RZECZPOSPOLITA POLSKA

Rzecznik Praw Obywatelskich
Irena LIPOWICZ

Warszawa, 17 stycznia 2011

Pan Donald Tusk

Prezes Rady Ministrów

RPO-662587-II-10/ST

00-090 Warszawa Tel. centr. 22 551 77 00
Al. Solidarności 77 Fax 22 827 64 53

Szanowny Panie Premierze,

W związku z pojawiającymi się w środkach masowego przekazu informacjami dotyczącymi pozyskiwania przez poszczególne służby informacji objętych tajemnicą komunikowania się w Biurze Rzecznika Praw Obywatelskich został zbadany stan prawny obowiązujący w tym zakresie. Analiza tego stanu prawnego prowadzi do konkluzji, iż jest on niezgodny z Konstytucją RP oraz z Europejską Konwencją o Ochronie Praw Człowieka i Podstawowych Wolności.

Na wstępie należy wskazać, iż w myśl art. 159 ust. 1 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 ze zm.) tajemnica komunikowania się w sieciach telekomunikacyjnych, zwana dalej „tajemnicą telekomunikacyjną", obejmuje:

1) dane dotyczące użytkownika;

2) treść indywidualnych komunikatów;

3) dane transmisyjne, które oznaczają dane przetwarzane dla celów przekazywania komunikatów w sieciach telekomunikacyjnych lub naliczania opłat za usługi telekomunikacyjne, w tym dane lokalizacyjne, które oznaczają wszelkie dane przetwarzane w sieci telekomunikacyjnej wskazujące położenie geograficzne urządzenia końcowego użytkownika publicznie dostępnych usług telekomunikacyjnych;

4) dane o lokalizacji, które oznaczają dane lokalizacyjne wykraczające poza dane niezbędne do transmisji komunikatu lub wystawienia rachunku;

5) dane o próbach uzyskania połączenia pomiędzy zakończeniami sieci, w tym dane o nieudanych próbach połączeń, oznaczających połączenia między telekomunikacyjnymi urządzeniami końcowymi lub zakończeniami sieci, które zostały zestawione i nie zostały odebrane przez użytkownika końcowego lub nastąpiło przerwanie zestawianych połączeń.

W świetle powyższego tajemnica komunikowania się obejmuje nie tylko samą treść przekazu (komunikatu, rozmowy), lecz obejmuje ona również takie elementy jak dane dotyczące użytkowników, dane lokalizacyjne urządzenia końcowego czy też dane o próbach uzyskania połączeń. Z art. 159 ust. 2 pkt 4 Prawa telekomunikacyjnego wynika natomiast, iż zakazane jest zapoznawanie się, utrwalanie, przechowywanie, przekazywanie lub inne wykorzystywanie treści lub danych objętych tajemnicą telekomunikacyjną przez osoby inne niż nadawca i odbiorca komunikatu, chyba, że będzie to konieczne z innych powodów niż wskazane w art. 159 ust. 2 pkt 1-3, przewidzianych ustawą lub przepisami odrębnymi. Ponadto z wyjątkiem przypadków określonych ustawą, ujawnianie lub przetwarzanie treści albo danych objętych

tajemnicą telekomunikacyjną narusza obowiązek zachowania tajemnicy telekomunikacyjnej (art. 159 ust. 3 Prawa telekomunikacyjnego).

W związku z powyższym wkroczenie w sferę tajemnicy komunikacyjnej jest możliwe co do zasady jedynie w przypadkach ściśle określonych ustawą. Zawarte w tym zakresie w Prawie telekomunikacyjnym rozwiązania korespondują z treścią art. 49 Konstytucji RP. Stanowi on, iż zapewnia się wolność i ochronę tajemnicy komunikowania się. Ich ograniczenie może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej określony. Z art. 8 ust. 1 Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności wynika zaś, że każdy ma prawo do poszanowania swojej korespondencji. Prawo to w rezultacie obejmuje bezpośrednie komunikowanie się z konkretnie oznaczonymi osobami. Korespondencja obejmuje przy tym wszelkie techniczne formy przekazywania wiadomości. Zgodnie z art. 8 ust. 2 Europejskiej Konwencji niedopuszczalna jest ingerencja władzy publicznej w korzystanie z prawa do poszanowania korespondencji, z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności innych osób.

Rozwiązania zawarte w Prawie telekomunikacyjnym nie budzą wątpliwości z punktu widzenia spełnienia standardu formalnego gwarantowanego przez art. 49 Konstytucji RP i art. 8 ust. 2 Europejskiej Konwencji. Ograniczenia w zakresie dotyczącym tajemnicy telekomunikacyjnej zostały bowiem wprowadzone ustawą. Poważne

wątpliwości natomiast dotyczą innych aspektów wiążących się z gwarancjami ochrony tajemnicy telekomunikacyjnej.

