RZECZPOSPOLITA POLSKA
MINISTERSTWO
ADMINISTRACJI I CYFRYZACJI
PODSEKRETARZ STANU
Igor Ostrowski

Warszawa, dnia 20 marca 2012 r.

SEKRETARIAT
Biura Prac Senackich
Wpłynęło dn. 26.03.12 zał.
nr 2385 podpis

ŁT1c-077-6-2/12

GABINET MARSZAŁKA SENATU
wpłynęło dn. 21.03.12.
nr 1293 podpis

Bogdan Borusewicz
Marszałek Senatu
Rzeczypospolitej Polskiej

Szanowny Panie Marszałku,

w odpowiedzi na oświadczenie Pana Senatora Jana Marii Jackowskiego z dnia 2 lutego br., w sprawie kontroli korespondencji telekomunikacyjnej, uprzejmie przedstawiam poniższe wyjaśnienia.

W celu udzielenia wyczerpującej odpowiedzi, z uwagi na szeroki zakres zagadnień poruszonych w oświadczeniu Pana senatora Jackowskiego, Ministerstwo Administracji i Cyfryzacji wystąpiło do Ministerstwa Spraw Wewnętrznych oraz do Ministerstwa Sprawiedliwości o przekazanie niezbędnych informacji z zakresu właściwości wskazanych resortów. W związku z tym, niniejsza odpowiedź uwzględnia informacje przekazane przez wspomniane resorty.

Odnosząc się do przedmiotu oświadczenia Pana Senatora, w pierwszej kolejności, warto wskazać na znaczenie i zakres pojęć związanych z szeroko rozumianą tajemnicą komunikowania się. Samo pojęcie „korespondencji telekomunikacyjnej" nie jest pojęciem normatywnym. Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (Dz. U. z 1997 r. Nr 89, poz.555 z późn. zm.), dalej „k.p.k.", w art. 236a posługuje się zwrotem normatywnym - „korespondencja przesyłana pocztą elektroniczną". Natomiast na gruncie ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm), dalej „Pt", występuje pojęcie „komunikatu" rozumianego, jako każda informacja wymieniana lub przekazywana między określonymi użytkownikami za pośrednictwem publicznie dostępnych usług telekomunikacyjnych, nie obejmująca informacji przekazanej jako część transmisji radiowych lub telewizyjnych transmitowanych poprzez sieć telekomunikacyjną, z wyjątkiem informacji odnoszącej się do możliwego do zidentyfikowania abonenta lub użytkownika otrzymującego informację. Zgodnie z art. 159

ust. 1 pkt 2 Pt treść wszelkich indywidualnych komunikatów objęta jest tajemnicą telekomunikacyjną. Tajemnica komunikowania się w sieciach telekomunikacyjnych (tajemnica telekomunikacyjna) 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.

Jak wynika z powyższego, pojęcie tajemnicy telekomunikacyjnej odnosi się nie tylko do danych dotyczących użytkowników, ale również do treści przekazu czy informacji o próbach uzyskania połączenia. Ustawa Pt zakazuje zapoznawania się, utrwalania, przechowywania, przekazywania lub innego wykorzystywania treści lub danych objętych tajemnicą telekomunikacyjną przez osoby inne niż nadawca i odbiorca komunikatu, z wyłączeniem przypadków wskazanych w ustawie.

Odnosząc się do zakresu uprawnień organów procesowych należy zauważyć, że zgodnie z art. 218 § 1 k.p.k. sąd lub prokurator ma prawo zatrzymać korespondencję i przesyłki, jak również dane, o których mowa w art. 180c i 180d Pt. Przywołane przepisy Pt odnoszą się do obowiązków przedsiębiorców telekomunikacyjnych na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego. Na podstawie art. 180a ust. 1 pkt 2 Pt, w zw. z art. 180c ust. 1 Pt przedsiębiorcy telekomunikacyjni mają obowiązek udostępniania uprawnionym podmiotom danych niezbędnych do:

1) ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego:

a) inicjującego połączenie,

b) do którego kierowane jest połączenie;

2) określenia:

a) daty i godziny połączenia oraz czasu jego trwania,

b) rodzaju połączenia,

c) lokalizacji telekomunikacyjnego urządzenia końcowego.

