

# W interesie naszego bezpieczeństwa

22 kwietnia 2014

9 kwietnia prokurator generalny przedstawił w Senacie sprawozdanie, w którym znalazły się informacje o skali inwigilacji prowadzonej przez państwo w zeszłym roku. Niestety dane te nie pokazują pełnego rozmiaru zjawiska, gdyż najprawdopodobniej dotyczą jedynie tych sposobów inwigilacji, których użycie wymaga zgody sądu. Policja nie chce bowiem udzielać informacji odnośnie tego, co dokładnie zawiera statystyka podawana do publicznej wiadomości. Z pewnością jednak obejmuje ona zaledwie ułamek działań inwigilacyjnych prowadzonych przez służby, co pokazuje choćby niedawny raport przygotowany przez Fundację Panoptikon, zajmującą się monitorowaniem ingerencji państwa w życie obywateli.

Nie wiadomo więc czy dane te obejmują np. śledzenie za pomocą ukrytego nadajnika GPS lub przeglądanie zawartości komputera, które (w odróżnieniu od czytania maili) nie wymaga zgody sądu. Z całą pewnością nie uwzględniono tu natomiast kontrolowania historii wszystkich telefonicznych połączeń wychodzących i przychodzących (tzw. bilingi), o których za chwilę.

Zgodnie z danymi, które znalazły się w sprawozdaniu, tylko liczba podsłuchów wzrosła o 300 w porównaniu z rokiem 2012. Prym w tym zakresie wiedzie oczywiście policja (wzrost o 7%), która jest zresztą odpowiedzialna za 82% wszystkich przeprowadzanych tzw. kontroli operacyjnych. Należy jednak pamiętać, że liczby te dotyczą jedynie osób, wobec których zastosowano inwigilacje, a nie ilości złożonych wniosków, których mogło być nawet 40% więcej[1].

Jak donosi Gazeta Wyborcza w artykule Podsłuchowe wzmoczenie, w tym roku policja nie chciała też podzielić się z dziennikarzami i organizacjami pozarządowymi informacjami o

liczbie kontroli, które trwały dłużej niż 3 miesiące (czyli okres przewidziany ustawowo) i „niecierpiącymi zwłoki”, czyli takimi, które rozpoczęto bez otrzymania zgody sądu, ubiegając się o nią w późniejszym czasie.

Co zaś tyczy się ABW i CBA, zwiększyły one zakres kontroli operacyjnej o odpowiednio 35 i 12%. Pierwsza z tych agencji przeprowadziła ponadto dwa razy więcej kontroli w trybie bezzwłocznym. W przypadku CBA była to liczba znacznie mniejsza niż w 2012 roku, co jest związane z przekształcaniem biura w służbę analityczną (pozbawioną kompetencji śledczych). Należy zresztą podkreślić, że zarówno ABW jak i CBA otwarcie przyznają, że zdecydowana większość prowadzonej przez nich inwigilacji ma charakter profilaktyczny; służy więc zbieraniu danych o osobach, wobec których nie wysunięto żadnych oskarżeń i których nie podejrzewa się o bezpośredni udział w przestępstwie.

Tego rodzaju rozszerzanie pola inwigilacji, które coraz częściej jest zwykłym nadużyciem ze strony policji i innych służb, opisuje wspomniana Fundacja Panoptikon. Jej zdaniem w/w nawet w błahych sprawach sięgają po tzw. metadane czyli informacje pochodzące z retencji danych telekomunikacyjnych, która oznacza przechowywanie przez pewien czas (w przypadku Polski jest to 12 miesięcy) danych z naszych telefonów.

Są to informacje dotyczące tego, gdzie się znajdujemy obecnie i gdzie byliśmy wcześniej oraz z kim i kiedy się kontaktowaliśmy, a także z jakich urządzeń korzystamy.

Poza tym, operator telekomunikacyjny zachowuje przez rok nasze billingi, czyli historię połączeń i wiadomości SMS, które odebraliśmy oraz sami wykonaliśmy. Do tego dochodzą też dane abonenckie obejmujące wszystko to, co podaliśmy operatorowi podczas podpisywania umowy, a także numer naszego telefonu i aparatu, którym się posługujemy oraz numer karty SIM (stały i tymczasowy). Wystarczy, że telefon jest zalogowany do sieci, czyli po prostu włączony, a wszystkie powyższe informacje

zapisują się w bazie danych.

Powyższe elementy składają się na całość, za pomocą której bez problemu można stworzyć profil osobowości i ustalić takie szczegóły, jak nasze codzienne zwyczaje czy relacje intymne i biznesowe. Taka perspektywa musi być więc wielce kusząca dla organów ścigania – zwłaszcza, że nie wymaga od nich żadnego wysiłku, nakładów finansowych ani niczyjej zgody. Najczęściej nie wiąże się też z jakimikolwiek konsekwencjami dla mundurowego, który nadużywa dostępu do tych niestety łatwo dostępnych informacji. Dlaczego tak się dzieje?

Po pierwsze, wszystkie koszty związane z przechowywaniem naszych danych i obsługą pytań ze strony policji, która chce uzyskać informacje na temat jakiejś osoby, ponoszą operatorzy telefonii komórkowej. Koszty te, jak nietrudno się domyślić, operator przerzuca na swoich klientów. Oznacza to, że to wyłącznie my płacimy (dosłownie i w przenośni) za przekazywanie policji naszych danych – opłacamy de facto własną inwigilację.