W tym kontekście należy zwrócić uwagę na regulacje prawne dotyczące pokrewnej materii. Otóż obowiązujące przepisy prawa przewidują możliwość zarządzenia kontroli operacyjnej. Kontrola taka jest niejawna i polega m. in. na stosowaniu środków technicznych umożliwiających uzyskiwanie w sposób niejawny informacji i dowodów oraz ich utrwalanie, a w szczególności treści rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych. Jednakże kontrola operacyjna jest zarządzana przez sąd, ma ona charakter subsydiarny (jest więc zarządzana, gdy inne środki okazały się bezskuteczne albo zachodzi wysokie prawdopodobieństwo ich nieskuteczności), a ponadto dotyczy ona co do zasady ściśle określonych czynów zabronionych, zaś materiały uzyskane w wyniku kontroli operacyjnej podlegają zniszczeniu, jeśli okazały się nieprzydatne z punktu widzenia prowadzonego postępowania (por. art. 19 ustawy z dnia 6 kwietnia 1990 r. o Policji - Dz. U. z 2007 r. Nr 43, poz. 277 ze zm.; art. 9e ustawy z dnia 12 października 1990 r. o Straży Granicznej - Dz. U. z 2005 r. Nr 234, poz. 1997 ze zm.; art. 36c ustawy z dnia 28 września 1991 r. o kontroli skarbowej - Dz. U. z 2004 r. Nr 8, poz. 65 ze zm.; art. 31 ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych - Dz. U. Nr 123, poz. 1353 ze zm.; art. 27 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu - Dz. U. z 2010 r. Nr 29, poz. 154; art. 17 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym - Dz. U. Nr 104, poz. 708 ze zm.; art. 31 ustawy z dnia 9 czerwca

2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego - Dz. U. Nr 104, poz. 709 ze zm.).

Powołane powyżej przepisy, z uwagi na to, że kontrola operacyjna z natury rzeczy ma charakter niejawny, mają charakter gwarancyjny. Ich celem jest przede wszystkim wykluczenie arbitralności działań podejmowanych w tym zakresie przez organy władzy publicznej.

Jednakże wymienione służby oprócz kontroli operacyjnej prowadzonej na podstawie wskazanych powyżej przepisów zostały wyposażone także w inne uprawnienia, których istota sprowadza się do ingerencji w tajemnicę komunikowania się. I tak w myśl art. 20c ust. 1 ustawy o Policji w celu zapobiegania lub wykrywania przestępstw Policja może mieć udostępnione dane, o których mowa w art. 180c i 180d ustawy Prawo telekomunikacyjne, zwane dalej „danymi telekomunikacyjnymi", oraz może je przetwarzać. Są to więc dane niezbędne do ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego (inicjującego połączenie, do którego kierowane jest połączenie), a także dane niezbędne do określenia daty i godziny połączenia oraz czasu jego trwania, rodzaju połączenia oraz lokalizacji telekomunikacyjnego urządzenia końcowego (art. 180c ust. 1 Prawa telekomunikacyjnego). Ponadto odwołanie się do art. 180d Prawa telekomunikacyjnego wskazuje, że w omawianym trybie Policja może pozyskiwać dane, o których w art. 159 ust. 1 pkt 1 i pkt 3-5, w art. 161 oraz w art. 179 ust. 9 Prawa telekomunikacyjnego. W grę wchodzi więc pozyskiwanie takich danych jak: dane dotyczące użytkownika; dane transmisyjne, które oznaczają dane przetwarzane dla celów przekazywania komunikatów w sieciach telekomunikacyjnych lub naliczania opłat za usługi

telekomunikacyjne, w tym dane lokalizacyjne, które oznaczają wszelkie dane przetwarzane w sieci telekomunikacyjnej wskazujące położenie geograficzne urządzenia końcowego użytkownika publicznie dostępnych usług telekomunikacyjnych; dane o lokalizacji, które oznaczają dane lokalizacyjne wykraczające poza dane niezbędne do transmisji komunikatu lub wystawienia rachunku; dane o próbach uzyskania połączenia między zakończeniami sieci, w tym dane o nieudanych próbach połączeń, oznaczających połączenia między telekomunikacyjnymi urządzeniami końcowymi lub zakończeniami sieci, które zostały zestawione i nie zostały odebrane przez użytkownika końcowego lub nastąpiło przerwanie zestawianych połączeń (art. 159 ust. 1 pkt 1 i 3-5 Prawa telekomunikacyjnego). W ramach pozyskiwania danych dotyczących użytkownika będącego osobą fizyczną Policja w tym trybie może również pozyskać takie dane jak: nazwisko i imię; imiona rodziców; miejsce i data urodzenia; adres miejsca zameldowania na pobyt stały; numer ewidencyjny PESEL - w przypadku obywatela Rzeczypospolitej Polskiej; nazwę, serię i numer dokumentu potwierdzającego tożsamość, a w przypadku cudzoziemca, który nie jest obywatelem państwa członkowskiego albo Konfederacji Szwajcarskiej - numer paszportu lub karty pobytu; zawarte w dokumentach potwierdzające możliwość wykonania zobowiązania wobec dostawcy publicznie dostępnych usług telekomunikacyjnych wynikające z umowy o świadczenie usług telekomunikacyjnych (art. 161 ust. 2 Prawa telekomunikacyjnego). Policja może ponadto pozyskać także inne dane użytkownika, jeśli pozostają one tylko w dyspozycji dostawcy publicznie dostępnych usług telekomunikacyjnych takie jak: numer identyfikacji podatkowej NIP; numer konta bankowego lub karty płatniczej; adres korespondencyjny użytkownika, jeżeli jest on inny niż adres miejsca zameldowania użytkownika, a także adres poczty elektronicznej

oraz numery telefonów kontaktowych (art. 161 ust. 3 Prawa telekomunikacyjnego). Wreszcie w trybie określonym w art. 20c ust. 1 ustawy o Policji funkcjonariusze Policji mogą pozyskać prowadzony przez przedsiębiorcę telekomunikacyjnego elektroniczny wykaz abonentów, użytkowników lub zakończeń sieci, uwzględniający dane uzyskane przy zawarciu umowy (art. 179 ust. 9 Prawa telekomunikacyjnego).

