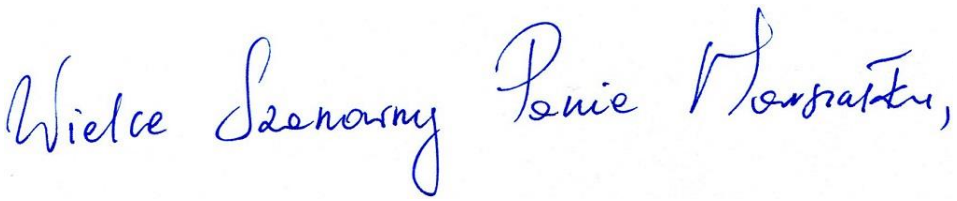
FUNDACJA PANOPTYKON

Warszawa, 15 stycznia 2014 r.

Szanowny Pan
Bogdan Borusewicz
Marszałek Senatu Rzeczpospolitej Polskiej



Fundacja Panoptykon jest organizacją pozarządową, której celem statutowym jest działanie na rzecz **ochrony praw człowieka w społeczeństwie nadzorowanym**. W swojej działalności diagnozujemy zagrożenia związane z nadzorem i wypracowujemy alternatywne rozwiązania systemowe. Jednym z ważniejszych tematów w naszej działalności jest dostęp Policji i innych służb do danych obywateli, w tym danych telekomunikacyjnych. Od kilku lat zwracamy uwagę na niezbędne zmiany prawne, które ograniczą dowolność w sięganiu po informacje o użytkownikach telefonów komórkowych przez służby.

Problem nadużywania dostępu do tzw. billingów zauważyła także Najwyższa Izba Kontroli, która w październiku 2013 r. opublikowała raport ze swojej kontroli. W raporcie NIK wskazała na negatywne konsekwencje dla prywatności obywateli, wynikające z wadliwej regulacji prawnej. Wcześniej problem ten dostrzegli również: Rzecznik Praw Obywatelskich, Generalny Inspektor Ochrony Danych Osobowych i Naczelna Rada Adwokacka.

Niestety, pomimo wielokrotnych zapowiedzi, Ministerstwo Spraw Wewnętrznych nie przygotowało propozycji kompleksowej reformy zasad dostępu Policji i innych służb do danych telekomunikacyjnych. Z informacji prasowych wynika natomiast, że projekt ustawy zmieniającej te zasady jest przygotowywany w Senacie. Uważamy, że jest to niezwykle cenna inicjatywa – cieszymy się, że Izba bierze na siebie ciężar troski o ochronę praw człowieka oraz zgodność obowiązującego porządku prawnego z Konstytucją RP.

Poniżej przedstawiamy propozycje rozwiązań, których przyjęcie w naszej opinii pozwoliłoby na zwiększenie standardu ochrony prywatności w Polsce. Zwracamy przy tym uwagę na szerszy problem dostępu Policji i innych służb do różnych typów danych osobowych – nie tylko danych telekomunikacyjnych, o którym piszemy w dalszej części niniejszego listu. Mamy nadzieję, że przygotowywany projekt doprowadzi do rozwiązania problemów sygnalizowanych od lat przez organizacje broniące praw człowieka i organy ochrony prawnej. Ze swojej strony deklarujemy gotowość włączenia się w prace nad projektem w charakterze organizacji społecznej i uszczegółowienia rekomendacji zawartych w niniejszym liście.

Fundacja Panoptykon | ul. Orzechowska 4 lok. 4 | 02-068 Warszawa
e: fundacja@panoptykon.org | t: +48 660 074 026 | w: panoptykon.org

1. Propozycje reformy zasad dostępu do danych telekomunikacyjnych

Fundacja Panoptykon, zajmując się od kilku lat tematem retencji i wykorzystywania danych telekomunikacyjnych, zebrała szereg informacji m.in. na temat zagranicznych regulacji dostępu służb do tego typu danych oraz praktyki ich wykorzystywania przez uprawnione podmioty. W związku z tym przedstawiamy najważniejsze problemy, które powinna rozwiązać projektowana ustawa wraz z naszymi propozycjami ich rozwiązania.

a. Ograniczenie celu pozyskiwania danych

Obecnie Policja i służby specjalne mogą pozyskiwać dane telekomunikacyjne w celu „zapobiegania lub wykrywania przestępstw" (Policja) czy realizacji wszystkich zadań ustawowych – w tym „prowadzenia działalności analitycznej" (Centralne Biuro Antykorupcyjne). Polskie przepisy, uprawniające Policję i inne służby do sięgania po dane telekomunikacyjne, stanowią implementację tzw. dyrektywy retencyjnej (dyrektywa 2006/24/WE), która zakłada dostęp do danych wyłącznie w sprawach „poważnych przestępstw". Rozszerzenie okoliczności uprawniających do sięgania po dane telekomunikacyjne na inne przestępstwa, a tym bardziej na działania niezwiązane ze ściganiem lub wykrywaniem przestępstw stanowi nieproporcjonalną ingerencję w prywatność i autonomię informacyjną jednostki.

Postulujemy:

Dostęp do danych telekomunikacyjnych powinien być możliwy tylko w związku ze ściganiem poważnych przestępstw, którymi w polskim porządku prawnym są zbrodnie, czyli przestępstwa zagrożone karą pozbawienia wolności na czas nie krótszy od lat 3 albo karą surowszą. Od tej zasady należy wprowadzić jedynie kilka wyjątków uzasadnionych charakterem przestępstwa (np. przestępstwa popełniane za pośrednictwem Internetu) lub szczególną sytuacją (np. poszukiwanie osób zaginionych).

b. Zewnętrzna kontrola nad sięganiem po dane

Zgodnie z obowiązującymi przepisami Policja i służby specjalne sięgają po dane telekomunikacyjne bez konieczności uzyskiwania zgody zewnętrznego organu. Przetwarzanie danych telekomunikacyjnych przez służby pozostaje również poza kontrolą Generalnego Inspektora Ochrony Danych Osobowych. Rodzi to niebezpieczeństwo sięgania po dane telekomunikacyjne w sytuacjach, w których nie jest to usprawiedliwione.

