MINISTER
SPRAW WEWNĘTRZNYCH

Warszawa, dnia 03 kwietnia 2014 r.

KANCELARIA SENATU
Kancelaria Ogólna
08. 04. 2014
Wpł. Nr dz. KPCP/118

DP-I-0232-119/14/ECh

Do wiadomości Członków KPCPP

Pan Michał Seweryński
Przewodniczący Komisji
Praw Człowieka, Praworządności
i Petycji Senatu RP

Szanowny Panie Przewodniczący,

W nawiązaniu do ustaleń podjętych na posiedzeniu Komisji Praw Człowieka, Praworządności i Petycji Senatu RP w dniu 4 marca 2014 r., przedstawiam stanowisko Ministra Spraw Wewnętrznych do projektu *ustawy o zmianie niektórych ustaw w zakresie przepisów dotyczących uzyskiwania i przetwarzania przez uprawnione podmioty danych gromadzonych przez przedsiębiorców telekomunikacyjnych,* zwanym dalej projektem ustawy.

W ocenie Ministra Spraw Wewnętrznych zaproponowana przez Senat RP regulacja prawna w istotny sposób skomplikuje procedury pozyskiwania przez służby danych telekomunikacyjnych oraz ograniczy możliwości ich wykorzystywania w celu zapobiegania lub wykrywania przestępstw. Przyjęcie rozwiązań prawnych przedstawionych w projekcie ustawy z dużym prawdopodobieństwem obniży skuteczność działań Policji oraz Straży Granicznej, prowadzonych w celu zapewnienia bezpieczeństwa obywateli oraz bezpieczeństwa Państwa.

Proponowane zmiany wprowadzają procedurę dotyczącą pozyskiwania danych telekomunikacyjnych analogiczną do procedury odnoszącej się do kontroli operacyjnej. Tymczasem pozyskiwanie danych telekomunikacyjnych nie jest tożsame z kontrolą korespondencji i utrwalaniem treści rozmów telefonicznych, a zatem powoduje znacząco mniejszą ingerencję w prawo do prywatności. W związku z powyższym zastosowanie jednolitych regulacji w obu przypadkach jest rozwiązaniem nieproporcjonalnym, a przez to w ocenie Ministra Spraw Wewnętrznych niewłaściwym. Podkreślić należy, iż kontrola operacyjna opiera się m.in. na analizie treści korespondencji pomiędzy osobami pozostającymi w zainteresowaniu Policji, natomiast retencja danych nie ingeruje w treść przekazu międzyludzkiego, służy do ustalenia m.in. jakie osoby używają telefonów (internetowych urządzeń) pozostających w zainteresowaniu Policji, lokalizacji telefonów i wykazu połączeń.

Specyfika działań służb podległych Ministrowi Spraw Wewnętrznych wymusza działania bez zbędnej zwłoki, aby skutecznie ująć sprawców przestępstw i zabezpieczyć dowody ich popełnienia. W przypadku wielu przestępstw, takich jak: uprowadzenie, groźba karalna, wymuszenie okupu itp.,

szybkość działań służb skutkuje niedopuszczeniem do utraty zdrowia lub życia przez osoby pokrzywdzone. Proponowane rozwiązania w istotny sposób wpłyną na czas podejmowania działań i mogą negatywnie wpłynąć na skuteczność wykrywania i ścigania sprawców przestępstw, także w przypadku przestępstw godzących w życie i zdrowie ludzkie.

Należy zauważyć, iż projekt ustawy stanowi wykonanie wniosków *de lege ferenda* zawartych w wynikach kontroli Najwyższej Izby Kontroli „Uzyskiwanie i przetwarzanie przez uprawnione podmioty danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180 c i d ustawy Prawo telekomunikacyjne". W tym miejscu należy zaznaczyć, iż Najwyższa Izba Kontroli oceniła pozytywnie działalność kontrolowanych służb i formacji w zakresie uzyskiwania i przetwarzania przez nie danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180 c i d ustawy Prawo telekomunikacyjne. NIK stwierdził, iż system pozyskiwania i przetwarzania danych umożliwiał realizację ustawowych zadań przez kontrolowane podmioty. Wprowadzone zasady i procedury umożliwiały szybkie i sprawne pozyskiwanie danych w związku z prowadzonymi postępowaniami. Możliwość sięgania po dane telekomunikacyjne mieli jedynie upoważnieni pracownicy i funkcjonariusze, a krąg osób posiadających takie upoważnienia był w kontrolowanych instytucjach ściśle określony. W toku kontroli nie ujawniono przypadków działania niezgodnie z ustawą o Policji czy też ustawą o Straży Granicznej.

Należy podkreślić, iż w aktualnie obowiązujących aktach normatywnych, zarówno w ustawie o Policji – art. 20c ust. 1, jak i w ustawie o Straży Granicznej – art. 10b, uregulowano podstawę prawną pozyskiwania danych telekomunikacyjnych – zapobieganie lub wykrywanie przestępstw. Rozstrzygnięty prawnie jest także tryb postępowania z materiałami zawierającymi informacje telekomunikacyjne – materiały, które zawierają informacje mające znaczenie dla postępowania karnego przekazywane są właściwemu miejscowo i rzeczowo prokuratorowi, natomiast materiały, które nie zawierają informacji mających znaczenie dla postępowania karnego, podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu – odpowiednio art. 20c ust. 6 i 7 ustawy o Policji oraz art. 10b ust. 5 i 6 ustawy o Straży Granicznej.

Ograniczenie uprawnień Policji oraz Straży Granicznej, w zakresie pozyskiwania danych telekomunikacyjnych, do przestępstw wymienionych w art. 19 ustawy o Policji oraz art. 9e ustawy o Straży Granicznej (przepisy dotyczące stosowania kontroli operacyjnej), spowoduje wyłączenie możliwości ścigania zarówno sprawców przestępstw, które w swojej istocie polegają na wykorzystywaniu urządzeń telekomunikacyjnych, jak i innych, wobec których stosowanie kontroli operacyjnej byłoby zbyt daleką ingerencją w prawa obywateli, a pozyskiwanie danych telekomunikacyjnych wydaje się być środkiem adekwatnym. Wejście w życie rozwiązań zawartych w projekcie ustawy uczyni Policję oraz Straż Graniczną całkowicie nieskuteczną w zwalczaniu przestępstw z użyciem sieci Internet. Wobec dynamicznego rozwoju technologii internetowej, jak i rozszerzania się katalogu przestępstw, których popełnienie możliwe jest przy użyciu sieci Internet, kierunek regulacji wydaje się być niewłaściwy. W tym zakresie projekt ustawy jest także

niekonsekwentny. Oprócz przestępstw wymienionych w art. 19 ustawy o Policji, projekt wymienia wykroczenie z art. 66 Kodeksu wykroczeń – powiadomienie o nieistniejącym zagrożeniu, jednocześnie pomijając skutkową formę tego samego czynu, skodyfikowaną jako przestępstwo w art. 224a Kodeksu karnego. Kolejne przykłady przestępstw, które najczęściej popełniane są z użyciem urządzeń telekomunikacyjnych to: groźba karalna – art. 190 kk, uporczywe nękanie (stalking) – art. 190a kk, zmuszenie do określonego zachowania – art. 191 kk, wpływanie na czynności urzędnicze – art. 224 kk, grupa przestępstw przeciwko ochronie informacji i wiele innych. W przypadku posłużenia się do popełnienia w/w przestępstw, urządzeniami telekomunikacyjnymi, służby nie będą miały żadnych możliwości ścigania sprawcy.

Kolejna grupa przestępstw, wobec których stosowanie kontroli operacyjnej było by zbyt dużą ingerencją w prawa obywatelskie, a pozyskiwanie danych telekomunikacyjnych jest uprawnieniem adekwatnym, to przestępstwa, takie jak: kradzież (w tym mienia znacznej wartości) – art. 278 kk, kradzież z włamaniem – art. 279 kk – tego rodzaju przestępczością zajmują się najczęściej „zawodowi złodzieje", których wykrycie wymaga od Policji dużego zaangażowania, w tym uzyskiwania danych telekomunikacyjnych. W grupie tej znajdują się także kradzieże samochodów, których sprawcy wykazują wysoki stopień zorganizowania i dynamikę działania, a dane telekomunikacyjne w postaci m.in. lokalizacji telefonu sprawcy, znacząco podnoszą skuteczność Policji w ich ściganiu. Warto wspomnieć, że w Polsce na przestrzeni ostatnich 10 lat, odnotowano ogromny spadek liczby kradzieży samochodów, spowodowany w znacznej mierze skutecznym działaniem Policji. W Niemczech, gdzie regulacje dotyczące pozyskiwania przez Policję danych telekomunikacyjnych są bardziej restrykcyjne, odnotowywany jest wzrost liczby kradzieży samochodów. Dane telekomunikacyjne wykorzystywane są także w zwalczaniu przestępczości pseudokibiców. Przestępstwa popełniane przez nich to w dużej mierze bójki i pobicia, kradzieże i uszkodzenia mienia (nie wymienione w art. 19 ustawy o Policji). Uniemożliwienie Policji pozyskiwania danych telekomunikacyjnych przy zwalczaniu przestępczości pseudokibiców znacząco obniży skuteczność zwalczania sprawców, a w konsekwencji może skutkować eskalacją działań pseudokibiców.

