FUNDACJA PANOPTYKON

Warszawa, 12 stycznia 2016 r.

DOSTĘP POLICJI I SŁUŻB SPECJALNYCH DO DANYCH TELEKOMUNIKACYJNYCH I INTERNETOWYCH – obecna sytuacja, standard praw człowieka, aktualne propozycje – wnioski[1]

1. Wstęp – najważniejsze pojęcia

Dane telekomunikacyjne, to dane, o których mowa w art. 180c ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (dalej: **PT**). Są to:

- tzw. dane abonenckie – np. imię i nazwisko i adres abonenta (por. art. 180c ust. 1 pkt 1 PT);
- billingi (data i godzina połączenia, czas jego trwania – por. art. 180c ust. 1 pkt 2 lit. a PT);
- lokalizacja telefonu komórkowego (por. art. 180c ust. 1 pkt 2 lit. c PT);
- inne dane, np. numer IP (por art. 180c ust. 1 i 2 PT).

Dane internetowe, to dane, o których mowa w art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (dalej: **uśude**). Są to m.in. informacje niezbędne do świadczenia usługi drogą elektroniczną (jak adres do doręczenia przesyłki zamówionej przez Internet – por. art. 18 ust. 1) oraz dane „charakteryzujące sposób korzystania przez usługobiorcę z usługi świadczonej drogą elektroniczną (dane eksploatacyjne), m.in. informacje o rozpoczęciu, zakończeniu oraz zakresie każdorazowego korzystania z usługi (por. art. 18 ust. 5 uśude). Pojęcie danych internetowych jest nieprecyzyjne: obejmuje m.in. numer IP, spersonalizowane informacje o systemie operacyjnym czy przeglądarce internetowej. Według niektórych (por. opinia prawna Helsińskiej Fundacji Praw Człowieka[2]) obejmują one również treść korespondencji mailowej.

Podmioty posiadające dostęp do danych telekomunikacyjnych i danych internetowych to: Policja, Straż Graniczna, Agencja Bezpieczeństwa Wewnętrznego, Centralne Biuro Antykorupcyjne, Żandarmeria Wojskowa, Służba Kontrwywiadu Wojskowego, kontrola skarbowa, służba celna (dalej: **podmioty uprawnione**).

2. Obowiązujące zasady dostępu uprawnionych podmiotów do danych telekomunikacyjnych i internetowych

a. Dostęp do danych telekomunikacyjnych

Polska wdrożyła tzw. dyrektywę retencyjną (dyrektywa 2006/24/WE) przyznając podmiotom uprawnionym dostęp do danych telekomunikacyjnych na następujących zasadach:

- dostęp do danych możliwy jest w sprawach wszystkich przestępstw będących we właściwości danej służby (por. art. 20c ust. 1 ustawy o policji), a także w celu prowadzenia działalności analitycznej (por. art. 18 ust. 1 pkt 1 ustawy o CBA);

[1] Opinia przygotowana przez Wojciecha Klickiego.
[2] http://www.hfhr.pl/uwagi-hfpc-do-projektu-zmian-w-uprawnieniach-sluzb/

- dostęp do danych nie jest poddany jakiejkolwiek zewnętrznej kontroli: sądu lub niezależnego organu;
- nie wprowadzono mechanizmów gwarantujących uzyskanie informacji na temat pobrania danych telekomunikacyjnych przez osobę, której to dotyczy;
- dostęp do danych odbywa się za pośrednictwem sieci telekomunikacyjnej, bez udziału pracownika firmy telekomunikacyjnej (por. art. 20c ust. 2a ustawy o policji)

Ze składanych co roku do Komisji Europejskiej raportów przygotowywanych przez Urząd Komunikacji Elektronicznej wynika, że uprawnione podmioty kierują do operatorów telekomunikacyjnych ok. 2 mln zapytań rocznie.

b. Dostęp do danych internetowych

- uprawnione podmioty mają dostęp do danych internetowych „na potrzeby prowadzonych postępowań" (por. art. 18 ust. 6 uśude);
- brak jakiejkolwiek zewnętrznej kontroli nad sięganiem przez uprawnione podmioty po dane internetowe;
- z badań przeprowadzonych przez Fundację Panoptykon[3] wynika, że dostęp do danych jest realizowany w formie pisemnych wniosków kierowanych do firm świadczących usługi drogą elektroniczną
- nieznana jest ogólna liczba zapytań uprawnionych podmiotów o dane internetowe. Z przywołanych badań wynika, że Agencja Bezpieczeństwa Wewnętrznego w 2012 r. ABW zwróciła się do firm z 692 pytaniami (dla porównania w tym samym roku ABW zadała operatorom telekomunikacyjnym 115 652 pytań)

3. Jakie wytyczne w tym obszarze wynikają z orzecznictwa

W wyroku z 30 lipca 2014 r. (sygn. K 23/11) Trybunał Konstytucyjny uznał, że przepisy na podstawie których uprawnione podmioty uzyskują dostęp do danych telekomunikacyjnych są niezgodne z Konstytucją „przez to, że nie przewidują niezależnej kontroli udostępniania danych telekomunikacyjnych". Trybunał uznał też za niezgodne z konstytucją przepisy ustaw o ABW, SKW i CBA ze względu na brak obowiązku niszczenia danych niemających znaczenia dla prowadzonego postępowania. Wyrok Trybunału wchodzi w życie po 18 miesiącach od orzeczenia, a więc 6 lutego 2016 r. Tego dnia przestaną obowiązywać przepisy uprawniające do sięgania po dane telekomunikacyjne. Trybunał wskazał, że konieczne jest wprowadzenie kontroli sądu lub innego niezależnego organu nad sięganiem po dane. Kontrola powinna mieć charakter uprzedni, choć Trybunał dopuszcza wyjątki w tym zakresie.

