FUNDACJA
PANOPTYKON

Warszawa, 23 listopada 2016 r.

Dotyczy: sygn. akt K 9/16

OPINIA *AMICUS CURIAE*

w sprawie z wniosku Rzecznika Praw Obywatelskich z 18 lutego 2016 r., sygn. K 9/16

Fundacja Panoptykon jest organizacją pozarządową, której statutowym celem[1] jest działanie na rzecz ochrony praw człowieka w społeczeństwie nadzorowanym. Jednym z najważniejszych tematów w ponad 7-letniej działalności Fundacji jest problematyka uprawnień policji i służb specjalnych, w związku z tym Fundacja postanowiła przedstawić Wysokiemu Trybunałowi opinię *amicus curiae* w sprawie zainicjowanej wnioskiem Rzecznika Praw Obywatelskich z 18 lutego 2016 r. zarejestrowaną pod sygnaturą K 9/16.

Sprawa obejmuje złożoną i wieloaspektową problematykę prowadzenia przez Policję i inne uprawnione podmioty czynności operacyjno-rozpoznawczych, w szczególności – prowadzenia kontroli operacyjnej oraz pozyskiwania danych telekomunikacyjnych, pocztowych i internetowych.

Fundacja Panoptykon w pełni popiera wniosek przedstawiony przez Rzecznika Praw Obywatelskich. Naszym zdaniem nie jest celowe powtarzanie argumentacji przedstawionej przez RPO – jest ona szeroka i przekonująca. Pragniemy jedynie zwrócić uwagę Wysokiego Trybunału na dodatkowe okoliczności, które mogą mieć wpływ na ocenę zawisłej przed Trybunałem sprawy.

1. Charakter danych telekomunikacyjnych, pocztowych i internetowych

W świetle argumentów przedstawionych przez Rzecznika Praw Obywatelskich, a także dotychczasowego orzecznictwa Trybunału Konstytucyjnego[2], Europejskiego Trybunału Praw Człowieka[3] i Trybunału Sprawiedliwości Unii Europejskiej[4] nie budzi wątpliwości, że ochrona tajemnicy komunikacji rozciąga się na tzw. metadane, czyli dane telekomunikacyjne, pocztowe i internetowe.

---

[1] Zgodnie z § 5 Statutu Fundacji Panoptykon celem Fundacji jest m.in. działanie na rzecz ochrony praw człowieka w społeczeństwie nadzorowanym.

[2] Por. wyrok Trybunału Konstytucyjnego z 30 lipca 2014 r., sygn. akt K 23/11.

[3] Por. wyrok Europejskiego Trybunału Praw Człowieka z 2 sierpnia 1984 r. w sprawie Malone przeciwko Wielkiej Brytanii, skarga nr 8691/79.

[4] Por. wyrok Trybunału Sprawiedliwości Unii Europejskiej z 8 kwietnia 2014 r. o sygn. C-293/12.

Jak zwrócił jednak uwagę TSUE[5], „całokształt tych danych 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 czynności, relacje społeczne i środowiska społeczne, w których osoby te się obracają".

Zwracamy uwagę, że w polskim systemie prawnym ustawodawca diametralnie zróżnicował warunki dopuszczalności prowadzenia kontroli operacyjnej oraz pozyskiwania tzw. metadanych. U podłoża takiej decyzji legło przekonanie, iż ten drugi rodzaj aktywności służb w znacznie mniejszym stopniu ingeruje w konstytucyjne prawo do prywatności.

Wobec wzrostu liczby metadanych telekomunikacyjnych czy internetowych, które w ramach codziennej aktywności generują użytkownicy nowoczesnych technologii w naszej ocenie podejście to budzi wątpliwości. Suma generowanych przez użytkowników danych, w łatwy i bezpośredni sposób dostępna dla Policji i innych uprawnionych organów, może stanowić równie głęboką ingerencję w konstytucyjnie chronione prawo do prywatności, co informacje pozyskane w ramach prowadzenia kontroli operacyjnej.

Na podstawie art. 20c ust. 2 pkt 3 ustawy o Policji[6] udostępnienie danych telekomunikacyjnych, pocztowych i internetowych może odbywać się za pośrednictwem sieci telekomunikacyjnej. Możliwość zdalnego pozyskiwania danych obejmuje dane telekomunikacyjne z 12-miesięcznego okresu[7], a uprawnione podmioty mogą jednorazowo sięgnąć po wszystkie te informacje. Ustawa z 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw[8] dodatkowo umożliwiła zdalny dostęp do danych internetowych. Prowadzi to do wniosku, że Policja i inne służby mogą w sposób zdalny uzyskać jednorazowo ogromny zasób informacji o konkretnych osobach i tworzyć ich profile.

