FUNDACJA PANOPTYKON

Warszawa, 27 grudnia 2015 r.

Stanowisko Fundacji Panoptykon

w sprawie projektu ustawy o zmianie ustawy o policji oraz niektórych innych ustaw[1]

W dniu 23 grudnia 2015 r. grupa posłów złożyła w Sejmie projekt ustawy o zmianie ustawy o policji oraz niektórych innych ustaw (dalej: **projekt**). Dotyczy on uprawnienia policji i służb specjalnych do prowadzenia kontroli operacyjnej, a także wykorzystywania różnego rodzaju danych na temat obywateli, zwłaszcza danych telekomunikacyjnych (m.in. billingi).

Jak wynika z uzasadnienia, projekt ma na celu dostosowanie systemu prawa do wyroku Trybunału Konstytucyjnego z 30 lipca 2014 r. o sygn. K 23/11 (dalej: **wyrok TK**). W ocenie Fundacji Panoptykon proponowane rozwiązania w sposób fragmentaryczny i niepełny wdrażają wyrok TK, a także pomijają treść wyroku Trybunału Sprawiedliwości Unii Europejskiej z 8 kwietnia 2014 r. w sprawach połączonych C-293/12 i C-594/12 (dalej: **wyrok TSUE**). W wyroku tym Trybunał orzekł o nieważności tzw. dyrektywy retencyjnej[2], na podstawie której wprowadzono krajowe przepisy o obowiązkowym zbieraniu i udostępnianiu policji i innym służbom danych telekomunikacyjnych. W konsekwencji, rozwiązania zaproponowane w projekcie **rodzą daleko idące wątpliwości co do zgodności z Konstytucją RP i prawem UE**.

Większość rozwiązań zaproponowanych w projekcie jest zbieżna z propozycjami senackiego projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw przygotowanym w poprzedniej kadencji Senatu (druk sejmowy nr 3765, dalej: **projekt senacki**)[3]. Prace nad nim zostały zawieszone ze względu na wątpliwości odnośnie zgodności projektu z Konstytucją i prawem unijnym. Projekt senacki był krytykowany również przez ówczesną opozycję.

Ze względu na zasadniczą zbieżność komentowanej propozycji z projektem senackim aktualność zachowuje większość uwag przedstawionych przez Fundację Panoptykon w lipcu 2015 r. Opiniowany projekt zawiera także zmiany, które osłabiają poziom gwarancji ochrony praw człowieka względem propozycji senackiej.

Zgodnie z projektem zmiany prawne mają wejść w życie 7 lutego 2016 r. Wynika to z faktu, że tego dnia tracą moc przepisy zakwestionowane przez Trybunał Konstytucyjny w wyroku z 30 lipca 2014 r. o sygn. K 23/11 (dalej: **wyrok**). Trybunał Konstytucyjny odroczył wejście w życie swojego wyroku o 18 miesięcy, spośród których 15 upłynęło w poprzedniej kadencji

[1] Stanowiska przygotowane przez Wojciecha Klickiego.
[2] Dyrektywy 2006/24/WE Parlamentu Europejskiego i Rady z dnia 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
[3] Projekt dostępny pod adresem: http://sejm.gov.pl/Sejm7.nsf/PrzebiegProc.xsp?id=EFEA200545F64605C1257E9200487C8A.

Parlamentu. W związku z tym istnieje konieczność pilnego przyjęcia przepisów regulujących wskazany wyżej obszar.

Ze względu na doniosłość projektu dla stopnia poszanowania konstytucyjnego prawa do prywatności, autonomii informacyjnej, a także prawa do sądu powinien on zostać poddany możliwie szerokim konsultacjom publicznym. Mimo krótkiego czasu pozostającego do wejścia w życie wyroku TK udział w nich powinny wziąć zarówno, organizacje pozarządowe, korporacje zawodowe, jak i eksperci.

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. Proponowane zasady dostępu do danych telekomunikacyjnych a prawo UE

Na wstępie przypominamy, że dane telekomunikacyjne stanowią integralny element tajemnicy komunikowania się. Potwierdził to m.in. Europejski Trybunał Praw Człowieka (dalej: **ETPC**) 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. billingach 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, 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 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 tzw. dyrektywy retencyjnej z Kartą praw podstawowych z wymienionych wyżej powodów powinno być wzięte pod uwagę przy pracach legislacyjnych w państwach członkowskich. Jak wskazał bowiem dr Maciej Taborowski w analizie skutków wyroku TSUE[4], „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

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

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.