Ponadto informuję, że w zdecydowanej większości spraw kryminalnych, wykrycie i zatrzymanie sprawców przestępstw odbyło się dzięki wykorzystaniu danych telekomunikacyjnych.

Ważnym obszarem działalności służb podległych Ministrowi Spraw Wewnętrznych, na który będzie miał wpływ proponowana regulacja, to poszukiwania osób ukrywających się przed organami ścigania. Wejście w życie projektu ustawy ograniczy możliwość poszukiwań osób do sprawców przestępstw wymienionych odpowiednio w art. 19 ustawy o Policji oraz art. 9e ustawy o Straży Granicznej. Znakomita większość przestępców ukrywających się przed organami ścigania to sprawcy przestępstw nie wymienionych w w/w artykule. W czasie ukrywania się przed organami ścigania, najczęściej popełniają kolejne przestępstwa. Obniżenie skuteczności Policji w tym zakresie, spowoduje pozostawanie na wolności coraz większej liczby osób, które zgodnie z decyzją sądu winny być izolowane od społeczeństwa, a w konsekwencji – wzrost przestępczości.

Kolejnym problemem, który wyłania się w związku z projektem ustawy jest skuteczność działań służb wobec odpowiedniego stosowania procedur właściwych dla instytucji kontroli operacyjnej. Kontrola operacyjna nigdy nie jest jedynym środkiem stosowanym przez Policję oraz Straż Graniczną w celu wykrycia sprawcy przestępstwa. Warunkiem skuteczności w zwalczaniu przestępczości jest dynamika działania oraz szybkość dostępu do niezbędnych informacji. Omawiany projekt ustawy przewiduje dwa tryby pozyskiwania danych telekomunikacyjnych: zwykły i „w sytuacjach niecierpiących zwłoki". Zastosowanie drugiego trybu w praktyce oznacza uzyskanie danych telekomunikacyjnych po 12-24 godzinach od zaistnienia potrzeby ich uzyskania. W przypadku Centralnego Biura Śledczego KGP – zwalczającego przestępczość zorganizowaną oraz Biura Spraw Wewnętrznych KGP – zwalczającego przestępczość funkcjonariuszy i pracowników Policji, czas ten może być jeszcze dłuższy. Dla wymienionych biur Komendy Głównej Policji przełożonym uprawnionym do zarządzenia pozyskania danych telekomunikacyjnych w aktualnym stanie prawnym byłby Komendant Główny Policji, a prokuratorem, którego opinii należałoby zasięgnąć – Prokurator Generalny. Wobec obowiązku złożenia wniosku wraz z materiałami uzasadniającymi konieczność pozyskania danych telekomunikacyjnych, funkcjonariusze CBŚ na przykład ze Szczecina musieliby dostarczyć do Warszawy komplet materiałów, uzyskać opinię Prokuratora Generalnego (z uwzględnieniem godzin pracy Prokuratury Generalnej i dni wolnych od pracy), a następnie zgodę Komendanta Głównego Policji. W przypadku zbiegu okoliczności takich jak święta, pora nocna itp., uzyskanie danych telekomunikacyjnych może zająć nawet trzy doby. Trudno wyobrazić sobie skuteczne działanie Policji np. w przypadku uprowadzenia osoby, kiedy wiedzę o lokalizacji telefonu, z którego sprawca żąda okupu, uzyskujemy po trzech dniach od rozmowy telefonicznej. W takim przypadku brak dynamicznych działań ze strony Policji może narazić życie i zdrowie osoby uprowadzonej.

Warto nadmienić, że treść kolejnych zapytań o dane telekomunikacyjne w większości przypadków determinowana jest treścią odpowiedzi od operatora (nie można zapytać o dane numeru telefonu, który wcześniej pracował w ustalanym aparacie telefonicznym, gdyż numer ten będzie się znajdował w odpowiedzi na pierwsze zapytanie). Uzyskanie odpowiedzi od operatora uruchamiałoby kolejną długotrwałą procedurę, wydłużając działania Policji w sposób trudny do oszacowania. Podobny problem wystąpi w przypadku ponad 400 jednostek Policji szczebla powiatowego, które w celu pozyskania danych telekomunikacyjnych, zmuszone będą dostarczyć materiały do prokuratora okręgowego właściwego dla siedziby komendy wojewódzkiej Policji w celu uzyskania opinii, a następnie uzyskać zgodę komendanta wojewódzkiego Policji. Projekt nie rozstrzyga czy zatwierdzony wniosek należy dostarczyć do operatora telekomunikacyjnego. W przypadku takiego rozwiązania, dochodzi także czas niezbędny na dostarczenie wniosku do właściwego operatora.

Omawiając czas niezbędny do uzyskania danych telekomunikacyjnych po wejściu w życie omawianej regulacji, uwzględnić należy znaczące zwiększenie obciążenia prokuratur

i sądów wnioskami o dane telekomunikacyjne, rozpatrywanych w trybie analogicznym do wniosków o kontrolę operacyjną. Taka liczba wniosków z całą pewnością istotnie wydłuży czas oczekiwania na decyzje prokuratury i sądu, a także może wpłynąć negatywnie na jakość prokuratorskiej i sadowej kontroli zasadności pozyskiwania danych.

Zagadnieniem budzącym poważne wątpliwości jest również wprowadzenie instytucji „pełnomocnika do spraw kontroli przetwarzania danych osobowych". Obok prokuratury oraz sądu byłby to kolejny podmiot, który badałby prawidłowość przetwarzania przez służby danych osobowych, w szczególności ich przechowywanie, weryfikację i usuwanie. W projekcie ustawy sposób powoływania i odwoływania pełnomocnika wykracza poza określony w ustawie o Policji oraz w ustawie o Straży Granicznej system podległości służbowej, co w ocenie Ministra Spraw Wewnętrznych nie wydaje się uzasadnione („odwołanie pełnomocnika z pełnionej funkcji następuje za zgodą ministra właściwego do spraw wewnętrznych po zasięgnięciu opinii Sejmowej Komisji do Spraw Służb Specjalnych"). Przewidziany tryb odwołania pełnomocnika nie jest znany w obecnie obowiązujących regulacjach prawnych, ponadto z uzasadnienia do projektu ustawy nie wynika, jaki cel przyświecał projektodawcom we wprowadzeniu tak rygorystycznych zasad w zakresie zwolnienia pełnomocnika z pełnionej funkcji. Ponadto nadmiernym wydaje się uprawnienie pełnomocnika do m.in. wglądu do wszelkich dokumentów związanych z wykonywaną kontrolą oraz swobodnego wstępu do pomieszczeń i obiektów kontrolowanej jednostki organizacyjnej bez szczegółowego określenia trybu i zasad postępowania w tym zakresie.

Mając na uwadze powyższe, zasadne jest aby wszelkiego typu działania zmierzające do ochrony przysługujących obywatelom praw i wolności obywatelskich pozostawały w proporcji z obowiązkiem Państwa, jakim jest zapewnienie obywatelom bezpiecznych warunków życia poprzez m.in. umożliwienie służbom bezpieczeństwa i porządku publicznego podejmowania szybkich i skutecznych działań zmierzających do ustalenia, wykrycia i ujęcia sprawców przestępstw. W związku z powyższym Minister Spraw Wewnętrznych negatywnie ocenia senacki projekt *ustawy o zmianie niektórych ustaw w zakresie przepisów dotyczących uzyskiwania i przetwarzania przez uprawnione podmioty danych gromadzonych przez przedsiębiorców telekomunikacyjnych.*

MINISTER
SPRAW WEWNĘTRZNYCH
z up. Grzegorz KARPIŃSKI
Podsekretarz Stanu

96/14

RZECZPOSPOLITA POLSKA

SZEF CENTRALNEGO
BIURA ANTYKORUPCYJNEGO

Paweł Wojtunik

Warszawa, 20 marca 2014 r.

P-1196/14/W
Do wiadomości
Członków KPCPP
9.04.2014

Przewodniczący Komisji
Praw Człowieka,
Praworządności i Petycji
Pan Michał Seweryński

Szanowny Panie Przewodniczący!

Nawiązując do ustaleń z posiedzenia senackiej Komisji Praw Człowieka, Praworządności i Petycji, które odbyło się w dniu 4 marca 2014 r., przedstawiam uwagi do *projektu ustawy o zmianie niektórych ustaw w zakresie przepisów dotyczących uzyskiwania i przetwarzania przez uprawnione podmioty danych gromadzonych przez przedsiębiorców telekomunikacyjnych*.