Dodatkowo, na mocy art. 180 d przedsiębiorcy telekomunikacyjni są obowiązani do zapewnienia warunków dostępu i utrwalania oraz do udostępniania uprawnionym podmiotom, a także Służbie Celnej, sądowi i prokuratorowi, na własny koszt, przetwarzanych przez siebie danych, o których mowa w art. 159 ust. 1 pkt 1 i 3–5 Pt, w art. 161 Pt oraz w art. 179 ust. 9 Pt, związanych ze świadczoną usługą telekomunikacyjną, na zasadach i przy zachowaniu procedur określonych w przepisach odrębnych. Do takich danych należą dane dotyczące użytkownika, dane transmisyjne, dane lokalizacyjne oraz dane o próbach uzyskania połączenia. Jednocześnie zgodnie z art. 236a k.p.k. przepisy rozdziału 25 k.p.k. *„Zatrzymanie rzeczy. Przeszukanie"*, w tym wspomniany przepis art. 218 tego rozdziału uprawniający do zatrzymania wskazanych powyżej danych, stosuje się odpowiednio do dysponenta i użytkownika urządzenia zawierającego dane informatyczne lub systemu informatycznego, w zakresie danych przechowywanych w tym urządzeniu lub systemie albo na nośniku znajdującym się w jego dyspozycji lub użytkowaniu, w tym korespondencji przesyłanej pocztą elektroniczną. W istocie zatem, sąd lub prokurator są uprawnieni w ramach procesu karnego do zatrzymania korespondencji przesyłanej pocztą elektroniczną. W ramach procesu karnego dostęp do danych telekomunikacyjnych, w tym wykazu połączeń realizowanych z określonego numeru telefonu, możliwy jest wyłącznie na podstawie postanowienia prokuratora lub sądu w wypadku, gdy dane tego rodzaju mają znaczenie dla toczącego się postępowania. Niewątpliwie w ramach zatrzymanej korespondencji może się znaleźć korespondencja pomiędzy oskarżonym a obrońcą, jak również inna korespondencja bezpośrednio związana z wykonywaniem funkcji obrońcy. Należy przy tym zauważyć, że poufność komunikowania się oskarżonego i obrońcy jest fundamentalną przesłanką realizacji przez oskarżonego jego podstawowego, konstytucyjnego prawa do obrony, podobnie jak wszelkie informacje związane z realizowaną funkcją obrończą, np. pomiędzy obrońcą a osobą, która występuje w procesie karnym z substytucji obrońcy. Z tego też względu ustawodawca przewidział szczególny tryb zatrzymania korespondencji, co do której zachodzi podejrzenie, że jest to korespondencja objęta tajemnicą obrończą. Zgodnie z art. 225 § 1 k.p.k. jeżeli obrońca lub inna osoba, od której żąda się wydania rzeczy lub u której dokonuje się przeszukania, oświadczy, że wydane lub znalezione w toku przeszukania pisma lub inne dokumenty obejmują okoliczności związane z wykonywaniem funkcji obrońcy,

