FUNDACJA PANOPTYKON

Warszawa, 17 lipca 2015 r.

Szanowny Pan Senator
Piotr Zientarski
Przewodniczący Komisji Ustawodawczej

Szanowny Panie,

Fundacja Panoptykon przedstawia swoje stanowisko dotyczące projektu zmiany ustawy o Policji oraz niektórych innych ustaw (druk senacki 967). Jednocześnie zgłaszamy zainteresowanie udziałem w pracach legislacyjnych nad projektem, które będą prowadzone w Komisji Ustawodawczej.

W imieniu Fundacji Panoptykon,

Katarzyna Szymielewicz

Prezeska

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

FUNDACJA PANOPTYKON

Warszawa, 17 czerwca 2015 r.

STANOWISKO FUNDACJI PANOPTYKON[1]

w sprawie projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (druk senacki 967)

Projekt zmiany ustawy o Policji oraz niektórych innych ustaw – jak wynika z jego uzasadnienia – ma na celu dostosowanie systemu prawa do wyroku Trybunału Konstytucyjnego z 30 lipca 2014 r. o sygn. K 23/11 (dalej: **wyrok TK**). Ze względu na skomplikowaną sytuację prawną, a także zbliżający się termin wejścia w życie wyroku Trybunału Konstytucyjnego, podjęcie przez Senat inicjatywy legislacyjnej jest niezwykle cenne. Jednak, w ocenie Fundacji Panoptykon, proponowane rozwiązania w sposób fragmentaryczny i niepełny wdrażają wyrok TK, a także pomijają wyrok Trybunału Sprawiedliwości Unii Europejskiej z 8 kwietnia 2014 r. w sprawach połączonych C-293/12 i C-594/12 (dalej: **wyrok TSUE**). Rodzi to daleko idące wątpliwości co do zgodności projektu z Konstytucją RP i prawem UE.

Na wstępie przypominamy, że dane telekomunikacyjne stanowią integralny element tajemnicy komunikowania się. Potwierdził to m.in. Europejski Trybunał Praw Człowieka w wyrokach Malone przeciwko Wielkiej Brytanii (skarga nr 8691/79) i Copland przeciwko Wielkiej Brytanii (skarga nr 62617/00). W pierwszym z tych wyroków ETPC wskazał, że „pozyskiwanie danych zawartych w tzw. bilingach nie może wprawdzie być utożsamiane z podsłuchem rozmów telefonicznych, jednakże ujawnienie policji tego rodzaju danych bez zgody abonenta powinno być traktowane jako równoważne ingerencji w prawo zagwarantowane w art. 8 ust. 1 Konwencji (prawo do prywatności)". Stanowisko to potwierdziły w swoich wyrokach zarówno TK, jak i TSUE. W związku z tym, jak wskazał TSUE „ochrona życia prywatnego w każdym wypadku wymaga, aby odstępstwa od ochrony danych osobowych i jej ograniczenia ograniczały się do tego, **co jest absolutnie konieczne**".

TSUE, stwierdzając niezgodność z Kartą praw podstawowych tzw. dyrektywy retencyjnej[2], zwrócił uwagę na następujące problemy:

- konieczność zapewnienia, by uprawnione organy miały dostęp do danych wyłącznie w sprawie przestępstw, „które z uwagi na zakres i wagę ingerencji w prawa podstawowe

[1] Stanowisko przygotowane przez Wojciecha Klickiego.
[2] 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 zmieniającej dyrektywę 2002/58/WE

ustanowione w art. 7 i 8 karty, można uznać za **wystarczająco poważne**, by taką ingerencję uzasadnić";

- uzyskanie dostępu do danych powinno podlegać **uprzedniej kontroli sądu lub niezależnego organu administracyjnego**, które pilnowałyby, aby udostępnienie i wykorzystywanie danych ograniczało się do przypadków, gdy jest to ściśle konieczne;
- dane telekomunikacyjne powinny być w należyty sposób chronione (zwłaszcza dotyczy to obowiązku przechowywania danych na terenie UE);