Możliwości te doskonale unaocznia przypadek Maltego Spitza - niemieckiego polityka Partii Zielonych, których na drodze sądowej uzyskał nakaz udostępnienia przez operatora telekomunikacyjnego wszystkich danych związanych z używaniem jego prywatnego telefonu komórkowego. Okazało się, że polityk otrzymał w sumie od firmy telekomunikacyjnej 35 831 informacji zgromadzonych w ciągu poprzedzających 6 miesięcy. Obok historii połączeń, czy wykazu wiadomości tekstowych znalazły się tam również dane geolokalizacyjne. Informatycy jednej z niemieckich gazet powiązali otrzymane informacje i stworzyli interaktywną mapę, dzięki której można prześledzić życie polityka[9].

Konkludując, w naszej ocenie - biorąc pod uwagę stopień ingerencji w prywatność, jaki wiąże się z udostępnieniem danych telekomunikacyjnych, pocztowych i internetowych, możliwość tworzenia zaawansowanych profili obejmujących sieć kontaktów i znajomości, zwyczajów

---

[5] Op.cit.

[6] Ustawa z 6 kwietnia 1990 r. o Policji (Dz. U. 1990 nr 30, poz. 179 ze zm.), **dalej: ustawa o Policji.** W opinii pomijamy przywoływanie przepisów innych ustaw, w których przyjęto rozwiązania analogiczne do tych zawartych w ustawie o Policji, w dalszej części opinii nazywane są one ustawami kompetencyjnymi.

[7] Na podstawie art. 168 ust. 2 oraz art. 180a ust. 1 pkt 1 ustawy z 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. 2004 nr 171 poz. 1800 ze zm.) operatorzy telekomunikacyjni przechowują dane telekomunikacyjne przez 12 miesięcy.

[8] Ustawa z 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw (Dz. U. 2016 poz. 147), **dalej: ustawa z 15 stycznia 2016 r.**

[9] Mapa dostępna jest pod adresem:http://www.zeit.de/datenschutz/malte-spitz-data-retention).

i nawyków – nie ma obecnie podstaw do zdecydowanego rozróżniania zasad dostępu do tych danych od warunków, jakim podlega możliwość prowadzenia kontroli operacyjnej.

2. „Kontrola" pozyskiwania danych telekomunikacyjnych, pocztowych i internetowych

Ustawa z 15 stycznia 2016 r. wprowadziła do ustawy o Policji oraz innych ustaw kompetencyjnych przepisy, zgodnie z którymi kontrolę nad uzyskiwaniem przez uprawnione podmioty danych telekomunikacyjnych, pocztowych lub internetowych sprawuje właściwy sąd okręgowy (por. art. 20ca ustawy o Policji). Wprowadzony model kontroli stał się przedmiotem wniosku Rzecznika Praw Obywatelskich (por. punkt 5 wniosku). RPO zwrócił uwagę, że przewidziana w ustawie o Policji kontrola nad pozyskiwaniem danych „może mieć w istocie charakter iluzoryczny i nie spełniać wymogów wynikających z Konstytucji RP, a także ze wskazanych umów międzynarodowych".

Fundacja Panoptykon podziela te zarzuty. Wprowadzony model kontroli jest niezgodny ze standardami wyznaczonymi przez Trybunał Konstytucyjny w wyroku z 30 lipca 2014 r. o sygn. akt K 23/11 oraz Trybunał Sprawiedliwości Unii Europejskiej w wyroku z 8 kwietnia 2014 r. o sygn. C-293/12. TK sformułował bowiem dwie wytyczne dotyczące kształtu kontroli nad sięganiem po dane. Po pierwsze, sposób kontroli może być uzależniony od charakteru danych telekomunikacyjnych oraz od charakteru działalności uprawnionego podmiotu. Po drugie, kontrola uprzednia nad sięganiem po dane powinna dotyczyć osób wykonujących zawody zaufania publicznego oraz sytuacji, w których nie ma konieczności pilnego działania. Trybunał w Luksemburgu wskazał zaś wprost, że uzyskanie dostępu do danych powinno podlegać uprzedniej kontroli sądu lub niezależnego organu administracyjnego. Jednak oba orzeczenia **w żadnym wypadku nie dopuszczają, by kontrola ta miała charakter zbiorczy, fakultatywny i wybiórczy.**

W związku z upłynięciem 6 miesięcy od wejścia w życie ustawy z 15 stycznia 2016 r. wprowadzającej kwestionowany model kontroli nad sięganiem po dane, Fundacja Panoptykon skierowała do wszystkich komend wojewódzkich Policji, a także Szefów Agencji Bezpieczeństwa Wewnętrznego i Centralnego Biura Antykorupcyjnego oraz Komendanta Głównego Straży Granicznej wnioski o udostępnienie informacji publicznej, w których prosiliśmy o udostępnienie pierwszych 6-miesięcznych sprawozdań, o których mowa w art. 20ca ustawy o Policji i analogicznych przepisach dotyczących pozostałych podmiotów. Większość zapytanych podmiotów wydało w sprawie wniosków decyzje odmowne opierając się na ustawie o ochronie informacji niejawnych[10]. Na tym tle wyróżnia się jednak Komenda Wojewódzka Policji w Białymstoku, która udostępniła nam przedłożone do sądu sprawozdanie (por. załącznik).