W związku z powyższym nie ulega wątpliwości, że regulacja zawarta w art. 20c ust. 1 ustawy o Policji zapewnia funkcjonariuszom Policji szeroki dostęp do danych, które są objęte tajemnicą komunikowania się. Analogiczny dostęp do wymienionych danych został zapewniony Straży Granicznej (art. lOb ust. 1 ustawy o Straży Granicznej), wywiadowi skarbowemu (art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej), Żandarmerii Wojskowej (art. 30 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych), Agencji Bezpieczeństwa Wewnętrznego (art. 28 ust. 1 pkt 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu), Centralnemu Biuru Antykorupcyjnemu (art. 18 ust. 1 pkt 1 ustawy o Centralnym Biurze Antykorupcyjnym), Służbie Kontrwywiadu Wojskowego (art. 32 ust. 1 pkt 1 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego).

Omawiane dane objęte tajemnicą komunikowania się są udostępniane: „w celu zapobiegania lub wykrywania przestępstw" (art. 20c ust. 1 ustawy o Policji); „w celu zapobiegania lub wykrywania przestępstw" (art. lOb ust. 1 ustawy o Straży Granicznej); „w celu zapobiegania lub wykrywania przestępstw skarbowych lub przestępstw, o których mowa w art. 2 ust. 1 pkt 14b, oraz naruszeń przepisów, o których mowa w art. 2 ust. 1 pkt 12", tj. także w celu zapobiegania i ujawniania przestępstw, o których mowa w art. 228-231 k. k., popełnianych przez osoby zatrudnione lub pełniące służbę w

jednostkach organizacyjnych podległych ministrowi właściwemu do spraw finansów publicznych oraz w celu zapobiegania i wykrywania naruszeń krajowych przepisów celnych oraz ścigania naruszeń krajowych lub wspólnotowych przepisów celnych (art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej); „w celu zapobiegania lub wykrywania przestępstw, w tym skarbowych" (art. 30 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych); w celu „realizacji przez AB W zadań, o których mowa w art. 5 ust. 1", tj. rozpoznawania, zapobiegania i zwalczania zagrożeń godzących w bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny, rozpoznawania, zapobiegania i wykrywania przestępstw określonych w art. 5 ust. 1 pkt 2; realizowania, w granicach swojej właściwości, zadań związanych z ochroną informacji niejawnych oraz wykonywania funkcji krajowej władzy bezpieczeństwa w zakresie ochrony informacji niejawnych w stosunkach międzynarodowych; uzyskiwania, analizowania, przetwarzania i przekazywania właściwym organom informacji mogących mieć istotne znaczenie dla ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego, podejmowania innych działań określonych w odrębnych ustawach i umowach międzynarodowych (art. 28 ust. 1 pkt 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu); w celu „realizacji przez CBA zadań określonych w art. 2", tj. w celu 1) rozpoznawania, zapobiegania i wykrywania przestępstw wymienionych w art. 2 ust. 1 pkt 1, oraz ścigania ich sprawców, 2) ujawniania i przeciwdziałania przypadkom nieprzestrzegania przepisów ustawy o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne, 3) dokumentowania podstaw i inicjowania realizacji przepisów ustawy z dnia 21 czerwca 1990 r. o zwrocie korzyści uzyskanych niesłusznie kosztem Skarbu Państwa lub innych państwowych osób prawnych (Dz. U. Nr 44, poz. 255 ze

zm.), 4) ujawniania przypadków nieprzestrzegania określonymi przepisami prawa procedur podejmowania i realizacji decyzji w przedmiocie: prywatyzacji i komercjalizacji, wsparcia finansowego, udzielenia zamówień publicznych, rozporządzenia mieniem jednostek lub przedsiębiorców oraz przyznawania koncesji, zwolnień, zwolnień podmiotowych i przedmiotowych, ulg, preferencji, kontyngentów, plafonów, poręczeń i gwarancji kredytowych, 5) kontroli prawidłowości i prawdziwości oświadczeń majątkowych lub oświadczeń o prowadzeniu działalności gospodarczej osób pełniących funkcje publiczne, o których mowa w art. 115 § 19 k. k., 6) prowadzenia działalności analitycznej dotyczącej zjawisk występujących w obszarze właściwości CBA oraz przedstawiania w tym zakresie informacji Prezesowi Rady Ministrów, Prezydentowi RP, Sejmowi oraz Senatowi, 7) podejmowania innych działań określonych w odrębnych ustawach i umowach międzynarodowych (art. 18 ust. 1 pkt 1 ustawy o Centralnym Biurze Antykorupcyjnym); w celu „realizacji przez SKW zadań określonych w art. 5", tj. 1) rozpoznawania, zapobiegania oraz wykrywania popełnionych przez żołnierzy, funkcjonariuszy SKW i SWW oraz pracowników SZ RP i innych jednostek organizacyjnych MON, przestępstw wymienionych w art. 5 ust. 1 pkt 1, 2) realizowania, w granicach swojej właściwości, zadań określonych w przepisach ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz.1228), 3) uzyskiwania, gromadzenia, analizowania, przetwarzania i przekazywania właściwym organom informacji mogących mieć znaczenie dla obronności państwa, bezpieczeństwa lub zdolności bojowej Sił Zbrojnych oraz podejmowania działań w celu eliminowania ustalonych zagrożeń, 4) prowadzenia kontrwywiadu radioelektronicznego oraz przedsięwzięć z zakresu ochrony kryptograficznej i kryptoanalizy, 5) uczestniczenia w planowaniu i przeprowadzaniu kontroli realizacji umów

międzynarodowych dotyczących rozbrojenia, 6) ochrony bezpieczeństwa jednostek wojskowych i innych jednostek organizacyjnych MON, 7) ochrony bezpieczeństwa badań naukowych i prac rozwojowych, 9) podejmowania innych działań przewidzianych dla Służby Kontrwywiadu Wojskowego (art. 32 ust. 1 pkt 1 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego).