Stwierdzenie niezgodności dyrektywy retencyjnej z Kartą praw podstawowych z wymienionych wyżej powodów powinny być wzięte pod uwagę przy pracach legislacyjnych w państwach członkowskich. Jak wskazał bowiem dr Maciej Taborowski w analizie skutków wyroku TSUE[3], „na mocy art. 4 ust. 3 TUE (zasada lojalności) **wyrok prejudycjalny stwierdzający nieważność aktu prawa UE wiąże** instytucje UE oraz **wszystkie organy państw członkowskich** (nie tylko sądy krajowe), **w tym organy legislacyjne**". Zwracamy przy tym uwagę, że nieuwzględnienie wytycznych płynących z wyroku TSUE może być podstawą do podjęcia działań przez Komisję Europejską, która – jako strażniczka traktatów UE – zobowiązana jest do weryfikacji zgodności przepisów krajowych z prawem UE[4].

Przed przejściem do omówienia szczegółowych propozycji zawartych w projekcie, zwracamy uwagę, że opinia dotyczy **wyłącznie** przepisów związanych z dostępem Policji i innych uprawnionych podmiotów do danych telekomunikacyjnych. W opinii nie odnosimy się do elementów projektu związanych z kontrolą operacyjną, co w żadnym razie nie powinno być traktowane jako ich akceptacja.

1. Kontrola nad sięganiem przez uprawnione podmioty po dane telekomunikacyjne

W wyroku K 23/11 Trybunał Konstytucyjny wskazał, że przepisy uprawniające do sięgania po dane telekomunikacyjne naruszają Konstytucję „**przez to, że nie przewidują niezależnej kontroli udostępniania danych telekomunikacyjnych**".

Opiniowany projekt zakłada dwa modele kontroli nad sięganiem po dane telekomunikacyjne. Pierwszy model, kontroli uprzedniej, ma dotyczyć jedynie danych telekomunikacyjnych „dotyczących bezpośrednio osoby wykonującej zawód lub funkcję, o których mowa w art. 180 § 2 Kodeksu postępowania karnego". W tym modelu niezbędne będzie uzyskanie zgody sądu na pozyskanie danych i ich wykorzystanie w postępowaniu karnym. Projektodawca przewidział także możliwość uzyskania następczej zgody sądu w przypadkach niecierpiących zwłoki, a także konieczność uzyskania zgody sądu na wykorzystanie w postępowaniu karnym materiałów potencjalnie naruszających tajemnicę zawodową w sytuacji, w której dopiero po ich pobraniu okazało się, że dotyczą one wskazanych kategorii osób.

Drugi model, w praktyce odnoszący się do przeważającej większości przypadków pobrania danych, sprowadza się do kontroli następczej, sprawowanej przez sąd. Zgodnie z projektem podmioty uprawnione do pobierania danych mają przekazywać, raz na 6 miesięcy, sprawozdania obejmujące liczbę i rodzaj pozyskanych danych: podstawę prawną pozyskania

[3] Analiza dostępna pod adresem: http://www.hfhr.pl/wp-content/uploads/2014/04/skutki_wyroku_TSUE_MTaborowski-3.pdf

[4] Do Komisji Europejskiej w tej sprawie zwróciła się koalicja organizacji pozarządowych European Digital Rights, której Fundacja Panoptykon jest członkiem, zwróciła się. Wystąpienie dostępne pod adresem: https://edri.org/files/DR_EDRi_letter_CJEU_Timmermans_20150702.pdf

danych, rodzaje przestępstw, w związku z zaistnieniem których wystąpiono o dane oraz liczbę przypadków, ze wskazaniem ich podziału na rodzaje spraw, w których wystąpiono o dane. W ramach prowadzonej kontroli sąd okręgowy **może** zapoznać się z materiałami uzasadniającymi udostępnienie danych telekomunikacyjnych oraz materiałami uzyskanymi w wyniku podjętych czynności. W przypadku stwierdzenia przez sąd braku podstaw do pozyskania danych, podlegają one zniszczeniu.

