Warszawa, 20 lipca 2015 r.

1652/2015/MPL/BGM

Szanowny Pan
Senator Piotr Zientarski
Komisja Ustawodawcza
Senat RP

Opinia do projektu ustawy
o zmianie ustawy o Policji oraz niektórych innych ustaw (druk senacki nr 967)

Celem opiniowanego projektu jest dostosowanie polskiego ustawodawstwa do wyroku Trybunału Konstytucyjnego z 30 lipca 2014 r. (sygn. K 23/11). Wyrok ten obejmuje swoim zakresem: po pierwsze, kwestie związane z zasadami prowadzenia kontroli operacyjnej, po drugie – zagadnienie zapewnienia odpowiedniej kontroli nad pozyskiwaniem przez uprawnione służby danych telekomunikacyjnych.

1. Cel i zakres projektu

Opiniowany projekt ma za zadanie docelowo realizować przede wszystkim sentencję i wytyczne wyroku Trybunału Konstytucyjnego z 30 lipca 2014 r. W ocenie Helsińskiej Fundacji Praw Człowieka, prawidłowe wykonanie wyroku Trybunału Konstytucyjnego w odniesieniu do drugiego zagadnienia wymaga uwzględnienia wytycznych wynikających z wyroku Trybunału Sprawiedliwości z 8 kwietnia 2014 r. w sprawie *Digital Rights Ireland*, którego przedmiotem była kwestia zgodności tzw. dyrektywy retencyjnej z Kartą Praw Podstawowych UE. Konieczność uwzględnienia wyroku Trybunału Sprawiedliwości wynika m.in. z faktu, że argumentacja Trybunału Konstytucyjnego była zbieżna ze wcześniejszymi ustaleniami Trybunału Sprawiedliwości, mimo iż nie znalazła odzwierciedlenia w samej sentencji wyroku.

Pierwotnie prace nad zmianami w systemie kontroli nad pozyskiwaniem danych telekomunikacyjnych przez służby prowadziła senacka Komisja Praw Człowieka, Praworządności i Petycji. Prace te miały na celu przede wszystkim realizację wniosków płynących z **raportu Najwyższej Izby Kontroli** nt. udostępniania danych telekomunikacyjnych[1]. Następnie Komisja Praw Człowieka, Praworządności i Petycji podjęła

1 Informacja o wynikach kontroli „Uzyskiwanie i przetwarzanie przez uprawnione podmioty danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180 c i d ustawy Prawo telekomunikacyjne" (Nr ewid. 107/2013/P/12/191/KPB).

00-018 Warszawa, ul. Zgoda 11; tel.: (48 22) 556-44-40, fax: (48 22) 556-44-50; e-mail: hfhr@hfhr.org.pl, www.hfhr.org.pl
NIP: 525-12-61-255, konto: PKO BP SA I O/Centrum 58 1020 1013 0000 0502 0002 9165, swift: BPKOPLPW

również próbę dostosowania obowiązujących przepisów do wymogów płynących z wyroku Trybunału Sprawiedliwości[2]. Jednak ostatecznie prace nad tym projektem[3] zostały porzucone[4] ze względu na podjęcie prac legislacyjnych przez Komisję Ustawodawczą nad projektem będącym przedmiotem niniejszej opinii (druk senacki nr 967).

Sentencja wyroku Trybunału Konstytucyjnego zobowiązuje ustawodawcę do dostosowania obowiązującego porządku prawnego do wymogów Konstytucji w zakresie:

1. zasad prowadzenia przez uprawnione służby **kontroli operacyjnej**, które swoim zakres powinny obejmować:
   1.1. sprecyzowanie przesłanki przedmiotowej prowadzenia kontroli operacyjnej przez ABW w zakresie jej kompetencji do rozpoznawania, zapobiegania i wykrywania „przestępstw godzących w podstawy ekonomiczne państwa" (art. 5 ust. 1 pkt 2 lit. b ustawy o ABW)
   1.2. zagwarantowanie, aby właściwy organ (sąd) zarządzający kontrolę operacyjną wskazywał (w postanowieniu o zarządzeniu kontroli) „określony w prawie rodzaj środka technicznego uzyskiwania informacji i dowodów oraz ich utrwalania stosowany w indywidualnej sprawie";
   1.3. stworzenie gwarancji procesowej polegającej na „niezwłocznym, komisyjnym i protokolarnym zniszczeniu materiałów zawierających informacje objęte zakazami dowodowymi, co do których sąd nie uchylił tajemnicy zawodowej bądź uchylenie było niedopuszczalne";

oraz

2. zasad zatrzymywania i udostępniania **danych telekomunikacyjnych**, tj:
   2.1. zapewnienia niezależnej kontroli udostępniania danych telekomunikacyjnych, o których mowa w art. 180c i art. 180d ustawy – Prawo telekomunikacyjne;
   2.2. wprowadzenia obowiązku niszczenia danych niemających znaczenia dla prowadzonego postępowania (art. 28 ustawy o ABW, art. 32 ustawy o SKW, art. 18 ustawy o CBA, art. 75d ust. 5 ustawy o Służbie Celnej).

2. Zmiany w zakresie zasad prowadzenia kontroli operacyjnej

2.1. Środki techniczne używane podczas kontroli operacyjnej

Trybunał Konstytucyjny orzekł, że m.in. art. 19 ust. 6 pkt 3 ustawy o Policji czy art. 27 ust. 6 pkt 3 ustawy o ABW – rozumiane w ten sposób, że właściwy organ zarządzający kontrolę operacyjną ma obowiązek wskazać określony w prawie rodzaj środka technicznego pozyskiwania informacji i dowodów oraz ich utrwalania stosowany w indywidualnej sprawie, są zgodne z art. 2 i art. 47 w związku z art. 31 ust. 3 Konstytucji.

---

2 Posiedzenie Komisji Praw Człowieka, Praworządności i Petycji z 13 maja 2014 r. Przedmiotem posiedzenia było omówienie wpływu orzeczenia Trybunału Sprawiedliwości UE z dnia 8 kwietnia 2014 roku w sprawie *Digital Rights Ireland* na zasady korzystania przez policję i inne organy publiczne z danych telekomunikacyjnych dla celów zapobiegania i zwalczania przestępczości. Program posiedzenia: http://senat.gov.pl/gfx/senat/userfiles/_public/k8/komisje/2014/kpcpp/materialy/140513p1.pdf.

3 Dostępny na stronie: http://www.senat.gov.pl/gfx/senat/userfiles/_public/k8/komisje/2015/kpcpp/materialy/bilingi/wniosek_nik_bilingi0312002014022109572 4.pdf.

4 Posiedzenie Komisji Praw Człowieka, Praworządności i Petycji w dniu 7 lipca 2015 r.

Obecne brzmienie przepisów poszczególnych ustaw służbowych przyznających kompetencje do prowadzenia kontroli operacyjnej oparte jest o brzmienie ustawy o Policji, która w art. 19 ust. 6 przewiduje, że kontrola operacyjna prowadzona jest niejawnie i polega na:

1) kontrolowaniu treści korespondencji;
2) kontrolowaniu zawartości przesyłek;
3) stosowaniu środków technicznych umożliwiających uzyskiwanie w sposób niejawny informacji i dowodów oraz ich utrwalanie, a w szczególności treści rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych.

Trybunał ocenił, że art. 19 ust. 6 pkt 3 spełnia standard precyzji przepisu zezwalającego na ingerencję w prawo do prywatności. Prokonstytucyjna wykładnia normy wynikającej z tego przepisu została oparta o obowiązek wskazania przez sąd zarządzający kontrolę operacyjną określonego w prawie rodzaju środka technicznego pozyskiwania informacji. Jak słusznie zauważył Trybunał ustawodawca nie sprecyzował elementów, jakie ma zawierać postanowienie sądu o zarządzeniu kontroli operacyjnej. Zawiera je jednak, m.in. rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 10 czerwca 2011 r. w sprawie sposobu dokumentowania prowadzonej przez Policję kontroli operacyjnej, przechowywania i przekazywania wniosków, zarządzeń i materiałów uzyskanych podczas stosowania tej kontroli, a także przetwarzania i niszczenia tych materiałów[5] lub analogiczne rozporządzenie Prezesa Rady Ministrów odnoszące się do Agencji Bezpieczeństwa Wewnętrznego. Przewidują one, że sąd okręgowy zarządzający kontrolę operacyjną wskazuje w postanowieniu „rodzaj stosowanej kontroli operacyjnej"[6].

