

Antoni Bojańczyk

## Opinia prawna na temat projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw<sup>1</sup>

Legal opinion on a bill amending the Police Act and other acts (Sejm Paper No 3765) (BAS-1778-1715): The author of the opinion welcomes the initiative to change regulations criticized by the Constitutional Court, but also expresses reservations about the submitted bill. From legal analysis of the bill it follows that the system of operational control proposed therein, appears to be illusory and capable for abuse by the officers, which in turn may lead to gross violations of privacy of the individual. Attention is drawn to the issue of the protection of professional secrets. The task of overseeing the operational activities should be assigned to central judicial authorities on the basis of regulations enabling them effective control over the activities of services, both in cases involving citizens as well as deputies, senators and President of the Republic.

**Keywords:** Police | wiretapping | operational and reconnaissance activities | professional secrecy | special forces

**Słowa kluczowe:** Policja | podsłuch | czynności operacyjno-rozpoznawcze | tajemnica zawodowa | Służby Specjalne

Doktor hab. nauk prawnych, profesor Uniwersytetu Warszawskiego, adwokat w Izbie Adwokackiej w Warszawie; a.bojanczyk@uw.edu.pl.

### Przedmiot opinii

Przedmiotem opinii prawnej jest ocena senackiego projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (uchwała Senatu RP z 24 lipca 2015 r., druk sejmowy nr 3765/VII kad.; dalej: projekt) pod kątem zgodności proponowanych w nim rozwiązań prawnych z Konstytucją RP, w szczególności zaś z wyrokiem Trybunału Konstytucyjnego z 30 lipca 2014 r. (sygn. akt. K 23/11, sentencja wyroku została ogłoszona 6 sierpnia 2014 r., Dz.U. poz. 1055).

<sup>1</sup> Opinia sporządzona 26 sierpnia 2015 r. na zlecenie Biura Analiz Sejmowych (druk sejmowy nr 3765/VII kad.); BAS-1778/15.

## Uzasadnienie

1. Opiniowany projekt ma charakter klasycznie implementacyjny. Impulsem do jego przygotowania stał się wyrok Trybunału Konstytucyjnego z 30 lipca 2014 r., (sygn. akt K 23/11; por. uzasadnienie projektu, s. 1). We wnioskach skierowanych do Trybunału zaskarżone zostały przepisy następujących aktów normatywnych: ustawy z 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U. z 2010 r., nr 29, poz. 154, ze zm., dalej: ustawa o ABW), ustawy z 6 kwietnia 1990 r. o Policji (Dz.U. z 2015 r., poz. 355 i 529; dalej: ustawa o Policji), ustawy z 12 października 1990 r. o Straży Granicznej (Dz.U. z 2014 r., poz. 1402, ze zm.; dalej: ustawa o SG), ustawy z 28 września 1991 r. o kontroli skarbowej (Dz.U. z 2011 r., nr 41, poz. 214, ze zm.; dalej: u.k.s.), ustawy z 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz.U. z 2013 r., poz. 568, ze zm.; dalej: ustawa o ŻW), ustawy z 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz.U. z 2014 r., poz. 253, ze zm.; dalej: ustawa o SKW), ustawy z 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz.U. z 2014 r., poz. 1411 i 1822; dalej: ustawa o CBA) oraz ustawy z 27 sierpnia 2009 r. o Służbie Celnej (Dz.U. z 2013 r., poz. 1404, ze zm.; dalej: ustawa o SC). W konsekwencji także tych właśnie przepisów dotyczyło orzeczenie w sprawie K 23/11. W podobny sposób kształtuje się zakres przedmiotowy opiniowanego projektu, który co do zasady ściśle odpowiada swym szkieletem konstrukcyjnym budowie i zagadnieniom będącym przedmiotem analizy wyroku Trybunału Konstytucyjnego z 30 lipca 2014 r.