Na wstępie należy przywołać stanowisko Trybunału Konstytucyjnego odnośnie kontroli nad sięganiem po dane telekomunikacyjne. TK „*nie przesądza, jak dokładnie ma wyglądać procedura dostępu do danych telekomunikacyjnych, a w szczególności, czy konieczne ma być w odniesieniu do każdego rodzaju zatrzymywanych danych, o których mowa w art. 180c i art. 180d prawa telekomunikacyjnego, uzyskanie zgody na ich udostępnienie. Nie wszystkie dane tego rodzaju powodują taką samą intensywność ingerencji w wolności i prawa człowieka. Zdaniem Trybunału, nie jest wobec tego wykluczone – w odniesieniu do udostępniania danych telekomunikacyjnych w toku czynności operacyjno-rozpoznawczych – wprowadzenie, jako zasady, kontroli następczej. Regulując ten mechanizm, ustawodawca powinien uwzględnić m.in.* ***specyfikę działania i ustawowy zakres zadań poszczególnych rodzajów służb****,* ***sytuacje niecierpiące zwłoki, w których szybkie pozyskanie danych telekomunikacyjnych może być niezbędne*** *dla zapobieżenia popełnieniu przestępstwa lub jego wykrycia. Zgodnie z konstytucyjną zasadą sprawności działania instytucji publicznych (wstęp do Konstytucji) należy wykreować mechanizm, który umożliwi służbom odpowiedzialnym za bezpieczeństwo państwa i porządek publiczny efektywną walkę z zagrożeniami. Trybunał dostrzega jednak argumenty za wprowadzeniem* ***kontroli uprzedniej*** *w pewnych wypadkach. W szczególności chodzić może o dostęp do danych telekomunikacyjnych* ***osób wykonujących zawody zaufania publicznego*** *lub* ***jeśli nie ma konieczności pilnego działania służb”.***

TK sformułował więc dwie wytyczne dotyczące kształtu kontroli nad sięganiem po dane. Po pierwsze, sposób kontroli może być uzależniony od charakteru danych telekomunikacyjnych oraz od charakteru działalności uprawnionego podmiotu. Po drugie, kontrola uprzednia nad sięganiem po dane powinna dotyczyć osób wykonujących zawody zaufania publicznego oraz sytuacji, w których nie ma konieczności pilnego działania. Trybunał w Luksemburgu wskazał zaś wprost, że uzyskanie dostępu do danych powinno podlegać **uprzedniej kontroli sądu lub niezależnego organu administracyjnego.**

W naszej ocenie mechanizmu kontroli nad sięganiem po dane przewidziany w projekcie nie uwzględnia wszystkich wytycznych płynących z wyroków TK i TSUE i **nie zrealizuje zakładanego celu z następujących względów:**

- kontrola następcza prowadzona przez sąd na podstawie składanych co 6 miesięcy sprawozdań ma mieć charakter fakultatywny: obawiamy się, że doprowadzi to do niepodejmowania przez sąd realnych czynności kontrolnych[5];
- czynności kontrolne podejmowane przez sąd będą miały charakter wyjątkowy i incydentalny, tymczasem zasadą powinno być kontrolowanie dostępu do danych telekomunikacyjnych w każdej sprawie, a brak takiej kontroli– wyjątkiem;

[5] W tym kontekście zwracamy uwagę na stanowisko Krajowej Rady Sądownictwa wobec projektu. KRS w swoim stanowisku wskazała, że przyznanie sądom dodatkowych uprawnień będzie się wiązać z dodatkowym obciążeniem budżetu sądów, tymczasem projektodawca nie przedstawił wielkości i źródeł ich pokrycia.

- kontrola prowadzona po 6 miesiącach od pobrania danych telekomunikacyjnych będzie mniej efektywna, a jednocześnie bardziej czasochłonna od kontroli prowadzonej przed lub bezpośrednio po pobraniu danych;
- projektodawca nie przewidział jakichkolwiek negatywnych konsekwencji dla funkcjonariuszy sięgających po dane telekomunikacyjne w przypadku stwierdzenia braku podstaw do pozyskania danych.

W naszej ocenie kontrola nad sięganiem po dane telekomunikacyjne powinna być wzorowana na tej dotyczącej kontroli operacyjnej. Jak wskazał w zdaniu odrębnym do wyroku TK sędzia Wojciech Hermeliński „celowe powinno być osiągnięcie porównywalnego standardu ochrony prawa do prywatności i wolności komunikowania się jak przy kontroli operacyjnej. Przy obecnym poziomie rozwoju technologii inwazyjność tych dwóch sposobów pozyskiwania informacji o obywatelach jest zbliżona (choć dane telekomunikacyjne – w przeciwieństwie do informacji uzyskiwanych w toku kontroli operacyjnej – nie dostarczają informacji o treści komunikatów, to w zamian za to można na ich podstawie ustalić np. fakt przebywania danej osoby w określonym miejscu lub grono osób, z którymi się ona kontaktuje)".