Projektodawca w uzasadnieniu projektu wskazał, że „wychodząc naprzeciw oczekiwaniom Trybunału odnośnie sprecyzowania w przepisach prawa zamkniętego rodzajowo katalogu środków i metod działania (...) ustawodawca (...) określił sposoby prowadzenia kontroli operacyjnej"[7]. **Niestety nie odpowiada temu brzmienie m.in. projektowanego art. 19 ust. 6 ustawy o Policji**:

„6. Kontrola operacyjna prowadzona jest niejawnie i polega na:
1) podsłuchu rozmów prowadzonych przy użyciu środków technicznych;
2) podsłuchu i podglądzie pomieszczeń i osób poza miejscami publicznymi;
3) kontroli treści korespondencji;
4) nadzorze elektronicznym osób, miejsc i przedmiotów oraz środków transportu."

W uzasadnieniu wyroku Trybunału Konstytucyjnego wskazano na potrzebę sprecyzowania „w przepisach prawa **zamkniętego rodzajowo katalogu środków i metod działania**, za pomocą których władze publiczne mogą w sposób niejawny gromadzić informacje o jednostkach". Trybunał zaznaczył przy tym słusznie, że „nie chodzi o wskazanie parametrów technicznych, ale **rodzajowych nazw poszczególnych środków i informacji możliwych do pozyskania** za ich pomocą (np. „podsłuch rozmów telefonicznych", „podsłuch i podgląd pomieszczeń i osób", „podsłuch techniczny środków łączności przewodowej i radiowej", „nadzór elektroniczny osób,

5 Dz.U. 2011 nr 122 poz. 697; Rozporządzenie zostało zmienione przez Rozporządzenie Ministra Spraw Wewnętrznych z dnia 10 marca 2014 r. zmieniające rozporządzenie w sprawie sposobu dokumentowania prowadzonej przez Policję kontroli operacyjnej, przechowywania i przekazywania wniosków, zarządzeń i materiałów uzyskanych podczas stosowania tej kontroli, a także przetwarzania i niszczenia tych materiałów (Dz.U. 2014 poz. 396) oraz Rozporządzenie Ministra Spraw Wewnętrznych z dnia 3 października 2014 r. zmieniające rozporządzenie w sprawie sposobu dokumentowania prowadzonej przez Policję kontroli operacyjnej, przechowywania i przekazywania wniosków, zarządzeń i materiałów uzyskanych podczas stosowania tej kontroli, a także przetwarzania i niszczenia tych materiałów (Dz.U. 2014 poz. 1357).

6 „Sąd Okręgowy (...) postanawia ZARZĄDZIĆ/PRZEDŁUŻYĆ/ODMÓWIĆ ZARZĄDZENIA/PRZEDŁUŻENIA kontrolę(-li) operacyjną(-nej) polegającą(-cej) na ...**[rodzaj stosowanej kontroli operacyjnej]**".

7 s. 7 uzasadnienia.

miejsc i przedmiotów oraz środków transportu", „nadzór elektroniczny środków łączności przewodowej lub radiowej")". Trybunał uznał, że docelowo rodzaje tych środków technicznych powinny zostać uregulowane w ustawie. „Zasadne jest tym samym, by to parlament zaakceptował dopuszczalność stosowania rodzajów środków technicznych, które w szerokim zakresie ingerują w wolności i prawa człowieka".

Projektowany przepis w dalszym ciągu jest bardzo ogólny. Ponadto wydaje się, że pojęcie „rozmowy", o których mowa w pkt 1 mieszczą się w pojęciu „korespondencji", o którym mowa w pkt 3. Zwrócił na to również uwagę Trybunał Konstytucyjny na gruncie obowiązujących obecnie przepisów: Zdaniem Trybunału, wyrażenie „kontrola treści korespondencji" nie zawęża się jedynie do tradycyjnej formy wymiany informacji, lecz obejmuje każdy sposób przekazywania informacji pomiędzy jednostkami, bez względu na formę (tradycyjna poczta, e-mail, SMS, MMS itp.).

Dla porównania poselski projekt ustawy o czynnościach operacyjno-rozpoznawczych skierowany do Sejmu VI kadencji (druk sejmowy nr 353) przewidywał nieco bardziej uszczegółowiony katalog środków technicznych (art. 2 ust. 3 pkt 10 projektu):

a) podsłuch rozmów telefonicznych,
b) podsłuch i podgląd pomieszczeń i osób,
c) podsłuch techniczny środków łączności przewodowej i radiowej,
d) nadzór elektroniczny osób, miejsc i przedmiotów oraz środków transportu,
e) nadzór elektroniczny środków łączności przewodowej i radiowej[8].

Wątpliwości Fundacji co do zgodności projektowanej regulacji z wymogami wynikającymi z Konstytucji[9] wynikają m.in. z postępowań sądowych prowadzonych przez Fundację przeciwko poszczególnym służbom w sprawie wniosków o dostęp do informacji publicznej. Przykładowo, Helsińska Fundacja Praw Człowieka skierowała do Centralnego Biura Antykorupcyjnego wniosek o udostępnienie informacji na temat korzystania przez CBA z oprogramowania „Remote Control System". System ten (RCS) umożliwia monitorowanie komputerów i telefonów, pozyskiwanie danych przechowywanych na tych urządzeniach, nawet w sytuacji gdy użytkownik nie jest podłączony do Internetu oraz śledzenie korespondencji w Internecie. RCS pozwala także kopiować pliki z dysku twardego komputera, nagrywać rozmowy Skype, przechwytywać hasła wprowadzone do wyszukiwarki, włączyć kamerę internetową lub mikrofon komputera. Centralne Biuro Antykorupcyjne odmówiło udzielenia wnioskowanej informacji[10], podczas gdy Agencja Bezpieczeństwa Wewnętrznego poinformowała, że takiego oprogramowania nie stosuje[11]. Ostatnie doniesienia medialne nt. ataku na serwery firmy Hacking Team – producenta oprogramowania RCS – wskazują, że Centralne Biuro Antykorupcyjne wykupiło licencję na ten program. **W świetle brzmienia projektowanych przepisów nadal nie jest jasne czy na ich gruncie zakup takiego oprogramowania przez Policję, ABW czy CBA a następnie ich stosowanie jest dopuszczalne**

8 Art. 14 ust. 6 projektu ustawy o czynnościach operacyjno-rozpoznawczych przewidywał, że kontrola operacyjna prowadzona jest niejawnie i polega na: 1) kontrolowaniu treści korespondencji, 2) kontrolowaniu zawartości przesyłek, 3) stosowaniu środków technicznych umożliwiających uzyskiwanie w sposób niejawny informacji i dowodów oraz ich utrwalanie, a w szczególności treści rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych, 4) tajnej lustracji pomieszczeń i środków transportu.

9 Trybunał wskazał, że „pożądane jest określenie w ustawie rodzajów środków niejawnego pozyskiwania informacji, a także rodzajów informacji pozyskiwanych za pomocą poszczególnych środków".

10 Por. Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 13 lutego 2015 r., sygn. II SA/Wa 1670/14.

11 http://www.hfhrpol.waw.pl/precedens/aktualnosci/abw-nie-stosuje-narzedzi-do-zdalnego-kontrolowania-komputerow-i-telefonow.html

na gruncie definicji kontroli operacyjnej. Nierozstrzygniętym problemem pozostaje również to czy dopuszczalne jest stosowanie takiego oprogramowania poza procedurą kontroli operacyjnej, np. w ramach kompetencji Agencji Wywiadu to prowadzenia wywiadu elektronicznego (art. 6 ust. 1 pkt 8 ustawy o ABW i AW).

2.2. Termin prowadzenia kontroli operacyjnej

Projekt przewiduje doprecyzowanie terminu prowadzenia kontroli operacyjnej na podstawie art. 19 ust. 9 ustawy o Policji. Odnosi się on do sytuacji, gdy podczas stosowania kontroli operacyjnej pojawią się nowe okoliczności istotne dla zapobieżenia lub wykrycia przestępstwa albo ustalenia sprawców i uzyskania dowodów przestępstwa. Wówczas możliwe jest przedłużenie przez sąd prowadzenia kontroli operacyjnej nawet po upływie terminów z art. 19 ust. 8 ustawy o Policji, tj. 6 miesięcy. Projekt zakłada, że to wyjątkowe przedłużenie prowadzenia kontroli operacyjnej będzie możliwe na okres oznaczony nie dłuższy niż **12 miesięcy**, przez co łączne prowadzenie kontroli operacyjne będzie mogło trwać nawet **18 miesięcy**.

