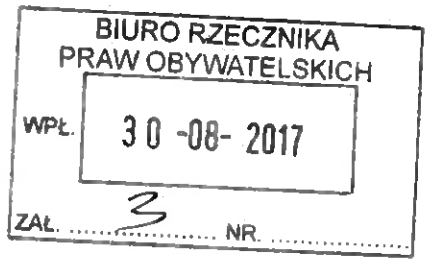
Ministerstwo Cyfryzacji
00-060 Warszawa
Królewska 27

DP-WPP.024.34.2015



Warszawa, 2017-08-30

Biuro Rzecznika Praw Obywatelskich

INFORMACJA

Dot: Państwa pisma nr Dot.: VII.520.11.2017.AG

Szanowni Państwo

W załączeniu uprzejmie przesyłam pismo skierowane do Pana Adama Bodnara - Rzecznika Praw Obywatelskich dotyczące skutków wydania przez Trybunał Sprawiedliwości Unii Europejskiej wyroku w sprawie c-203/15 i c-698/15 Tele2 Sverige i In. oraz ewentualnych działań Ministerstwa Cyfryzacji w celu uwzględnienia wyroku w polskim porządku prawnym.

Załączniki:

1. Odpowiedź na wystąpienie RPO dot. tele 2doc.(1777071_2055983).pdf

Dokument nie zawiera podpisu
Podpis elektroniczny

Warszawa, dnia 30 sierpnia 2017 r.

RZECZPOSPOLITA POLSKA
MINISTER CYFRYZACJI

Anna Streżyńska

DP-WPP.024.34.2015

Dot.: VII.520.11.2017.AG

Pan
Adam Bodnar

Rzecznik Praw Obywatelskich

Szanowny Panie Rzeczniku,

Odpowiadając na pismo zawierające prośbę o przedstawienie stanowiska Ministerstwa Cyfryzacji dotyczącego skutków wydania przez Trybunał Sprawiedliwości Unii Europejskiej wyroku w sprawie c-203/15 i c-698/15 Tele2 Sverige i In. oraz ewentualnych działań Ministerstwa Cyfryzacji w celu uwzględnienia wyroku w polskim porządku prawnym, przestawiam następujące stanowisko:

Trybunał Sprawiedliwości Unii Europejskiej w wyroku z dnia 21 grudnia 2016 r. w sprawach C-203/15 Tele 2 Sverige AB/Post-ochtelestyrelsen i C-698/15 Secretary of State for the Hone Department/Tom Watson i in. (sprawy połączone) wskazał, że nie jest zgodne z prawem UE[1] wprowadzenie przepisów w prawie państw członkowskich przewidujących uogólnione i niezróżnicowane zatrzymywanie wszystkich danych o ruchu oraz danych dotyczących lokalizacji wszystkich abonentów i zarejestrowanych użytkowników wszystkich środków łączności elektronicznej z uwagi na prewencyjny charakter zapobiegania przestępstwom. Zdaniem TSUE nie jest też zgodne z prawem UE [2] wprowadzenie w prawie krajowym państw członkowskich uregulowań dotyczących ochrony i bezpieczeństwa danych o ruchu i danych o lokalizacji, a w szczególności dostępu właściwych organów władz krajowych do przechowywanych danych, jeżeli przepisy te nie ograniczają tego dostępu jedynie do celów walki z poważną przestępczością albo nie uzależniają przyznania go od uprzedniej kontroli sprawowanej przez sąd lub niezależny organ administracyjny i nie ustanawiają wymogu, aby dane te były przechowywane na obszarze Unii.

TSUE podkreślił, że całokształt tych danych, do których zatrzymania zobowiązani są operatorzy telekomunikacyjni tj. danych o ruchu oraz danych dotyczących lokalizacji wszystkich abonentów, może dostarczyć bardzo precyzyjnych wskazówek dotyczących życia prywatnego osób, których dane są zatrzymywane, takich jak ich codzienne nawyki, miejsca stałego lub czasowego pobytu, codziennie lub okazyjnie pokonywane trasy, podejmowane

[1] Artykuł 15 ust. 1 dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej, zmieniona dyrektywą 2009/136/WE Parlamentu Europejskiego i Rady z dnia 25 listopada 2009 r., w związku z art. 7, 8, 11 i art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej.