Stoimy na stanowisku – które znajduje oparcie w wyroku TK – że tryb uzyskania dostępu do danych telekomunikacyjnych powinien być uzależniony od ich charakteru – np. z rozróżnieniem danych abonenckich od pozostałych kategorii danych telekomunikacyjnych. Dostęp dodanych abonenckich , które w mniejszym stopniu ingerują w prywatność jednostki, nie musi być uzależniony od każdorazowej zgody organu zewnętrznego. Taka zgoda powinna być natomiast konieczna do uzyskania dostępu do takich danych, jak wykaz połączeń czy geolokalizacja. Przy czym zasadą powinno być uzyskanie zgody przed sięgnięciem po dane, natomiast możliwość uzyskiwania zgody następczej w przypadkach niecierpiących zwłoki powinna zostać dopuszczona jako wyjątek.

Zwracamy uwagę, że wbrew stanowisku projektodawcy, możliwe jest sprawne funkcjonowanie systemu kontroli uprzedniej nad pozyskiwaniem danych telekomunikacyjnych. W Danii i Finlandii dostęp do danych telekomunikacyjnych możliwy jest po uprzednim uzyskaniu zgody sądu. Krajowe przepisy umożliwiają – jedynie w wyjątkowych sytuacjach – uzyskanie tej zgody w trybie następczym.

2. Pozostałe problemy związane z dostępem do danych telekomunikacyjnych

a. Zasada subsydiarności

Zgodnie z uzasadnieniem projektu „zastosowanie zasady subsydiarności przed wystąpieniem po dane telekomunikacyjne w przypadku ścigania niektórych przestępstw mogłoby okazać się niemożliwe, a także utrudnić skuteczne ściganie ich sprawców". Projektodawcy wskazują przy tym na przestępstwa internetowe, w których nie ma innych czynności, które można wykonać przed pobraniem danych telekomunikacyjnych albo wykazać ich nieskuteczność.

Brak zasady subsydiarności zobowiązującej uprawnione podmioty do wykorzystywania danych telekomunikacyjnych był poruszony przez Rzecznik Praw Obywatelskich we wniosku do Trybunału Konstytucyjnego, inicjującym postępowanie o sygn. K 23/11. Należy w tym miejscu przypomnieć, że TK – uznając niekonstytucyjność braku kontroli nad sięganiem po dane – nie rozstrzygnął, czy pozostałe zarzuty sformułowane przez Rzecznik Praw Obywatelskich i Prokuratora Generalnego zasługują na uwzględnienie. Zwracamy uwagę, że zdaniem Prokuratora Generalnego „brak wymogu subsydiarności sięgania po dane telekomunikacyjne

świadczy o nieproporcjonalnej ingerencji, niespełniającej warunku konieczności"; w postępowaniu przed TK to stanowisko podzielił także Marszałek Sejmu.

W naszej ocenie ustawodawca powinien wprowadzić zasadę subsydiarności. Argumenty przywołane przeciwko wprowadzeniu tej zasady w uzasadnieniu projektu są niewłaściwe i nie odnoszą się do istoty zasady subsydiarności. Jeśli w konkretnej sprawie nie istnieją inne czynności, które można wykonać przed pobraniem danych telekomunikacyjnych albo wykazać ich nieskuteczność, zasada subsydiarności nie stoi na przeszkodzie wykorzystaniu danych.

Jak wskazał w zdaniu odrębnym do wyroku TK sędzia Wojciech Hermeliński „wskazany **brak subsydiarności** zaskarżonych przepisów **otwiera możliwość wykorzystywania danych telekomunikacyjnych** nie tylko wówczas, gdy jest to rzeczywiście konieczne do wykrywania lub zapobiegania przestępstwom, ale także wtedy **gdy jest to po prostu najprostsze i najwygodniejsze** (…) Istnieje ryzyko, że sprawdzenie bilingów z rozmów telefonicznych czy odczytów z GPS zamontowanego w telefonie czy samochodzie będzie wkrótce pierwszą czynnością podejmowaną we wszystkich sprawach na przykład w celu wytypowania wstępnego kręgu osób zamieszanych w dane przestępstwo, nawet wtedy gdy – bez szkody dla wyniku postępowania – można ten sam cel osiągnąć tradycyjnymi metodami śledczymi, bez ingerencji w prywatność dużej liczby obywateli".