1) Przepis art. 4 projektu, rozszerzający kompetencje Generalnego Inspektora Ochrony Danych Osobowych o możliwość kontroli uzyskiwania, przechowywania, weryfikowania i usuwania danych telekomunikacyjnych nie może być zaakceptowany. Określony w ten sposób zakres kontroli obejmowałby dostęp do materiałów operacyjnych służb specjalnych, co pozostaje w kolizji z art. 28 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. z 2012 r. poz. 621, z późn. zm.), regulującym zasady udostępniania informacji niejawnych przez m.in. funkcjonariuszy i pracowników CBA określonym osobom lub instytucjom. Przepis ten ogranicza możliwość udzielania informacji o:
- osobach, jeżeli zostały uzyskane w wyniku prowadzonych przez CBA albo inne organy, służby lub instytucje państwowe czynności operacyjno-rozpoznawczych,
- szczegółowych formach i zasadach przeprowadzania czynności operacyjno-rozpoznawczych oraz stosowanych środkach i metodach pracy operacyjnej,
- osobach udzielających pomocy CBA,
jedynie do dwóch przypadków, żądania prokuratora lub sądu, zgłoszonego w celu ścigania karnego za przestępstwo, którego skutkiem jest śmierć człowieka, uszczerbek na zdrowiu lub szkoda w mieniu, lub żądania prokuratora, lub sądu uzasadnionego podejrzeniem popełnienia przestępstwa ściganego z oskarżenia publicznego w związku z wykonywaniem czynności operacyjno-rozpoznawczych.

   W przypadku takiego ukształtowania kompetencji GIODO, Szef Centralnego Biura Antykorupcyjnego nie miałby prawnej możliwości udostępnienia materiałów operacyjnych dla GIODO, a tym samym prowadzenie takiej kontroli stałoby się niemożliwe.

   Dlatego proponuję skreślenie projektowanego przepisu.

2) Przepis art. 7 projektu wprowadzający wyodrębnienie danych adresowych i osobowych abonentów lub użytkowników końcowych, uznać należy za niezasadny. Dane opisane w tym przepisie mieszczą się w zakresie danych wskazanych w art. 180c i 180d prawa telekomunikacyjnego.

Przyjęcie tych rozwiązań spowoduje dualizm postępowania w stosunku do tych samych informacji uzyskiwanych na podstawie dwóch różnych przepisów. Dane teleadresowe uzyskiwane na podstawie projektowanego art. 17a ustawy o CBA będą objęte obowiązkiem uzyskania zgody sądu, a dane te same dane uzyskiwane na podstawie projektowanego art. 18 ustawy o CBA, będzie można uzyskać bez konieczności przechodzenia procedury sądowej.

Z tego względu projektowany przepis należy skreślić.

3) Z przepisu art. 8 pkt 1 projektu, w zakresie, w którym wprowadza, ustanawiający obostrzenia w zakresie pozyskiwania danych telekomunikacyjnych art. 17a do ustawy o Centralnym Biurze Antykorupcyjnym, wynika błędne założenie, polegające na utożsamieniu pozyskiwania danych telekomunikacyjnych z kontrolą operacyjną.

Należy pamiętać, że prawa i wolności przyznane w ustawie zasadniczej nie mają, co do zasady, charakteru absolutnego. Zgodnie bowiem z przepisem art. 49 ustawy z dnia 2 kwietnia 1997 r. - Konstytucja Rzeczypospolitej Polskiej (Dz. U. Nr 78, poz. 483, z późn. zm.), ograniczenie przyznanej obywatelowi ochrony tajemnicy komunikowania się musi nastąpić w ustawie. Konstytucja nakłada na ustawodawcę w art. 31 ust. 3 dodatkowe ograniczenia, zgodnie z którymi ingerencja w prawa i wolności obywatelskie może być wprowadzona tylko wtedy, gdy jest konieczna w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Nie może ona naruszać istoty wolności i praw. Nie znajduje więc uzasadnienia pogląd, zgodnie z którym każda aktywność służb państwowych, polegająca na jakiejkolwiek ingerencji w prawa i wolności obywatelskie, musi podlegać kontroli sądowej.

Niezaprzeczalne jest, że kontrola operacyjna, polegająca m.in. na zapoznawaniu się z treścią przekazów telekomunikacyjnych, stanowi istotne naruszenie konstytucyjnej wolności komunikowania się. W tym przypadku poddanie tej formy działania organów państwa pod kontrolę sądową nie budzi żadnych wątpliwości.

Możliwość dostępu do danych telekomunikacyjnych stanowi jednak znacznie „płytszą" od kontroli operacyjnej ingerencję w tajemnicę komunikowania się i dlatego nie powinna być poddawana tym samym rygorom nadzoru sądowego co kontrola operacyjna.

Z tego powodu kształtowanie ewentualnych obostrzeń powinno się odbywać proporcjonalnie do poziomu ingerencji w prywatność obywateli.

Niezrozumiałe jest również ograniczenie możliwości pozyskiwania danych tylko i wyłączenie w celu wykrycia, ustalenia sprawców i utrwalenia dowodów przestępstw. Taką redakcją przepisu projektodawca pominął inne cele ustawowe, dla których realizacji powołane zostało Centralne Biuro Antykorupcyjne. Chodzi mianowicie o rozpoznawanie i zapobieganie przestępstwom oraz działalność analityczno-informacyjną, będącą wyrazem prewencyjnej roli CBA.

Ograniczenie katalogu przestępstw, w związku z którymi będzie można sięgać po dane telekomunikacyjne, do tych, w stosunku do których możliwe jest zarządzenie kontroli operacyjnej, zdecydowanie ograniczy możliwości realizowania przez Centralne Biuro Antykorupcyjne ustawowych zadań.

Wprowadzenie konieczności uzyskania zgody sądu na dostęp do danych retencyjnych, spowoduje znaczne obciążenie czasowe i finansowe poszczególnych uczestników postępowania. Należy pamiętać, że zakres tych danych jest precyzyjnie określony w przepisach. Duża liczba zapytań spowoduje znaczne obciążenie sądów i Prokuratury Generalnej.

Zastosowanie procedury uzyskania zgody na kontrolę operacyjną do pozyskiwania danych telekomunikacyjnych, może doprowadzić niejednokrotnie do niemożliwości realizacji ustawowych zadań służb. Niekiedy pozbawiło by je możliwości korzystania z narzędzi pracy, gdyż dane uzyskane z opóźnieniem stałyby się danymi archiwalnymi, pozostającymi bez znaczenia dla prowadzonych spraw.

Błędne jest również odesłanie do odpowiedniego stosowania art. 17 ustawy o Centralnym Biurze Antykorupcyjnym. Ze względu na przesłanki stosowania kontroli operacyjnej, brak określenia zakresu odpowiedniego stosowania, *de facto* uniemożliwia wystąpienie z wnioskiem do sądu. Przy założeniu, że w oparciu o dane telekomunikacyjne dokonuje się pierwszej i podstawowej weryfikacji kierunku prowadzenia sprawy, projektodawca nie wskazał w jaki sposób zrealizować konieczność wskazania we wniosku faktu, że inne środki okazały się bezskuteczne albo będą nieprzydatne.

W przepisie art. 17 ustawy o Centralnym Biurze Antykorupcyjnym wskazano, że Sąd, wyrażając zgodę na taką kontrolę, określa ramy czasowe jej stosowania. Zgodnie z proponowanym rozwiązaniem pozyskiwanie danych telekomunikacyjnych dozwolone będzie wyłącznie od dnia wydania postanowienia i przez okres w nim określony. Służby zostaną tym samym pozbawione możliwości otrzymania danych z okresu przypadającego przed datą wydania postanowienia oraz po wskazanym w nim okresie.

Trudno znaleźć uzasadnienie dla obarczenia Prokuratora Generalnego obowiązkiem każdorazowego decydowania o zakresie i sposobie wykorzystania uzyskanych materiałów, w tym przypadku danych telekomunikacyjnych. Biorąc pod uwagę ilość pozyskiwanych w ten sposób danych, będzie to znaczne obciążenie dla Prokuratora Generalnego.

Mając to na uwadze, proponuję rezygnację z wprowadzania przepisu art. 17a do ustawy o Centralnym Biurze Antykorupcyjnym.

W celu zapewnienia skuteczniejszej ochrony konstytucyjnego prawa obywateli do swobodnego komunikowania się, proponuję zmianę brzmienia art. 231 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. Nr 88, poz. 553, z późn. zm.) poprzez dodanie § 1a w brzmieniu:

„§ 1a. Jeżeli sprawca dopuszcza się czynu określonego w § 1, w związku z stosowaniem kontroli operacyjnej, zakupu kontrolowanego lub pobierania danych telekomunikacyjnych podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 5.”.

4) Na akceptację zasługuje art. 8 pkt 1 projektu w zakresie wprowadzenia do ustawy o Centralnym Biurze Antykorupcyjnym art. 17b, dotyczącego sporządzania statystyk o uzyskiwanych przez służbę danych telekomunikacyjnych. Trzeba jednak zauważyć, że wprowadzenie obowiązku podawania liczby osób, w stosunku do których pozyskiwano dane telekomunikacyjne, może rodzić wiele problemów praktycznych i interpretacyjnych, prowadzących także do niezgodnych ze stanem faktycznym wyników statystyk. Projektowany przepis powinien zawierać szczegółową i precyzyjną metodologię opracowywania statystyk. Dla przykładu nie jest czytelne czy wysłanie zapytania o dane abonenckie dla danego numeru telefonu najpierw do czterech największych operatorów, a po uzyskaniu negatywnej odpowiedzi, do kolejnych przedsiębiorców telekomunikacyjnych będzie liczone jako jedno zapytanie, czy też każde wystąpienie o te

same dane będzie uwzględniane w statystyce oddzielnie. Kolejną kwestią problemową będzie pozyskiwanie bilingów telefonów na kartę pre-paid, ze względu na często występującą niemożność przypisania takiego numeru telefonu do jednego abonenta.

