Do druku nr 154

PIERWSZY PREZES
SĄDU NAJWYŻSZEGO
RZECZYPOSPOLITEJ POLSKIEJ

BSA II-021-536/15

Warszawa, dnia 25 stycznia 2016 r.

SEKRETARIAT Z-CY SZEFA KS
L. dz. AP-173-30/16
Data wpływu 26.01.2016

Pan
Adam Podgórski
Zastępca Szefa
Kancelarii Sejmu

Szanowny Panie Ministrze,

W odpowiedzi na pismo z dnia 28 grudnia 2015 r., GMS-WP-173-293/15 uprzejmie przesyłam uwagi Sądu Najwyższego do ***poselskiego projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw.***

Z poważaniem

Prof. dr hab. Małgorzata Gersdorf

SĄD NAJWYŻSZY
BIURO STUDIÓW i ANALIZ
Pl. Krasińskich 2/4/6, 00-951 Warszawa

Warszawa, dnia 25 stycznia 2016 r.

BSA II – 021 – 536/15

Opinia
w sprawie poselskiego projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw

I. Przedłożony do zaopiniowania projekt ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw ma na celu, w założeniach projektodawców, wykonanie obowiązku dostosowania systemu prawa do wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r., K 23/11 (sentencja wyroku została opublikowana w Dz. U. z 2014 r., poz. 1055), w zakresie w jakim stwierdzono w nim, że „(...) 2) art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. b ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (...) jest niezgodny z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji (....) 5) a) art. 20c ust. 1 ustawy o Policji, b) art. 10b ust. 1 ustawy o Straży Granicznej, c) art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej, d) art. 30 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, e) art. 28 ust. 1 pkt 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, f) art. 32 ust. 1 pkt 1 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, g) art. 18 ust. 1 pkt 1 ustawy o Centralnym Biurze Antykorupcyjnym, h) art. 75d ust. 1 ustawy z dnia 27 sierpnia 2009 r. o Służbie Celnej (Dz. U. z 2013 r. poz. 1404 oraz z 2014 r. poz. 486) – przez to, że nie przewidują niezależnej kontroli udostępniania danych telekomunikacyjnych, o których mowa w art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243), są niezgodne z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji, 6a) art. 19 ustawy o Policji, b) art. 9e ustawy o Straży Granicznej, c) art. 36c ustawy o kontroli skarbowej, d) art. 31 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, e) art. 27

ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, f) art. 31 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, g) art. 17 ustawy o Centralnym Biurze Antykorupcyjnym – w zakresie, w jakim nie przewidują gwarancji niezwłocznego, komisyjnego i protokolarnego zniszczenia materiałów zawierających informacje objęte zakazami dowodowymi, co do których sąd nie uchylił tajemnicy zawodowej bądź uchylenie było niedopuszczalne, są niezgodne z art. 42 ust. 2, art. 47, art. 49, art. 51 ust. 2 i art. 54 ust. 1 w związku z art. 31 ust. 3 Konstytucji (....) 8) a) art. 28 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, b) art. 32 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, c) art. 18 ustawy o Centralnym Biurze Antykorupcyjnym – w zakre sie, w jakim nie przewidują zniszczenia danych niemających znaczenia dla prowadzonego postępowania, są niezgodne z art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji, 9) art. 75d ust. 5 ustawy o Służbie Celnej w zakresie, w jakim zezwala na zachowanie materiałów innych, niż zawierające informacje mające znaczenie dla postępowania w sprawach wykroczeń skarbowych lub przestępstw skarbowych określonych w rozdziale 9 ustawy z dnia 10 września 1999 r. – Kodeks karny skarbowy (Dz. U. z 2013 r. poz. 186, ze zm.), jest niezgodny z art. 51 ust. 4 Konstytucji.

II. W związku z powyższym wyrokiem Trybunału Konstytucyjnego w projekcie zakłada się znowelizowanie wyżej wskazanych ustaw w zakresie w jakim zawierają regulacje dotyczące kontroli operacyjnej, pozyskiwania danych telekomunikacyjnych, pocztowych i internetowych, ochrony tajemnicy zawodowej w toku kontroli operacyjnej oraz niszczenia zbędnych danych telekomunikacyjnych, pocztowych i internetowych.