Rozwiązania ujęte w projekcie, wbrew stwierdzeniu zawartemu w jego uzasadnieniu, trudno uznać za zgodne z prawem Unii Europejskiej.

2. **Uwagi szczegółowe**

    a. **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 wprowadzenie kontroli następczej sprawowanej przez sąd. Zgodnie z projektem podmioty uprawnione do pobierania danych mają przekazywać, raz na 6 miesięcy, sprawozdania obejmujące liczbę przypadków pozyskania danych telekomunikacyjnych, rodzaj tych danych, a także kwalifikacje prawne czynów, w związku z zaistnieniem których wystąpiono o te dane. W ramach prowadzonej kontroli sąd okręgowy **może** zapoznać się z materiałami uzasadniającymi udostępnienie danych telekomunikacyjnych oraz materiałami uzyskanymi w wyniku podjętych czynności. Spod takiej kontroli sądu wyłączone zostały tzw. dane abonenckie, o których mowa w art. 161 i 179 ust. 9 ustawy – Prawo telekomunikacyjne.

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 mechanizm kontroli nad sięganiem po dane przewidziany w projekcie nie uwzględnia wytycznych płynących z wyroków TK oraz 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;
- projekt ignoruje konieczność zwiększonej ochrony danych telekomunikacyjnych osób wykonujących zawody zaufania publicznego;
- 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 przewidział, że w ramach kontroli sąd może zapoznać się z „materiałami uzasadniającymi udostępnienie danych", co wiąże się z ryzykiem, że sąd nie będzie mógł dokonać kompleksowej weryfikacji zasadności sięgnięcia po dane, a pozna jedynie jednostronną oceną zaistniałej sytuacji;
- w przypadku negatywnej oceny działania uprawnionego organu projekt nie przewiduje obowiązku zniszczenia danych pobranych w sposób niezgodny z prawem;
- projektodawca nie przewidział także jakichkolwiek negatywnych konsekwencji dla funkcjonariuszy bezpodstawnie sięgających po dane telekomunikacyjne.

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 do danych 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 powinna zostać dopuszczona jako wyjątek w przypadkach niecierpiących zwłoki.

[5] W tym kontekście należy zwrócić uwagę, że przyznanie sądom dodatkowych uprawnień wiąże się z dodatkowym obciążeniem budżetów sądów, tymczasem projektodawca nie przewiduje ich wzrostu.

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.

b. **Zasada subsydiarności**

Projektodawcy nie zakładają wprowadzenia do projektu zasady subsydiarności ograniczającej możliwość sięgania po dane do sytuacji, gdy inne środki okazały się bezskuteczne albo mogą być nieprzydatne.

Problem ten był poruszony przez Rzecznik Praw Obywatelskich we wniosku do Trybunału Konstytucyjnego, inicjującym postępowanie o sygn. K 23/11. W tym miejscu należy 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. 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".

Brak zasady subsydiarności wzmacnia fikcyjność kontroli sprawowanej przez sąd nad sięganiem po dane. Wobec braku przesłanek merytorycznych: niezbędności i subsydiarności ewentualna kontrola sądu będzie musiała sprowadzić się jedynie do weryfikacji kryteriów formalnych umożliwiających sięgnięcie po dane (np. czy funkcjonariusz miał właściwe upoważnienie i czy przestępstwo, w sprawie którego pobrano dane mieści się w katalogu przestępstw uprawniających konkretną służbę do sięgania po dane).

c. **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. Niezrozumiałe jest także zawarte w uzasadnieniu projektu ustawy stwierdzenie, jakoby wprowadzenie takiego obowiązku „pozostawałoby w sprzeczności z ustawowym wymogiem ochrony form i metod czynności operacyjno-rozpoznawczych oraz faktu ich prowadzenia".

Dodatkowo 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.

d. **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.

e. **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 zliczania realizowanych zapytań o dane telekomunikacyjne, a zarówno operatorzy

telekomunikacyjni, jak i poszczególne uprawnione podmioty stosują w tym zakresie różne standardy.