W uzasadnieniu nie wskazano jednak czemu projektodawca zaproponował aż tak długi okres. Projektodawca wydaje się porównywać ten okres z 12 miesięcznym terminem retencji danych telekomunikacyjnych. Porównanie to jednak jest zupełnie nieadekwatne. **W ocenie Fundacji powinien on być nie dłuższy niż okres prowadzenia kontroli operacyjnej przewidziany w ustępie 8, tj. 6 miesięcy**. Co więcej projektodawca nie przedstawił informacji jak obecnie wygląda praktyka w zakresie stosowania art. 19 ust. 9, w którym termin nie został w ogóle oznaczony. **Uzyskanie takich informacji wydaje się niezbędne na dalszych etapach prowadzenia prac legislacyjnych nad projektem.**

Odmienny standard zastosowano na gruncie przepisów ustawy o CBA, ABW czy SKW. Przewidują one, że w sytuacji pojawienia się nowych istotnych okoliczności dla zapobieżenia lub wykrycia przestępstwa albo ustalenia sprawcy i uzyskania dowodów przestępstwa, „sąd (...) może wydawać, również po upływie okresów, o których mowa w ust. 8, kolejne **postanowienia** o przedłużeniu kontroli operacyjnej **na następujące po sobie okresy**, z których **żaden** nie może trwać dłużej niż **12 miesięcy**". **Tym samym projektodawca nie ustanawia *de facto* i *de iure* maksymalnego okresu prowadzenia kontroli operacyjnej przez CBA, ABW i SKW**. W uzasadnieniu wskazano, że takie zróżnicowanie wynika ze specyfiki zadań realizowanych przez służby specjalne. „*Przyjęcie takiego rozwiązania w odniesieniu do służb specjalnych jest niezbędne z perspektywy bieżących zagrożeń, m.in. w kontekście przyjmowanego obecnie modus operandi sprawców takich przestępstw jak przestępstwa o charakterze terrorystycznym, sabotaż, czy szpiegostwo, wykorzystujących tzw. uśpione ogniwo.*" - wskazano w uzasadnieniu[12]. **Problem polega jednak na tym, że żadnego z tych przestępstw nie ściga Centralne Biuro Antykorupcyjne.**

Projektodawca powołuje się przy tym na stanowisko Trybunału Konstytucyjnego, który zaznaczył, że „nie jest wykluczone zróżnicowanie intensywności ochrony prywatności, autonomii informacyjnej oraz tajemnicy komunikowania się z uwagi na to, czy dane o osobach pozyskują służby wywiadowcze i zajmujące się ochroną bezpieczeństwa państwa, czy też czynią to służby policyjne". Projektowana regulacja (m.in. art. 27 ust. 9 ustawy o ABW czy art. 17 ust. 9 ustawy CBA) w zestawieniu z powyższym standardem rodzi szereg wątpliwości. Po pierwsze, w świetle powyższych kryteriów nie wydaje się, aby Centralne Biuro Antykorupcyjne spełniało kryterium służby wywiadowczej ani służby zajmującej się ochroną bezpieczeństwa państwa. Po drugie, przedstawione uzasadnienie projektu opiera się na wnioskowaniu „z mniejszego na większe". W oparciu o prawdopodobną specyfikę *modus operandi* niektórych przestępstw (np. o charakterze

12 s. 8 uzasadnienia.

terrorystycznym) proponuje się stworzyć normę generalną mającą zastosowanie do wszystkich przestępstw ściganych np. przez ABW (np. niektórych przestępstw określonych w kodeksie karnym skarbowym)[13].

W ocenie Fundacji **rozwiązanie zaproponowane w art. 27 ust. 9 ustawy o ABW, art. 17 ust. 9 ustawy o CBA oraz art. 31 ust. 7 ustawy o SKW jest nieproporcjonalnym wkroczeniem w prawo do prywatności oraz tajemnicę korespondencji**. Realizacja zamierzeń projektodawcy odnosząca się do specyfiki niektórych przestępstw (zresztą niezwykle lakonicznie przedstawiona w uzasadnieniu projektu) powinna być precyzyjnie powiązana z poszczególnymi przestępstwami (np. sabotażu albo o charakterze terrorystycznym). W odniesieniu do pozostałych przestępstw, standard precyzji przepisów dotyczących czasu trwania kontroli operacyjnej powinien być zbliżony do terminów prowadzenia kontroli operacyjnej przez Policję, tj. nie powinien przekraczać 6 miesięcy (art. 19 ust. 8) przedłużony maksymalnie o kolejne 6 miesięcy (po spełnieniu przesłanej z art. 19 ust. 9).

2.3. Niszczenie materiałów kontroli operacyjnych zawierających tajemnice zawodowe

Kolejny wymóg wynikający z wyroku Trybunału Konstytucyjnego odnoszący się do zasad prowadzenia kontroli operacyjnej wiąże się z obowiązkiem zapewnienia ochrony tajemnicy zawodowej, o której mowa w art. 180 § 2 k.p.k. oraz tajemnicy obrończej i tajemnicy spowiedzi (art. 178 k.p.k.). Trybunał orzekł, że m.in. art. 19 ustawy o Policji jest niezgodny z art. 42 ust. 2, art. 47, art. 49, art. 51 ust. 2 i art. 54 ust. 1 w związku z art. 31 ust. 3 Konstytucji **w zakresie, w jakim nie przewidują gwarancji niezwłocznego, komisyjnego i protokolarnego zniszczenia materiałów zawierających informacje objęte zakazami dowodowymi, co do których sąd nie uchylił tajemnicy zawodowej bądź uchylenie było niedopuszczalne.**

Projekt wprowadza w poszczególnych ustawach specjalną procedurę zawartą m.in. w art. 19 ust. 15f-15i ustawy o Policji. Procedura ta odmiennie traktuje informacje, o których mowa w art. 178 k.p.k., odmiennie zaś tajemnice zawodowe z art. 180 § 2 k.p.k. **Wydaje się, że stoi to w sprzeczności ze standardem, który Trybunał zastosował jednakowo w odniesieniu do obu rodzaju informacji.**

W przypadku tajemnicy obrończej[14] i tajemnicy spowiedzi właściwy komendant Policji nakazuje niezwłoczne, komisyjne i protokolarne zniszczenie materiałów zawierających te informacje (art. 19 ust. 15f pkt 1). Natomiast w odniesieniu do tajemnicy zawodowej, o której mowa w art. 180 § 2 k.p.k. projekt przewiduje obowiązek przekazania materiałów prokuratorowi (art. 19 ust. 15f pkt 2 ustawy o Policji), który następnie kieruje je obowiązkowo do sądu wraz z wnioskiem o 1. wyrażenie zgody na ich wykorzystanie w postępowaniu karnym albo 2. wydanie zarządzenia o niezwłocznym komisyjnym, protokolarnym zniszczeniu.

Nie jest przy tym jasne jaki jest cel przekazania tych informacji prokuratorowi, jeśli nie jest on w stanie nakazać zniszczenia tych materiałów Policji, a jedynie może wnioskować do sądu o takie zniszczenie. Projektowany przepis nie wyraża nadzorczej roli prokuratora w procedurze kontroli

13 Projekt przewiduje daleko idące uporządkowanie kompetencji ABW zawartych art. 5 ust. 1 ustawy o ABW. Rozwiązanie to stanowi kopię propozycji rządowej z 2014 r. (por. projekt ustawy o ABW, druk sejmowy nr 2295).

14 Art. 178 pkt 1 k.p.k. w brzmieniu obowiązującym od 1 lipca 2015 r. odwołuje się do „obrońcy albo adwokata lub radcy prawnego działającego na podstawie art. 245 § 1, co do faktów, o których dowiedział się udzielając porady prawnej lub prowadząc sprawę".

operacyjnej. Prowadzi jedynie do poszerzenia kręgu osób, które mogą się zapoznać z informacjami zawierającymi tajemnice zawodowe znajdującymi w materiałach z kontroli operacyjnej.

Art. 19 ust. 15h ustawy o Policji przewiduje, że sąd wydaje – w terminie 14 dni – postanowienie w przedmiocie wniosków prokuratora. Przepis ten nie wskazuje jednak **jakie przesłanki sąd bierze pod uwagę** wydając postanowienie na podstawie tego przepisu. W przypadku, o którym mowa art. 180 § 2 k.p.k., sąd może wyrazić zgodę na przesłuchanie osób zobowiązanych do zachowania tajemnicy notarialnej, adwokackiej, radcy prawnego, doradcy podatkowego, lekarskiej, dziennikarskiej lub statystycznej ***„tylko wtedy, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu"***. Taka przesłanka nie występuje na gruncie ust. 15h co może oznaczać dowolność po stronie sądu podejmującego decyzje w przedmiocie wniosków prokuratora.

Co więcej, w odróżnieniu z procedurą z art. 180 § 2 k.p.k. projekt przewiduje że na postanowienie sądu z art. 19 ust. 15h ustawy o Policji nie przysługuje zażalenie stronie objętej kontrolą operacyjną. Jest to zatem o wiele niższy poziom ochrony tajemnicy zawodowej (adwokackiej czy dziennikarskiej) niż ma to miejsce na etapie procesowym[15], mimo iż w uzasadnieniu projektodawca wskazał, że „nie ma żadnych uzasadnionych podstaw, by na tym etapie postępowania stosować łagodniejsze standardy niż przewidziane w postępowaniu karnym"[16].