5) Przewidziane w przepisie art. 8 pkt 2 projektu ograniczenie katalogu danych telekomunikacyjnych, w których zakresie nie jest konieczna zgoda Sądu, jedynie do danych teleadresowych i osobowych nie znajduje uzasadnienia, gdyż pozbawi Szefa CBA możliwości skutecznego realizowania zadań. Pozyskiwanie danych w drodze teletransmisji będzie możliwe tylko w tym zakresie, w efekcie czego wydłużony zostanie okres oczekiwania na pozostałe dane.

   Niemożliwe będzie również skuteczne i sprawne korzystanie z narzędzi służących określaniu geolokalizacji lub ustalaniu połączeń pomiędzy poszczególnymi abonentami.

   Ograniczenie dostępu do danych telekomunikacyjnych w drodze teletransmisji jest nieuzasadnione również z punktu widzenia kosztów poniesionych przez służby i przedsiębiorców telekomunikacyjnych w celu budowy systemów służących wymianie informacji.

   Należy wskazać, że obecne rozwiązania teleinformacyjne gwarantują większe bezpieczeństwo danych niż korespondencja tradycyjna.

   Ponadto dzięki systemom teleinformatycznym zapewnia się pełną rozliczalność pozyskiwanych danych.

   Mając to na uwadze proponuję wykreślenie z projektu art. 8 pkt 2.

Oceniając projekt, należy stwierdzić, że wprowadzenie proponowanych rozwiązań w znacznym stopniu ograniczy możliwość nie tylko ścigania popełnianych przestępstw, ale również ich zapobiegania i wykrywania. Ponadto osłabiona zostanie skuteczność realizacji ustawowych działań o charakterze informacyjno-prewencyjnym.

Ukształtowane w proponowany sposób przepisy wywołują wrażenie braku zaufania w stosunku do funkcjonariuszy służb realizujących ustawowe obowiązki w zakresie zapewnienia porządku i bezpieczeństwa publicznego.

W projekcie pominięto również kwestię rejestracji numerów „pre-paid", których dość powszechne występowanie generuje dużą ilość zapytań o dane telekomunikacyjne.

Na akceptację zasługuje postulat ujednolicenia zasad sprawozdawczości i postępowania ze zbędnymi danymi, niemniej jednak należy zmodyfikować go we wskazanym powyżej zakresie.

107/14

RZECZPOSPOLITA POLSKA

Szef
Agencji Bezpieczeństwa Wewnętrznego

płk Dariusz Łuczak

P - 3748 /2014/2179/MO

Warszawa, 28 marca 2014 r.

Do wiadomości Członków KPCPP

Pan senator Michał SEWERYŃSKI

PRZEWODNICZĄCY
KOMISJI PRAW CZŁOWIEKA,
PRAWORZĄDNOŚCI I PETYCJI
SENAT RZECZYPOSPOLITEJ POLSKIEJ

Szanowny Panie Przewodniczący,

W związku z podjętymi pracami dotyczącymi projektu *ustawy o zmianie niektórych ustaw w zakresie przepisów dotyczących uzyskiwania i przetwarzania przez uprawnione podmioty danych gromadzonych przez przedsiębiorców telekomunikacyjnych*, przedstawiam stanowisko Agencji Bezpieczeństwa Wewnętrznego wobec przedmiotowego dokumentu.

W ocenie Agencji Bezpieczeństwa Wewnętrznego, nie kwestionując słuszności celu projektodawców w zakresie podniesienia standardów ochrony praw i wolności obywatelskich, ponownego rozważenia wymaga jednak zasadność i kierunek projektowanych rozwiązań.

Cel zaproponowanych rozwiązań ma być realizowany poprzez stworzenie regulacji, zgodnie z którymi kontrolą sądową objęte zostaną wszelkie czynności polegające na uzyskiwaniu przez uprawnione podmioty danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2014 r., poz. 243). W obecnym stanie prawnym brak jest obowiązku uzyskania zgody sądu na otrzymanie danych, o których mowa powyżej, które są niezbędne do realizacji zadań przez ABW, określonych w art. 5 ust. 1 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2010 r. Nr 29, poz. 154, z późn. zm.), zwaną dalej "ustawą o ABW". W ocenie Agencji Bezpieczeństwa Wewnętrznego wprowadzenie zmian w proponowanym kształcie spowoduje utrudnienie, czy wręcz uniemożliwienie – z uwagi na dynamikę sytuacji – wykonywania czynności operacyjno-rozpoznawczych, służących do realizacji ustawowych zadań ABW oraz pozostałych służb odpowiedzialnych za ochronę bezpieczeństwa państwa i porządku publicznego.

Obowiązujący obecnie system gradacji związany z trybem uzyskiwania ww. danych powiązany jest z rodzajem uzyskiwanych informacji. Tryb ten oceniany jest w szczególności pod kątem możliwości ingerencji w sferę praw i wolności obywatelskich. Od tego elementu

uzależniony jest sposób przeprowadzenia kontroli realizowanej przez wewnętrzne mechanizmy kontrolne, nadzór prokuratora, czy też kontrolę Sądu Okręgowego w przypadku informacji uzyskiwanych w związku z prowadzoną kontrolą operacyjną. Przedstawione w opiniowanym projekcie rozwiązania nie mając oparcia na tle wzorca konstytucyjnego, w efekcie burzą przyjęte obecnie i prawidłowo funkcjonujące mechanizmy skupiając się na objęciu uprzednia kontrolą sądu uzyskiwania danych z bilingów, informacji o lokalizacji oraz danych o których mowa w art. 180c i 180d Prawa telekomunikacyjnego.

W pierwszej kolejności stwierdzić należy, iż wprowadzenie trybu, zgodnie z którym dla uzyskania wszelkich danych zawartych w tzw. bilingach, niezbędne będzie uzyskanie pisemnej zgody sądu (czyli przeprowadzenie procedury analogicznej do trybu dotyczącego kontroli operacyjnej), wydaje się rozwiązaniem zbyt restrykcyjnym dla tej kategorii danych i nieadekwatnym do zakresu oraz potencjalnej wartości uzyskiwanych informacji. Zauważyć bowiem należy, iż kontrola prokuratorska realizowana jest przy uzyskiwaniu danych w związku z realizacją czynności określonych w art. 29 (zakup kontrolowany, wręczenie korzyści majątkowej) i art. 30 (przesyłka niejawnie nadzorowana) ustawy o ABW, a wówczas podejmowane są czynności, które znacznie głębiej ingerują w sferę prywatności obywatela, a tym samym uzyskiwane są znacznie szersze informacje o osobie, niż te określone w art. 180c i 180d Prawa telekomunikacyjnego. Kontrola sądu połączona z oceną Prokuratora Generalnego stosowana jest przy realizacji kontroli operacyjnej. Taki model uzyskiwania poszczególnych danych jest właściwy, gdyż związany jest z gradacją podejmowanych czynności, jak również z zakresem uzyskiwanych informacji. W przypadku bilingów, ABW może otrzymać jedynie informacje dotyczące danych osobowych właścicieli telefonów, z wyjątkiem numerów kart *pre-paid*, czasu nawiązania połączenia, stacji BTS, na których logował się numer oraz długości połączenia. Uzyskane w ten sposób informacje mają charakter ogólny i nie zawierają treści, jakie zostały przekazane pomiędzy rozmówcami.

Jednocześnie wskazać w tym miejscu należy, iż karty *pre-paid* stanowią około 56% całkowitej liczby kart telefonicznych w kraju. Z uwagi na fakt, iż w polskim systemie prawnym nie ma obowiązku imiennej rejestracji kart tego typu, ani żadnego mechanizmu, który pozwalałby na oznaczenie osoby nabywającej taką kartę, wątpliwość budzi celowość występowania do sądu o wyrażenie zgody na pozyskanie danych związanych z osobą użytkującą kartę *pre-paid*. Ponadto biorąc pod uwagę liczbę funkcjonujących na rynku telekomunikacyjnym tego typu kart, ustalenie użytkownika danego numeru telefonu wymusza wygenerowanie znacznej liczby zapytań, co w istocie ma znaczący wpływ na ilościową skalę zapytań, mającą odzwierciedlenie w statystykach okresowych przedstawianych przez podmioty uprawnione.

