legalności przetwarzania danych przed niezależnym organem kontrolnym. W polskim systemie prawnym brakuje skutecznych mechanizmów weryfikujących, czy uznanie konkretnej informacji za informację niejawną nie jest nadmiarowe. W konsekwencji prowadzi to do faktycznego podważenia możliwości skutecznej ochrony danych osobowych, dane osobowe będą bowiem mogły być w sposób arbitralny i nadmiarowy uznawane za informacje niejawne. Komentowany przepis nie tylko uniemożliwi jednostce prawo żądania realizacji jej uprawnień,

[20] Dz.U. 2010, nr 182, poz. 1228.

ale także zablokuje możliwość działania Prezesowi Urzędu Ochrony Danych Osobowych, którego zadaniem ma być stanie na straży przestrzegania ochrony danych osobowych także w sektorze bezpieczeństwa.

Problemy te w praktyce mogą doprowadzić do uniemożliwienia jednostce ochrony swoich praw. Tymczasem opisane wyżej zagadnienia mają jedynie charakter przykładowy. Dlatego nieprzypadkowo przepisy ustawy są komentowane niezwykle krytycznie nie tylko przez instytucje zajmujące się ochroną praw człowieka (np. Rzecznik Praw Obywatelskich, organizacje pozarządowe).

W opinii autora wyłączenie przez ustawę przekazania informacji oraz nieudostępnianie danych osobowych jest jednak w pełni uzasadnione, jeżeli mogłoby ono powodować:

– ujawnienie informacji uzyskanych w wyniku czynności operacyjno-rozpoznawczych;

– utrudnienie lub uniemożliwienie rozpoznawania, zapobiegania, wykrywania lub zwalczania czynów zabronionych;

– utrudnienie prowadzenia postępowania karnego, karnego wykonawczego, karnego skarbowego lub w sprawach o wykroczenia lub wykroczenia skarbowe;

– zagrożenie życia, zdrowia ludzkiego lub bezpieczeństwa i porządku publicznego;

– zagrożenie bezpieczeństwa narodowego, w tym obronności lub bezpieczeństwa oraz ekonomicznych podstaw funkcjonowania państwa;

– istotne naruszenie dóbr osobistych innych osób.

Nie sposób bowiem wyobrazić sobie pracy służb bezpieczeństwa Państwa bez możliwości zachowania informacji o zainteresowaniu daną osobą. Stawiałoby to pod znakiem zapytania istnienie i funkcjonowanie tych służb. Interes Państwa jest w tym przypadku ważniejszy od praw jednostki i jej indywidualnych praw, w tym prawa do ochrony danych osobowych. Niezwykle istotną okolicznością w tym przypadku jest już samo zobowiązanie administratorów danych osobowych do ich sukcesywnej weryfikacji i ewentualnego usuwania w przypadku stwierdzenia braku przydatności, a także kontrola przestrzegania tego obowiązku przez niezależny organ administracji publicznej.