III. Przed merytorycznym odniesieniem się do planowanych zmian wskazać należy, że z orzeczenia Trybunału Konstytucyjnego dnia 30 lipca 2014 r., K 23/11, które dało asumpt do przeprowadzenia opiniowanej nowelizacji, jasno wynika, jakie są minimalne wymagania, które muszą być zrealizowane przez regulację dotyczącą niejawnego pozyskiwanie przez władze publiczne informacji o jednostkach, tj.:

- gromadzenie, przechowywanie oraz przetwarzanie danych dotyczących jednostek, a zwłaszcza sfery prywatności, dopuszczalne jest wyłącznie na podstawie wyraźnego i precyzyjnego przepisu ustawy;

- konieczne jest precyzyjne określenie w ustawie organów państwa upoważnionych do gromadzenia oraz przetwarzania danych o jednostce, w tym do stosowania czynności operacyjno-rozpoznawczych;
- w ustawie muszą być sprecyzowane przesłanki niejawnego pozyskiwania informacji o osobach, którymi są: wykrywanie i ściganie wyłącznie poważnych przestępstw oraz zapobieganie im; ustawa powinna wskazywać rodzaje takich przestępstw;
- ustawa musi określać kategorie podmiotów, wobec których mogą być podejmowane czynności operacyjno-rozpoznawcze;
- pożądane jest określenie w ustawie rodzajów środków niejawnego pozyskiwania informacji, a także rodzajów informacji pozyskiwanych za pomocą poszczególnych środków;
- czynności operacyjno-rozpoznawcze winny być subsydiarnym środkiem pozyskiwania informacji lub dowodów o jednostkach, gdy nie da się ich uzyskać w inny, mniej dolegliwy dla nich sposób;
- w ustawie należy określić maksymalny okres prowadzenia czynności operacyjno-rozpoznawczych wobec jednostek, który nie może przekraczać ram koniecznych w demokratycznym państwie prawa;
- niezbędne jest precyzyjne unormowanie w ustawie procedury zarządzenia czynności operacyjno-rozpoznawczych, obejmującej w szczególności wymóg uzyskania zgody niezależnego organu na niejawne pozyskiwanie informacji;
- precyzyjne określenie w ustawie zasad postępowania z materiałami zgromadzonymi w toku czynności operacyjno-rozpoznawczych, zwłaszcza zasad ich wykorzystania oraz niszczenia danych zbędnych i niedopuszczalnych;
- zagwarantowanie bezpieczeństwa zgromadzonych danych przed nieuprawnionym dostępem ze strony innych podmiotów;
- unormowanie procedury informowania jednostek o niejawnym pozyskaniu informacji na ich temat, w rozsądnym czasie po zakończeniu działań operacyjnych i zapewnienie na wniosek zainteresowanego poddania sądowej ocenie legalności zastosowania tych czynności; odstępstwo jest dopuszczalne wyjątkowo;

- zagwarantowanie transparentności stosowania czynności operacyjno-rozpoznawczych przez poszczególne organy władzy publicznej, przejawiające się w publicznej jawności i dostępności zagregowanych danych statystycznych, nadających się do porównania, o ilości i rodzaju stosowanych czynności operacyjno-rozpoznawczych;
- nie jest wykluczone zróżnicowanie intensywności ochrony prywatności, autonomii informacyjnej oraz tajemnicy komunikowania się z uwagi na to, czy dane o osobach pozyskują służby wywiadowcze i zajmujące się ochroną bezpieczeństwa państwa, czy też czynią to służby policyjne;
- zróżnicowanie poziomu ochrony prywatności, autonomii informacyjnej oraz tajemnicy komunikowania się może także nastąpić z uwagi na to, czy niejawne pozyskiwanie informacji dotyczy obywateli, czy osób niemających polskiego obywatelstwa

Uznać należy, że przedłożony projekt ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw powinien spełniać wszystkie przedstawione powyżej wymogi. Uchybienie im będzie istotną przesłanką skłaniająca do wyrażenia poglądu o braku poszanowania standardów konstytucyjnych.