Kolejną różnicą pomiędzy ww. procedurami jest fakt, iż zastosowanie kontroli operacyjnej, czy też czynności określonych w art. 29 i 30 ustawy o ABW, daje możliwość uzyskania dowodów w sprawie, podczas gdy uzyskanie danych bilingowych ma na celu weryfikację przyjętych hipotez w toku kolejnych czynności. Z tego względu zaproponowane rozwiązania mogą znacząco obniżyć dynamikę i decyzyjność w niektórych procedurach oraz opóźnić czas reakcji na potencjalne zagrożenia (np. zagrożenie przestępstwem o charakterze terrorystycznym), a w konsekwencji negatywnie wpłynąć na poziom bezpieczeństwa wewnętrznego państwa oraz bezpieczeństwo ludności. Ponadto realizacja czynności

w proponowanym kształcie znacznie zwiększy ilość wniosków kierowanych do sądu okręgowego, co z kolei przełoży się na jego obciążenie i wydłużenie procesu decyzyjnego, która będzie miała negatywne skutki dla dynamiki realizowanych zadań. Bardzo często następuje bowiem konieczność wykonywania dodatkowych ustaleń, będących wynikiem przeprowadzonej analizy już pozyskanego materiału. Co więcej proces ten może mieć charakter wieloetapowy. Zatem wprowadzenie instytucji zgody sądu jako organu decyzyjnego w praktyce może uniemożliwić realizację zadań ABW, szczególnie w sytuacjach realnego zagrożenia, np. ataku terrorystycznego. W tej sytuacji należałoby rozważyć możliwość wprowadzenia instytucji zgody następczej, analogicznej do instytucji, o której mowa w art. 27 ust. 15c ustawy o ABW.

Dalsze wątpliwości ABW budzą także zaproponowane w projekcie zmiany w zapisach ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.), zgodnie z którymi przewiduje się objęcie procesu przetwarzania i niszczenia w ABW danych telekomunikacyjnych kontrolą Generalnego Inspektora Ochrony Danych Osobowych. Dotychczasowy zapis art. 43 ust 2 ww. ustawy określał, iż Generalnemu Inspektorowi Ochrony Danych Osobowych nie przysługują uprawnienia określone w art. 12 pkt 2, art. 14 pkt 1 i 3-5 oraz art. 15-18 ustawy (m.in. wydawanie decyzji administracyjnych, rozpatrywanie skarg, prawo przeprowadzenia czynności kontrolnych, wglądu do zbioru) w stosunku do przetwarzanych przez ABW zbiorów danych osobowych zawierających informacje niejawne lub informacje niejawne, które zostały uzyskane w wyniku czynności operacyjno-rozpoznawczych. Biorąc pod uwagę fakt, iż pozyskiwanie i przetwarzanie danych telekomunikacyjnych następować będzie w ramach działań operacyjno-rozpoznawczych, wprowadzona zmiana skutkować może zaistnieniem problematycznych sytuacji, w których Generalny Inspektor Ochrony Danych Osobowych w ramach swoich działań kontrolnych będzie uzyskiwał dostęp do istotnych informacji niejawnych ABW, co jest sprzeczne z art. 35 ustawy o ABW, który w ust. 1 wskazuje, iż w związku z wykonywaniem swoich zadań Agencje zapewniają ochronę zgromadzonych informacji. Ponadto wskazać w tym miejscu należy, iż Najwyższa Izba Kontroli, w wystąpieniu pokontrolnym nr KPB-BOE-Z-11/2013 z 13 stycznia 2013 r. jednoznacznie stwierdziła, iż działania ABW w kontrolowanym zakresie zasługują na pozytywną ocenę. W uzasadnieniu oceny poszczególnych obszarów objętych kontrolą stwierdzono między innymi, iż ocenę pozytywną uzasadniają: opracowanie i wdrożenie kompletnych procedur regulujących kwestie pozyskiwania danych telekomunikacyjnych; pozyskiwanie i wykorzystywanie danych telekomunikacyjnych zgodnie z przepisami oraz regulacjami wewnętrznymi; prawidłowo działający w powyższym zakresie system kontroli wewnętrznej. Jednocześnie w swojej ocenie NIK wskazała, iż wyniki kontroli wskazują, iż opracowane i wdrożone procedury były zgodne z przepisami ogólnie obowiązującymi, jak również pozwalały na minimalizację ryzyka wystąpienia nadużyć czy nieprawidłowości. W ocenie NIK przepisy wewnętrzne i zawarte w nich procedury były kompletne, precyzyjne, spójne oraz gwarantowały optymalny poziom wykorzystania oraz bezpieczeństwa pozyskanych danych telekomunikacyjnych. Ponadto przepisy określające wewnętrzną organizację i porządek funkcjonowania jednostek organizacyjnych ABW gwarantowały uzyskiwanie danych telekomunikacyjnych wówczas, gdy było to uzasadnione specyfiką lub zakresem zadań wykonywanych przez jednostki organizacyjne ABW, albo prowadzonych przez nie czynności. Z tego względu przepisy regulujące te kwestie w aktach prawnych wszystkich uprawnionych podmiotów powinny kłaść nacisk na możliwość

weryfikacji zasadności pozyskiwania danych, sposób ich wykorzystania, a także rozliczalność dostępu do danych. Regulacje powinny określać zasady odnoszące się do czasu i sposobu przechowywania danych, gwarantującego ich poufność, jak również do sposobu ich niszczenia w przypadku, gdy stają się bezużyteczne.

Odnosząc się następnie do propozycji wprowadzenia „pełnomocnika do spraw kontroli przetwarzania przez ABW danych osobowych", można wskazać, iż propozycje dot. wprowadzenia tej instytucji prawnej zawiera także przyjęta przez Radę Ministrów opracowywana aktualnie, nowa ustawa o Agencji Bezpieczeństwa Wewnętrznego (art. 32 projektu z 11.03.2014 r.) – formułująca praktycznie analogiczne zapisy (opierające się bezpośrednio na funkcjonujących już przepisach dotyczących pełnomocnika do spraw kontroli przetwarzania przez CBA danych osobowych – tj. art. 22b ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. z 2012 r. poz. 621, z późn. zm.).

Jednocześnie zwrócenia uwagi wymaga fakt, iż zaproponowane w projekcie rozwiązania istotnie ograniczają możliwość realizacji zadań przez ABW jako służby właściwej w sprawach ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego. Wniosek ten wynika z propozycji zawężenia zakresu i celu pozyskiwanych danych, która skutkować może między innymi uniemożliwieniem wykorzystania przez ABW określonych danych telekomunikacyjnych w celach prewencyjnych umożliwiających podjęcie szybkich działań zapobiegających popełnieniu przestępstw. Zgodnie bowiem z uzasadnieniem opiniowanego dokumentu wszystkie służby zostały uprawnione do składnia wniosków o udostępnienie danych w celu wykrycia, ustalenia sprawców, uzyskania i utrwalenia dowodów przestępstw. W związku z powyższym mechanizmy związane z uzyskiwaniem informacji powinny być tak skonstruowane aby pozwalały na ich szybkie uzyskanie, analizę i właściwe wykorzystanie. Z drugiej zaś strony nowe przepisy powinny zapewnić adekwatny poziom ochrony dla poszczególnych kwestii związanych z prawami i wolnościami obywatelskimi, w tym tajemnicę korespondencji, czy też komunikowania się.

Z poważaniem

ZASTĘPCA SZEFA
Agencji Bezpieczeństwa Wewnętrznego
płk Kazimierz MORDASZEWSKI

110/14

RZECZPOSPOLITA POLSKA
PROKURATOR GENERALNY

Warszawa, dnia 31.03 2014 roku

PG VII G 070/17/14

Do wiadomości
Członków KPCPP
9.04.2014

Pan
Michał Seweryński

Przewodniczący
Komisji Praw Człowieka,
Praworządności i Petycji
Senatu Rzeczypospolitej Polskiej

Szanowny Panie Przewodniczący

W nawiązaniu do ustaleń poczynionych w trakcie posiedzenia Komisji w dniu 4 marca 2014 roku oraz w związku z przekazanym przy piśmie z dnia 27 lutego b.r. (nr BPS KPCPP-034-164-165/14) projektem ustawy o zmianie niektórych ustaw w zakresie przepisów dotyczących uzyskiwania i przetwarzania przez uprawnione podmioty danych gromadzonych przez przedsiębiorców telekomunikacyjnych, uprzejmie przekazuję uwagi do powyższego projektu, podtrzymując zastrzeżenia zgłoszone przez prokuratora Prokuratury Generalnej na posiedzeniu Komisji w dniu 4 marca b.r.