organ dokonujący czynności pozostawia te dokumenty wymienionej osobie bez zapoznawania się z ich treścią lub wyglądem. Jeżeli jednak oświadczenie osoby nie będącej obrońcą budzi wątpliwości, organ dokonujący czynności przekazuje te dokumenty bez odczytywania w opieczętowanym opakowaniu sądowi, który po zapoznaniu się z dokumentami zwraca je w całości lub w części osobie od której je zabrano, albo wydaje postanowienie o ich zatrzymaniu dla celów postępowania. Z przedstawionych wyżej reguł postępowania z dokumentami zawierającymi tajemnicę obrończą wynika, że ustawodawca przewidział niezwykle rygorystyczny tryb postępowania z tego rodzaju dokumentami, w tym zwłaszcza regułę pozostawiania dokumentów w dyspozycji osoby pełniącej funkcje obrończe wyłącznie na skutek złożenia przez tą osobę stosownego oświadczenia, a w przypadku, gdy dokument zawierający informacje objęte tajemnicą obrończą znajduje się w dyspozycji innej osoby, a oświadczenie tej osoby budzi wątpliwości – wyłączną kompetencję sądu w zakresie weryfikacji prawdziwości tego rodzaju oświadczenia. Wskazane normy określające sposób postępowania z dokumentami zawierającymi tajemnicę obrończą znajdują odpowiednie, na mocy art. 236a k.p.k., zastosowanie do korespondencji przesyłanej pocztą elektroniczną. Oczywistym jest przy tym, że zabezpieczenie dla potrzeb postępowania karnego korespondencji przesyłanej pocztą elektroniczną cechuje się szczególnymi właściwościami, dlatego też nie ma możliwości bezpośredniego zastosowania wskazanych wyżej reguł postępowania. Znajdują one jednak odpowiednie zastosowanie, co oznacza, że po zabezpieczeniu korespondencji (a więc przekazaniu przez operatora nośnika informatycznego, na którym utrwalona została korespondencja przesyłana pocztą elektroniczną) organ dokonujący zatrzymania, ma obowiązek odebrać od osoby, której korespondencja jest zabezpieczana, stosowne oświadczenia mające na celu ustalenie, czy w ramach zabezpieczonej korespondencji znajduje się taka, która zawiera informacje objęte tajemnicą obrończą czy też inne tajemnice podlegające szczególnej ochronie prawnej. W razie ustalenia, że w ramach powyższej czynności zabezpieczono korespondencję, która obejmuje okoliczności związane z wykonywaniem funkcji obrońcy organ ma obowiązek postąpić w sposób wcześniej opisany, a więc zwrócić obrońcy tę korespondencję bez zapoznawania się z jej treścią, a w przypadku, gdy stosowne oświadczenie nie pochodzi od obrońcy i jednocześnie budzi wątpliwości – przekazać korespondencję do dyspozycji sądu, który w tym zakresie podejmuje odpowiednią decyzję procesową po zapoznaniu się z treścią korespondencji. W istocie zatem procesowe zabezpieczenie korespondencji przesyłanej pocztą elektroniczną w pełni respektuje tajemnicę obrończą.

Odrębnym zagadnieniem jest pozyskiwanie korespondencji w ramach tzw. kontroli operacyjnej stosowanej przez Policję oraz inne uprawnione służby. Zgodnie z art. 19 ust. 6 ustawy o Policji kontrola operacyjna polega na kontrolowaniu treści korespondencji, zawartości przesyłek, a także 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. Wskazane czynności, jako ingerujące w prawa i wolności obywatelskie, w tym tajemnicę korespondencji i komunikowania się, poddano kontroli sądowo – prokuratorskiej, ograniczając jednocześnie możliwość ich przeprowadzenia wyłącznie w odniesieniu do enumeratywnie wskazanego katalogu najpoważniejszych przestępstw oraz wskazując, że czynności tego rodzaju mogą być podjęte tylko w sytuacji, gdy inne środki okazały się bezskuteczne albo będą nieprzydatne. Decyzję w przedmiocie wyrażenia zgody na prowadzenie kontroli operacyjnej podejmuje sąd okręgowy na pisemny wniosek Komendanta Głównego Policji złożony po uzyskaniu zgody Prokuratora Generalnego albo na pisemny wniosek komendanta wojewódzkiego policji złożony po uzyskaniu pisemnej zgody właściwego miejscowo prokuratura okręgowego. Stosowanie kontroli operacyjnej zostało również ograniczone pod względem czasowym, bowiem kontrolę tego rodzaju sąd okręgowy zarządza na okres 3 miesięcy, z możliwością przedłużenia jej stosowania na okres dalszych 3 miesięcy. Jedynie wyjątkowo, w uzasadnionych wypadkach, na wniosek Komendanta Głównego Policji, po uzyskaniu zgody Prokuratora Generalnego, sąd władny jest przedłużyć kontrolę operacyjną na dalszy czas oznaczony. Należy jednocześnie pamiętać, że materiał pozyskany w toku kontroli operacyjnej, aby mógł być wykorzystany w procesie karnym, musi respektować zakazy dowodowe obowiązujące w procedurze karnej. Za niemożliwy do wykorzystania w procesie karnym należy uznać taki materiał kontroli operacyjnej, który dotyczy okoliczności objętych bezwzględnym zakazem dowodowym np. dotyczy faktów objętych tajemnicą obrończą. W odniesieniu do innego rodzaju materiału kontroli operacyjnej, który obejmuje inne tajemnice prawnie chronione, powinno się stosować zasady ogólne dotyczące możliwości ich uchylenia przez sąd lub prokuratora. Należy zatem uznać, że w sytuacji braku zgody na uchylenie tajemnicy materiał kontroli operacyjnej nie może być wprowadzony do procesu karnego i podlega niezwłocznemu zniszczeniu. W tym miejscu należy wskazać, że kontrola operacyjna realizowana w stosunku do obrońcy, w celu uzyskania informacji objętych tajemnicą obrończą, jest niedopuszczalna Tego rodzaju czynność organów w sposób rażący

podważałaby konstytucyjne prawo do obrony, stąd też należy stanowczo stwierdzić, że stosowanie kontroli operacyjnej w takim celu jest prawnie niedopuszczalne.