W ocenie Helsińskiej Fundacji Praw Człowieka, projektowana procedura nie wykonuje standardu zawartego w orzeczeniu Trybunału Konstytucyjnego.

2.4. Wykonanie postanowienia sygnalizacyjnego S 2/06

Uzasadnienie projektu odwołuje się do wymogu płynącego z postanowienia sygnalizacyjnego Trybunału Konstytucyjnego z 25 stycznia 2006 r. (sygn. S 2/06). Trybunał wskazał na potrzebę uregulowania obowiązku informowania osób objętych kontrolą operacyjną o fakcie jej prowadzenia. Trybunał argumentował, że *„istnienie takiego obowiązku policji byłoby zapewne wskazane i odpowiadałoby potrzebie efektywnej instrumentalizacji proceduralnej konstytucyjnego prawa określonego w art. 51 ust. 4 Konstytucji. Podobny problem w innych państwach europejskich doprowadził do podwyższenia standardu gwarancji proceduralnych (na tle sprawy Klass i inni wprowadzono w niemieckim ustawodawstwie, pozytywny obowiązek informacji o prowadzonej, zakończonej kontroli operacyjnej)*". Wskazał na to również Trybunał Konstytucyjny w wyroku z 30 lipca 2014 r. wskazując wśród standardów konstytucyjnych odnoszących się do prowadzonych czynności operacyjno-rozpoznawczych wymóg *„unormowania procedury informowania jednostek o niejawnym pozyskaniu informacji na ich temat, w rozsądnym czasie po zakończeniu działań operacyjnych i zapewnienie na wniosek zainteresowanego poddania sądowej ocenie legalności zastosowania tych czynności; odstępstwo jest dopuszczalne wyjątkowo*".

Projektodawca nie podziela jednak konkluzji płynących z postanowienia sygnalizacyjnego z 2006 r. oraz z wyroku z 2014 r. i wskazuje na trzy rodzaje przeszkód związanych z wykonaniem postanowienia sygnalizacyjnego:

- „wiązałoby się z naruszeniem podstawowych zasad na podstawie których funkcjonują służby i poważnie mogłoby zaważyć na skutecznym działaniu służb, ale także mogłoby zagrozić bezpieczeństwu Sił Zbrojnych RP oraz osób, które w niejawny sposób udzielają pomocy służbom"

15 Zgodnie z art. 180 § 2 zd. 3 na postanowienie sądu przysługuje zażalenie.

16 s. 5 uzasadnienia

- wiązałoby się z tym trudności z ustaleniem danych osób z uwagi na znaczną skalę używania tzw. telefonów pre-paid
- obowiązek informowania pozostawałby w sprzeczności z ustawowym wymogiem ochrony form i metod czynności operacyjno-rozpoznawczych oraz faktu ich prowadzenia.

Wspomniany obowiązek ochrony form i metod jest obowiązkiem wynikającym z ustawy, podczas gdy obowiązek informowania jednostki o prowadzeniu wobec niej kontroli operacyjnej wynika z przywołanej interpretacji art. 51 ust. 4 Konstytucji. Należy zatem przede wszystkim zadać sobie pytanie czy ustawowy obowiązek ochrony form i metod w takim zakresie w jakim wynika z ustaw resortowych jest zgodny z Konstytucją. Odmienna argumentacja oparta o twierdzenie iż wymóg wynikający z Konstytucji jest niezgodny z unormowaniem ustawowym nie znajduje oparcia w konstytucyjnej hierarchii źródeł prawa powszechnie obowiązującego.

W ocenie Helsińskiej Fundacji Praw Człowieka wykonanie wyroku Trybunału Konstytucyjnego z 30 lipca 2014 r. wymaga implementowania postanowienia sygnalizacyjnego Trybunału z 25 stycznia 2006 r.

3. Dane telekomunikacyjne

Jak zostało wskazane na początku, wyrok Trybunału Konstytucyjnego odnoszący się zasad pozyskiwania przez służby danych telekomunikacyjnych zobowiązuje ustawodawcę do:

1. zapewnienia niezależnej kontroli udostępniania danych telekomunikacyjnych, o których mowa w art. 180c i art. 180d ustawy – Prawo telekomunikacyjne;
2. wprowadzenia obowiązku niszczenia danych niemających znaczenia dla prowadzonego postępowania (art. 28 ustawy o ABW, art. 32 ustawy o SKW, art. 18 ustawy o CBA, art. 75d ust. 5 ustawy o Służbie Celnej).

Drugi z powyższych wymogów projektodawca realizuje dodając do obowiązujących przepisów nowe jednostki redakcyjne (np. art. 28 ust. 6 ustawy o ABW i AW, art. 18 ust. 6 ustawy o CBA, art. 75d ust. 6 ustawy o Służbie Celnej), które analogicznie przewidują, że „materiały uzyskane w wyniku czynności związanych z udostępnieniem danych telekomunikacyjnych, które nie zawierają informacji mających znaczenie dla postępowania karnego lub postępowania karnego skarbowego, podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu".

Wykonanie jednak pierwszego wymogu dotyczącego zapewnienia niezależnej kontroli udostępniania danych telekomunikacyjnych wymaga od ustawodawcy szerzej zakrojonych działań. Wskazał na to m.in. przedstawiciel Prokuratora Generalnego podczas posiedzenia senackiej Komisji Ustawodawczej w dniu 8 czerwca 2015 r.[17] Z takim stanowiskiem zgodził się wówczas przedstawiciel Ministra Spraw Wewnętrznych, który wskazał zespół rządowy pracujący nad projektem wykonującym wyrok Trybunału Konstytucyjnego nie koncentruje się jedynie na sentencji wyroku, ale również bierze pod uwagę kwestie związane z dyrektywą retencyjną. Należy jednak wyraźnie podkreślić, że wbrew tym zapewnieniom, projekt nie realizuje wytycznych wynikających z wyroku Trybunału Sprawiedliwości, który sformułował pod adresem dyrektywy szereg zarzutów, które skutkowały ostatecznie uznaniem jej za nieważną:

17 Obecny na posiedzeniu przedstawiciel Prokuratora Generalnego wskazał, że przy wykonaniu tego wyroku projektodawcy będą musieli uwzględnić duże szersze tło wynikające, w szczególności, z wyroku Trybunału Sprawiedliwości. Wskazał on również, że deficyty dyrektywy retencyjnej są odzwierciedlone w polskim prawie.

- bardzo szeroki zakres dyrektywy i gromadzonych na jej podstawie danych co skutkuje brakiem wyłączeń m.in. wobec osób których komunikacja objęta jest tajemnicą zawodową;
- brak kryteriów do określenia najpoważniejszych przestępstw, które uzasadniałyby dostęp do tych danych;
- brak wymogów odnoszących się do **uprzedniej kontroli**, tym samym - brak gwarancji ochrony przed nadużyciami;
- brak zależności między okresem retencji a rodzajem przechowywanych danych oraz brak kryteriów co do czasu ich zatrzymania (duża rozbieżność między okresem minimalnym i maksymalnym);
- brak regulacji dotyczących odpowiedniego zabezpieczenia danych przez podmioty prywatne, w szczególności w odniesieniu do obowiązku zatrzymania danych na obszarze Unii, co powoduje, że nie można zagwarantować kontroli poszanowania wymogów ochrony i bezpieczeństwa.

Projekt nie uwzględnia również postulatów wynikających z raportu Najwyższej Izby Kontroli, będący punktem wyjście do prac legislacyjnych Komisji Praw Człowieka, Praworządności i Petycji. W informacji o wynikach kontroli „Uzyskiwanie i przetwarzanie przez uprawnione podmioty danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180 c i d ustawy Prawo telekomunikacyjne", zawarto szereg wniosków i zaleceń - skierowanych pod adresem Prezesa Rady Ministrów – mających na celu:

- doprecyzowanie **zakresu danych**, które powinny podlegać retencji;
- weryfikację **katalogu spraw**, na potrzeby których dane telekomunikacyjne mogą być przez uprawnione służby pozyskiwane;
- przeanalizowanie możliwości wprowadzenia dodatkowych **rozwiązań o charakterze gwarancyjnym**, ograniczających możliwość pozyskiwania danych retencyjnych w stosunku do osób wykonujących tzw. „zawody zaufania publicznego";
- ustanowienie **kontroli zewnętrznej** nad procesem pozyskiwania danych, obejmującej weryfikację zasadności ich pozyskiwania;
- wprowadzenie skutecznych instrumentów gwarantujących **niezwłoczne niszczenie** pozyskanych danych w sytuacji, gdy nie są już one dalej niezbędne dla osiągnięcia celów prowadzonego postępowania;
- ustanowienie **mechanizmów sprawozdawczych**, które zapewnią rzetelną informację o zakresie pozyskiwania danych telekomunikacyjnych;
- wprowadzenie przepisów gwarantujących osobom, których dane bilingowe były pobierane, **prawa do informacji o zakresie i czasie zbierania tych danych**, po zakończeniu w danej sprawie czynności – wyjątki w tym zakresie powinny określić przepisy ustawy;
- opracowanie wytycznych dotyczących technicznych i organizacyjnych **środków bezpieczeństwa** w zakresie uzyskiwania dostępu do danych, w tym procedur ich przekazywania;
- wzmocnienie, do czasu wprowadzenia zmian systemowych, **nadzoru** nad wykorzystaniem przez organy państwa uprawnień w zakresie pozyskiwania danych obywateli.