Na wstępie stwierdzić należy, iż przedstawiony projekt zmiany ustawy „o zmianie niektórych ustaw w zakresie przepisów dotyczących uzyskiwania i przetwarzania przez uprawnione podmioty danych gromadzonych przez przedsiębiorców telekomunikacyjnych", jest co najmniej kontrowersyjny, a w niektórych unormowaniach wręcz szkodliwy dla Państwa w realizacji zadania w zakresie ścigania przestępstw, a przy tym nie rozwiązuje żadnego z problemów opisanych przez NIK. Nie jest również bez znaczenia okoliczność, bezzasadnie

zdeprecjonowana w trakcie posiedzenia Komisji przez Generalnego Inspektora Ochrony Danych Osobowych, iż problematyka zawarta w projekcie ustawy, była wcześniej przedmiotem prac zespołu działającego Kancelarii Prezesa Rady Ministrów, w którym uczestniczył m.in. przedstawiciel Prokuratora Generalnego. Zespół ten, pod przewodnictwem Ministra Jacka Cichockiego, wypracował stanowisko odmienne w wielu punktach od projektowanych zmian. Nie jest rzeczą Prokuratora Generalnego ustalanie dlaczego dotychczas Rada Ministrów nie przedłożyła swego projektu w tym zakresie, pomimo upływu znacznego okresu czasu. Nie może jednak ulegać żadnej wątpliwości, iż to Rząd lub wskazany minister powinien wystąpić z inicjatywą ustawodawczą w tym zakresie, gdyż rozpoczął już prace nad projektem i poczynił ustalenia z zainteresowanymi podmiotami, które to ustalenia w wielu aspektach są odmienne od przedłożonego projektu. Dlatego też odnosząc się z szacunkiem do inicjatywy Senatu RP, wydaje się słuszne przekazanie niniejszego projektu do Prezesa Rady Ministrów, zgodnie z wnioskiem Najwyższej Izby Kontroli, zawartym w „Informacji o wynikach kontroli" z następującymi uwagami do ewentualnego wykorzystania w toku dalszych prac legislacyjnych.

Opracowany przez Biuro Legislacyjne Kancelarii Senatu RP projekt ustawy o zmianie niektórych ustaw w zakresie przepisów dotyczących uzyskiwania i przetwarzania przez uprawnione podmioty danych gromadzonych przez przedsiębiorców telekomunikacyjnych zawiera unormowania, które w żadnym przypadku nie mogą zostać uznane za uzasadnione, przeciwnie- powinny zostać wyeliminowane, gdyż są niemożliwe do wykonania. Sprowadzają się one, poprzez słowa „Art. 19 stosuje się odpowiednio" w art. 1 pkt 1 projektu

(powyższe zdanie odnosi się do Policji-podobnie jest do innych organów) do uznania, iż uzyskanie danych telekomunikacyjnych przez Policję (w tym przypadku) może nastąpić jedynie po wyczerpaniu procedury takiej jak w przypadku kontroli operacyjnej (podsłuchu), tj. najpierw pisemny wniosek

komendanta wojewódzkiego Policji lub innego upoważnionego organu w świetle ustaw kompetencyjnych, przekazywany wraz z materiałami uzasadniającymi ten wniosek, według właściwości prokuratorowi okręgowemu lub Prokuratorowi Generalnemu, następnie po wyrażeniu zgody przez prokuratora na powyższy wniosek, przekazanie go do właściwego sądu okręgowego, a po zarządzeniu przez ten sąd udostępnienia Policji danych wymienionych we wniosku, zwrócenie się do właściwego przedsiębiorcy telekomunikacyjnego o ich udostępnienie organowi Policji. Procedura taka spowoduje, że dane telekomunikacyjne, które niejednokrotnie potrzebne są w kilkanaście minut, będą udostępnione po kilku dniach, a wyjątkowych przypadkach - po kilku godzinach w trybie niecierpiącym zwłoki. Należy mieć na uwadze okoliczność, iż Policja oraz inne upoważnione organy zwracają się o dane telekomunikacyjne w setkach tysięcy przypadków rocznie. Przyjmując, przy tym, choć z projektu ustawy nie wynika to wprost, zgodnie z propozycją Najwyższej Izby Kontroli (str. 62 „Informacji o wynikach kontroli"), iż jako dane bilingowe nie powinny być traktowane informacje pozwalające na ustalenie, do kogo należy dany numer telefonu, czy jakie są jego dane adresowe. Prokuratorowi Generalnemu nie jest znana nawet przybliżona lub szacunkowa liczba danych bilingowych pozyskiwanych przez uprawnione podmioty, dlatego też zasadnym jest w pierwszej kolejności zdiagnozowanie problemu, tj. dokładne policzenie kto, ile i jakich danych pozyskiwał w określonych latach z podziałem na typowe bilingi, dane lokalizacyjne i zapytania adresowe, albowiem być może okaże się, iż zaproponowana w projekcie procedura, identyczna jak w sprawach dotyczących kontroli operacyjnych, jest niewykonalna, gdyż spowoduje paraliż prokuratur, sądów i innych instytucji pozyskujących i przetwarzających dane telekomunikacyjne. Z informacji przekazanych na posiedzeniu Komisji Senatu RP w dniu 4 marca b.r. przez Szefa Centralnego Biura Antykorupcyjnego można było się dowiedzieć, że kierowany przez niego organ miał w 2013 roku ok. 124 tys. jednostkowych

pobrań danych telekomunikacyjnych. Natomiast z informacji Najwyższej Izby Kontroli zawartej na str.32 wynika, iż Policja w 2011 roku wystąpiła do przedsiębiorców telekomunikacyjnych z ponad milionem zapytań, przy czym ponad 100 tys. były to zapytania o dane lokalizacyjne. Już tych kilka zaledwie liczb wskazuje jaka jest wielkość problematyki którą autor (autorzy) projektu usiłują załatwić słowami :„Art.19 stosuje się odpowiednio" (odnośnie Policji). Otóż procedury właściwej podsłuchom nie można, bez szkody dla Państwa, zastosować do pozyskiwania danych telekomunikacyjnych. Wnioski o kontrolę operacyjną w 2013 roku dotyczyły 4509 osób, co wynika z informacji Prokuratora Generalnego przekazanej jak co roku Marszałkowi Senatu. W poprzednim roku liczba ta była podobna. Natomiast wniosków o dane telekomunikacyjne było w tym czasie 400, a może 500 razy więcej. Przyjmując optymistycznie, że wniosków będzie „tylko" 100 razy więcej, gdyż skomplikowana procedura będzie pewną barierą dla uprawnionych organów, nie może ulegać żadnej wątpliwości, że wnioskami tymi zajmować się będzie musiało dodatkowo kilkaset lub nawet kilka tysięcy osób - prokuratorów, sędziów, urzędników(kancelarie tajne), funkcjonariuszy Policji, ABW, CBA i innych upoważnionych organów, przygotowując, rozpoznając i wykonując wnioski o dane, które nie mają zasadniczego znaczenia dowodowego. Okoliczność ta została już zasygnalizowana przez prokuratora Prokuratury Generalnej na posiedzeniu Komisji Senatu RP i sprowadza się do stwierdzenia, że w sprawach dotyczących kontroli operacyjnej (podsłuchu) procedura jest wieloszczeblowa i skomplikowana, gdyż kontrola ta pozwala na uzyskiwanie bezpośrednich dowodów popełnienia przestępstw, które w procesie karnym mogą być i bardzo często są uznane przez sąd za dowodowy winy danej osoby. Natomiast dane telekomunikacyjne nigdy nie mogą samoistnie przesądzić o czyjejś winie mogą być i często są poszlaką, która wymagać będzie jednak przeprowadzenia dalszych istotnych dowodów. Dlatego też sformułowanie medialne („Gazeta Wyborcza" z 28 lutego 2014 roku) „Bilingi jak podsłuchy"

jest błędne i dlatego jest nie do zaakceptowania również i dlatego, że podsłuch jest najgłębszą ingerencją w tajemnice telekomunikacyjną, natomiast biling lub inne dane telekomunikacyjne zaledwie tej tajemnicy dotykają i to nie zawsze, gdyż są jedynie dowodem na połączenie lub próbę połączenia telefonów o danych numerach, lub wskazuje gdzie dany telefon się logował, a nie są dowodem na rozmowę telefoniczną określonych osób, nie mówiąc już o jej treści. Konieczne jest w tym miejscu zaznaczenie, iż biling lub dane lokalizacyjne mogą być natomiast dowodem eliminującym daną osobę z kręgu podejrzeń, dlatego też ta osoba powinna być zainteresowana możliwie szybkim wykazaniem, iż nie była np. w miejscu zdarzenia, o czym świadczą dane lokalizacyjne telefonu, którego używa. Na marginesie tych rozważań należy mieć również na uwadze i tę okoliczność, iż praktycznie niczym nieograniczona możliwość zakupu telefonu (karty SIM) bez konieczności ujawnienia swych danych osobowych czyni w praktyce bardzo trudnym, a niekiedy wręcz niemożliwym ustalenie, kto posługiwał się telefonem o danym numerze zlokalizowanym w określonym miejscu. Nie jest żadną tajemnicą informacja, iż bezproblemowe zakupienie „telefonu na kartę" bardzo utrudnia, a niekiedy wręcz uniemożliwia ustalenie, kto ten telefon w danej chwili posiadał, a tym bardziej kto przez niego rozmawiał w danym momencie. Dlatego też długotrwałe i skomplikowane procedowanie z udziałem sądów i prokuratury, w tym Prokuratora Generalnego po to, by w końcu otrzymać od przedsiębiorcy telekomunikacyjnego informację, iż telefon ten należy do osoby, która nie podała przy zakupie swych danych jest mało sensowne a na dodatek kosztowne, gdyż wiąże się z koniecznością zatrudnienia kilkuset, a może i kilku tysięcy dodatkowych wykwalifikowanych osób, oraz szkodliwe dla Państwa, gdyż w efekcie utrudni ściganie osób popełniających przestępstwa w sprawach, w których liczy się każda wręcz godzina, a także nieuzasadnione, gdyż często będzie prowadziło donikąd, czyli nie pozwoli na ustalenie tych danych, które były przedmiotem wniosku. Procedura „podsłuchowa" nie gwarantuje też, że

prawa i wolności obywatelskie będą przestrzegane w każdym przypadku, gdyż z prawa wielkich liczb wynika, iż możliwe jest i tak się obecnie dzieje, skrupulatne rozpatrywanie wniosków o podsłuchiwanie roczne 4509 osób (w skali 2013 roku), natomiast stosowanie takiej procedury wobec kilkuset tysięcy, a może i więcej osób jest bardzo trudne. Przyjęcie proponowanej procedury spowoduje, iż Prokurator Generalny, lub jego zastępcy, podobnie jak prokuratorzy okręgowi pełnić będą dyżury 24 godzinne, gdyż może zachodzić konieczność rozpoznania wniosków w trybie niecierpiącym zwłoki: (art. 19 stosuje się odpowiednio - dot. Policji).