Z powyższego wyliczenia wynika, że omawiane dane objęte tajemnicą komunikowania się są udostępniane Policji, Straży Granicznej oraz Żandarmerii Wojskowej w celu zapobiegania lub wykrywania wszelkich czynów stanowiących przestępstwo. Nie ma więc w tym przypadku znaczenia charakter czynu zabronionego. Natomiast funkcjonariuszom Centralnego Biura Antykorupcyjnego, Służby Kontrwywiadu Wojskowego i Agencji Bezpieczeństwa Wewnętrznego są udostępniane dane objęte tajemnicą komunikowania się w celu realizacji ich wszystkich, bez wyjątku, ustawowych zadań. W przypadku pozyskiwania danych przez organy kontroli skarbowej ustawodawca odwołał się w zasadzie do ogólnej kategorii przestępstw skarbowych decydując o udostępnieniu organom kontroli skarbowej danych objętych tajemnicą komunikowania się. Ponadto ustawodawca odwołał się w zakresie ingerencji w tajemnicę komunikowania się do tak ogólnej kategorii jak zapobieganie i wykrywanie wszelkich naruszeń przepisów celnych (art. 2 ust. 1 pkt 12 ustawy o kontroli skarbowej).

Ustawodawca nie wyłączył również żadnej kategorii użytkowników z kręgu podmiotów, których dane mogą być pozyskiwane w tym trybie, chociaż dane te mogą być objęte tajemnicą notarialną, adwokacką, radcy prawnego, lekarską lub dziennikarską (art. 180 § 2 k. p. k.), której zniesienie jest możliwe wyłącznie, gdy jest

to niezbędne dla dobra wymiaru sprawiedliwości, a dana okoliczność nie może być ustalona na podstawie innego dowodu.

Zwraca uwagę także i to, że omawiane przepisy dotyczące udostępnienia danych, o których mowa w art. 180c i art. 180d Prawa telekomunikacyjnego nie wprowadzają zasady subsydiarności. Obowiązek udostępnienia danych aktualizuje się po stronie podmiotu wykonującego działalność telekomunikacyjną w każdym przypadku, gdy zwrócą się o to odpowiednie służby, a nie tylko wówczas, gdy inne środki podejmowane w celu realizacji ustawowego celu okazały się bezskuteczne.

Przepisy dotyczące udostępniania odpowiednim służbom danych, o których mowa w art. 180c i art. 180d Prawa telekomunikacyjnego nie przewidują ponadto potrzeby ubiegania się przez te służby o zgodę sądu na wkroczenie w sferę tajemnicy komunikowania się. Z art. 28 ust. 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu, art. 18 ust. 1 ustawy o Centralnym Biurze Antykorupcyjnym oraz art. 32 ust. 1 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego wynika wprost, iż taka zgoda nie jest wymagana. Należy jednak przyjąć, że taka zgoda nie jest jednak wymagana także w pozostałych przypadkach, skoro podmiot prowadzący działalność telekomunikacyjną zobowiązany jest udostępnić dane objęte tajemnicą komunikowania się na pisemny wniosek szefa danej służby lub na ustne żądanie funkcjonariusza posiadającego pisemne upoważnienie (art. 20c ust. 2 ustawy o Policji, art. lOb ust. 2 ustawy o Straży Granicznej, art. 30 ust. 2 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 36b ust. 2 ustawy o kontroli skarbowej).

Natomiast w ramach prowadzonego postępowania karnego (zarówno w fazie in rem, jak i w fazie in personam) podmioty prowadzące działalność telekomunikacyjną obowiązane są wydać sądowi lub prokuratorowi, na żądanie zawarte w postanowieniu, dane, o których mowa w art. 180c i art. 180d Prawa telekomunikacyjnego, jeżeli dane te mają znaczenie dla toczącego się postępowania (art. 218 § 1 k. p. k.). Postanowienie dotyczące tej materii doręcza się abonentowi telefonu lub nadawcy, którego wykaz połączeń lub innych przekazów informacji został wydany. Doręczenie postanowienia może być odroczone na czas oznaczony, niezbędny ze względu na dobro sprawy, lecz nie później niż do czasu prawomocnego zakończenia postępowania (art. 218 § 2 k. p. k.). Na postanowienie prokuratora przysługuje zażalenie do sądu właściwego do rozpoznania sprawy (art. 465 § 2 k. p. k.).

W świetle powyższego, w ramach prowadzonego postępowania karnego wkroczenie w sferę tajemnicy komunikowania się podlega kontroli sądowej. Taka kontrola jest natomiast wyłączona wtedy, gdy ingerencja w ową sferę ma miejsce poza ramami postępowania karnego.

