

Służby wiedzą, ale nie powiedzą

17 sierpnia 2012

Każdy zastanawia się czasem, kto oglądał nasz profil na Facebooku albo szukał o nas informacji w wyszukiwarce. My postanowiliśmy sprawdzić, czy informacji na nasz temat szukała... policja i inne służby. A konkretniej, czy – policja, ABW, CBA i Straż Graniczna sięgały po nasze billingi. Wszystkie służby, choć z rozmaitych powodów, odmówiły nam tej wiedzy.

O retencji danych i zasadach, na jakich policja i służby mają do nich dostęp, pisaliśmy już na naszej stronie bardzo dużo. Obowiązkowe zatrzymywanie i przechowywanie tzw. danych transmisyjnych (telekomunikacyjnych), czyli danych o szczegółach wszystkich rodzajów połączeń telekomunikacyjnych jest bardzo poważnym zagrożeniem dla prywatności każdego użytkownika telefonów komórkowych i internetu. Polskie przepisy nie tylko nakładają na wszystkich operatorów obowiązek przechowywania danych przez 2 lata, ale też pozwalają aż 9 podmiotom – policji i innym służbom – sięgać po nie niemal bez żadnych ograniczeń.

Postanowiliśmy sprawdzić w praktyce, na własnym przykładzie, jedną szczegółową kwestię związaną z retencją – możliwość zdobycia informacji o tym, że było się przedmiotem zainteresowania służb. W zeszłym roku prokuratury, sądy, policja i inne służby sięgały po dane transmisyjne obywateli niemal 2 mln razy, statystycznie nie byliśmy więc bez szans!

SKĄD TEN POMYSŁ?

Z Konstytucji RP. Zgodnie z jej art. 51 ust. 3 każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. To uprawnienie, będące elementem tzw. autonomii informacyjnej jednostki, nawiązuje bezpośrednio do prawa do

prywatności z art. 47 Konstytucji i je rozwija. Skoro każdy z nas jest wyłącznym dysponentem informacji na swój temat, musi mieć też możliwość dostępu do swoich danych zebranych przez inne podmioty. Realizację tego ogólnego uprawnienia (nazwijmy je konstytucyjnym prawem dostępu) przewiduje m.in. Rozdział 4 ustawy o ochronie danych osobowych („Prawa osoby, której dane dotyczą”).

Powołując się na to konstytucyjne prawo, wszyscy członkowie zespołu Fundacji Panoptikon złożyli do policji, Straży Granicznej, Agencji Bezpieczeństwa Wewnętrznego i Centralnego Biura Antykorupcyjnego wnioski, w których domagali się poinformowania:

„1. Czy służba pozyskiwała, pozyskuje lub w inny sposób przetwarza dane telekomunikacyjne dotyczące mojej osoby, o których mowa w art. 180c ustawy – Prawo telekomunikacyjne;

2. O treści przetwarzanych na mój temat danych telekomunikacyjnych;

3. O celu i sposobie ich przetwarzania.”

Jednocześnie domagaliśmy się zaprzestania przetwarzania i usunięcia wszystkich danych telekomunikacyjnych, które na nasz temat posiada dana służba.

NIE POWIEMY, CZY COŚ WIEMY

Każda z wywołanych do tablicy służb odmówiła realizacji naszego wniosku, co niestety nie było też dla nas specjalnym zaskoczeniem. Przypuszczaliśmy, że służby odmówią nam informacji powołując się na odpowiednie przepisy kompetencyjne, które pozwalają im przetwarzać dane obywateli w sposób niejawny, bez wiedzy i zgody zainteresowanych. Zaskoczyło nas więc to, że każda ze służb inaczej uzasadniła swoją odmowę. W każdej odpowiedzi można też dostrzec pewne nieścisłości.

Centralne Biuro Antykorupcyjne uznało, że informacja na temat sięgania przez Biuro po nasze dane telekomunikacyjne stanowi informację niejawną, nie podlegającą udostępnieniu na wniosek osoby zainteresowanej. Tak się składa, że definicję informacji niejawnej zawiera... ustawa o ochronie informacji niejawnych. Są nimi tylko te informacje, którym nadano – ze szczególnych względów – odpowiednią klauzulę („ściśle tajne” lub „tajne”). Prawo nie przewiduje jednak nadawania takich klauzul danym telekomunikacyjnym.