Analiza przedłożonych sprawozdań prowadzi do wniosku, że wyłącznie na ich podstawie **niemożliwa jest weryfikacja, czy konkretne pozyskanie danych telekomunikacyjnych, pocztowych czy internetowych było zasadne**. Sąd sprawujący kontrolę nad pozyskiwaniem danych otrzymuje bowiem jedynie informacje o: numerze sprawy, jednostce w ramach wewnętrznej struktury Policji, podstawę prawną pozyskania danych, kwalifikację prawną czynu, w związku z którym pobrano dane, a także liczbę pobranych danych w konkretnej sprawie (z podziałem na rodzaje danych).

Należy zwrócić uwagę, że przewidziana w art. 20ca ustawy o Policji kontrola ma charakter fakultatywny. Co więcej, zgodnie z ust. 3 w ramach kontroli sąd może zapoznać się jedynie

[10] Ustawa z 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. 2010 nr 182 poz. 1228).

z materiałami **uzasadniającymi** udostępnienie Policji danych. Rodzi to wątpliwości analogiczne do tych, które Rzecznik Praw Obywatelskich wyraził w swoim wniosku do Trybunału Konstytucyjnego z 4 grudnia 2015 r. (sygn. akt K 41/15), w którym zakwestionował zgodność z Konstytucją art. 19 ust. 1a ustawy o Policji oraz analogicznych przepisów ustaw kompetencyjnych, zgodnie z którymi wniosek do sądu o zarządzenie kontroli operacyjnej przedstawia się wraz z materiałami **uzasadniającymi** potrzebę zastosowania kontroli operacyjnej. Jak zwrócił uwagę w swoim wniosku RPO, takie brzmienie przepisów powoduje, że „sąd wydaje postanowienie wyłącznie na podstawie materiału selektywnie wybranego i przekazanego sądowi przez organ wnioskujący o zastosowanie kontroli operacyjnej, albowiem nie ma on obowiązku załączać do wniosku całości materiałów zgromadzonych w sprawie". Jak wskazuje przywołany we wniosku Rzecznika, M. Tomkiewicz[11] „taki stan rzeczy trudno uznać za optymalny z punktu widzenia standardów demokratycznych państwa prawa (...) Rozwiązania istniejące w aktualnym stanie prawnym wyraźnie legitymizują przewagę informacyjną służb operacyjnych nad sądem, który ową działalność wymienionych służb w zakresie podsłuchów ma weryfikować". Powyższe rozważania należy w całości rozciągnąć na model kontroli nad uzyskiwaniem danych telekomunikacyjnych, pocztowych i internetowych.

Podsumowując, w naszej ocenie kontrola nad pozyskiwaniem danych telekomunikacyjnych, pocztowych i internetowych, o której mowa w art. 20ca ustawy o Policji, ma charakter iluzoryczny. Załączone do niniejszej opinii sprawozdania złożone właściwym sądom przez Komendę Wojewódzką Policji w Białymstoku oraz Komendę Stołeczną Policji potwierdzają tę tezę, bowiem na ich podstawie nie jest możliwa rzetelna weryfikacja zasadności pobierania poszczególnych danych. W przypadku, gdy sąd skorzysta ze swojej możliwości zapoznania się z materiałami (por. art. 20ca ust. 3 ustawy o Policja), taka ewentualna kontrola będzie miała wybiórczy charakter, a jej podstawą będą wyłącznie „jednostronne" materiały - uzasadniające pobranie danych.

***

Mamy nadzieję, że powyższa opinia pomoże Wysokiemu Trybunałowi na wszechstronne i kompleksowe wyjaśnienie sprawy zainicjowanej wnioskiem Rzecznika Praw Obywatelskich.

Małgorzata Szumańska

Wiceprezeska

Załączniki:

1. Sprawozdanie Komendy Wojewódzkiej Policji w Białymstoku.

[11] M. Tomkiewicz, Podsłuchy operacyjne w orzecznictwie sądowym, Prokuratura i Prawo 2015, nr 4, s. 157.