IV. W związku z powyższymi przesłankami pozytywnie należy wypowiedzieć się o regulacjach projektu, w których przewiduje się okoliczności uzasadniające zarządzenie kontroli operacyjnej w toku czynności operacyjno-rozpoznawczych prowadzonych przez Policję, Straż Graniczną (dalej SG), Wywiad Skarbowy (dalej WS), Żandarmerię Wojskową (dalej ŻW), Służbę Kontrwywiadu Wojskowego (dalej SKW) i Agencję Bezpieczeństwa Wewnętrznego (dalej ABW). W odniesieniu do „przestępstw ściganych na mocy umów i porozumień międzynarodowych", „przestępstw godzących w bezpieczeństwo państwa", czy „bezpieczeństwo Sił Zbrojnych, jednostek organizacyjnych MON i państw zapewniających wzajemność" doprecyzowano, że każdorazowo kontrola operacyjna może zostać zarządzona wyłącznie w odniesieniu do przestępstw ściganych na mocy umów międzynarodowych ratyfikowanych za uprzednią zgodą wyrażoną w ustawie, określonych w polskiej ustawie karnej.

Na aprobatę zasługuje również dookreślenie w odniesieniu do wyżej wskazanych służb katalogu przestępstw pozostających w związku z ich kompetencjami, do których rozpoznawania, zapobiegania i zwalczania służby te

mogą stosować kontrolę operacyjną. Wątpliwości wzbudza jednak brak wprowadzenia sprecyzowanej przesłanki w miejsce zawartego w art. art. 27 ust. 1 ustawy o ABW i AW wyrażenia normatywnego „jeżeli godzą w podstawy ekonomiczne interesu państwa". Jak pokazują zakończone i toczące się postępowania przed sądami powszechnymi, interpretacja wskazanej przesłanki budzi liczne wątpliwości. Nie jest bowiem jasne do czego przyrównywać czyny sprawców, tj. do odpowiedniego sektora gospodarki, do całości budżetu określonych instytucji publicznych czy może do całości budżetu państwa. Przy skrajnych, acz niepozbawionych racji, interpretacjach wskazanej przesłanki, zastosowanie art. 27 ust. 1 ustawy o ABW i AW jest praktycznie niemożliwe. Zastanawia także odwołanie się w treści regulacji do rozdziałów 35-37 Kodeksu karnego. Nie wszystkie bowiem z określonych tam typów czynów zabronionych pozostają we właściwości Agencje Bezpieczeństwa Wewnętrznego i Agencji Wywiadu.

V. Z aprobatą należy się odnieść do zmian mających za zasadnie ujednolicenie zakresu działania poszczególnych służb m.in. przez odesłania ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. poz. 1529, z późn. zm.), ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2013 r., poz. 1422, z późn. zm.), czy ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243, 827 i 1198). Choć powyższej uwagi nie można odczytywać jako akceptacji co do zakresu udostępniania określonych danych, jak również co do ostrości znaczeniowej stosowanej terminologii (o czym dalej).

VI. Pozytywnie należy ocenić sprecyzowanie katalogu rodzajów środków niejawnego pozyskiwania informacji, który został ujednolicony odnośnie do wszystkich służb i zawarty odpowiednio w art. 19 ust. 6 i 6a ustawy o Policji, art. 9e ust. 7 i 7a ustawy o SG, art. 36c ust. 4 i 4a ustawy o kontroli skarbowej, art. 31 ust. 7 i 7a ustawy o ŻW, art. 27 ust. 6 i 6a ustawy o ABW oraz AW, art. 31 ust. 4 i 4a ustawy o SKW oraz SWW oraz w art. 17 ust. 5 i 5a ustawy o CBA.

VII. Realizację wyroku Trybunału Konstytucyjnego K 23/11 stanowi określenie w ustawie maksymalnego czasu prowadzenia niejawnych czynności, po upływie których dalsze ich prowadzenie jest już niedopuszczalne. Zarazem nie wydaje się aby łączny czas kontroli w wymiarze 18 miesięcy przekraczał okres, który świadczyłby o naruszeniu przez ustawodawcę podstawowych praw obywatelskich i wartości ujętych w Konstytucji, a tym samym ram koniecznych w demokratycznym państwie prawa. Uzasadnione jest również, mające charakter wyjątku, odstępstwo od

warunku określenia w ustawie czasu niejawnych czynności w zakresie kontrwywiadu, które znalazło się w projektowanym art. 27 ust. 9 ustawy o ABW i AW i w art. 31 ust. 7 ustawy o SKW i SWW. Słusznie w projekcie przyjęto, że przedłużenie kontroli w każdym przypadku będzie dokonywane decyzją sądu, co zapewni kontrolę niezależnego organu nad prawidłowością działań podejmowanych przez te służby.