b. Informowanie

Projektodawca nie przewidział procedury informowania osób, których dane zostały pobrane, o tym fakcie. Stoi to w sprzeczności z wytycznymi sformułowanymi w uzasadnieniu wyroku TK, zgodnie z którym: *„ma istnieć obowiązek poinformowania jednostki o podjętych wobec niej działaniach operacyjno-rozpoznawczych oraz pozyskaniu informacji na jej temat, i to bez względu na to, czy były to osoby podejrzane o naruszenie prawa, czy osoby postronne, które przypadkowo stały się obiektem kontroli. Powiadomienie jednostki na etapie wykonywania działań operacyjno-rozpoznawczych i gromadzenia informacji, co oczywiste, narażałoby je na nieskuteczność. Dlatego ustawodawca powinien zagwarantować późniejsze poinformowanie o tym fakcie".*

Naszym zdaniem należy rozważyć wprowadzenie mechanizmu informowania o pobraniu danych telekomunikacyjnych, analogicznego do rozwiązań przewidzianych w Kodeksie postępowania karnego. Wprowadzenie tego mechanizmu jest niezbędnym elementem wdrożenia wyroku TK, który jednoznacznie stwierdził, że zaniechanie poinformowania o zebraniu o jednostkach informacji przez władze publiczne samo w sobie stanowi naruszenie art. 51 ust. 3 i 4 Konstytucji. Zdaniem TK „obowiązek informacyjny w powyższym zakresie ma eliminować ryzyko niekontrolowanego tworzenia oraz utrzymywania zbiorów danych nieprzydatnych dla postępowań prowadzonych przez organy państwa, lecz potencjalnie wartościowych z punktu widzenia przyszłych, bliżej nieokreślonych czynności".

Niewątpliwie od zasady informowania powinny zostać wprowadzone wyjątki, uwzględniające sytuacje, w których dane zostały pozyskane przypadkowo i nie podlegają dalszej analizie bądź pozyskano je w ramach działań wywiadowczych, których cel byłby zniweczony przez informowanie osób objętych zainteresowaniem służb. Takie – uzasadnione – wyjątki nie mogą jednak podważać potrzeby wprowadzenia zasady informowania o pobraniu danych telekomunikacyjnych.

Na marginesie zwracamy uwagę, że na brak obowiązku powiadamiania osób, których dotyczyły działania służb, o fakcie pobrania danych telekomunikacyjnych skrytykował również Federalny Sąd Konstytucyjny Niemiec, który wyrokiem z 2 marca 2010 r. (sygn. 1 BvR 256/08) unieważnił

krajowe przepisy wdrażające dyrektywę retencyjną. Jednym z powodów takiej decyzji był brak konieczności powiadamiania podmiotu poddanego inwigilacji o pozyskaniu dotyczących go danych.

c. Długość przechowywania danych

W swoim wyroku TK zwrócił uwagę, że 12-miesięczny okres zatrzymywania danych telekomunikacyjnych jest „stosunkowo długi". Analizując statystyki wskazujące na średni czas przechowywania danych telekomunikacyjnych przed ich pobraniem przez uprawnione podmioty, TK wskazał, że „może budzić wątpliwości, czy zatrzymywanie danych o ruchu i lokalizacji na czas dłuższy niż 6 miesięcy spełnia konstytucyjny wymóg przydatności, wynikający z zasady proporcjonalności".

Na problem czasu przechowywania danych zwrócił uwagę TSUE, który niezgodności dyrektywy retencyjnej z Kartą praw podstawowych dopatrzył się m.in. w braku zróżnicowania między okresem przechowywania różnych kategorii danych telekomunikacyjnych w zależności od ewentualnej użyteczności danych w stosunku do zakładanego celu, a także stopnia ich ingerencji w prywatność jednostki.