Kolejnym elementem, na który należy zwrócić uwagę jest usuwanie przez poszczególne służby zgromadzonych danych, o których mowa w art. 180c i art. 180d Prawa telekomunikacyjnego. Art. 20c ust. 7 ustawy o Policji, art. lOb ust. 6 ustawy o Straży Granicznej, art. 30 ust. 6 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych przewidują, iż dane te, jeśli nie zawierają informacji mających znaczenie dla postępowania karnego, podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu.

Z kolei w myśl art. 36b ust. 5 ustawy o kontroli skarbowej minister właściwy do spraw finansów publicznych nakazuje niezwłoczne, komisyjne i protokolarne zniszczenie danych uzyskanych od podmiotu prowadzącego działalność telekomunikacyjną, w przypadku, gdy uzna wystąpienie z wnioskiem o te dane za nieuzasadnione. Art. 36b ust. 5 ustawy o kontroli skarbowej nie przewiduje więc w istocie zniszczenia danych, jeśli nie zawierają one informacji mających znaczenie dla prowadzonego przez organy skarbowe postępowania, lecz tylko wtedy, gdy sam wniosek o ich udostępnienie okazał się niezasadny. W związku z tym ustawodawca w tym przypadku w istocie dopuszcza taką sytuację, kiedy sam wniosek o udostępnienie danych był uzasadniony, zaś zgromadzone w wyniku jego realizacji dane nie zostaną zniszczone, pomimo że nie mają one znaczenia z punktu widzenia prowadzonego postępowania.

Natomiast przepisy art. 28 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 32 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, a także art. 18 ustawy o Centralnym Biurze Antykorupcyjnym w ogóle nie przewidują możliwości usunięcia zgromadzonych przez te służby danych, o których mowa w art. 180c i art. 180d Prawa telekomunikacyjnego.

Przeprowadzona analiza przepisów regulujących materię dostępu poszczególnych służb do danych objętych tajemnicą komunikowania się wskazanych w art. 180c i art. 180d Prawa telekomunikacyjnego pozwala na sformułowanie wniosków natury ogólnej. Po pierwsze, omawiane przepisy nie regulują w sposób precyzyjny celu gromadzenia danych, gdyż odwołują się jedynie do zakresu zadań poszczególnych służb bądź ogólnego stwierdzenia, iż dane te są pozyskiwanie w celu zapobiegania lub wykrywania

przestępstw. Po drugie, przepisy te nie wskazują kategorii osób, w stosunku do których niezbędne jest respektowanie ich tajemnicy zawodowej. Po trzecie, warunkiem uzyskania dostępu do tych danych nie jest wyczerpanie innych, mniej ingerujących w sferę praw lub wolności obywatelskich, możliwości pozyskania niezbędnych informacji. Po czwarte, dziedzina dotycząca pozyskiwania w tym trybie danych nie podlega żadnej zewnętrznej formie kontroli (a w szczególności nie podlega kontroli sądowej). Po piąte, istotna część danych gromadzonych przez służby nie podlega zniszczeniu także wtedy, gdy dane te okazały się nieprzydatne z punktu widzenia realizowanych zadań.

W związku z powyższym przyjęte przez ustawodawcę rozwiązania w interesującym zakresie powinny zostać ocenione na tle przewidzianych w Konstytucji RP i Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności standardów dotyczących tajemnicy komunikowania się.

W literaturze przyjmuje się (por. S. Hoc, glosa do uchwały Sądu Najwyższego z dnia 22 stycznia 2003 r., sygn. akt I KZP 45/02, Przegląd Sądowy z 2003 r., Nr 11-12, s. 203; J. Misztal-Konecka, J. Konecki „Biling, jako dowód w postępowaniu w sprawach o wykroczenia", Państwo i Prawo z 2010 r., Nr 7, s. 84), że informacje zawarte w bilingu telefonicznym podlegają ochronie na podstawie art. 49 Konstytucji RP oraz na podstawie art. 8 Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności. Według A. Bojańczyka (por. „Karnoprawne aspekty ochrony praw pracownika do tajemnicy komunikowania się", cz. I, Palestra z 2003 r., Nr 1-2, 49) „(…) prawo do tajemnicy komunikowania się obejmuje również i prawo do zachowania w tajemnicy przed innymi podmiotami faktu, że do komunikacji pomiędzy danymi podmiotami w ogóle doszło. Uznanie, że sam fakt komunikacji pomiędzy podmiotami

nie jest objęty ochroną konstytucyjną z art. 49, w praktyce byłoby tożsame ze znaczącym faktycznym ograniczeniem tego prawa. Ustawa zasadnicza gwarantuje bowiem nie tylko tajemnicę przekazywanej informacji, lecz całego procesu komunikowania się - a więc i tego, że pomiędzy podmiotami doszło do komunikacji. Prawo to nie może być więc rozumiane wyłącznie wąsko (znaczenie podstawowe), lecz konieczna jest jego pełna interpretacja, tak, aby obejmowało cały proces komunikowania się."

Europejski Trybunał Praw Człowieka w wyroku z dnia 2 sierpnia 1984 r. (sprawa Malone przeciwko Zjednoczonemu Królestwu, skarga nr 8691/79, lex nr 80974) stwierdził zaś, że z samej swej natury biling musi być rozróżniany od podsłuchu, który jest zjawiskiem niepożądanym i bezprawnym w społeczeństwie demokratycznym, chyba, że istnieją ku niemu uzasadnione powody. Jednak użycie danych wynikających z bilingu może, w niektórych okolicznościach, stanowić naruszenie art. 8. Dane bilingowe zawierają informacje szczególnie o wybieranych numerach, które stanowią integralny składnik komunikacji telefonicznej. W efekcie, ujawnienie tej informacji policji, bez zgody abonenta, może również stanowić ingerencję w prawa zagwarantowane art. 8.