[2] Artykuł 15 ust. 1 dyrektywy 2002/58, po zmianach wprowadzonych dyrektywą 2009/136, w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 Karty praw podstawowych.

czynności, relacje społeczne i środowiska społeczne, w których osoby te się obracają. Uregulowanie takie stanowi szczególnie daleko posuniętą ingerencję w prawa podstawowe. Okoliczność, że użytkownicy usług łączności elektronicznej nie wiedzą o tym, że dane te są zatrzymywane, może pociągnąć za sobą powstanie po ich stronie wrażenia, iż ich prywatne życie podlega ciągłej obserwacji.

Co więcej, TSUE podkreślił, że nawet jeżeli takie uregulowanie nie zezwala na zatrzymywanie treści komunikatu, a zatem nie jest w stanie naruszyć istoty tych praw to obowiązek zatrzymywania danych o ruchu i danych o lokalizacji może mieć wpływ na korzystanie ze środków łączności elektronicznej, a w konsekwencji – na korzystanie przez użytkowników owych środków z zagwarantowanej w art. 11 Karty praw podstawowych swobody wypowiedzi. Ze względu na wagę ingerencji w rozpatrywane prawa podstawowe, jaką niosą ze sobą przepisy krajowe przewidujące obowiązek zatrzymywania danych o ruchu i danych o lokalizacji do celów zwalczania przestępczości, uzasadniać taki środek może jedynie walka z poważną przestępczością.

TSUE wskazał również, że przepisy krajowe winny opierać się na obiektywnych kryteriach umożliwiających określenie okoliczności i warunków przyznania dostępu właściwym organom władz krajowych do danych abonentów lub zarejestrowanych użytkowników. W tym względzie, biorąc pod uwagę cel polegający na zwalczaniu poważnej przestępczości, dostęp ten może co do zasady zostać przyznany jedynie w odniesieniu do danych dotyczących osób podejrzewanych o planowanie, popełnianie czy też popełnienie już poważnego przestępstwa bądź też zaangażowanych w taki czy inny sposób w dane przestępstwo. Niemniej jednak w szczególnych sytuacjach, takich jak te, w których istotne interesy związane z bezpieczeństwem narodowym, obroną czy też bezpieczeństwem publicznym są zagrożone wskutek działań terrorystycznych, dostęp do danych dotyczących innych osób może zostać przyznany również wówczas, gdy istnieją obiektywne elementy pozwalające uznać, że dane te mogłyby w konkretnym przypadku rzeczywiście przyczynić się do zwalczania takich działań.

Przenosząc powyższe stanowisko TSUE na stan prawny polskiego porządku prawnego należy wskazać, że w zakresie działania Ministra Cyfryzacji, kwestia obowiązku zatrzymywania danych przez operatorów wynika z następujących przepisów ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. z 2016 r. poz. 1489 z późn. zm.):

1) art. 180a ust. 1 pkt 2, który wskazuje, że operator publicznej sieci telekomunikacyjnej oraz dostawca publicznie dostępnych usług telekomunikacyjnych są obowiązani na własny koszt zatrzymywać i przechowywać dane, o których mowa w art. 180c, generowane w sieci telekomunikacyjnej lub przez nich przetwarzane, na terytorium Rzeczypospolitej Polskiej, przez okres 12 miesięcy, licząc od dnia połączenia lub nieudanej próby połączenia, a z dniem upływu tego okresu dane te niszczyć, z wyjątkiem tych, które zostały zabezpieczone, zgodnie z przepisami odrębnymi. Dane o których mowa w art. 180c to m.in. dane niezbędne do:
    a) ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego:
        - inicjującego połączenie,
        - do którego kierowane jest połączenie;
    b) określenia:
        - daty i godziny połączenia oraz czasu jego trwania,
        - rodzaju połączenia,

- lokalizacji telekomunikacyjnego urządzenia końcowego.[3]