2. W postępowaniu przed Trybunałem została m.in. zakwestionowana zbyt daleko posunięta ogólność niektórych spośród przedmiotowych przesłanek stosowania czynności operacyjno-rozpoznawczych określonych w następujących ustawach: ustawie o Policji (art. 19 ust. 1 pkt 8), ustawie o SG (art. 9e ust. 1 pkt 7), ustawie o kontroli skarbowej (art. 36c ust. 1 pkt 5), ustawie o ŻW (art. 31 ust. 1 pkt 17), ustawie o ABW (art. 19 ust. 1 pkt 8). Domniemanie zgodności z Konstytucją RP tych przepisów udało się utrzymać przede wszystkim dzięki określonemu kierunkowi interpretacji zakwestionowanych przepisów dokonanej przez Trybunał Konstytucyjny oraz zaakcentowaniu tego, że: *w świetle obowiązującego stanu prawnego przestępstwa ścigane na mocy umów międzynarodowych nie mogą jednakże być uznane za oczywiście nieproporcjonalnie ingerujące w prawo do ochrony prywatności i tajemnicę komunikowania się gwarantowane przez art. 47, art. 49 Konstytucji i art. 8 Konwencji [Europejskiej]* (s. 93–94 uzasadnienia wyroku). Dlatego też Trybunał Konstytucyjny przyjął (por. pkt I.1 sentencji wyroku TK, w uzasadnieniu wyroku tych kwestii dotyczą wywoły na s. 89–96), że wyżej wymienione przepisy, zakwestionowane w postępowaniu w przedmiocie kontroli ich zgodności z Konstytucją RP i Konwencją o ochronie praw człowieka i podstawowych wolności (konwencja

europańska) są zgodne z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji RP oraz z art. 8 konwencji europejskiej, ale wyłącznie wtedy, jeżeli: *są rozumiane w ten sposób, że dotyczą określonych w polskiej ustawie karnej przestępstw ściganych na mocy umów międzynarodowych ratyfikowanych za uprzednią zgodą wyrażoną w ustawie*. Naprzeciw tym ustaleniom Trybunału Konstytucyjnego wychodzi opiniowany projekt. Harmonizuje on brzmienie zakwestionowanych przepisów ustaw w kierunku wynikającym wprost z sentencji wyroku Trybunału Konstytucyjnego (w zakresie ustawy o ŻW chodzi o nadanie przepisowi art. 31 ustawy o ŻW nowego brzmienia, także uwzględniającego wymogi orzeczenia w sprawie K 23/11). Zmiany te zasługują na aprobatę. Wprawdzie Trybunał wskazał w uzasadnieniu orzeczenia, że odpowiednie zabiegi interpretacyjne (w tym przede wszystkim uwzględnienie bezpośredniego kontekstu normatywnego przepisu uzależniającego inicjowanie czynności operacyjno-rozpoznawczych od konieczności zapobieżenia, wykrycia, ustalenia sprawców, a także uzyskania i utrwalenia dowodów przestępstw umyślnych ściganych z oskarżenia publicznego, które są „ścigane na mocy umów i porozumień międzynarodowych”; por. przede wszystkim s. 91 i n. uzasadnienia wyroku w sprawie K 23/11) pozwalają na rozumienie zakwestionowanych przepisów w sposób zgodny z Konstytucją, to trzeba powiedzieć, że brak jest jednak jakichkolwiek przeciwwskazań, by rozwiązać ewentualne wątpliwości co do zgodności inkryminowanych przepisów z Konstytucją na drodze legislacyjnej, przez nadanie im w tekście ustaw brzmienia w sposób jednoznaczny spełniającego wskazania wynikające z orzeczenia Trybunału Konstytucyjnego z 30 lipca 2014 r.