Wszystkie przytoczone powyżej argumenty prowadzą do konstatacji, iż zaproponowane w projekcie rozwiązanie: „Art. 19 stosuje się odpowiednio" (dot. Policji) jest nie do zaakceptowania i nie powinno zostać wprowadzone w życie.

Nie jest rolą Prokuratora Generalnego proponowanie rozwiązań legislacyjnych pozostających poza zakresem jego ustawowych kompetencji. Tym niemniej „ustanowienie kontroli zewnętrznej nad procesem pozyskiwania danych, obejmującej weryfikację zasadności pozyskiwania ", jak o to wnosi Najwyższa Izba Kontroli, być może powinno skutkować znaczącym poszerzeniem kompetencji Generalnego Inspektora Ochrony Danych Osobowych, a może ustanowieniem właściwego do tych spraw niezależnego organu administracyjnego, jak to jest we Francji, Wielkiej Brytanii, Irlandii i na Malcie. Nie przesądzając rozwiązania legislacyjnego w tym zakresie Prokurator Generalny jako organ zobowiązany przez ustawę o prokuraturze do strzeżenia praworządności, jak również czuwający nad ściganiem przestępstw, będzie wspierał wszystkie te rozwiązania legislacyjne, które będą realizacją Dyrektywy 2006/24/WE, a jednocześnie nie spowodują znaczącego wzrostu kosztów osobowych i materiałowych (kilkaset tysięcy, a może więcej pisemnych wniosków w trzech, a może w czterech egzemplarzach, po kilka stron każdy, rejestry, kontrolki, nowe programy komputerowe), a także nie doprowadzą do

paraliżu działalności ustawowej wymiaru sprawiedliwości oraz instytucji zobowiązanych do ścigania przestępstw, poprzez skupienie się na formułowaniu, rozpatrywaniu i realizowaniu wniosków telekomunikacyjnych przy jednoczesnym znaczącym wydłużeniu czasu realizacji wniosków, nawet w „przypadkach niecierpiących zwłoki", gdyż sformułowanie „Art.19 stosuje się odpowiednio" (dot. Policji) oznacza, że tylko komendanci wojewódzcy Policji i Komendant Główny Policji mogą kierować wnioski o te dane, a nie mogą tego czynić nawet komendanci miejscy czy powiatowi, lub naczelnicy zarządów Centralnego Biura Śledczego i dyrektorzy biur w Komendzie Głównej Policji

W konsekwencji zauważyć należy, iż krótkie zdanie: „Art. 19 stosuje się odpowiednio" dotyczące Policji (podobne są zadania dotyczące innych organów) powoduje bardzo poważne reperkusje i nie może zostać przyjęte do stosowania. Oczywiście zastrzeżenia do sformułowania „stosuje się odpowiednio" dotyczy również art.2 pkt1, art.3 ust.8 pkt 3, art.5 pkt 2, art. 6 pkt 3, art. 8 pkt1, art. 9 pkt 1 i art.10 (w całości- dotyczy Służby Celnej, która nie może prowadzić kontroli operacyjnej).

W pozostałym zakresie projektu uwag nie zgłaszam.

Z poważaniem

Andrzej Seremet

Owczarek Elżbieta

Od: Fundacja Panoptykon <fundacja@panoptykon.org>
Wysłano: 31 marca 2014 14:42
Do: Komisja Praw Człowieka, Praworządności i Petycji
Temat: opinia w sprawie projektu ustawy zmieniającej zasady dostępu do danych telekomunikacyjnych
Załączniki: Panoptykon_retencja_projekt senacki_opinia_31.03.2014.pdf; signature.asc

Szanowni Państwo,

w imieniu Fundacji Panoptykon przesyłam stanowisko Fundacji dotyczące projektu "ustawy o zmianie niektórych ustaw w zakresie przepisów dotyczących uzyskiwania i przetwarzania przez uprawnione podmioty danych gromadzonych przez przedsiębiorców telekomunikacyjnych", przygotowanego przez Biuro Legislacyjne.

Będziemy wdzięczni za umożliwienie zapoznania się z innymi opiniami przedstawionymi do projektu.

Z poważaniem,
Wojciech Klicki

Na posiedzenie KPCPP 9.04.2014

FUNDACJA PANOPTYKON

Warszawa, 31 marca 2014 r.

Szanowny Pan
Senator Michał Seweryński
Przewodniczący Komisji Praw Człowieka,
Praworządności i Petycji

Opinia Fundacji Panoptykon[1] w sprawie projektu ustawy[2] dotyczącej dostępu uprawnionych podmiotów do danych telekomunikacyjnych

1. Wstęp

Fundacja Panoptykon jest organizacją pozarządową zajmującą się ochroną praw człowieka w społeczeństwie nadzorowanym, a jednym z ważniejszych tematów w naszej działalności jest dostęp organów państwa do danych o obywatelach, w tym dostęp policji i innych służb do danych telekomunikacyjnych.

Problem braku wystarczających gwarancji dla ochrony praw jednostki w kontekście dostępu do danych telekomunikacyjnych dostrzegło wiele podmiotów, m.in. Rzecznik Praw Obywatelskich, Prokurator Generalny, Naczelna Rada Adwokacka i Najwyższa Izba Kontroli. Projekt ustawy o zmianie niektórych ustaw w zakresie przepisów dotyczących uzyskiwania i przetwarzania przez uprawnione podmioty danych gromadzonych przez przedsiębiorców telekomunikacyjnych (**dalej: projekt**) jest jednak pierwszą konkretną propozycją kompleksowych zmian ograniczających dostęp uprawnionych podmiotów do danych telekomunikacyjnych i wzmacniających ochronę prywatności użytkowników telefonów komórkowych i Internetu.

W naszej ocenie projekt zasługuje na akceptację, choć w dalszej części opinii zwracamy uwagę na kilka problemów z nim związanych oraz przedstawimy możliwe kierunki ich rozwiązania. Na wstępie zwracamy jednak uwagę na kontekst, w jakim powstał projekt. Na początku kwietnia br.

---

[1] Opinia przygotowana przez Wojciecha Klickiego.
[2] Projekt przygotowany przez Biuro Legislacyjne Kancelarii Senatu RP pod pełną nazwą: ustawa o zmianie niektórych ustaw w zakresie przepisów dotyczących uzyskiwania i przetwarzania przez uprawnione podmioty danych gromadzonych przez przedsiębiorców telekomunikacyjnych.

Trybunał Konstytucyjny przeprowadzi rozprawę w sprawie o sygn. K 23/11, zainicjowanej m.in. wnioskami Rzecznik Praw Obywatelskich kwestionującymi konstytucyjność obecnej regulacji zasad dostępu policji i innych służb do danych telekomunikacyjnych.

Jesteśmy przekonani, że wyrok Trybunału Konstytucyjnego zdeterminuje dalsze prace nad projektem. Zwracamy jedynie uwagę, że bez względu na jego treść, ustawodawca może wprowadzić wyższy standard ochrony konstytucyjnych praw i wolności. W przypadku stwierdzenia niekonstytucyjności przepisów regulujących zasady dostępu do danych telekomunikacyjnych ustawodawca powinien kierować się sugestiami Trybunału, które często zamieszczone są w uzasadnieniach wyroku. Należy jednak pamiętać, że konstytucja określa **minimalny** standard ochrony praw człowieka, który może zostać poszerzony i doprecyzowany na gruncie ustawowym – podobnie wyroki Trybunału Konstytucyjnego określają nieprzekraczalną granicę zgodności z konstytucją. Ustawodawca zobowiązany jest zatem przyjąć rozwiązania niesprzeczne z ustawą zasadniczą, jednak w zakresie poszerzania ochrony praw obywatelskich nie jest w żaden sposób ograniczony. Dlatego wykonując wyrok Trybunały Konstytucyjnego, ustawodawca może wyjść poza niezbędne dla zgodności z konstytucją rozwiązania, wprowadzając wyższe wymogi odnośnie ingerowania w konstytucyjne prawa obywateli.