Fundacja Panoptykon co roku zbiera i 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 informacji uzyskanych przez Fundację od części uprawnionych podmiotów (policji, Straży Granicznej, Centralnego Biura Antykorupcyjnego, Agencji Bezpieczeństwa Wewnętrznego, Żandarmerii Wojskowej, kontroli skarbowej i Służby Celnej), 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 i Senatowi. W szczególności 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 – Parlamentowi.

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

Projekt poszerza katalog sytuacji, w których niektóre uprawnione podmioty mogą sięgać po dane telekomunikacyjne. Dla przykładu, w dotychczasowym stanie prawnym Policja uprawniona była do sięgania po dane „w celu zapobiegania lub wykrywania przestępstw". Natomiast zgodnie z projektem możliwe ma być sięganie przez Policję po dane „w celu rozpoznawania, zapobiegania, zwalczania, wykrywania albo uzyskania i utrwalenia dowodów przestępstw albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych".

Z kolei względem niektórych innych podmiotów, projekt nie zmienia obecnego katalogu sytuacji uprawniających do sięgania po dane. Dla przykładu CBA uprawnione jest do sięgania po dane telekomunikacyjne w celu realizacji zadań wymienionych w art. 2 ustawy o CBA, wśród których wymienione jest nie tylko rozpoznawanie i zapobieganie określonym przestępstwom, ale także m.in. prowadzenie działalności analitycznej dotyczącej zjawisk występujących w obszarze właściwości CBA.

Krytycznie oceniamy brak realizacji wytycznych płynących z wyroku TSUE i nieograniczenie katalogu przestępstw, w sprawie których możliwe jest sięganie po dane telekomunikacyjnej chociażby do przestępstw ściganych **z oskarżenia publicznego**. 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.

g. 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.

h. Niszczenie danych telekomunikacyjnych

Trybunał Konstytucyjny w wyroku K 23/11 uznał za niezgodne z Konstytucją przepisy ustaw o ABW, SKW i CBA w zakresie, w jakim nie przewidują zniszczenia danych niemających znaczenia dla prowadzonego postępowania. Komentowany projekt tylko częściowo odpowiada na ten problem, wprowadzając przepisy nakładające na wspomniane służby obowiązek niszczenia danych, które nie mają znaczenia dla postępowania karnego. Naszym zdaniem niezbędne jest również wprowadzenie przepisów zobowiązujących służby do cyklicznej oceny dalszej przydatności danych. Jedynie taki mechanizm uniemożliwi długotrwałe przetwarzanie danych telekomunikacyjnych, które w momencie początkowej oceny zostały uznane za przydatne, jednak później ta sytuacja uległa zmianie. Ocena przydatności danych powinna być także przeprowadzona względem danych, które dotychczas pobrały wspomniane służby, a których – wobec braku właściwych przepisów – nie zniszczyły, nawet wobec ich nieprzydatności dla dalszego postępowania. Wprowadzenie takich mechanizmów jest niezbędne dla zagwarantowania przestrzegania autonomii informacyjnej jednostki (art. 51 Konstytucji), zgodnie z którą niedopuszczalne jest przechowywanie informacji o obywatelach dłużej, niż jest to niezbędne w demokratycznym państwie prawa.

3. Podsumowanie

W ocenie Fundacji Panoptykon projekt jest niezgodny zarówno z prawem UE, jak i Konstytucją RP. Nie wprowadza on skutecznej kontroli nad sięganiem przez policję i inne służby po dane telekomunikacyjne. Zawarta w projekcie propozycja „kontroli" ma jedynie fasadowy charakter, ponieważ:

- ma charakter fakultatywny (sąd „może", nie musi jej przeprowadzić);
- sąd przeprowadzający kontrolę będzie miał dostęp jedynie do materiałów uzasadniających pobranie danych, a nie wszystkich materiałów postępowania. Kontrola będzie miała jedynie formalny charakter – sąd nie będzie oceniał, czy sięgnięcie po dane było konieczne i proporcjonalne.

Projekt oparty jest na rozwiązaniach zaproponowanych w minionej kadencji, które były słusznie krytykowane jako niezgodne z konstytucyjnym standardem ochrony prawa do prywatności. Ponadto w porównaniu z poprzednim, projekt wprowadza **słabsze** gwarancje ochrony praw człowieka, m.in. nie gwarantuje właściwej ochrony tajemnicy adwokackiej i nie ogranicza możliwości sięgania przez policję i inne służby po dane telekomunikacyjne jedynie do poważnych przestępstw.