3.1. Projekt ustawy a wymogi płynące z wyroku Trybunału Sprawiedliwości w sprawie *Digital Rights Ireland*

Niestety projekt całkowicie pomija wymogi i wskazówki płynące z wyroku Trybunału Sprawiedliwości w sprawie *Digital Right Ireland*. Co prawda wyrok skutkuje przede wszystkim unieważnieniem dyrektywy retencyjnej, to jednak należy mieć na uwadze, że stanowi on element dorobku konstytucyjnego Unii Europejskiej, zaś orzecznictwo Trybunału Sprawiedliwości jest wiążące dla Państw Członkowskich.

Z całą pewnością skutkiem wyroku jest konieczność przeanalizowania regulacji krajowej pod kątem ich zgodności z art. 15 dyrektywy 2002/58 o prywatności i łączności elektronicznej[18]. Dopuszcza on możliwość wprowadzenia przez Państwa Członkowskie ograniczeń od zasad ochrony danych osobowych, m.in. danych o ruchu[19] pod warunkiem, że „takie ograniczenia stanowią środki **niezbędne, właściwe i proporcjonalne** w ramach społeczeństwa demokratycznego do zapewnienia bezpieczeństwa narodowego (m.in. bezpieczeństwa państwa), obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania przestępstw kryminalnych lub niedozwolonego używania systemów łączności elektronicznej".

W ocenie Helsińskiej Fundacji Praw Człowieka elementem wykonania wyroku w sprawie *Digital Rights Ireland* powinno być **zweryfikowanie czy obecny system retencji danych telekomunikacyjnych na gruncie Prawa telekomunikacyjnego jest zgodny z art. 15 dyrektywy 2002/58**. Z kolei do przeprowadzenia tej weryfikacji niezbędne może się okazać skorzystanie ze wskazówek zawartych właśnie w wyroku *Digital Rights Ireland*[20]. Trybunał Sprawiedliwości ocenił bowiem, że zakres danych gromadzonych jest niezmiernie szeroki, nie przewiduje żadnych wyłączeń podmiotowych, co umożliwia zbieranie informacji dotyczących życia prywatnego wszystkich obywateli Unii Europejskiej. **Tymczasem opiniowany projekt nie zawiera żadnej analizy co do jego zgodności z prawem UE.** Na samym końcu uzasadnienia projektu wskazano jedynie, że „zakres przedmiotowy projektowanej ustawy jest zgodny z prawem UE".

Brak analizy projektu pod kątem jego zgodności z prawem Unii Europejskiej może się okazać jego najpoważniejszym mankamentem, w szczególności w świetle ostatniego wyroku z 17 lipca 2015 r. High Court of Justice w sprawie ***David Davis and others -v- Secretary of State for the Home Department***[21]. Przedmiotem sprawy była ocena (przez sąd krajowy) zgodności z prawami człowieka brytyjskiego prawa krajowego dotyczącego retencji danych telekomunikacyjnych (*Data Retention and Investigatory Powers Act 2014*) uchwalonego w lipcu 2014, tj. już po ogłoszeniu wyroku przez Trybunał Sprawiedliwości. Pomimo iż dyrektywa retencyjna nie jest aktem obowiązującym, High Court of Justice ocenił, że kwestie związane z zasadami ochrony danych osobowych (a tym samym również ograniczeń takich danych) objęte są prawem Unii Europejskiej od ponad 20 lat. Z kolei analiza wyroku *Digital Rights Ireland* doprowadziła sąd brytyjski do wniosku, że prawodawstwo ustanawiające generalny reżim retencji danych telekomunikacyjnych narusza prawa z art. 7 i 8 Karty Praw Podstawowych, chyba że towarzyszy takiemu reżimowi system, który gwarantuje adekwatne zabezpieczenia dla ochrony tych praw[22]. High Court of Justice

18 Dyrektywa 2002/58/WE parlamentu europejskiego i rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej.; J. Raughofer, D.M. Sitgigh, *The Data Retention Directive Never Existed*, SrpitEd 1/2014, s. 126.

19 Art. 6 dyrektywy 2002/58.

20 Podobne stanowisko zostało wyrażone w opinii prawnej zamówionej przez Parlament Europejski „LIBE - Questions relating to the judgment of the Court of Justice of 8 April 2014 in Jolned Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and others - Directive 2006/24/EC on data retention - Consequences of the judgment (Legal Opinion), 22 grudnia 2014 r. (dokument dostępny jest na stronie http://www.statewatch.org/news/2015/apr/ep-ls-opinion-digital-rights-judgment.pdf); S. Peers, Are national data retention laws within the scope of the Charter? - http://eulawanalysis.blogspot.com/2014/04/are-national-data-retention-laws-within.html.

21 Sprawa [2015] EWHC 2092 (Admin), Case No: CO/3665/2014, CO/3667/2014, CO/3794/2014. Wyrok dostępny jest na stronie:https://www.judiciary.gov.uk/judgments/david-davis-and-others-v-secretary-of-state-for-the-home-department/.

22 § 89 uzasadnienia wyroku.

uznał *Data Retention and Investigatory Powers Act 2014* za niezgodny z prawem Unii Europejskiej ponieważ:

- nie zawiera jasnych i precyzyjnych reguł ograniczających korzystanie z danych telekomunikacyjnych jedynie do ścigania najpoważniejszych przestępstw;
- dostęp do danych telekomunikacyjnych nie zależy od wcześniejszej kontroli ze strony sądu lub niezależnego organu administracyjnego, którego decyzje mogłyby taki dostęp ograniczyć i gwarantować że sąd wykorzystywane do ścigania najpoważniejszych przestępstw[23].

Z kolei opiniowany projekt nie zawiera żadnej propozycji zróżnicowania poszczególnych rodzajów danych telekomunikacyjnych według głębokości ingerencji w prawo do prywatności i skutkującym zróżnicowaniem mechanizmów kontroli według poszczególnych rodzajów danych. Brak również w projekcie jakichkolwiek odniesień do wymogów zapewnienia bezpieczeństwa danych gromadzonych przez operatorów telekomunikacyjnych, w szczególności w odniesieniu do obowiązku zatrzymania danych na obszarze Unii Europejskiej.

Co więcej, dyrektywa retencyjna przewidywała, że dostęp do zgromadzonych danych telekomunikacyjnych będzie możliwy „celu dochodzenia, wykrywania i ścigania poważnych przestępstw" (art. 1 ust. 1). Tymczasem polskie przepisy krajowe umożliwiają obecnie sięganie po te dane w przypadku ścigania wszystkich przestępstw, które znajdują zakresie zadań danej służby. Obecne brzmienie art. 20c ustawy o Policji przewiduje, że „w celu zapobiegania lub wykrywania przestępstw Policja może mieć udostępniane dane, o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (...)". Projektowane brzmienie art. 20c ustawy o Policji praktycznie nie wprowadza żadnych zmian w tym zakresie: „W celu rozpoznawania, zapobiegania, zwalczania, wykrywania albo uzyskania i utrwalenia dowodów przestępstw ściganych z oskarżenia publicznego albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych". Można wręcz odnieść wrażenie, że podstawa do uzyskiwania danych telekomunikacyjnych przez Policję została poszerzona. **Zaproponowanie zmian w katalogu przestępstw dających podstawę do wykorzystania danych telekomunikacyjnych wymagałoby jednak przeprowadzenia odpowiednich analiz w tym zakresie, w szczególności określenia w przypadku których przestępstw najczęściej pozyskiwane są dane telekomunikacyjne, w przypadku których przestępstw technika ta jest zbędna, oraz przede wszystkim na ile jest to narzędzie skuteczne i niezbędne to realizacji zadań poszczególnych służb**. Na gruncie przywołanego wyroku *David Davis and others -v- Secretary of State for the Home Department* sąd brytyjski orzekający w tej sprawie dysponował m.in. *Report of the Interception of Communications Commissioner*[24] przygotowanym przez urząd specjalnego komisarza ds. komunikacji oraz prawie 400-stronicowym opracowaniem "*A question of Trust. Report of the Invetigatory powers review*"[25] analizującym m.in. uprawnienia służb brytyjskich pod kątem ich zgodności z prawami człowieka, w szczególności prawem do prywatności.

