FUNDACJA PANOPTYKON

Warszawa, 31 marca 2014 r.

Szanowny Pan
Senator Michał Seweryński
Przewodniczący Komisji Praw Człowieka,
Praworządności i Petycji

Opinia Fundacji Panoptykon[1] w sprawie projektu ustawy[2] dotyczącej dostępu uprawnionych podmiotów do danych telekomunikacyjnych

1. Wstęp

Fundacja Panoptykon jest organizacją pozarządową zajmującą się ochroną praw człowieka w społeczeństwie nadzorowanym, a jednym z ważniejszych tematów w naszej działalności jest dostęp organów państwa do danych o obywatelach, w tym dostęp policji i innych służb do danych telekomunikacyjnych.

Problem braku wystarczających gwarancji dla ochrony praw jednostki w kontekście dostępu do danych telekomunikacyjnych dostrzegło wiele podmiotów, m.in. Rzecznik Praw Obywatelskich, Prokurator Generalny, Naczelna Rada Adwokacka i Najwyższa Izba Kontroli. Projekt ustawy o zmianie niektórych ustaw w zakresie przepisów dotyczących uzyskiwania i przetwarzania przez uprawnione podmioty danych gromadzonych przez przedsiębiorców telekomunikacyjnych (**dalej: projekt**) jest jednak pierwszą konkretną propozycją kompleksowych zmian ograniczających dostęp uprawnionych podmiotów do danych telekomunikacyjnych i wzmacniających ochronę prywatności użytkowników telefonów komórkowych i Internetu.

W naszej ocenie projekt zasługuje na akceptację, choć w dalszej części opinii zwracamy uwagę na kilka problemów z nim związanych oraz przedstawimy możliwe kierunki ich rozwiązania. Na wstępie zwracamy jednak uwagę na kontekst, w jakim powstał projekt. Na początku kwietnia br.

[1] Opinia przygotowana przez Wojciecha Klickiego.
[2] Projekt przygotowany przez Biuro Legislacyjne Kancelarii Senatu RP pod pełną nazwą: ustawa o zmianie niektórych ustaw w zakresie przepisów dotyczących uzyskiwania i przetwarzania przez uprawnione podmioty danych gromadzonych przez przedsiębiorców telekomunikacyjnych.

Trybunał Konstytucyjny przeprowadzi rozprawę w sprawie o sygn. K 23/11, zainicjowanej m.in. wnioskami Rzecznik Praw Obywatelskich kwestionującymi konstytucyjność obecnej regulacji zasad dostępu policji i innych służb do danych telekomunikacyjnych.

Jesteśmy przekonani, że wyrok Trybunału Konstytucyjnego zdeterminuje dalsze prace nad projektem. Zwracamy jedynie uwagę, że bez względu na jego treść, ustawodawca może wprowadzić wyższy standard ochrony konstytucyjnych praw i wolności. W przypadku stwierdzenia niekonstytucyjności przepisów regulujących zasady dostępu do danych telekomunikacyjnych ustawodawca powinien kierować się sugestiami Trybunału, które często zamieszczone są w uzasadnieniach wyroku. Należy jednak pamiętać, że konstytucja określa **minimalny** standard ochrony praw człowieka, który może zostać poszerzony i doprecyzowany na gruncie ustawowym – podobnie wyroki Trybunału Konstytucyjnego określają nieprzekraczalną granicę zgodności z konstytucją. Ustawodawca zobowiązany jest zatem przyjąć rozwiązania niesprzeczne z ustawą zasadniczą, jednak w zakresie poszerzania ochrony praw obywatelskich nie jest w żaden sposób ograniczony. Dlatego wykonując wyrok Trybunały Konstytucyjnego, ustawodawca może wyjść poza niezbędne dla zgodności z konstytucją rozwiązania, wprowadzając wyższe wymogi odnośnie ingerowania w konstytucyjne prawa obywateli.

2. Uwagi szczegółowe

W naszej ocenie większość propozycji zawartych w projekcie zmierza w dobrym kierunku. Poniżej prezentujemy uwagi dotyczące niektórych spośród zaproponowanych rozwiązań.

a. Reforma dostępu do danych telekomunikacyjnych

i. Ograniczenie celu pozyskiwania danych

Naszym zdaniem ograniczenie celu pozyskiwania danych telekomunikacyjnych tylko do wykrywania i ustalania sprawców przestępstw, a także uzyskiwania i utrwalania dowodów, stanowi prawidłową implementację tzw. dyrektywy retencyjnej[3]. Dyrektywa stanowi podstawę stworzenia mechanizmu retencji danych, czyli nałożonego na operatorów telekomunikacyjnych obowiązku przechowywania i udostępniania uprawnionym podmiotom danych telekomunikacyjnych.