Zgodnie z art. 180a ust. 5 Prawa Telekomunikacyjnego obowiązkowi zatrzymania podlegają dane dotyczące połączeń zrealizowanych i nieudanych prób połączeń, o których mowa w art. 159 ust. 1 pkt 5 Prawa Telekomunikacyjnego, tj. 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. Przepis ten stanowi także, że operator publicznej sieci telekomunikacyjnej oraz dostawca publicznie dostępnych usług telekomunikacyjnych są obowiązani udostępniać ww. dane uprawnionym podmiotom, a także sądowi i prokuratorowi, na zasadach i w trybie określonych w przepisach odrębnych (art. 180a ust. 1 pkt 2 Prawa Telekomunikacyjnego). Obowiązani są oni także chronić dane, przed przypadkowym lub bezprawnym zniszczeniem, utratą lub zmianą, nieuprawnionym lub bezprawnym przechowywaniem, przetwarzaniem, dostępem lub ujawnieniem.

2) art. 180d Prawa Telekomunikacyjnego, który stanowi, że 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[4], w art. 161[5] oraz w art. 179 ust. 9[6] Prawa Telekomunikacyjnego, związanych ze świadczoną usługą telekomunikacyjną, na zasadach i przy zachowaniu procedur określonych w przepisach odrębnych.

---

[3] Zgodnie z delegacją ustawową art. 180c ust. 2 ustawy – Prawo telekomunikacyjne, zostało wydane Rozporządzenie Ministra Infrastruktury z dnia 28 grudnia 2009 r. (Dz. U. z 2009 r. Nr 226, poz.1828) w sprawie szczegółowego wykazu danych oraz rodzajów operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do ich zatrzymywania i przechowywania. Rozporządzenie określa szczegółowy wykaz danych niezbędnych do: a) ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego, inicjującego połączenie, b) ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego, do którego jest kierowane połączenie, c) określenia daty i godziny połączenia oraz czasu jego trwania, d) określenia rodzaju połączenia, e) określenia lokalizacji telekomunikacyjnego urządzenia końcowego oraz rodzaje operatorów publicznej sieci telekomunikacyjnej i dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do zatrzymywania i przechowywania ww. danych.

[4] Są to następujące dane: 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 lub w ramach usług telekomunikacyjnych 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.

[5] Przepis ten stanowi w art. 161 ust. 2 Prawa Telekomunikacyjnego, że dostawca publicznie dostępnych usług telekomunikacyjnych jest uprawniony do przetwarzania następujących danych dotyczących użytkownika będącego osobą fizyczną:
1) nazwisk i imion; 2) imion rodziców; 3) miejsca i daty urodzenia; 4) adresu miejsca zamieszkania i adresu korespondencyjnego jeżeli jest on inny niż adres miejsca zamieszkania; 5) numeru ewidencyjnego PESEL - w przypadku obywatela Rzeczypospolitej Polskiej; 6) nazwy, serii i numeru dokumentów potwierdzających tożsamość, a w przypadku cudzoziemca, który nie jest obywatelem państwa członkowskiego albo Konfederacji Szwajcarskiej - numeru paszportu lub karty pobytu; 7) zawartych w dokumentach potwierdzających możliwość wykonania zobowiązania wobec dostawcy publicznie dostępnych usług telekomunikacyjnych wynikającego z umowy o świadczenie usług telekomunikacyjnych. Oprócz ww. danych, dostawca publicznie dostępnych usług telekomunikacyjnych może, za zgodą użytkownika będącego osobą fizyczną, przetwarzać inne dane tego użytkownika w związku ze świadczoną usługą, w szczególności numer konta bankowego lub karty płatniczej, a także adres poczty elektronicznej oraz numery telefonów kontaktowych.