23 § 114 uzasadnienia wyroku.

24 Sir Anthony May, Report of the Interception of Communications Commissioner, March 2015, dostępny na stronie: http://www.iocco-uk.info/docs/IOCCO%20Report%20March%202015%20%28Web%29.pdf.

25 David Anderson, Independent Reviewer of Terrorism Legislation, "*A question of Trust. Report of the Invetigatory powers review*" https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Web-Accessible1.pdf.

Błędem wydaje się ograniczenie projektowanych zmian w zakresie Prawa telekomunikacyjnego jedynie do propozycji usunięcia art. 180g Prawa telekomunikacyjnego[26]. Zdaniem projektodawcy jest to jedyny obowiązek „implementacyjny" wynikający z wyroku w sprawie *Digital Rights Ireland*. Z jednej strony projektodawca nakłada obowiązki sprawozdawcze na służby w zakresie pozyskiwania danych telekomunikacyjnych (pkt 3.4 opinii), z drugiej zaś zdejmuje się te obowiązki z operatorów telekomunikacyjnych. Takie rozwiązanie wydaje się być niezgodne z sugestiami zawartymi w raporcie NIK[27] oraz z wyroku Trybunału Konstytucyjnego z 30 lipca 2014 r.:

> *„Trybunał Konstytucyjny zwraca także uwagę na konieczność wprowadzenia prawnego obowiązku* ***podawania do publicznej wiadomości zagregowanych danych statystycznych o liczbie i rodzaju stosowanych czynności operacyjno-rozpoznawczych ingerujących w konstytucyjne wolności i prawa człowieka****. Wymóg ten wynika z zasady demokratycznego państwa prawnego (art. 2 Konstytucji). Stanowi także urzeczywistnienie konstytucyjnego prawa do uzyskiwania informacji o działalności organów władzy publicznej (art. 61 ust. 1 Konstytucji). Transparentność danych statystycznych obrazujących skalę niejawnego pozyskiwania danych o jednostkach przez organy państwa powinna być w szczególności nieodzownym elementem demokratycznej kontroli nad działalnością organów państwa (zob. orzeczenie ETPC z 25 czerwca 2013 r. w sprawie Youth Initiative for Human Rights przeciwko Serbii, nr skargi 48135/06). Zdaniem Trybunału Konstytucyjnego, prawodawca i organy stosujące prawo mają szanować ten obowiązek. Prawodawca powinien także, w celu efektywnego i rzetelnego wykonywania obowiązku sprawozdawczego,* ***ustalić w miarę możliwości jedną, stosowaną przez wszystkie zobowiązane podmioty, metodologię sporządzania statystyk, gwarantującą jednoznaczność i porównywalność upubliczniania danych, nawet w odniesieniu do ubiegłych lat"****.*

Dotychczasowe problemy na tym tle wiązały się właśnie ze stosowaniem art. 180g Prawa telekomunikacyjnego, tj. informacji rocznej przekazywanej Komisji Europejskiej przez Prezesa Urzędu Komunikacji Elektronicznej. Z uwagi na brak ujednoliconej metodologii liczenia przypadków sięgania po dane telekomunikacyjnej[28] dane te są nieporównywalne między poszczególnymi Państwami Członkowskimi, ale co więcej nie dają informacji na temat rzeczywistej praktyki pozyskiwania danych telekomunikacyjnych przez uprawnione do tego służby w Polsce. W ocenie Helsińskiej Fundacji Praw Człowieka, projekt ustawy nie powinien ograniczać się do uchylenia art. 180g, ale powinien odzwierciedlać wytyczne Trybunału Konstytucyjnego oraz Najwyższej Izby Kontroli co do stworzenia ram prawnych dla optymalnej informacji nt. częstotliwości pozyskiwania danych telekomunikacyjnych przez służby.

---

26 Przepis ten nakłada na przedsiębiorców telekomunikacyjnych obowiązek przekazywania przez Prezesowi Urzędu Komunikacji Elektronicznej określonego rodzaju informacji na potrzeby sporządzenia sprawozdania dla Komisji Europejskiej.

27 „Jak wykazała kontrola NIK, funkcjonujący obecnie system gromadzenia informacji o pozyskiwaniu danych retencyjnych, **nie zapewnia rzetelnej informacji o liczbie tego rodzaju przypadków**. Brak jest precyzyjnie określonych wskaźników pomiarowych, a ustanowione procedury nie zapobiegają wystąpieniu rażących błędów. Również zakres gromadzonych danych sprawozdawczych nie pozwala na ocenę, dla jakich celów, jak często i z jakim skutkiem retencja danych jest stosowana. W ocenie NIK, dla prawidłowej oceny funkcjonowania systemu retencji danych niezbędne jest gromadzenie danych w zakresie: liczby przypadków, w których uprawnione organy uzyskiwały od przedsiębiorców telekomunikacyjnych dane retencyjne (z wyodrębnieniem sytuacji, gdy były to wyłącznie dane osobowe użytkownika); liczby osób, których dane telekomunikacyjne były pozyskiwane i wykorzystywane przez uprawnione organy; łącznej liczby odmów udostępnienia danych (ze wskazaniem zasadniczych przyczyn); informacji na temat rodzaju spraw, w których środek ten wykorzystywano oraz jego skuteczności." (Raport NIK, s. 16-17).

28 Trybunał wskazał w wyroku, że „liczba zapytań o dane telekomunikacyjne na podstawie zakwestionowanych przepisów nie odzwierciedla rzeczywistej liczby abonentów, których dane telekomunikacyjne pozyskiwano. (...) Jak wynika z udzielonych wyjaśnień najwięcej zapytań (około 50%) dotyczy ustalenia danych osobowych abonenta. Wynika to z braku centralnej bazy abonentów, z której można pobrać stosowne dane, a także z dużej liczby użytkowników telefonów komórkowych korzystających z tzw. kart przedpłaconych *pre paid* (według przekazanych Trybunałowi danych, około 52% użytkowników telefonów komórkowych w Polsce korzysta z tej formy rozliczeń)".

3.2. Zasada subsydiarności wnioskowania o udostępnienie danych telekomunikacyjnych

Jak wynika z uzasadnienia wyroku Trybunału Konstytucyjnego przepisy kompetencyjnej upoważniające do niejawnego pozyskiwania informacji o jednostkach w toku czynności operacyjno-rozpoznawczych (np. danych telekomunikacyjnych) **„musi być środkiem subsydiarnym, czyli stosowanym, gdy inne rozwiązania są nieprzydatne lub nieskuteczne"**. Projektodawca uznał jednak, że zasada subsydiarności w odniesieniu do danych telekomunikacyjnych nie powinna zostać wyrażona w ustawie. W uzasadnieniu projektu wskazano, że „zastosowanie zasady subsydiarności przed wystąpieniem o udostępnienie danych telekomunikacyjnych w przypadku ścigania niektórych przestępstw mogłoby okazać się niemożliwe, a także utrudniać skuteczne ściganie ich sprawców". Podając jako przykład przestępstwa popełnione przy użyciu urządzeń telekomunikacyjnych oraz przestępstw internetowych, gdzie podstawową metodą pracy operacyjnej jest najprawdopodobniej dostęp do danych telekomunikacyjnych, projektodawca wskazuje, że zasada subsydiarności nie jest możliwa do zastosowania w przypadku innych przestępstw.

W ocenie Helsińskiej Fundacji Praw Człowieka, możliwe jest zastosowanie do procesu udostępniania danych telekomunikacyjnych zasady subsydiarności analogicznej do tej zawartej w procedurze zarządzania kontroli operacyjnej ***„gdy inne środki okazały się bezskuteczne albo będą nieprzydatne"***. Wówczas ściganie np. przestępstw internetowych przy użyciu danych telekomunikacyjnych będzie dopuszczalne z uwagi fakt, że inne środki z zakresu czynności operacyjno-rozpoznawczych – mniej ingerujące w prawo do prywatności – okażą się nieprzydatne.