Postulujemy:

Dostęp do danych telekomunikacyjnych zawsze powinien podlegać ścisłym mechanizmom kontroli wewnętrznej w ramach organu prowadzącego postępowanie. Od momentu, w którym postępowanie przechodzi z fazy *ad rem* do fazy *ad personam*, dostęp do danych telekomunikacyjnych powinien być uzależniony od zgody zewnętrznego organu – sądu lub prokuratora (w zależności od stopnia ingerencji w prywatność obywateli) – przy czym, analogicznie jak w przypadku kontroli operacyjnej, w uzasadnionych przypadkach przepisy powinny dopuszczać możliwość uzyskania zgody *ex post*.

c. Obowiązki sprawozdawcze

Obecnie obowiązek zbierania informacji na temat ilości zapytań o dane telekomunikacyjne spoczywa na operatorach telekomunikacyjnych, którzy corocznie przekazują te informacje do Urzędu Komunikacji Elektronicznej. Przedstawiane przez UKE liczby różnią się jednak od informacji uzyskiwanych przez Fundację Panoptykon od podmiotów uprawnionych do sięgania

po dane. Jak potwierdza kontrola przeprowadzona przez NIK, dostępne dziś informacje nie pozwalają na rzetelną ocenę skali zjawiska sięgania po dane telekomunikacyjne.

Postulujemy:

Projektowana ustawa powinna nakładać obowiązek sprawozdawczy na podmioty uprawnione do sięgania po dane telekomunikacyjne. Obowiązek sprawozdawczy powinien obejmować informacje na temat: liczby przypadków, w których podmiot pobierał dane; rodzaje pobieranych danych; liczbę urządzeń (telefony komórkowe, komputery), których dotyczyły zapytania; a także rodzaj spraw, w których zastosowano ten środek.

d. Niszczenie zbędnych danych

Obowiązujące przepisy nie nakładają na niektóre uprawnione podmioty obowiązku niszczenia pobranych danych telekomunikacyjnych bez względu na to, czy są one wciąż potrzebne w prowadzonym postępowaniu. Jest to niezgodne z konstytucyjną zasadą autonomii informacyjnej, która uprawnia organy państwa do gromadzenia informacji o obywatelach wyłącznie wtedy, gdy jest to niezbędne.

Postulujemy:

Projektowana ustawa powinna nałożyć na wszystkie uprawnione podmioty obowiązek niezwłocznego niszczenia pobranych danych, jeżeli nie zawierają one informacji mających znaczenie dla prowadzonego postępowania.

2. Dostęp organów państwa do innych kategorii danych osobowych

Ewentualne zmiany zasad dostępu Policji i innych służb do danych nie powinny pomijać tego, że dane telekomunikacyjne to tylko jedna z kategorii danych osobowych pozyskiwanych na temat obywateli przez organy państwa. Kolejną kategorią danych, która zyskuje na znaczeniu wraz z rozwojem technologii teleinformatycznych i usług internetowych, są dane o użytkownikach usług świadczonych drogą elektroniczną. Wnikliwa analiza zasad sięgania przez organy państwa po tego rodzaju dane doprowadziła nas do wniosku, że problemy nie mniej istotne, niż zarysowane w kontekście danych telekomunikacyjnych, pojawiają się w odniesieniu do innych kategorii danych osobowych. Poniżej sygnalizujemy tylko niektóre ze zdiagnozowanych problemów.

Z wyjątkiem tzw. danych ubezpieczeniowych i danych bankowych, Policja i inne służby sięgają po dane osobowe obywateli bez jakiejkolwiek kontroli, a zwłaszcza bez konieczności uzyskiwania zgody zewnętrznego organu. Co więcej, zgodnie z ustawą o ochronie danych osobowych Generalnemu Inspektorowi Ochrony Danych Osobowych nie przysługuje większość uprawnień w zakresie kontroli zgodności z prawem przetwarzania danych osobowych przez służby specjalne. Jedynie w Centralnym Biurze Antykorupcyjnym funkcjonuje Pełnomocnik do spraw ochrony danych osobowych, który – ze względu na swoje umocowanie – nie może być jednak uznany za ekwiwalent niezależnego organu kontrolnego.

Nie jest również znana skala zjawiska sięgania przez Policję i inne służby po poszczególne kategorie danych osobowych. Brak rzetelnej informacji w tym zakresie uniemożliwia społeczną kontrolę nad aktywnością służb i częstotliwością ich ingerencji w prywatność obywateli.

Problemy specyficzne dla dostępu organów państwa do danych użytkowników usług świadczonych drogą elektroniczną podsumowaliśmy w analizie „Dostęp państwa do danych użytkowników usług internetowych. Siedem problemów i kilka hipotez", która stanowi załącznik do niniejszego listu.

W naszej opinii, pracując nad rewizją zasad dostępu Policji i innych służb do danych telekomunikacyjnych, Senat powinien rozważyć poszerzenie zakresu proponowanej regulacji i zwiększenie gwarancji ochrony prywatności w odniesieniu do innych rodzajów danych osobowych. Ze swojej strony deklarujemy gotowość włączenia się w prace nad tym projektem w charakterze organizacji społecznej oraz uszczegółowienia rekomendacji zawartych w niniejszym liście.

Małgorzata Szumańska
Wiceprezeska

Katarzyna Szymielewicz
Prezeska