[6] Zgodnie z art. 179 ust. 9 Prawa Telekomunikacyjnego przedsiębiorca telekomunikacyjny świadczący publicznie dostępne usługi telekomunikacyjne jest obowiązany prowadzić elektroniczny wykaz abonentów, użytkowników lub zakończeń sieci, uwzględniając w nim dane uzyskiwane przy zawarciu umowy

Przedstawiając powyższe, należy wskazać że przepisy pozostające we właściwości Ministra Cyfryzacji ustanawiają dla operatorów publicznej sieci telekomunikacyjnej oraz dostawców publicznie dostępnych usług telekomunikacyjnych ogólny obowiązek zatrzymywania i przechowywania danych telekomunikacyjnych, celem umożliwienia dostępu do tych danych dla uprawnionych podmiotów. Przepisy ustawy – Prawo telekomunikacyjne nie regulują natomiast kwestii dostępu do tych danych, w tym zasad i procedur. Zgodnie bowiem z przytoczonymi regulacjami zasady i procedury dostępu do danych określone są w przepisach odrębnych dotyczących funkcjonowania sądów, prokuratury i uprawnionych służb. Zainicjowanie procesu zmiany przepisów odrębnych, do których odsyła Prawo telekomunikacyjne, pozostaje jednak poza zakresem właściwości Ministra Cyfryzacji. Reasumując, w ocenie Ministerstwa Cyfryzacji, obowiązujące przepisy ustawy – Prawo telekomunikacyjne regulujące problematykę retencji danych nie wymagają zmian w związku z tezami zawartych w wyroku w sprawie c-203/15 i c-698/15 Tele2 Sverige i In. Otwartą kwestią pozostaje natomiast przeprowadzenie analizy, w tym oceny, zasadności dokonania zmian w przepisach odrębnych zawierających upoważnienie do dostępu do danych telekomunikacyjnych. W tym zakresie stanowisko winien jednak zająć Minister Sprawiedliwości oraz Minister Spraw Wewnętrznych i Administracji.

Na koniec można dodać, że przed TSUE toczy się postępowanie w sprawie (C-207/16 Ministerio Fiscal). Dotyczy ono stanu faktycznego w którym sędzia prowadzący czynności przygotowawcze odmówił zgody na przekazanie przez operatorów telefonii danych (takich jak: numer IMEI, numery telefonów, które zostały uruchomione z tym kodem IMEI i dane osobowe właścicieli i użytkowników numerów telefonu odpowiadających kartom SIM uruchomionym z kodem IMEI) na wniosek Policji w dochodzeniu w związku z napaścią, argumentując m.in., że przedmiot prowadzonego dochodzenia nie dotyczy przestępstwa poważnego (w prawie hiszpańskim – zbrodni), a zatem nie uzasadnia przekazania żądanych danych. W hiszpańskim ustawodawstwie waga przestępstwa określana jest na podstawie dwojakiego kryterium: materialnego (określonego zachowaniami odpowiadającymi kwalifikacji karnej, których charakter przestępczy jest szczególny i poważny, jak np. przestępstwa popełnione w ramach organizacji przestępczej czy terroryzm) oraz kryterium formalnego, które kładzie nacisk na wysokość kary (co najmniej trzy lata pozbawienia wolności). Sąd odsyłający w omawianej sprawie zwrócił się do TSUE z dwoma pytaniami:

a) Czy można określić wystarczającą wagę przestępstwa, jako kryterium uzasadniające ingerencję w prawa podstawowe uznane w art. 7 i 8 Karty praw podstawowych Unii Europejskiej, jedynie ze względu na karę grożącą za przestępstwo będące przedmiotem dochodzenia, czy też jest ponadto konieczne wskazanie w bezprawnym zachowaniu szczególnego niekorzystnego skutku dla indywidualnych lub publicznych dóbr prawnych?
b) W danym przypadku, gdyby określenie wagi przestępstwa jedynie w zależności od kary, która może zostać nałożona, było zgodne z podstawowymi zasadami Unii zastosowanymi przez Trybunał w wyroku z dnia 8 kwietnia 2014 r. jako kryteria ścisłej kontroli dyrektywy, jaka powinna być dolna granica tej kary? Czy ta dolna granica jest zgodna z granicą ustaloną w sposób ogólny na trzy lata pozbawienia wolności?

Odpowiedź Trybunału udzielona na pytania w sprawie C-207/16 Ministerio Fiscal powinna być wzięta pod uwagę w analizie dotyczącej niezbędnych zmian przepisów

odrębnych dotyczących dostępu do zatrzymywanych i przechowywanych danych retencyjnych.

Z poważaniem

Anna Streżyńska
Minister Cyfryzacji
/-podpisano elektronicznie/