Zgodnie z dyrektywą retencyjną dane telekomunikacyjne mają być udostępniane organom ścigania w sprawie „poważnych przestępstw". Naszym zdaniem obecne przepisy, pozwalając na sięganie po dane w związku z zapobieganiem lub wykrywaniem sprawców **wszystkich** przestępstw, umożliwiają nieproporcjonalną ingerencję w prawa jednostki. W związku z tym popieramy zawartą w projekcie propozycję ograniczenia katalogu przestępstw, w związku

[3] Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE.

z którymi policja i inne służby mogą sięgać po dane telekomunikacyjne, do tych przypadków, w których możliwe jest przeprowadzenie kontroli operacyjnej, przy jednoczesnym dopuszczeniu wyjątków od tej zasady. Zgodnie z projektem takim wyjątkiem ma być wykrywanie wykroczeń, o których mowa w art. 66 Kodeksu wykroczeń (fałszywe alarmy bombowe). Naszym zdaniem należy rozważyć poszerzenie listy wyjątków o poszukiwanie osób zaginionych[4], przestępstwo uporczywego nękania, o którym mowa w art. 190a Kodeksu karnego (tzw. stalking), a także przestępstwa popełnione za pośrednictwem środków komunikacji elektronicznej w sytuacji, gdy dane telekomunikacyjne są niezbędne do przeprowadzenia innych czynności w śledztwie.

ii. Kontrola nad sięganiem po dane

Pozytywnie oceniamy postulat uzależnienia trybu uzyskania dostępu do danych telekomunikacyjnych od ich charakteru; popieramy również zaproponowany podział – na dane „abonenckie"[5] oraz pozostałe dane telekomunikacyjne.

Naszym zdaniem dostęp do danych abonenckich, który ingeruje w prywatność jednostki w mniejszym stopniu niż dostęp do innych rodzajów danych telekomunikacyjnych, nie musi być uzależniony od każdorazowej zgody organu zewnętrznego. Mimo to projektowane przyznanie policji i innym służbom blankietowego uprawnienia do sięgania po dane abonenckie – bez ograniczenia tej możliwości chociażby do „wykrywania, ustalenia sprawców, uzyskania i utrwalenia dowodów przestępstw" jest zbyt daleko idące.

Z drugiej strony, projekt przewiduje uzależnienie dostępu do innych danych telekomunikacyjnych (np. wykazu połączeń) od uzyskania zgody prokuratora i sądu. Naszym zdaniem to rozwiązanie wprowadza bardzo wysoki standard ochrony praw jednostki. Należy rozważyć, czy nie powinien on obowiązywać dopiero na drugim etapie postępowania przygotowawczego, w którym prowadzone jest ono nie „w sprawie", a „przeciwko" konkretnej osobie (faza *in personam*). Zwracamy również uwagę na konieczność zapewnienia uprawnionym podmiotom możliwości uzyskania tzw. zgody następczej prokuratora lub sądu w sprawach niecierpiących zwłoki.

iii. Sprawozdawczość

Fundacja Panoptykon co roku publikuje informacje dotyczące skali sięgania po dane telekomunikacyjne. Zgodnie z danymi przekazanymi Urzędowi Komunikacji Elektronicznej przez operatorów telekomunikacyjnych w 2013 r. otrzymali oni 1,75 mln zapytań. Natomiast zgodnie z danymi przekazanymi Fundacji przez część uprawnionych podmiotów (policję, Straż Graniczną, Centralne Biuro Antykorupcyjne, Żandarmerię Wojskową, kontrolę skarbową i służbę celną) tylko te podmioty skierowały do operatorów telekomunikacyjnych 2,18 mln zapytań[6]. Naszym zdaniem te rozbieżności świadczą o braku możliwości zweryfikowania, jaka jest

---

[4] Poszerzenie uprawnień policji o możliwość sięgania po dane telekomunikacyjne w celu poszukiwania osób zaginionych zawiera rządowy projekt ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (druk sejmowy nr 2192).

[5] Przez dane abonenckie rozumiemy dane, o których mowa w projektowanych art. 180ca ustawy – Prawo telekomunikacyjne. Z danych zebranych przez Fundację Panoptykon od uprawnionych podmiotów wynika, że zapytania o dane abonenckie stanowią około 42% zapytań kierowanych przez uprawnione podmioty do operatorów telekomunikacyjnych.