Kolejną kwestią budzącą sprzeciw jest sposób, w jaki służby uzyskują interesujące ich szczegóły z naszej aktywności telekomunikacyjnej. Są trzy drogi pozyskania informacji. Jedną z nich jest wystosowanie do operatora pisemnego wniosku komendanta głównego policji, drugą zaś ustne żądanie funkcjonariusza posiadającego odpowiednie uprawnienia. Zarówno jedna, jak i druga metoda wymagają sporo biurokracji i czasu, przez co nie cieszą się zbytnią popularnością. Zupełnie inaczej jest natomiast w przypadku rozwiązania nr 3, z którego policja korzysta zdecydowanie najchętniej. Polega ono mianowicie na wykorzystaniu specjalnego interfejsu, czyli zabezpieczonego połączenia internetowego między policją a danym operatorem. Za jego pomocą pobierane są dane z baz telekomunikacyjnych wprost do policyjnego komputera. Podczas tej operacji udział operatora jest zbędny, tak samo jak jego wiedza o jej przeprowadzeniu. Co więcej, najczęściej systemy informatyczne są zbudowane w taki sposób, że w bazie danych

nie zostaje jakikolwiek ślad po policyjnej ingerencji z zewnątrz.

W praktyce wygląda to więc tak, że któryś z 500 uprawnionych do tego policjantów siada przed monitorem i za pomocą kilku uderzeń w klawiaturę ściąga wrażliwe dane dowolnej osoby niczym kolejny odcinek popularnego serialu. Szybko, sprawnie i wygodnie, z tą tylko różnicą, że nasza aktywność w sieci jest monitorowana (inwigilowanie użytkowników Internetu to temat na osobny tekst), a działania policji nie pozostawiają za sobą śladów i najczęściej nie wiążą się z jakimikolwiek konsekwencjami. Co więcej, jeśli „trzeba” wszystko odbywa się poza czyjąkolwiek wiedzą.

Zastanawiające jest również to, że nie istnieje żadne rzetelne źródło pokazujące skalę inwigilacji społeczeństwa przez policję i inne służby. Choćby przybliżonego rozmiaru tego zjawiska nie jest w stanie przedstawić nawet Najwyższa Izba Kontroli. Urząd Komunikacji Elektronicznej podaje, że w 2009 roku ze strony samej tylko policji było milion zapytań skierowanych do operatorów, w roku następnym ponad 1,3 mln, w kolejnym 1,87 mln, a w roku 2012 – 1,72 mln. Dane te nie pokrywają się jednak z informacjami przekazanymi Fundacji Panoptikon przez samą policję, według której liczba zapytań była większa. W 2011 roku miało ich być 1,92 mln, a w 2012 roku już 2,13 mln. Warto przy tym zauważyć, że w przywołanym okresie nie zwiększyła się liczba przestępstw popełnianych w Polsce, nie wzrósł też poziom ich wykrywalności – ale skala inwigilacji już tak.

Każdy z nas musi więc pamiętać, że telefon to kieszonkowa baza informacji na nasz temat. Baza, z której państwo może korzystać (i z pewnością korzysta) w dogodny dla siebie sposób. Wszystko to, co dzieje się z naszym telefonem i co przez niego przechodzi jest gromadzone oraz przechowywane przez operatora sieci. Może być analizowane nie tylko przez policję, ale też przez prokuraturę, sąd, CBA, ABW, Straż Graniczną, Żandarmerię Wojskową, Służbę Kontrwywiadu

Wojskowego, kontrolę skarbową i Służbę Celną. Wszystkie te podmioty posiadają bowiem właściwie niczym nieograniczony dostęp do naszych danych. To, czy jesteśmy podejrzewani o popełnienie przestępstwa czy nie, nie ma tu żadnego znaczenia. Stajemy się po prostu bezwiednym elementem tzw. działań prewencyjnych służb, które bez przerwy zasłaniają się potrzebą gromadzenia informacji „w interesie naszego bezpieczeństwa”. W rzeczywistości jest to jednak pole do nadużyć, narzędzie umożliwiające śledzenie niemal każdego człowieka i wymówka np. dla policji, która nic sobie nie robi z przysłowiowego zaglądania ludziom pod kołdrę.

Elektroniczne wersje przewodników Fundacji Panoptikon, dotyczące inwigilacji telefonicznej, internetowej i ulicznej dostępne są [TUTAJ](#).

Źródła: [ack.most.org.pl](http://ack.most.org.pl), [Grecja w Ogniu](#)

## **PRZYPIS**

[1] Dane te nie zostały podane do wiadomości publicznej ale na taką właśnie liczbę wskazuje porównanie z rokiem 2012, kiedy to złożono 5995 wniosków, a inwigilowano 4351 osób.

## **BIBLIOGRAFIA**

1. Ewa Siedlecka, „Podsłuchowe wzmożenie”, Gazeta Wyborcza, wydanie z dnia 10/04/2014, nr 84, s. 4.
2. Przewodnik Fundacji Panoptikon „Telefoniczna kopalnia informacji”.