VIII. Realizując pkt 5 wyroku Trybunału Konstytucyjnego w sprawie K 23/11, w projekcie przewidziano, że podmiotem uprawnionym do kontroli uzyskiwania danych telekomunikacyjnych będzie odpowiedni sąd okręgowy, któremu uprawnione służby mają przekazywać raz na 6 miesięcy sprawozdania dotyczące pozyskanych danych telekomunikacyjnych, pocztowych lub internetowych wraz z określeniem ich rodzaju, rodzaju przestępstw, w związku z zaistnieniem których wystąpiono o dane telekomunikacyjne, pocztowe lub internetowe oraz liczbę przypadków, ze wskazaniem ich podziału na rodzaje spraw, w których wystąpiono o dane.

W tym zakresie wątpliwość budzi zakres wskazanej kontroli i jej ewentualne konsekwencje. Z projektu wynika jedynie, że sąd informuje szefa służby o wyniku kontroli w terminie 30 dni od jej zakończenia. Zarazem domniemywać należy, że w razie stwierdzenia nieprawidłowości sąd poinformuje również prokuratora o podejrzeniu popełnienia przestępstwa urzędniczego (przykładowo określonego w art. 231 § 1 KK). Jednakże w dalszym ciągu ustawodawca nie planuje wyposażyć sądów w skuteczny i efektywny sposób kontroli, z którym wiązałoby się faktyczne i doraźne egzekwowanie stwierdzonych naruszeń (w szczególności przez szczątkową ilość przesłanych informacji sąd pozbawiony będzie możliwości oceny adekwatności, niezbędności i celowości udostępniania danych). Wątpliwości wzbudza również wprowadzenie jedynie kontroli następczej. Ograniczenie niebezpieczeństwa arbitralnego i dyskrecjonalnego postępowania służb stanowiłoby z pewnością wdrożenie mechanizmów bazujących na konieczności uzyskania zgody uprzedniej na zebranie wskazanych danych osobowych. W tym aspekcie zauważyć należy na brak realizacji jednoznacznych wskazań wynikających z orzecznictwa Europejskiego Trybunału Sprawiedliwości (zob. wyrok z dnia 8 kwietnia 2014 r. w połączonych sprawach o sygn. C-293/12 i C-594/12 *Digital Rights Ireland*).

Systematyka projektowanej ustawy o Policji wskazuje, że z obowiązku kontroli wyłączone zostały dane telekomunikacyjne, dane pocztowe i dane internetowe uzyskane w sytuacji, o której mowa w art. 20da ust. 1 ustawy o Policji. Z uwagi na

zbieżność treściową wskazanych danych, brak nawet następczej kontroli nie znajduje jakiegokolwiek uzasadnienia.

W projekcie nie przewidziano żadnych regulacji, które nakładałyby na służby obowiązek niezwłocznego zniszczenia materiałów, co do których sąd przesłałby negatywną ocenę kontrolną. Stosowany brak przekonuje zarazem o iluzoryczności zakładanej kontroli sądowej.

IX. Zastrzeżenia wzbudza rozszerzenie zakresu udostępniania uprawnionym służbom obok danych telekomunikacyjnych także danych pocztowych – w odniesieniu do ustawy z dnia 23 listopada 2012 r. Prawo pocztowe (Dz. U. z 2012 r. poz. 1529) oraz danych internetowych – w odniesieniu do ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422). Jak słusznie zauważa się w uzasadnieniu do projektu, w wyroku Trybunału Konstytucyjnego K 23/11 w żadnym razie nie odnoszono się do powyższych danych, w szczególności Trybunał nie wskazał na konieczność rozszerzenia danych, do których dostęp będą mieć uprawnione służby. W tym przedmiocie projektowane regulacje wykraczają poza dostosowanie porządku prawnego do standardów konstytucyjnych i jako takie nie mogą być uznawane za realizację wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r., K 23/11. Co więcej, projekt nie respektuje orzeczenia w zakresie w jakim wskazuje się w nim na konieczność przyjęcia zasady subsydiarnego sięgania po dane osobowe, a więc wprowadzenia jasnego ograniczenia do przypadków, w których inne środki okazały się bezskuteczne albo nieprzydatne.