Według Straży Granicznej (ten argument przytoczyło również CBA) dane, po które potencjalnie mogła sięgnąć Straż „nie tworzą zbioru danych, o których mowa w przepisie art. 32 ustawy o ochronie danych osobowych z 29 sierpnia 1997 r.” (przepis, na który powoływaliśmy się w naszych wnioskach). Gwoli wyjaśnienia: faktycznie, sformułowane w art. 32 uprawnienie dotyczy jedynie danych przetwarzanych w zbiorach. Jednak podstawą prawną naszych wniosków był nie tylko art. 32 ustawy o ochronie danych osobowych, ale również Konstytucja RP, która prawo dostępu definiuje szerzej, nie ograniczając go do informacji przetwarzanych w zbiorach danych.

Zgodnie z odpowiedzią z Agencji Bezpieczeństwa Wewnętrznego „nie jest możliwe udzielenie przez ABW żądanych przez Pana informacji w trybie wskazanym we wniosku”. Być może w jakimś innym jest? W każdym razie, zdaniem ABW, uprawnienie wskazane w art. 32 ustawy „nie dotyczy ustawowo przewidzianych przypadków przetwarzania danych osobowych uzyskiwanych bez wiedzy i zgody osoby, której dane te dotyczą, co przewiduje wprost art. 25 ust. 2 pkt 1 ustawy o ochronie danych osobowych”. Nieścisłość odpowiedzi polega na tym, że art. 25 ustawy dotyczy podobnej, lecz innej sytuacji, niż opisana w naszym wniosku. Zgodnie z tym przepisem, sam podmiot zbierający dane ma obowiązek poinformować o tym osobę, której one dotyczą. Wyjątkowo może tego nie zrobić, jeśli przepisy dopuszczają zbieranie danych osobowych bez wiedzy osoby, której one dotyczą. Zgadza się z ABW, że art. 25 wyłącza

obowiązek aktywnego informowania nas przez służbę o zbieraniu danych na nasz temat. To byłoby już nieco za dużo. Jednak absolutnie nie widzimy w tym przepisie podstaw do nieuwzględnienia naszych wniosków.

Wreszcie policja. W odpowiedzi od Komendy Głównej Policji czytamy, że Policja pozyskane dane albo przekazuje niezwłocznie prokuratorowi albo niezwłocznie niszczy. W związku z tym „czas przetwarzania udostępnionych danych telekomunikacyjnych jest wyjątkowo krótki i ogranicza się do czasu liczonego od momentu udostępnienia ich do chwili przekazania tych danych do prokuratury bądź też ich zniszczeniu”. Wynika z tego, że policja, owszem, przetwarza dane ale też niezwłocznie je niszczy. Każdy prawnik wie, że „niezwłocznie” oznacza jedynie „bez zbędnej zwłoki”, czyli... nie ma określonego terminu, w którym ma się to stać.

CO Z TEGO WYNIKA?

Żeby nie było wątpliwości: od początku przypuszczaliśmy, że nie otrzymamy informacji, o które prosiliśmy we wnioskach. Mimo to postanowiliśmy podjąć próbę „odzyskania swoich danych” i sprawdzić, jakie odpowiedzi otrzymamy od policji i służb. Dzięki tej próbie wiemy o wiele więcej i z pełną odpowiedzialnością możemy wskazać konkretny problem. Obowiązujące przepisy faktycznie uniemożliwiają zdobycie informacji, czy było się przedmiotem inwigilacji. Tymczasem zdarza się, że dochodzi do bezprawnego i nielegalnego sięgania przez służby specjalne po dane telekomunikacyjne. Narusza to dobra osobiste i prywatność osoby inwigilowanej. Potwierdził to niedawny wyrok warszawskiego Sądu Okręgowego, w którym sąd uznał, że „billingowanie” dziennikarza Bogdana Wróblewskiego przez CBA naruszyło jego dobra osobiste. Być może służby naruszyły i naruszają dobra osobiste wielu z nas. Wróblewski dowiedział się o działaniu CBA względem siebie przez przypadek, ponieważ prawo nie przewiduje obowiązku informowania o działaniach służb. Naszym zdaniem to błąd. Oczywiście nie postulujemy, by taki obowiązek istniał w każdym

przypadku: trzeba znaleźć odpowiedni kompromis i precyzyjnie wskazać, kiedy służby mają prawo nie informować o dokonywanych sprawdzaniach. Jednak zasadą powinno być informowanie obywateli – oczywiście post factum – o tym, że byli przedmiotem zainteresowania służb a ich dane telekomunikacyjne były pobierane od operatorów.

Autor: Wojciech Klicki

Źródło: [Fundacja Panoptikon](#)