Odnosząc się do poruszonej przez Pana Senatora kwestii pozyskiwania wykazu połączeń realizowanych z określonego numeru telefonu, należy stwierdzić, że dane te nie mogą być one uznane za korespondencję w rozumieniu przepisów k.p.k. Ustawodawca wyraźnie bowiem różnicuje na gruncie art. 218 § 1 k.p.k. pojecie korespondencji i pojęcie danych telekomunikacyjnych. W toku procesu karnego zarówno sąd jak i prokurator uprawniony jest do uzyskania danych telekomunikacyjnych wskazanych w art. 180c i 180d Pt, o czym była mowa wcześniej. Wskazane dane telekomunikacyjne objęte są tajemnicą telekomunikacyjną i w ramach procesu karnego dostęp do tego rodzaju informacji możliwy jest wyłącznie na podstawie postanowienia prokuratora lub sądu w wypadku, gdy dane tego rodzaju mają znaczenie dla toczącego się postępowania.

Od pozyskiwania danych telekomunikacyjnych przez sąd lub prokuratora w toku postępowania karnego, a więc czynności dowodowej w procesie karnym, należy odróżnić pozyskiwanie tego rodzaju danych przez Policję i inne służby na podstawie szczególnego upoważnienia ustawowego, jako jednej z form czynności operacyjno - rozpoznawczych wykorzystywanych przez Policję i służby specjalne dla realizacji stawianych przed nimi zadań państwowych związanych z bezpieczeństwem i porządkiem publicznym, w zakresie zapobieżenia, wykrycia, ustalenia sprawców a także uzyskania i utrwalenia dowodów przestępstw oraz realizacji innych ustawowych celów wyznaczanych zwłaszcza służbom specjalnym w zakresie ochrony bezpieczeństwa państwa. Przykładowo można wskazać, że zgodnie z art. 20c ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2007 r., Nr 43, poz. 277, z późn. zm.) Policja może pozyskiwać w ramach czynności operacyjno – rozpoznawczych takie same dane jak sąd lub prokurator w postępowaniu karnym, w celu zapobiegania lub wykrywania przestępstw. Analogiczne regulacje jak w przypadku Policji zawierają ustawy określające kompetencje poszczególnych służb – Straży Granicznej (art. 10b ustawy z dnia 12 października 1990 r. o Straży Granicznej - Dz. U z 2005 r., Nr 234, poz. 1997, z późn. zm.), Kontroli Skarbowej (art. 36b ustawy z dnia 28 września 1991 r. o Kontroli skarbowej - Dz. U. z 2004 r., nr 8 poz. 65, z późn. zm.), Żandarmerii Wojskowej (art. 30 ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych - Dz. U. Nr 123, poz. 1353, z późn. zm), Agencji Bezpieczeństwa Wewnętrznego (art. 28 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu - Dz. U. z 2010 r., Nr 29, poz. 154), Centralnego Biura Antykorupcyjnego (art. 18 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze

Antykorupcyjnym - Dz. U. Nr 104, poz. 708, z późn. zm), a także Służby Kontrwywiadu Wojskowego (art. 32 ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego i Służbie Wywiadu Wojskowego - Dz. U. Nr 104, poz. 709, z późn. zm.).