Nie negując tezy, że rozszerzenie przedmiotowego obszaru kontroli może być słuszne, zawsze zakres owego rozszerzenia należałoby każdorazowo poddać pod publiczną debatę. Dodatkowe kompetencje służb powinny zostać w sposób bardzo dokładny uzasadnione i znajdować swoje umocowanie w art. 31 ust. 3 Konstytucji RP. Zdecydowanie nie wystarczające jest wskazanie na ich podobieństwo do danych telekomunikacyjnych, w szczególności jeśli zważyć na niejasność zakresu znaczeniowego terminów „dane pocztowe" i „dane internetowe". O ile w pierwszym przypadku odesłanie do art. 82 ust. 1 pkt 1 ustawy Prawo pocztowe ma charakter klaryfikacyjny i nie pozostawia wątpliwości, że dane pocztowe to jedynie „dane o operatorze pocztowym, świadczonych usługach pocztowych oraz informacji umożliwiających identyfikację korzystających z tych usług", o tyle dane internetowe nie poddają się tak oczywistemu zawężeniu. Odesłania do art. art. 18 ust. 1-5 ustawy

o świadczeniu usług drogą elektroniczną, gdzie posłużono się klauzulą „inne dane niezbędne ze względu na właściwość świadczonej usługi lub sposób jej rozliczenia", jak również klauzulą „inne dane dotyczące usługobiorcy, które nie są niezbędne do świadczenia usługi drogą elektroniczną" powoduje, że katalog „danych internetowych" nie jest zamknięty, co rodzi obawy o jego kształtującą interpretację, mogącą polegać m.in. na przyjęciu, że dane takie to także informacje o aktywności użytkownika w Internecie, tj. o odwiedzanych przez niego stornach internetowych, o aktywności na formach dyskusyjnych, czy portalach społecznościowych. O niebezpieczeństwie takiej wykładni nie trzeba szerzej przekonywać.

W związku z powyższym, w pierwszej kolejności zachodzi potrzeba trafniejszego uzasadnienia wprowadzanych zmian, wprowadzenia klauzuli subsydiarności, jak również sprecyzowania jaki zakres desygnatów ma wyrażenie „dane internetowe".

X. Wątpliwości budzi również brak jasnego katalogu przestępstw, które uzasadniałyby możliwość udostępniania danych telekomunikacyjnych, danych pocztowych oraz danych internetowych. W tym zakresie ponownie należy odwołać się do wyroku TSUE z dnia 8 kwietnia 2014 r. w połączonych sprawach o sygn. C-293/12 i C-594/12, w którym jasno wskazano, że dostęp do danych osobowych możliwy jest jedynie w odniesieniu do „poważnych przestępstw", które powinny być enumeratywnie wskazane w ustawie. Nadmienić należy, że zawarte w projekcie rozwiązanie polegające na odesłaniu w treści art. 18 ust. 1 ustawy o CBA do art. 2 tejże ustawy uprawnia CBA m.in. do pozyskiwania danych telekomunikacyjnych, danych pocztowych i danych internetowych w celach analitycznych, co pozostaje w jawnej kolizji z celem wprowadzenia do sytemu prawa instytucji udostępniania danych.

XI. W projekcie nie przewidziano również unormowań dotyczących okresu, w jakim powyższe dane mają być przetwarzane i weryfikowane, co przekłada się na niedopuszczalną sytuację, w której dane będą mogłyby być przechowywane bez jasnych i precyzyjnych ograniczeń czasowych. Z uwagi na niekompletność zakresową, zdecydowanie niewystarczająca jest regulacja art. 20c ust. 6 i 7 ustawy o Policji (odpowiednio do kompetencji innych służb zawartych w nowelizowanych ustawach).

XII. Reasumując uwagi przedstawione w pkt. IX-XI, stwierdzić należy, że istnieją bardzo poważne obawy co do zgodności z Konstytucją art. 20c ustawy o

Policji (odpowiednio innych ustaw), jak również co do jego zgodności z prawem europejskim (m.in. z dyrektywą 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. o prywatności i łączności elektronicznej Dz. Urz. WE L 201 z 31.7.2002 ze zm.). W sposób oczywisty opiniowana regulacja stanowi także naruszenie przytoczonych powyżej warunków minimalnych sprecyzowanych przez Trybunał Konstytucyjny w orzeczeniu K 23/11.