W rezultacie trzeba przyjąć, że art. 49 Konstytucji RP oraz art. 8 Europejskiej Konwencji i Ochronie Praw Człowieka i Podstawowych Wolności stanowią właściwy punkt odniesienia do oceny przepisów dotyczących wkraczania w interesującym zakresie przez służby w sferę tajemnicy komunikowania się.

Przede wszystkim - co już zostało wykazane powyżej - przepisy regulujące materię dostępu poszczególnych służb do danych objętych tajemnicą komunikowania się

wskazanych w art. 180c i art. 180d Prawa telekomunikacyjnego nie regulują w sposób konkretny, kiedy możliwe jest wkroczenie w wolność komunikowania się. Przepisy te bowiem odwołują się wyłącznie do zakresu zadań poszczególnych służb bądź też do ogólnego stwierdzenia, że dane te są pozyskiwane przez służby w celu zapobiegania lub wykrywania przestępstw. Tymczasem z art. 49 Konstytucji RP wynika, że ograniczenie wolności i ochrony tajemnicy komunikowania się może nastąpić „jedynie w przypadkach określonych w ustawie". Nie wystarczy więc, że ustawodawca regulując kwestie związane z wolnością komunikowania się i jej ochroną odwoła się do klauzul ogólnych czy też ogólnych kompetencji organów uprawnionych do zbierania danych. Z punktu widzenia realizacji wolności określonej w art. 49 Konstytucji RP przepisy muszą być na tyle precyzyjne, aby mogły dostarczyć obywatelom wystarczających wskazówek, w jakiej sytuacji służby uzyskują prawo wkroczenia w sferę objętą zakresem tajemnicy. Nie jest więc w tym przypadku wcale wystarczające odwołanie się do tak ogólnych celów zbierania danych jak „zapobieganie lub wykrywanie przestępstw" czy też „realizacja zadań" określonych w przepisach prawa dla poszczególnych służb. Regulacja taka nie odpowiada bowiem precyzji wymaganej przez art. 49 Konstytucji RP i w istocie pozwala w sposób dowolny ingerować w tajemnicę komunikowania się.

Przedstawione stanowisko znajduje potwierdzenie w orzecznictwie Trybunału Konstytucyjnego. W wyroku z dnia 12 grudnia 2005 r. (sygn. akt K 32/04, OTK z 2005 r., Nr 11/A, poz. 132) Trybunał Konstytucyjny stwierdził, że „(…) w zakresie art. 49 Konstytucji (wolność komunikowania się) dopuszcza się ograniczenie tej wolności w przypadkach określonych w ustawodawstwie zwykłym. Oznacza to, że - po pierwsze -

ustawodawca zwykły może decydować o zakresie wolności komunikowania się, jeśli - po drugie - uczyni to w akcie rangi ustawy, wskazującym - po trzecie - „określone przypadki" i „sposób ograniczenia" (wymóg konkretności, wyłączenie użycia w tych zakresach otwartych klauzul generalnych)".

Otóż zdaniem Rzecznika Praw Obywatelskich przepisy art. 20c ust. 1 ustawy o Policji, art. lOb ust. 1 ustawy o Straży Granicznej, art. 36b ust. 1 ustawy o kontroli skarbowej, art. 30 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28 ust. 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 18 ust. 1 ustawy o Centralnym Biurze Antykorupcyjnym oraz art. 32 ust. 1 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego nie spełniają kryterium konkretności wymaganego przez art. 49 Konstytucji RP. Brak owej konkretności powoduje zaś, że wymienione służby w istocie w dowolnym i tylko przez siebie ustalonym przypadku, a nie przypadku określonym ustawą, mogą sięgać po dane objęte tajemnicą komunikowania się. Stąd też wymienione przepisy pozostają w kolizji z art. 49 Konstytucji RP.

Ze względu na brak konkretności przepisy te są także niezgodne z art. 8 ust. 2 Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności. Przewiduje on, iż niedopuszczalna jest ingerencja władzy publicznej w korzystanie z prawa do korespondencji, z wyjątkiem przypadków przewidzianych przez ustawę. Jak zaś wskazał Europejski Trybunał Praw Człowieka (sprawa Malone) sformułowanie użyte w art. 8 ust. 2 Konwencji „przewidzianych przez ustawę" nie jest tożsame z prostym odwołaniem się do prawa krajowego, ale odnosi się także do jakości tego prawa. Oznacza to, że prawo krajowe musi być w tym zakresie wystarczająco

precyzyjne i musi wskazywać obywatelom adekwatne okoliczności oraz warunki, w jakich władze są uprawnione stosować niejawne techniki zdobywania informacji.

W ocenie Rzecznika Praw Obywatelskich przepisy te są również niezgodne z art. 49 w związku z art. 31 ust. 3 Konstytucji RP. Z art. 31 ust. 3 Konstytucji RP wynika, iż ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Ograniczenia te nie mogą naruszać istoty wolności i praw.