2. Uwagi szczegółowe

W naszej ocenie większość propozycji zawartych w projekcie zmierza w dobrym kierunku. Poniżej prezentujemy uwagi dotyczące niektórych spośród zaproponowanych rozwiązań.

a. Reforma dostępu do danych telekomunikacyjnych

i. Ograniczenie celu pozyskiwania danych

Naszym zdaniem ograniczenie celu pozyskiwania danych telekomunikacyjnych tylko do wykrywania i ustalania sprawców przestępstw, a także uzyskiwania i utrwalania dowodów, stanowi prawidłową implementację tzw. dyrektywy retencyjnej[3]. Dyrektywa stanowi podstawę stworzenia mechanizmu retencji danych, czyli nałożonego na operatorów telekomunikacyjnych obowiązku przechowywania i udostępniania uprawnionym podmiotom danych telekomunikacyjnych.

Zgodnie z dyrektywą retencyjną dane telekomunikacyjne mają być udostępniane organom ścigania w sprawie „poważnych przestępstw". Naszym zdaniem obecne przepisy, pozwalając na sięganie po dane w związku z zapobieganiem lub wykrywaniem sprawców **wszystkich** przestępstw, umożliwiają nieproporcjonalną ingerencję w prawa jednostki. W związku z tym popieramy zawartą w projekcie propozycję ograniczenia katalogu przestępstw, w związku

[3] Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE.

z którymi policja i inne służby mogą sięgać po dane telekomunikacyjne, do tych przypadków, w których możliwe jest przeprowadzenie kontroli operacyjnej, przy jednoczesnym dopuszczeniu wyjątków od tej zasady. Zgodnie z projektem takim wyjątkiem ma być wykrywanie wykroczeń, o których mowa w art. 66 Kodeksu wykroczeń (fałszywe alarmy bombowe). Naszym zdaniem należy rozważyć poszerzenie listy wyjątków o poszukiwanie osób zaginionych[4], przestępstwo uporczywego nękania, o którym mowa w art. 190a Kodeksu karnego (tzw. stalking), a także przestępstwa popełnione za pośrednictwem środków komunikacji elektronicznej w sytuacji, gdy dane telekomunikacyjne są niezbędne do przeprowadzenia innych czynności w śledztwie.

ii. Kontrola nad sięganiem po dane

Pozytywnie oceniamy postulat uzależnienia trybu uzyskania dostępu do danych telekomunikacyjnych od ich charakteru; popieramy również zaproponowany podział – na dane „abonenckie"[5] oraz pozostałe dane telekomunikacyjne.

Naszym zdaniem dostęp do danych abonenckich, który ingeruje w prywatność jednostki w mniejszym stopniu niż dostęp do innych rodzajów danych telekomunikacyjnych, nie musi być uzależniony od każdorazowej zgody organu zewnętrznego. Mimo to projektowane przyznanie policji i innym służbom blankietowego uprawnienia do sięgania po dane abonenckie – bez ograniczenia tej możliwości chociażby do „wykrywania, ustalenia sprawców, uzyskania i utrwalenia dowodów przestępstw" jest zbyt daleko idące.

Z drugiej strony, projekt przewiduje uzależnienie dostępu do innych danych telekomunikacyjnych (np. wykazu połączeń) od uzyskania zgody prokuratora i sądu. Naszym zdaniem to rozwiązanie wprowadza bardzo wysoki standard ochrony praw jednostki. Należy rozważyć, czy nie powinien on obowiązywać dopiero na drugim etapie postępowania przygotowawczego, w którym prowadzone jest ono nie „w sprawie", a „przeciwko" konkretnej osobie (faza *in personam*). Zwracamy również uwagę na konieczność zapewnienia uprawnionym podmiotom możliwości uzyskania tzw. zgody następczej prokuratora lub sądu w sprawach niecierpiących zwłoki.

iii. Sprawozdawczość

Fundacja Panoptykon co roku publikuje informacje dotyczące skali sięgania po dane telekomunikacyjne. Zgodnie z danymi przekazanymi Urzędowi Komunikacji Elektronicznej przez operatorów telekomunikacyjnych w 2013 r. otrzymali oni 1,75 mln zapytań. Natomiast zgodnie z danymi przekazanymi Fundacji przez część uprawnionych podmiotów (policję, Straż Graniczną, Centralne Biuro Antykorupcyjne, Żandarmerię Wojskową, kontrolę skarbową i służbę celną) tylko te podmioty skierowały do operatorów telekomunikacyjnych 2,18 mln zapytań[6]. Naszym zdaniem te rozbieżności świadczą o braku możliwości zweryfikowania, jaka jest

---

[4] Poszerzenie uprawnień policji o możliwość sięgania po dane telekomunikacyjne w celu poszukiwania osób zaginionych zawiera rządowy projekt ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (druk sejmowy nr 2192).

[5] Przez dane abonenckie rozumiemy dane, o których mowa w projektowanych art. 180ca ustawy – Prawo telekomunikacyjne. Z danych zebranych przez Fundację Panoptykon od uprawnionych podmiotów wynika, że zapytania o dane abonenckie stanowią około 42% zapytań kierowanych przez uprawnione podmioty do operatorów telekomunikacyjnych.

[6] Zebrane przez Fundację Panoptykon dane nie obejmują pytań skierowanych do operatorów telekomunikacyjnych przez sądy, prokuratorów i Służbę Kontrwywiadu Wojskowego. Więcej na ten temat: http://panoptykon.org/wiadomosc/miliony-zapytan-jeden-problem.

rzeczywista skala ingerencji policji i innych służb w prywatność użytkowników telefonów komórkowych i Internetu.

W związku z tymi wątpliwościami, popieramy propozycję nałożenia na uprawnione podmioty obowiązków sprawozdawczych. Zwracamy jedynie uwagę na brak możliwości wskazania przez uprawnione podmioty liczby osób, których dotyczyły udostępniane dane – policja i inne służby w większości przypadków (w szczególności na etapie postępowania prowadzonego „w sprawie") nie weryfikują, do kogo należą urządzenia, których dotyczyły zapytania. Ponieważ częstą praktyką jest wykorzystywanie kart typu pre-paid oraz korzystanie z więcej, niż jednego urządzenia, ustalenie, do kogo należała konkretna karta lub telefon może się okazać nadmiernie utrudnione, a z pewnością oznaczałoby konieczność gromadzenia dodatkowych danych.

iv. Niszczenie zbędnych danych

Zgodnie z obowiązującymi przepisami nie wszystkie z podmiotów uprawnionych do sięgania po dane telekomunikacyjne zobowiązane są do ich niszczenia. Naszym zdaniem projekt powinien nakładać na te służby (Agencja Bezpieczeństwa Wewnętrznego, Centralne Biuro Antykorupcyjne, Służba Kontrwywiadu Wojskowego oraz kontrola skarbowa) analogiczny obowiązek niszczenia zbędnych danych, jaki został nałożony na policję w art. 20c ust. 6 i 7 ustawy o policji.

b. Pozyskiwanie danych osobowych

Projekt częściowo dotyczy również szerszego problemu, jakim jest pozyskiwanie przez policję i inne służby różnych danych osobowych dotyczących obywateli. Naszym zdaniem problem ten wymaga gruntownej analizy pod kątem wzmocnienia ochrony prywatności jednostki. Projektowane powołanie wewnętrznego pełnomocnika, który będzie kontrolować przetwarzanie danych osobowych z pozycji osoby zatrudnionej przez dany podmiot, jest dobrą, ale z pewnością nie wystarczającą zmianą. Obecnie przepisy nie chronią bowiem w wystarczający sposób autonomii informacyjnej jednostki i nie gwarantują, że będzie ona narusza wyłącznie wtedy, gdy jest to niezbędne w demokratycznym państwie prawnym.

i. Pełnomocnicy do spraw kontroli przetwarzania danych osobowych

Z powyższymi zastrzeżeniami, popieramy postulat powołania we wszystkich służbach pełnomocnika do spraw kontroli przetwarzania danych osobowych. Nasze zastrzeżenia – podobnie jak w przypadku pełnomocnika funkcjonującego w Centralnym Biurze Antykorupcyjnym – budzi jedynie założenie, że na to stanowisko będzie mógł zostać powołany funkcjonariusz danej służby. Naszym zdaniem może to mieć negatywny wpływ na niezależność jego funkcjonowania.

ii. Uprawnienia Generalnego Inspektora Ochrony Danych Osobowych

Zgodnie z projektem znowelizowany zostanie art. 43 ust. 2 ustawy o ochronie danych osobowych – Generalny Inspektor Ochrony Danych Osobowych uzyska uprawnienie do przeprowadzania czynności kontrolnych związanych z przetwarzaniem przez uprawnione podmioty danych telekomunikacyjnych (z wyjątkiem danych abonenckich). Naszym zdaniem dotychczasowa regulacja, wyłączająca uprawnienia Generalnego Inspektora Ochrony Danych Osobowych względem danych osobowych przetwarzanych przez służby specjalne, jest

nieuzasadniona. Proponowana zmiana prowadzi w dobrym kierunku, niejasne jest jednak, dlaczego w projekcie proponuje się rozszerzenie uprawnień GIODO wyłącznie na kontrolę przetwarzania niektórych danych telekomunikacyjnych.

Z poważaniem,

Małgorzata Szumańska
Wiceprezeska

Katarzyna Szymielewicz
Prezeska