XIII. Konsekwentnie, jako niedopuszczalną należy ocenić regulację art. 20cb ustawy o Policji (odpowiednio innych ustaw), w której wskazano, że w celu rozpoznawania, zapobiegania, zwalczania, wykrywania albo uzyskania i utrwalenia dowodów przestępstw albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych Policja może uzyskiwać dodatkowe dane. Analiza regulacji wskazuje, że dane te zostały określone bardzo szeroko i zaliczają się do nich:

- wykaz abonentów, użytkowników lub zakończeń sieci, uwzględniający dane uzyskiwane przy zawarciu umowy, o którym mowa w art. 179 ust. 9 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne,
- nazwiska i imiona, imion rodziców,
- miejsca i daty urodzenia,
- adres miejsca zamieszkania i adres korespondencyjny jeżeli jest on inny niż adres miejsca zamieszkania,
- numer ewidencyjny PESEL – w przypadku obywatela Rzeczypospolitej Polskiej,
- nazwa, seria i numeru dokumentów potwierdzających tożsamość, a w przypadku cudzoziemca, który nie jest obywatelem państwa członkowskiego Unii Europejskiej albo Konfederacji Szwajcarskiej – numeru paszportu lub karty pobytu,
- zawartą w dokumentach potwierdzających możliwość wykonania zobowiązania wobec dostawcy publicznie dostępnych usług telekomunikacyjnych wynikającego z umowy o świadczenie usług telekomunikacyjnych,
- inne dane użytkownika pozyskane w związku ze świadczoną usługą, w szczególności numer konta bankowego lub karty płatniczej, a także adres poczty elektronicznej oraz numery telefonów kontaktowych, tj. dane o których mowa w art. 161 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne,

- w przypadku użytkownika, który nie jest osobą fizyczną numer zakończenia sieci oraz siedzibę lub miejsce wykonywania działalności gospodarczej, firmę lub nazwę i formę organizacyjną tego użytkownika,
- w przypadku stacjonarnej publicznej sieci telekomunikacyjnej, nazwę miejscowości oraz ulicy, przy której znajduje się zakończenie sieci, udostępnione użytkownikowi.

Oprócz uchybień zbieżnych z opisanymi w pkt X-XIII niniejszej opinii, w projekcie nie zawarto żadnych procedur kontrolnych dotyczących pozyskiwania informacji tego rodzaju, co przy jednoczesnym braku obowiązku informacyjnego oznacza, że działania służb w zakresie pozyskiwania, przetwarzania, przechowywania i niszczenia wskazanych danych pozostaną poza jakąkolwiek kontrolą zewnętrzną.

XIV. W perspektywie regulacji art. 20c, art. 20cb oraz art. 20da ustawy o Policji (odpowiednio innych ustaw) szczególnie niepokojący jest brak obowiązku poinformowania przez służby osób, co do których uzyskano stosowne dane. Osoba taka nie jest również uczestnikiem ewentualnego postępowania kontrolnego przed sądem okręgowym. W praktyce oznaczać to będzie, że podmiot, co do którego przeprowadzano kontrolę, w większości przypadków nigdy się o niej nie dowie (co stanowi ewidentne naruszenie jednego z przytoczonych powyżej warunków minimalnych sprecyzowanych przez Trybunał Konstytucyjny w orzeczeniu K 23/11).

W szerszym aspekcie, w kategoriach uchybienia należy również oceniać brak procedury, z którą wiązałaby się możliwość zakwestionowania zasadności dokonania kontroli operacyjnej czy pozyskania danych o których mowa w art. 20c, 20cb i 20da ustawy o Policji (odpowiednio innych ustaw) przez osobę, która twierdziłaby, że jej prawa zostały naruszone.

XV. Zastrzeżenia budzą także zasady postępowania z materiałami, które mogą zawierać informacje objęte tajemnicą zawodową (notarialną, adwokacką, radcy prawnego, doradcy podatkowego, lekarską, dziennikarską lub statystyczną) albo są objęte zakazami dowodowymi. W projekcie zawarto schodkową procedurę, zgodnie z którą w przypadku, gdy zachodzi przypuszczenie, że materiały uzyskane w wyniku kontroli operacyjnej zawierają informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 k.p.k. albo informacje, o których mowa w art. 178, art. 178a albo art. 180 § 3 k.p.k., szef służby przekazuje je właściwemu prokuratorowi, który z kolei niezwłocznie kieruje je do sądu

wraz z wnioskiem o stwierdzenie, które z nich zawierają informacje, o jakich mowa w przytoczonych przepisach k.p.k., a także z wnioskiem o dopuszczenie do wykorzystania w postępowaniu karnym materiałów zawierających informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o jakich mowa w art. 180 § 2 k.p.k. nieobjęte zakazami, określonymi w art. 178, art. 178a i art. 180 § 3 k.p.k., z wyłączeniem informacji o przestępstwach, o których mowa w art. 240 § 1 k.k.