Przesłanka „konieczności" ograniczenia, o której mowa w art. 31 ust. 3 Konstytucji RP jest merytorycznie tożsama z zasadą proporcjonalności. „Konieczność" zastosowania ograniczenia, do której odwołuje się art. 31 ust. 3 Konstytucji RP oznacza zaś w świetle orzecznictwa Trybunału Konstytucyjnego (por. wyrok z dnia 26 kwietnia 1999 r., sygn. akt K 33/98, OTK z 1999 r., Nr 4, poz. 71; wyrok z dnia 11 maja 1999 r., sygn. akt K 13/98, OTK z 1999 r., Nr 4, poz. 74) obowiązek ustawodawcy wyboru najmniej uciążliwego środka. Jeśli więc ten sam cel jest możliwy do osiągnięcia przy zastosowaniu innego środka, nakładającego mniejsze ograniczenia na prawa i wolności jednostki, to zastosowanie przez ustawodawcę środka bardziej uciążliwego wykracza poza ramy tego, co jest konieczne.

W przypadku kontroli operacyjnej, będącej formą ingerencji w tajemnicę komunikowania się, regulowanej przepisami art. 19 ustawy o Policji, art. 9e ustawy o Straży Granicznej, art. 36c ustawy o kontroli skarbowej, art. 31 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 27 ustawy o Agencji

Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 17 ustawy o Centralnym Biurze Antykorupcyjnym, art. 31 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego ustawodawca dotrzymał warunków wynikających z zasady proporcjonalności. Ingerencja w tajemnicę komunikowania się jest możliwa jedynie wówczas, gdy „inne środki okazały się bezskuteczne albo zachodzi wysokie prawdopodobieństwo, że będą nieskuteczne lub nieprzydatne." Warunek ten nie został jednak dochowany w zakresie pozyskiwania danych, o których mowa w art. 180 c i art. 180d Prawa telekomunikacyjnego. Służby mogą bowiem wkraczać w sferę objętą konstytucyjną ochroną z mocy art. 49 Konstytucji RP w dowolnym momencie, a nie tylko wówczas, gdy jest to konieczne i niezbędne, a więc wówczas, gdy owych danych nie można było pozyskać w inny sposób. W rezultacie to komfort (wygoda) działania służb, a nie względy konieczności decydują o ingerencji w konstytucyjną wolność i ochronę tajemnicy komunikowania się. Tymczasem - na co zwracał uwagę Trybunał Konstytucyjny (por. wyrok z dnia 12 grudnia 2005 r., sygn. akt K 32/04, OTK z 2005 r., Nr 1 l/A, poz. 132) - „(…) nie wystarczy, aby stosowane środki sprzyjały zamierzonym celom, ułatwiały ich osiągnięcie albo były wygodne dla władzy, która ma je wykorzystać do osiągnięcia tych celów. (...) Minimalnym wymogiem konstytucyjnym jest to, aby przeszły one test „konieczności w demokratycznym państwie prawnym". Nie wystarczy zatem sama celowość, pożyteczność, taniość czy łatwość posługiwania się przez władzę - w odniesieniu do użytego środka. Bez znaczenia jest też argument porównawczy, że podobne środki w ogóle bywają stosowane w innych państwach. Tylko bowiem odwołanie się geograficznie i historycznie do środków koniecznych w demokratycznym państwie prawnym może mieć wartość perswazyjną. Chodzi zatem o zastosowanie środków niezbędnych (koniecznych) w tym sensie, że będą one chronić

określone wartości w sposób, bądź w stopniu, który nie mógłby być osiągnięty przy zastosowaniu innych środków, a jednocześnie winny to być środki jak najmniej uciążliwe dla podmiotów, których prawo bądź wolność ulegają ograniczeniu (...)" •

Tak więc kwestionowane przepisy są również niezgodne z art. 49 w zw. z art. 31 ust. 3 Konstytucji RP przez to, że pozwalają na pozyskiwanie danych objętych tajemnicą komunikowania się także wówczas, gdy nie jest to konieczne w demokratycznym państwie prawnym.

Przepisy art. 20c ust. 2 ustawy o Policji, art. lOb ust. 1 ustawy o Straży Granicznej, art. 36b ust. 2 ustawy o kontroli skarbowej, art. 30 ust. 2 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28 ust. 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 18 ust. 1 ustawy o Centralnym Biurze Antykorupcyjnym, a także przepisy art. 32 ust. 1 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego powinny zostać ocenione także z punktu widzenia konstytucyjnego standardu prawa do sądu. Dochowanie tego standardu ma szczególne znaczenie w sytuacji, gdy dane o jednostce są pozyskiwane przez organy władzy publicznej bez jej wiedzy i zgody. Wówczas w sposób bezwzględny musi istnieć procedura zewnętrznej kontroli legalności działań podejmowanych przez organy władzy publicznej. Nie może bowiem być tak, że jedyną władzą oceniającą zasadności pozyskiwania danych objętych treścią art. 180c i art. 180 d Prawa telekomunikacyjnego są same służby.

W wyroku z dnia 4 maja 2000 r. (Rotaru przeciwko Rumunii, skarga nr 28341/95) Europejski Trybunał Praw Człowieka stwierdził, że systemy niejawnej inwigilacji musza zawierać gwarancje procesowe stosowane do kontroli działań służb. Kontrola ta

powinna być prowadzona przynajmniej przez organy zewnętrzne wobec służb dokonujących czynności operacyjnych. Pożądane zaś jest, aby w normalnych warunkach, kontrolę prowadziły organy sądowe. Kontrola sądowa zapewnia bowiem gwarancję niezależności, bezstronności oraz gwarancję stosowania właściwej procedury. Kontrola niesądowa, sprawowana przez inne organy zewnętrzne wobec kontrolowanych, o odpowiednio reprezentatywnym składzie - nie uchybia jednak Konwencji. Alternatywą wobec poddania czynności operacyjnych-rozpoznawczych kontroli sądu może być poddanie tych czynności kontroli sprawowanej przez specjalny organ, którego usytuowanie i skład powinien zapewniać niezależność od władzy wykonawczej.