Pozyskiwanie danych telekomunikacyjnych w ramach czynności operacyjno - rozpoznawczych przez Policję oraz służby specjalne nie zostało poddane kontroli sądowej czy też prokuratorskiej. Należy zwrócić uwagę, że pozyskiwanie danych telekomunikacyjnych jest niewątpliwie mniej intensywną formą ingerencji w prawa i wolności obywatelskie w porównaniu z czynnościami składającymi się na kontrolę operacyjną umożliwiającą Policji oraz innym uprawnionym służbom, w wypadkach wskazanych w ustawie, daleko posuniętą inwigilację obywatela, m.in. poprzez kontrolowanie treści korespondencji, zawartości przesyłek, a także stosowanie 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. Dane telekomunikacyjne pozwalają bowiem najczęściej na ustalenie osób, które kontaktowały się z danym numerem telefonu, ewentualnie miejsc, w których określone osoby przebywały, co możliwe jest na podstawie analizy logowań telefonów komórkowych do stacji BTS. W istocie zatem czynności te nie prowadzą do pozyskiwania wiedzy o treści rozmów prowadzonych z danego aparatu telefonicznego, a pozwalają jedynie ustalić podstawowe dane o połączeniach realizowanych z danego numeru telefonu, czy też przybliżone miejsce przebywania określonej osoby dysponującej aktywnym aparatem telefonii komórkowej. Warto także zauważyć, że w dobie społeczeństwa zinformatyzowanego, gdy przepływ informacji jest niezwykle szybki i dokonywany za pomocą różnych urządzeń technicznych, możliwość pozyskiwania danych telekomunikacyjnych przez Policję czy służby specjalne wydaje się niezbędnym instrumentem z punktu widzenia zwalczania przestępczości, w tym zwłaszcza przestępczości zorganizowanej. Szybki dostęp do tego rodzaju danych w wielu wypadkach pozwala na niezwłoczne dokonanie analizy niezbędnych informacji, w celu wykrycia sprawców przestępstwa, osób współdziałających w jego popełnieniu, a także w niektórych wypadkach na ustalenie miejsca, w którym mogą znajdować się dowody popełnionego przestępstwa, czy też może znajdować się osoba pokrzywdzona przestępstwem. Bezpośredni, niezwłoczny dostęp do tego rodzaju danych w wielu wypadkach warunkuje skuteczność czynności wykrywczych w fazie przedprocesowej. Należy stwierdzić, że ustawodawca nie wprowadził procedur zapewniających kontrolę sądu lub prokuratora nad pozyskiwaniem danych telekomunikacyjnych przez Policję i inne uprawnione organy z uwagi na okoliczność, że tego rodzaju kontrola miałaby w rzeczywistości charakter ściśle formalny,

a tym samym iluzoryczny, a nadto powodowałaby nadmierne obciążenie sądów i prokuratur. Powyższy argument wiąże się z doświadczeniami wynikającymi z analizy praktyki działań sądów w zakresie udzielania zezwolenia na stosowanie kontroli operacyjnej, które skłoniły Rząd do wprowadzenia w ustawie z dnia 4 lutego 2011 r. *o zmianie ustawy - Kodeks postępowania karnego oraz niektórych innych ustaw* (Dz.U. Nr 53, poz. 273) odpowiednich regulacji w ustawach kompetencyjnych dotyczących Policji oraz służb specjalnych, obligujących sąd do merytorycznego badania materiałów uzasadniających wniosek o przeprowadzenie kontroli operacyjnej, przed podjęciem decyzji o wyrażeniu zgody na tego rodzaju kontrolę. Należy także zauważyć, że liczba wystąpień organów ścigania do przedsiębiorców telekomunikacyjnych z żądaniem udostępnienia danych uwarunkowana jest także innymi czynnikami. Znaczna liczba wystąpień Policji i służb specjalnych o dane telekomunikacyjne dotyczy prób ustalenia danych adresowych użytkowników telefonów komórkowych. Zjawisko to jest związane z powszechnym w Polsce brakiem rejestrowania się przez użytkowników kart SIM pracujących w systemie przedpłaconym (pre-paid). Należy również podkreślić, że poprzez analizę bilingów telefonicznych i logowań telefonów na poszczególnych stacjach przekaźnikowych Policja i służby specjalne nie wchodzą w materię treści prowadzonych rozmów, treści prowadzonej korespondencji oraz podglądu zachowań osób poza miejscami publicznymi. Działania te są pomocne i nieodzowne w procesie precyzyjnego typowania użytkowników stacji telefonicznych, w stosunku do których prowadzone są działania operacyjne, czego następstwem może być zastosowanie środków techniki specjalnej.

Wyrażam nadzieję, że powyższe wyjaśnienia Pan Senator uzna za wystarczające.

Z poważaniem,

Do wiadomości:

- Departament Spraw Parlamentarnych KPRM.