Przyjęty w projekcie sposób postępowania budzi poważne wątpliwości. Przede wszystkim w opiniowanych regulacjach nie określono terminu, w którym służby mają obowiązek przekazać informacje prokuratorowi, jednocześnie zastrzegając, że ten ma je skierować do właściwego sądu „niezwłocznie". Obowiązek postępowania z tak newralgicznymi informacjami powinien być uregulowany analogicznie w stosunku do służb, jak i organów procesowych. Przesłanka niezwłoczności powinna zatem odnosić się również do obowiązku przekazania przez szefa służby informacji prokuratorowi. W każdym przypadku zasadne byłoby także odgórne ograniczenie niezwłoczności, np. przez przyjęcie „niezwłocznie, nie później jednak niż trzy dni od uzyskania informacji". Regulacja taka wykluczy wszelkie wątpliwości co do wymaganej sprawności postępowania. Jednocześnie, zasadne byłoby wprowadzenie obowiązku komisyjnego i protokolarnego zniszczenia uzyskanych materiałów w razie upływu wskazanego terminu, bez konieczności angażowania w tym zakresie dodatkowych podmiotów (tj. sądu).

Wątpliwości budzi również sam udział prokuratora w analizowanym postępowaniu. Jego powinność ogranicza się bowiem wyłącznie do przekazania informacji sądowi wraz ze stosownymi wnioskami. Czynnikiem decyzyjnym w przedmiocie dopuszczalnego prawem wykorzystania materiałów z kontroli operacyjnej, jak również w przedmiocie zniszczenia materiałów w przypadkach niemieszczących się w normach kompetencyjnych jest zawsze sąd wydający uprzednio zezwolenie na przeprowadzenie kontroli operacyjnej. Powstaje zatem pytanie, jaka jest w istocie rola prokuratora. Wydaje się bowiem, że nie ma żadnych przeszkód, w sprawie materiałów, które mogą zawierać informacje objęte tajemnicą zawodową albo są objęte zakazami dowodowymi służby zwracałby się bezpośrednio do właściwego sądu. Włączanie w tego rodzaju procedurę innych podmiotów, w sposób zbędny i nieuzasadniony nakłada na nie dodatkowe obowiązki, wydłuża

samo postępowanie, zmniejsza jego gwarancyjność, a tym samym zwiększa niebezpieczeństwo ujawnienia rzeczonych informacji.

Z niezrozumiałych względów w projekcie ustawy nie przewidziano możliwości zgłoszenia zażalenia na postanowienie sądu przez beneficjenta tajemnicy obrończej albo zawodowej. Sytuacja taka stanowi naruszenie podstawowych reguł procesowych, jeśli zważyć że prawo do zaskarżenia postanowienia sądu przyznano prokuratorowi. Jak wskazano w uzasadnieniu orzeczenia Trybunału Konstytucyjnego K 23/11, postępowanie w zakresie standardów ochrony powinno być w tym zakresie uregulowane zbieżnie do art. 180 § 2 k.p.k., który jednoznacznie przewiduje instancyjną kontrolę sądu, mogącą zostać zainicjowaną przez każdą ze stron.

Prezentowane uwagi jednoznacznie dowodzą, że opiniowane rozwiązania legislacyjne stanowią naruszenie przytoczonych powyżej warunków minimalnych sprecyzowanych przez Trybunał Konstytucyjny w orzeczeniu K 23/11.

XVI. W konkluzji należy wyrazić pogląd, że wbrew twierdzeniom zawartym w pkt 3 uzasadnienia projektu nie uwzględniono w nim wszytskich sformułowanych przez Trybunał Konstytucyjny minimalnych wymagań, jakie łącznie powinny spełniać przepisy ustaw normujących niejawne pozyskiwanie przez władze publiczne informacji o osobach. W zakresie dotyczącym kontroli operacyjnej, poza problematyką zasad postępowania z materiałami, które mogą zawierać informacje objęte tajemnicą zawodową albo są objęte zakazami dowodowymi oraz sprecyzowaniem przesłanek kontroli operacyjnej podejmowanej przez ABW i AW, projekt zasadniczo spełnia przytoczone minima, w części zaś przewidującej obowiązek udostępniania służbom danych telekomunikacyjnych, danych pocztowych oraz danych internetowych przedłożony projekt wymaga daleko idących korekt.