3.3. Kontrola nad udostępnianiem danych telekomunikacyjnych

Konkluzja Trybunału Konstytucyjnego o potrzebie zapewnienia niezależnej kontroli nad pozyskiwaniem danych telekomunikacyjnych została poprzedzona szeregiem uwag odnoszących się do obecnej regulacji pozyskiwania przez służby danych telekomunikacyjnych. Trybunał wytknął obecnej regulacji, że ***„ustawodawca nie uzależniał możliwości żądania danych od okoliczności faktycznych konkretnej sprawy, rzeczywistego stopnia zagrożenia, a wreszcie – wyczerpania innych, mniej dolegliwych dla jednostki, środków pozyskania informacji***". Trybunał zdecydował się położyć cały nacisk na kwestie proceduralne związane z zewnętrzną kontrolą nad pozyskiwaniem danych.

Brak kontroli uprzedniej, brak wymogu zgody prokuratora, brak kontroli *ex post* doprowadziło Trybunał do wniosku, że ***„pozyskiwanie danych telekomunikacyjnych (...) pozostaje zatem poza jakąkolwiek stałą kontrolą, niezależną od organu pozyskującego te dane***". Trybunał nie zdecydował się jednak na zarysowanie jak powinien wyglądać optymalny – z punktu widzenia Konstytucji – model kontroli nad dostępem służb do danych telekomunikacyjnych.

Trybunał zaznaczył, że „nie wszystkie dane tego rodzaju powodują taką samą intensywność ingerencji w wolności i prawa człowieka". Stąd nie wykluczył jako zasady kontroli następczej, zaznaczając przy tym, że, ustawodawca regulując ten mechanizm 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. Jako sytuacje, które – przykładowo – powinny wymagać kontroli uprzedniej ustawodawca wskazał na dostęp do danych telekomunikacyjnych osób wykonujących zawody zaufania publicznego lub jeśli nie ma

konieczności pilnego działania służb. O ile opiniowany projekt realizuje pierwszą z sytuacji, to całkowicie pomija sytuacje niewymagające pilnego działania służb.

W odniesieniu zaś do kwestii podmiotowych – organu, który powinien sprawować taką kontrolę – Trybunał wskazał, że nie wymaga by kontrolę udostępniania danych telekomunikacyjnych sprawowały sądy. **„Konieczne jest natomiast, by był to organ niezależny od rządu i niepozostający z funkcjonariuszami pozyskującymi dane w bezpośredniej lub pośredniej relacji zwierzchności"**.

Idea stworzenia niezależnego organu pełniącego kontrolę nad działalnością służb została również zawarta w „Raporcie dotyczących retencji danych telekomunikacyjnych" zaprezentowanym przez ministra J. Cichockiego w 2011 r.[29] Próbą realizacji tego pomysłu był projekt ustawy o Komisji Kontroli Służb Specjalnych[30] opracowany przez Ministerstwo Spraw Wewnętrznych w 2013 r.

Niestety wbrew tym zapowiedziom opiniowany projekt ustawy ogranicza planowany system kontroli nad pozyskiwaniem danych telekomunikacyjnych do:

- **uprzedniej kontroli sądowej** odnoszącej się jedynie do przypadków pozyskiwania danych telekomunikacyjnych osób wykonujących zawody zaufania publicznego;
- **obowiązku sprawozdawczego służb**, który – w założeniu projektodawcy – ma stanowić efektywny mechanizm kontroli *ex post*.

Tym samym projekt opiera się na zupełnie odmiennych założeniach i **prezentuje o wiele niższy standard ochrony prawa do prywatności** niż projekt ustawy opracowany przez senacką Komisję Praw Człowieka, Praworządności i Petycji, która zakładała uprzednią kontrolę sądową w każdym wypadku uzyskiwania danych telekomunikacyjnych, kontrolę Generalnego Inspektora Ochrony Danych Osobowych oraz kontrolę ze strony specjalnych pełnomocników ds. ochrony danych osobowych.

Projektowany art. 20ca ustawy o Policji przewiduję procedurę – analogiczną do tej zastosowanej przy kontroli operacyjnej – weryfikacji danych dotyczących osób, o których mowa w art. 180 § 2 k.p.k. Podobnie jak w przypadku art. 19 ust. 15f ustawy o Policji materiały zawierające takie informacje są przekazywane prokuratorowi, który następnie kieruje te materiały do sądu z wnioskiem „o wyrażenie zgody na ich wykorzystanie w postępowaniu karnym" (art. 20ca ust. 2). W takiej procedurze **udział prokuratora wydaje się automatyczny**, ponieważ może on jedynie skierować do sądu tylko jeden rodzaj wniosku (o wyrażenie zgody na ich wykorzystanie w postępowaniu karnym), podczas gdy w przypadku materiałów z kontroli operacyjnej mógł również złożyć wniosek o zniszczenie materiałów. Nie jest zatem zrozumiałe jaka *de facto* jest rola prokuratora w niniejszej procedurze. Jeśli ostatecznie ma decydować w tym przedmiocie sąd, być może lepszym rozwiązaniem byłoby bezpośrednie kierowanie materiałów do sądu. Ponadto, podobnie jak w przypadku niszczenia materiałów z kontroli operacyjnych projekt nie zawiera przesłanek, które sąd podejmując decyzję w przedmiocie wniosku prokuratora powinien wziąć po uwagę.

Udział prokuratora został z kolei pominięty w procedurze na podstawie art. 20cb ustawy o Policji, tj. wymagających pozyskania *ab initio* danych telekomunikacyjnych lub pocztowych dotyczących bezpośrednio osób, o których mowa w art. 180 § 2 k.p.k. **W kontekście postanowienia**

29 Raport, s. 8-10.

30 Projekt UD107 – dostępny na stronie Rządowego Procesu Legislacyjnego: http://legislacja.rcl.gov.pl/projekt/181401.

sygnalizacyjnego S 2/06 należy rozważyć czy w przypadku braku zgody sądu na udostępnienie danych telekomunikacyjnych nie należy poinformować o tym fakcie osoby, których dotyczą wnioskowane dane.

3.4. Obowiązek sprawozdawczy służb

Jednym z elementów systemu kontroli zaproponowanym w opiniowanym projekcie jest procedura sprawozdawczości przewidziana m.in. w art. 20cc ust. 2 ustawy o Policji. Przewiduje ona, że właściwy organ Policji[31] raz na 6 miesięcy przekazuje sądowi sprawozdanie obejmujące:

1) liczbę i rodzaj pozyskanych danych telekomunikacyjnych lub pocztowych;
2) podstawę prawną pozyskania danych telekomunikacyjnych lub pocztowych;
3) rodzaje przestępstw, w związku z zaistnieniem których wystąpiono o dane telekomunikacyjne lub pocztowe;
4) liczbę przypadków, ze wskazaniem ich podziału na rodzaje spraw, w których wystąpiono o dane telekomunikacyjne lub pocztowe.

Projekt następnie zakłada, że **sąd może zapoznać** się z materiałami uzasadniającymi udostępnieniu Policji danych telekomunikacyjnych oraz z materiałami uzyskanymi w wyniku podjętych czynności. Tym samym projekt zakłada pewne zręby sądowej kontroli następczej nad pozyskiwaniem przez służby danych osobowych. Jednak, w ocenie Helsińskiej Fundacji Praw Człowieka, zaproponowany model kontroli nosić będzie cechy fasadowości tworząc jedynie fikcję skutecznej kontroli nad pozyskiwaniem danych telekomunikacyjnych. Przede wszystkim kierowane do sądów sprawozdania nie będą najprawdopodobniej zawierać informacji w sprawie poszczególnych rodzajów spraw, lecz jedynie pewnie dane zagregowane. Oznacza to, że nawet jeśli sąd podejmie wątpliwości co do prawidłowości udostępnienia danych telekomunikacyjnych, sąd nie będzie wiedział o jakie materiały powinien wystąpić do Policji.

Ponadto, aby taka kontrola była efektywna jej merytoryczne prowadzenie musi opierać się o ustawowy wymóg subsydiarnego charakteru sięgania po te dane. W przeciwnym wypadku, sąd nie będzie miał kryteriów według których miałby weryfikować prawidłowość podjętych działań, w szczególności w Policji, której projektowana podstawa do sięgania po dane telekomunikacyjne jest bardzo ogólna i obejmuje „rozpoznawanie, zapobieganie, zwalczanie, wykrywanie albo uzyskanie i utrwalenie dowodów przestępstw ściganych z oskarżenia publicznego".

Wydaje się jednak, że w świetle projektowanych zmian (art. 4 i 5 opiniowanego projektu ustawy) podstawowym celem kierowania przez służby sprawozdań do sądów ma na celu ich dalsze przekształcenie w roczne sprawozdanie kierowane do Ministra Sprawiedliwości (projektowane art. 6a Prawa o ustroju sądów wojskowych oraz art. 175b prawa o ustroju sądów powszechnych), który następnie przedstawia corocznie Sejmowi i Senatowi zagregowaną informację na temat przetwarzania danych telekomunikacyjnych i pocztowych oraz wyników przeprowadzonych kontroli, w terminie do dnia 30 czerwca roku następującego po roku nią objętym. Zdaniem Helsińskiej Fundacji Praw Człowieka, przebieg rozprawy przed Trybunałem Konstytucyjnym (w szczególności problemy z uzyskaniem informacji na temat zarządzania kontroli operacyjnej przez Sąd Okręgowy w Warszawie) wskazuje na pilną **potrzebę objęcia obowiązkiem sprawozdawczości informacji na temat działalności sądów w zakresie zarządzania (lub odmowy zarządzania) kontroli operacyjnej**.