W naszej ocenie ustawodawca – chcąc w pełni zrealizować wyrok TK, a jednocześnie zapewnić wysoki stopień ochrony praw jednostki, powinien w przekonujący sposób wykazać konieczność 12-miesięcznej retencji danych, a także rozważyć zróżnicowanie okresu ich przechowywania od ich charakteru i przydatności.

d. Obowiązki sprawozdawcze – sądy i Minister Sprawiedliwości

Zdaniem TK, brak jednolitych standardów sprawozdawczości stanowi istotny konstytucyjny mankament obowiązujących unormowań. Istniejące przepisy nie wprowadzają bowiem spójnej metodologii liczenia realizowanych zapytań o dane telekomunikacyjne, a zarówno operatorzy telekomunikacyjni, jak i poszczególne uprawnione podmioty stosują w tym zakresie różne standardy.

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 przekazanymi Fundacji przez część uprawnionych podmiotów (policję, Straż Graniczną, Centralne Biuro Antykorupcyjne, Agencję Bezpieczeństwa Wewnętrznego, Żandarmerię Wojskową, kontrolę skarbową i służbę celną[6]), tylko te podmioty skierowały do operatorów telekomunikacyjnych 2,18 mln zapytań. Ta rozbieżność potwierdza brak jednolitych standardów i przejrzystości w ocenie rzeczywistej skali ingerencji policji i innych służb w prywatność użytkowników telefonów komórkowych i Internetu.

Pozytywnie oceniamy projektowane przeniesienie obowiązku sprawozdawczego dotyczącego częstotliwości sięgania po dane telekomunikacyjne z operatorów telekomunikacyjnych na organy państwowe. W naszej ocenie daje to szanse na zwiększenie spójności i przejrzystości generowanych statystyk.

Naszym zdaniem ponownego rozważenia wymaga jednak zakres informacji, jakie mają być przekazywane przez sądy ministrowi, a następnie przez ministra – Sejmowi. W szczególności

[6] Informacje te nie obejmują pytań skierowanych do operatorów telekomunikacyjnych przez sądy, prokuratorów i Służbę Kontrwywiadu Wojskowego.

sądzimy, że obowiązkiem sprawozdawczym powinien zostać objęty także rodzaj przestępstw, w związku z zaistnieniem których wystąpiono o dane telekomunikacyjne. Skoro projekt zakłada przedkładanie przez uprawnione organy prezesom sądów okręgowych danych tego rodzaju, nie ma przeszkód, by sądy przedstawiały je Ministrowi Sprawiedliwości, a ten – Sejmowi. Jednocześnie postulujemy rozważenie przeniesienia uprawnienia do wydania rozporządzenia, o którym mowa w art. 180c ust. 2 Prawa telekomunikacyjnego z ministra właściwego do spraw łączności na Ministra Sprawiedliwości, który w ten sposób uzyskałby pełną kontrolę nad sprawozdawczością dotyczącą sięgania po dane telekomunikacyjne.

e. Przestępstwa, w związku z którymi możliwe jest sięganie po dane telekomunikacyjne

Projekt doprecyzowuje, w jakich sytuacjach policja i inne uprawnione podmioty będą mogły wykorzystywać dane telekomunikacyjne. W przypadku policji mają to być **przestępstwa ścigane z oskarżenia publicznego**, a także działania w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych, w przypadku Straży Granicznej: przestępstwa i **wykroczenia,** o których mowa w art. 1 ust. 2 pkt 4 ustawy o Straży Granicznej, w przypadku kontroli skarbowej: przestępstwa skarbowe, jeżeli wartość przedmiotu czynu lub uszczuplenie należności publicznoprawnej przekracza pięćdziesięciokrotną wysokość minimalnego wynagrodzenia za pracę, w przypadku Żandarmerii Wojskowej: przestępstwa, w tym przestępstwa skarbowych popełnione przez żołnierzy, a także działania w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych, w przypadku Agencji Bezpieczeństw Wewnętrznego, Służby Kontrwywiadu Wojskowego i Centralnego Biura Antykorupcyjnego: rozpoznawanie, zapobieganie, zwalczanie i wykrywanie albo utrwalanie dowodów przestępstw w celu realizacji ustawowych zadań.