Natomiast 8 kwietnia 2014 r. Trybunał Sprawiedliwości UE stwierdził (połączone sprawy C-293/12 i C-594/12) nieważność tzw. dyrektywy retencyjnej (dyrektywa 2006/24/WE) ze względu na jej niezgodność z art. 7 i 8 Karty praw podstawowych. TSUE wskazał, że dla zgodności z prawem UE niezbędne jest:

- ograniczenie dostępu do danych telekomunikacyjnych wyłącznie do spraw „poważnych przestępstw";

[3] Raport Access of public authorities to the data of Internet service users dostępny w wersji ang. pod adresem: https://panoptykon.org/sites/default/files/publikacje/transparency_report_pl_1.pdf)

- wprowadzenie każdorazowej, uprzedniej zgody sądu na sięgnięcie po dane telekomunikacyjne;
- wprowadzenie mechanizmu informowania jednostki, że jej dane telekomunikacyjne były pobierane (następczo, z możliwymi wyjątkami).

4. Jakie zmiany wprowadza projekt

Najważniejsze zmiany, jakie wprowadza projekt, to:

- zrównanie zasad pozyskiwania danych telekomunikacyjnych i internetowych: będzie to możliwe w celu „wykrywania, pozyskiwania, ścigania i wykrywania przestępstw" (por. projektowany art. 20c ustawy o policji), a w niektórych wypadkach także w celu prowadzenia działań analitycznych (por. projektowany art. 18 ust. 1 pkt 1 ustawy o CBA);
- wprowadzenie możliwości pozyskiwania danych internetowych za pośrednictwem sieci teleinformatycznych;
- wprowadzenie kontroli nad pozyskiwaniem danych telekomunikacyjnych i internetowych (por. projektowany art. 20c ustawy o policji). Ma ona polegać na: składaniu co 6 miesięcy przez uprawnione podmioty sprawozdania do sądu mówiącego o łącznej liczbie zapytań. Sąd będzie mógł (nie jest to obowiązkowe) wyrywkowo weryfikować zapytania. Dane, o których sąd stwierdził, że zostały pobrane niezgodnie z prawem, nie będą musiały być usuwane.
- projekt nałożył obowiązek weryfikacji, czy pobrane dane są niezbędne dla dalszego postępowania – zbędne dane mają być usuwane.

5. Ocena – najważniejsze problemy

Projekt jest niezgodny z Konstytucją RP i prawem Unii Europejskiej – zagwarantowaną w Karcie praw podstawowych ochroną danych osobowych i prywatności[4]. Nie realizuje podstawowego wymogu wynikającego z przytoczonych wyroków Trybunału Konstytucyjnego i Trybunału Sprawiedliwości, nie wprowadza bowiem niezależnej zewnętrznej kontroli nad sięganiem po dane telekomunikacyjne. Proponowana kontrola ma fikcyjny charakter:

- będzie sprawowana po pobraniu danych, a nie wcześniej;
- ma charakter fakultatywny: przy jednoczesnym braku dodatkowych etatów w sądach, sędziowie nie będą podejmowali tego dodatkowego zadania;
- skutkiem ewentualnej kontroli nie jest zniszczenie danych.

Projekt poszerza i ułatwia możliwości uzyskiwania danych internetowych: wcześniej było to możliwe wyłącznie w ramach prowadzonych postępowań, zgodnie z projektem będzie możliwe w celu „wykrywania, pozyskiwania, ścigania i wykrywania przestępstw". Jednocześnie projekt umożliwia pobieranie danych telekomunikacyjnych za pomocą sieci telekomunikacyjnej (tzw. bezpiecznego łącza). Wiąże się to z ryzykiem radykalnego wzrostu liczby zapytań o dane internetowe. Ze względu na podobny stopień ingerencji w prywatność, dostęp do danych internetowych powinien być kontrolowany w podobny sposób, jak do danych telekomunikacyjnych.

[4] Por. opinię Biura Analiz Sejmowych na temat projektu (w jęz. Polskim): http://sejm.gov.pl/Sejm8.nsf/druk.xsp?documentId=B30BB05699C73CE8C1257F310040516D

Projekt nie rozwiązuje też problemu niszczenia danych telekomunikacyjnych oraz internetowych: brak cyklicznej weryfikacji, czy dane wciąż są potrzebne pozwala na bezterminowe przechowywanie informacji o obywatelach.