---

31 Obowiązek ten dotyczy również, m.in. Straży Granicznej (art. 10bc ustawy o Straży Granicznej), Generalnego Inspektora Kontroli Skarbowej (art. 36bc ustawy o kontroli skarbowej), Żandarmeria Wojskowa (art. 30d ustawy o Żandarmerii Wojskowej).

W ocenie Helsińskiej Fundacji Praw Człowieka równolegle do tak projektowanej kontroli sądowej rolę organu oceniającego sprawozdania powinien pełnić specjalny pełnomocnik ds. danych osobowych, funkcjonujący obecnie jedynie na gruncie ustawy o CBA (por. pkt 3.5 opinii).

3.5. Pełnomocnicy ds. ochrony danych osobowych

Opiniowany projekt całkowicie pomija rozwiązania zawarte wcześniej w projekcie Komisji Praw Człowieka, Praworządności i Petycji, który zawierał propozycję ustanowienia w poszczególnych służbach niezależnych pełnomocników ds. danych osobowych. Organ taki funkcjonuje obecnie na gruncie ustawy o CBA. Rozwiązanie to stanowi wynik wykonania wyroku Trybunału Konstytucyjnego z 23 czerwca 2009 r. (sygn. K 54/07). Trybunał orzekł wówczas o niezgodności z Konstytucją art. 22 ust. 4-7 ustawy o CBA z uwagi na brak zagwarantowania instrumentów kontroli sposobu przechowywania i weryfikacji danych wskazanych w art. 27 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz sposobu usuwania danych zbędnych dla wykonywania ustawowych zadań Centralnego Biura Antykorupcyjnego. Projekt Komisji Praw Człowieka, Praworządności i Petycji przewidywał utworzenie urzędu pełnomocnika w każdej służbie prowadzącej czynności operacyjno-rozpoznawcze, które przetwarzają dane osobowe. Propozycja taka stanowi przejaw wzmocnienia nadzoru wewnętrznego nad działalnością służb.

Niestety do takiego rozwiązania nie odnosi się w ogóle opiniowany projekt ustawy. Zdaniem Fundacji **należałoby powrócić do pomysłu zaproponowanego przez Komisję Praw Człowieka, Praworządności i Petycji**, jednak w miejsce kilku pełnomocników w poszczególnych służbach można rozważyć powołanie jednego pełnomocnika dla wszystkich służb, działającego np. przy Generalnym Inspektorze Ochrony Danych Osobowych, dysponującego kadrą i środkami do prowadzenia takiej bieżącej kontroli w sprawach danych osobowych jedynie w zakresie funkcjonowania służb policyjnych i specjalnych. Taki pełnomocnik mógłby np. rozpoznawać sprawozdania poszczególnych służb, które – w świetle opiniowanego projektu – będą kierowane do właściwych sądów okręgowych.

4. Podsumowanie

W ocenie Helsińskiej Fundacji Praw Człowieka projekt wymaga dalszych prac legislacyjnych, które dostosują go wymogów wynikających z wyroku Trybunału Konstytucyjnego, ale również do wytycznych zawartych w wyroku *Digitial Rights Ireland*. Projekt w obecnym kształcie nie wykonuje wyroku Trybunału Konstytucyjnego i całkowicie pomija wyrok Trybunału Sprawiedliwości UE, przez co jest również niezgodny z prawem Unii Europejskiej (m.in. dyrektywą 2002/58).

Helsińska Fundacja Praw Człowieka postuluje przede wszystkim o poszerzenie zakresu projektu o wytyczne wynikające z orzeczenia Trybunału Sprawiedliwości UE oraz o tezy raportu Najwyższej Izby Kontroli, tak jak czynił to projekt opracowany przez Komisję Praw Człowieka, Praworządności i Petycji. Projekt w obecnym kształcie nie realizuje wymogu zapewnienia zewnętrznej kontroli nad pozyskiwaniem danych telekomunikacyjnych. Uprzednia kontrola (sądowa) obejmuje jedynie bardzo wąski zakres danych (osób wykonujących zawody zaufania publicznego), przez co prawdopodobnie nie będzie obejmować zdecydowanej większości przypadków sięgania po te dane. Poważne wątpliwości co do skuteczności budzi także propozycja związana z fakultatywną kontrolą następczą opartą o sprawozdania służb.

Dlatego też zdaniem Fundacji należy powrócić do postulatu wyrażonego w raporcie ministra J. Cichockiego z 2011 r. powołania niezależnego organu kontrolującego pracę operacyjną służb

specjalnych. Zarówno raport, jak i projekt ustawy o Komisji Kontroli Służb Specjalnych przewidywał, że organ taki byłby powoływany przez Sejm i składał się m.in. z byłych sędziów posiadających doświadczenie w sprawach karnych. W założeniach miał on również posiadać prawo rozpatrywania skarg indywidualnych obywateli. Niestety kwestia związana ze stworzeniem skutecznego mechanizmu skargowego nie znajduje odzwierciedlenia w projekcie mimo iż wynika m.in. z art. 13 Europejskiej Konwencji Praw Człowieka[32].

Być może pewnym substytutem takiego rozwiązania byłoby skorzystanie z połączenia dwóch propozycji zawartych w projekcie Komisji Praw Człowieka, Praworządności i Petycji. Przewidywał on utworzenie w poszczególnych służbach pełnomocników ds. danych osobowych oraz umożliwienie Generalnemu Inspektorowi Ochrony Danych Osobowych prowadzenia kontroli nad służbami w zakresie udostępnienia danych telekomunikacyjnych. W ocenie Fundacji propozycja powołania kilku urzędów pełnomocników działających w ramach służb niezależnie od siebie może okazać się nie najlepszym rozwiązaniem z punktu widzenia zagwarantowania jednolitego poziomu ochrony danych osobowych we wszystkich służbach oraz nie realizuje w pełni wymogu niezależności (pomimo gwarancji istniejących na gruncie ustawy o CBA). Dlatego w ocenie Fundacji należy rozważyć umożliwienie GIODO prowadzenia kontroli nad pozyskiwaniem i przetwarzaniem danych telekomunikacyjnych przez służby. Mógłby to czynić wyszkolony w tym zakresie wyodrębniony zespół osób mających uprawnienia pozwalające na dostęp do informacji niejawnych, podlegający bezpośrednio GIODO oraz posiadający kompetencję do rozpoznawania skarg indywidualnych na działania służb.

Ponadto, projekt nie zawiera oceny skutków regulacji, m.in. dotyczących zmian w zakresie wymiaru sprawiedliwości. Projektodawca przewiduje, że sądy będą rozpatrywały sprawozdania poszczególnych służb w zakresie uzyskiwania i przetwarzania przez nich danych telekomunikacyjnych. Taki obowiązek sprawozdawczy został powiązany z fakultatywnym trybem kontroli takich sprawozdań, w szczególności poprzez zapoznanie się z materiałami uzasadniającymi udostępnienie danych telekomunikacyjnych. Projektodawca nie przedstawia informacji czy będzie się to wiązało z potrzebą zapewnienia dodatkowych etatów sędziowskich oraz jak wpłynie to na obciążenie pracą sędziów. Na marginesie pragniemy również wskazać na prowadzone w Ministerstwie Sprawiedliwości prace nad ograniczeniem kognicji sądów powszechnych, których projekt nie uwzględnia.

Projekt opinii został sporządzony przez Barbarę Grabowską-Moroz w ramach programu „Monitoring procesu legislacyjnego w obszarze wymiaru sprawiedliwości" realizowanego przez Helsińską Fundację Praw Człowieka dzięki dotacji otrzymanej z programu „Obywatele dla Demokracji" finansowanego z Funduszy EOG.

HELSIŃSKA FUNDACJA PRAW CZŁOWIEKA * 00-026 Warszawa ul. Zgoda 11

Z wyrazami szacunku,

Barbara Grabowska-Moroz
koordynator „Monitoringu procesu legislacyjnego w obszarze wymiaru sprawiedliwości"

dr Adam Bodnar
Wiceprezes Zarządu

32 Por.: Report on the Democratic Oversight of the Security Services (adopted by the Venice Commission, 1-2 June 2007), CDL-AD(2007)016, § 251-262.