[6] Zebrane przez Fundację Panoptykon dane nie obejmują pytań skierowanych do operatorów telekomunikacyjnych przez sądy, prokuratorów i Służbę Kontrwywiadu Wojskowego. Więcej na ten temat: http://panoptykon.org/wiadomosc/miliony-zapytan-jeden-problem.

rzeczywista skala ingerencji policji i innych służb w prywatność użytkowników telefonów komórkowych i Internetu.

W związku z tymi wątpliwościami, popieramy propozycję nałożenia na uprawnione podmioty obowiązków sprawozdawczych. Zwracamy jedynie uwagę na brak możliwości wskazania przez uprawnione podmioty liczby osób, których dotyczyły udostępniane dane – policja i inne służby w większości przypadków (w szczególności na etapie postępowania prowadzonego „w sprawie") nie weryfikują, do kogo należą urządzenia, których dotyczyły zapytania. Ponieważ częstą praktyką jest wykorzystywanie kart typu pre-paid oraz korzystanie z więcej, niż jednego urządzenia, ustalenie, do kogo należała konkretna karta lub telefon może się okazać nadmiernie utrudnione, a z pewnością oznaczałoby konieczność gromadzenia dodatkowych danych.

iv. Niszczenie zbędnych danych

Zgodnie z obowiązującymi przepisami nie wszystkie z podmiotów uprawnionych do sięgania po dane telekomunikacyjne zobowiązane są do ich niszczenia. Naszym zdaniem projekt powinien nakładać na te służby (Agencja Bezpieczeństwa Wewnętrznego, Centralne Biuro Antykorupcyjne, Służba Kontrwywiadu Wojskowego oraz kontrola skarbowa) analogiczny obowiązek niszczenia zbędnych danych, jaki został nałożony na policję w art. 20c ust. 6 i 7 ustawy o policji.

b. Pozyskiwanie danych osobowych

Projekt częściowo dotyczy również szerszego problemu, jakim jest pozyskiwanie przez policję i inne służby różnych danych osobowych dotyczących obywateli. Naszym zdaniem problem ten wymaga gruntownej analizy pod kątem wzmocnienia ochrony prywatności jednostki. Projektowane powołanie wewnętrznego pełnomocnika, który będzie kontrolować przetwarzanie danych osobowych z pozycji osoby zatrudnionej przez dany podmiot, jest dobrą, ale z pewnością nie wystarczającą zmianą. Obecnie przepisy nie chronią bowiem w wystarczający sposób autonomii informacyjnej jednostki i nie gwarantują, że będzie ona narusza wyłącznie wtedy, gdy jest to niezbędne w demokratycznym państwie prawnym.

i. Pełnomocnicy do spraw kontroli przetwarzania danych osobowych

Z powyższymi zastrzeżeniami, popieramy postulat powołania we wszystkich służbach pełnomocnika do spraw kontroli przetwarzania danych osobowych. Nasze zastrzeżenia – podobnie jak w przypadku pełnomocnika funkcjonującego w Centralnym Biurze Antykorupcyjnym – budzi jedynie założenie, że na to stanowisko będzie mógł zostać powołany funkcjonariusz danej służby. Naszym zdaniem może to mieć negatywny wpływ na niezależność jego funkcjonowania.

ii. Uprawnienia Generalnego Inspektora Ochrony Danych Osobowych

Zgodnie z projektem znowelizowany zostanie art. 43 ust. 2 ustawy o ochronie danych osobowych – Generalny Inspektor Ochrony Danych Osobowych uzyska uprawnienie do przeprowadzania czynności kontrolnych związanych z przetwarzaniem przez uprawnione podmioty danych telekomunikacyjnych (z wyjątkiem danych abonenckich). Naszym zdaniem dotychczasowa regulacja, wyłączająca uprawnienia Generalnego Inspektora Ochrony Danych Osobowych względem danych osobowych przetwarzanych przez służby specjalne, jest

nieuzasadniona. Proponowana zmiana prowadzi w dobrym kierunku, niejasne jest jednak, dlaczego w projekcie proponuje się rozszerzenie uprawnień GIODO wyłącznie na kontrolę przetwarzania niektórych danych telekomunikacyjnych.

Z poważaniem,

Małgorzata Szumańska
Wiceprezeska

Katarzyna Szymielewicz
Prezeska