W polskiej rzeczywistości konstytucyjnej ramy kontroli zewnętrznej wyznacza przede wszystkim art. 45 ust. 1 i art. 77 ust. 2 Konstytucji RP. Treść art. 77 ust. 2 Konstytucji RP przesądza w zasadzie o tym, że w sprawach dotyczących konstytucyjnych wolności i praw (a więc także w sprawie objętej zakresem art. 49 Konstytucji RP) takim zewnętrznym organem kontroli powinien być sąd. Jeśli bowiem - w świetle wyroku Trybunału Konstytucyjnego z dnia 10 maja 2000 r. (sygn. akt K 21/99, OTK z 2000 r., Nr 4, poz. 109) - „(…) art. 45 ust. 1 konstytucji dotyczy dochodzenia przed sądem wszelkich praw (także ustanowionych w innych aktach normatywnych niż konstytucja), to art. 77 ust. 2 konstytucji obejmuje swym zakresem jedynie prawa i wolności gwarantowane konstytucyjnie. W tym znaczeniu art. 77 ust. 2, stanowiąc uzupełnienie i rozwinięcie ogólniejszego ujęcia z art. 45 ust. 1, zawiera zarazem swoistą regulację szczególną w stosunku do art. 45 ust. 1 konstytucji. Płynie stąd istotny wniosek, co do zakresu dopuszczalnych ograniczeń praw do sądu.

Ograniczenia prawa do sądu ustanawiane normą ustawową, stosownie do art. 31 ust. 3 konstytucji, muszą uwzględniać kategoryczny zakaz zamykania drogi do sądu zawarty w art. 77 ust. 2 w zakresie dochodzenia konstytucyjnych wolności i praw (...)".

Tymczasem powołane powyżej przepisy w sposób wyraźny bądź w sposób wynikający z ich kontekstu normatywnego (udostępnianie danych na pisemny wniosek szefa danej służby, ustne żądanie funkcjonariusza) wyłączają zarówno uprzednią jak też następczą zgodę sądu na ingerencję w konstytucyjną wolność i ochronę tajemnicy komunikowania się. Sfera ta nie podlega więc żadnej kontroli zewnętrznej, w tym przypadku kontroli sądowej. Dzieje się tak, chociaż pozyskiwanie danych, o których mowa w art. 180c i art. 180d Prawa telekomunikacyjnego jest wyłączone zarówno spod kontroli samego zainteresowanego (nie jest on powiadamiany o gromadzeniu dotyczących go danych) jak też jest wyłączone spod jakiejkolwiek kontroli społecznej. Stąd też trzeba uznać, że omawiane przepisy są niezgodne z art. 45 ust. 1 i art. 77 ust. 2 Konstytucji RP.

Wreszcie wskazać trzeba, iż przepisy art. 28 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 32 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, a także art. 18 ustawy o Centralnym Biurze Antykorupcyjnym w ogólne nie przewidują możliwości usunięcia zgromadzonych przez te służby danych, o których mowa w art. 180c i art. 180d Prawa telekomunikacyjnego, także wówczas, gdy dane te są nieprzydatne z punktu widzenia realizacji celu, dla którego zostały zebrane. Z kolei - na co już zwrócono uwagę - art. 36b ust. 5 ustawy o kontroli skarbowej przewiduje zniszczenie danych tylko wtedy, gdy minister właściwy do spraw finansów publicznych uzna wystąpienie o te dane za

nieuzasadnione. W tym więc przypadku ustawodawca dopuszcza sytuację, gdy sam wniosek o udostępnienie danych był uzasadniony. Nie zostaną one jednak zniszczone, jeżeli następnie okaże się, iż nie są przydatne z punktu widzenia prowadzonego postępowania.

W świetle powyższych regulacji prawnych należy uznać, iż w istocie w tym zakresie ustawodawca zezwala na gromadzenie i bezterminowe przechowywanie danych, które nie są niezbędne z punktu widzenia realizacji celów, dla których zostały zebrane. Dzieje się tak, chociaż z art. 51 ust. 2 Konstytucji RP wynika zakaz gromadzenia danych innych niż niezbędne w demokratycznym państwie prawnym. Skoro gromadzenie danych nie spełnia w tym zakresie warunku niezbędności, to trzeba uznać, że wymienione przepisy są niezgodne z art. 51 ust. 2 Konstytucji RP przez to, że nie przewidują zniszczenia danych, o których mowa w art. 180 c i art. 180d Prawa telekomunikacyjnego w sytuacji, gdy nie zawierają informacji mających znaczenie z punktu widzenia realizacji ustawowych zadań przez poszczególne służby.

Mając na względzie powyższe uwagi, zwracam się do Pana Premiera stosownie do art. 16 ust. 2 pkt 1 ustawy z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich (Dz. U. z 2001 r. Nr 14, poz. 147 ze zm.) o podjęcie działań w celu zmiany obowiązującego w interesującym zakresie stanu prawnego i jego dostosowanie do standardów konstytucyjnych. Będę wdzięczna za stanowisko Pana Premiera w tej sprawie.

Łączę wyrazy szacunku

Lena Kolarska-Bobińska