Pozytywnie oceniamy kierunek proponowanych zmian, który uwzględnia zasadę, zgodnie z którą ingerencja w prawo do prywatności związana z pozyskiwaniem danych telekomunikacyjnych powinna być dopuszczalna tylko w związku z poważnymi przestępstwami. Projekt nie realizuje jednak tego celu w sposób konsekwentny, dopuszczając m.in. wykorzystywanie przez Straż Graniczną danych telekomunikacyjnych w sprawach wykroczeń.

Naszym zdaniem pożądane byłoby ograniczenie możliwości sięgania po dane telekomunikacyjne do tych samych przypadków, w których prawo przewiduje możliwość prowadzenia kontroli operacyjnej, przy jednoczesnym dopuszczeniu wyjątków od tej zasady. Takim wyjątkiem mogłoby być wykrywanie wykroczeń, o których mowa w art. 66 Kodeksu wykroczeń (fałszywe alarmy bombowe), przestępstwo uporczywego nękania (tzw. stalking), a także przestępstwa popełnione za pośrednictwem środków komunikacji elektronicznej w sytuacji, gdy dane telekomunikacyjne są niezbędne do przeprowadzenia czynności w śledztwie.

f. Przechowywanie danych telekomunikacyjnych poza terenem Unii Europejskiej

Na konieczność szczególnej ochrony danych telekomunikacyjnych przechowywanych przez operatorów telekomunikacyjnych zwróciły uwagę zarówno TK, jak i TSUE. W ocenie Trybunału w Luksemburgu brak zapewnienia, by dane były przechowywane na terenie UE, oznacza, iż dyrektywa nie gwarantuje „kontroli poszanowania wymogów ochrony i bezpieczeństwa". Obecnie – jak wskazał podczas rozprawy przed TK przedstawiciel Urzędu Komunikacji Elektronicznej – przedsiębiorcy zastrzegają informacje dotyczące umiejscowienia serwerów lub

dotyczące własnej sieci, jako tajemnicę przedsiębiorstwa. Organ ten nie zna więc miejsca ich przechowywania".

W naszej ocenie niezbędne jest wprowadzenie takich regulacji, które wymuszą na operatorach telekomunikacyjnych przechowywanie danych na terenie Unii Europejskiej ze względu na obowiązujące tu standardy ochrony danych osobowych.

3. Podsumowanie

W ocenie Fundacji Panoptykon projekt nie odpowiada na kluczowe problemy związane z pozyskiwaniem przez policję i inne uprawnione podmioty danych telekomunikacyjnych. Jego przyjęcie byłoby jedynie **fasadowym** wdrożeniem wyroku Trybunału Konstytucyjnego. W szczególności, kształt proponowanego mechanizmu kontroli nad sięganiem po dane telekomunikacyjne nie realizuje standardów niezbędnych w demokratycznym państwie prawa.

Jednocześnie projekt nie realizuje innych, ważnych wytycznych wynikających z wyroku Trybunału Sprawiedliwości Unii Europejskiej, w szczególności wprowadzenia zasady subsydiarności, informowania osób, których dane zostały pobrane oraz ograniczenia celu, w jakim dane mogą zostać pobrane.

Z powyższych względów, w naszej ocenie, opiniowany projekt jest niezgodny zarówno z Konstytucją RP, jak i prawem UE. Jego przyjęcie w tym kształcie doprowadzi zatem do ponownego uchylenia odpowiednich przepisów przez Trybunał Konstytucyjny lub podjęcia odpowiednich kroków przez Komisję Europejską. Do tego czasu będzie jednak dochodziło do systematycznego naruszenia prawa do prywatności osób, których dane telekomunikacyjne będą pobierane przez policję i inne uprawnione podmioty.

W naszej ocenie niezbędna jest:

- Gruntowna rewizja przewidzianego modelu kontroli nad wykorzystywaniem danych telekomunikacyjnych w taki sposób, by konieczność uzyskania zgody sądu bądź innego niezależnego organu było zasadą, a nie wyjątkiem;
- wprowadzenie zasady subsydiarności, która zapewni, że uprawnione podmioty będą sięgać po dane wyłącznie w sytuacjach, w których inne środki okażą się niewystarczające lub nieprzydatne;
- wprowadzenie mechanizmu informowania osób, których dane zostały pobrane, o tym fakcie;
- konsekwentne ograniczenie sytuacji, w których możliwe jest sięganie po dane telekomunikacyjne, do spraw dotyczących poważnych przestępstw.