3. Podobnych zabiegów harmonizacyjnych, mających dostosować obowiązujący stan prawny do wymogów wynikających z orzeczenia Trybunału z 30 lipca 2014 r. dokonuje opiniowany projekt również w ustawach: o Policji (art. 19 ust. 6 pkt 3), ustawie o SG (art. 9e ust. 7 pkt 3), ustawie o kontroli skarbowej (art. 36c ust. 4 pkt 3), ustawie o ŻW (art. 31 ust. 7 pkt 3), ustawie o ABW (art. 27 ust. 6 pkt 3), ustawie o SKW (art. 31 ust. 4 pkt 3) i ustawie o CBA (art. 17 ust. 5 pkt 3). I w tym wypadku Trybunał Konstytucyjny przyjął, że powołane powyżej przepisy są zgodne ze wskazanymi we wniosku wzorcami kontroli konstytucyjnej (art. 2 i art. 47 w związku z art. 31 ust. 3 Konstytucji), jednakże tylko pod warunkiem takiego ich interpretowania, które pozwala na przyjęcie, że: *właściwy organ zarządzający kontrolę operacyjną ma obowiązek wskazać określony w prawie rodzaj środka technicznego przekazywania informacji i dowodów oraz ich utrwalania stosowany w indywidualnej sprawie*. Uwzględniając także ten postulat, wynikający z orzeczenia Trybunału, projektodawca zmierza do zastąpienia dość ogólnego dotychczas obowiązującego określenia, występującego jednolicie we wszystkich wyżej wymienionych ustawach, na określenie środków prowadzenia kontroli operacyjnej (*środki techniczne umożliwiające uzyskiwanie w sposób niejawni informacji i dowodów oraz ich utrwalanie*) bar-

dziej szczegółowym wyliczeniem tych środków technicznych (podsluch rozmów prowadzonych przy użyciu środków technicznych, podgląd pomieszczeń i osób poza miejscami publicznymi, kontrolę treści korespondencji, nadzór elektroniczny osób, miejsc i przedmiotów oraz środków transportu, kontrolę zawartości przesyłek). Wprawdzie Trybunał Konstytucyjny ostatecznie uznał, że kwestionowane przepisy zdają (co prawda tylko warunkowo, bowiem wyłącznie przy ich określonej wykładni i wskazanym przez Trybunał sposobie stosowania w praktyce) test konstytucyjności, ale jednocześnie zastrzegł, że: *organ wnoszący o zarządzenie kontroli operacyjnej ma obowiązek wskazać nie jakikolwiek sposób prowadzenia kontroli operacyjnej, ale wyłącznie sposób przewidziany przez prawo* (s. 109 uzasadnienia orzeczenia Trybunału Konstytucyjnego). Dlatego też Trybunał przyjął, że: *obowiązujące prawo musi precyzować dopuszczalne dla każdej ze służb „sposoby stosowania kontroli operacyjnej”, spośród których organ składający wniosek o taką kontrolę ma dopiero wskazać rekomendowany w danej sprawie (ibidem)*. Uwzględniając powyższe wskazania, projektodawca proponuje zmiany polegające na doprecyzowaniu metod prowadzenia kontroli operacyjnej. Korekty te należy ocenić pozytywnie (projektowane przepisy: art. 19 ust. 6 o Policji, art. 9e ust. 7 ustawy o SG, art. 36c ust. 4 u.k.s., art. 31 ust. 7 ustawy o ŻW, art. 27 ust. 6 ustawy o ABW, art. 31 ust. 4 ustawy o SKW i art. 17 ust. 5 ustawy o CBA), jako zmierzające niewątpliwie w kierunku implementacji wyroku Trybunału Konstytucyjnego z 30 lipca 2015 r. i odpowiadające wymogom postawionym w tym wyroku.

4. Nieco inaczej przedstawia się sprawa, gdy idzie o zakwestionowane przez Trybunał Konstytucyjny przepisy ustawy o ABW. Nie spełniały one – zdaniem Trybunału – wymogów zgodności z przepisami art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji (chodzi o przepis art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. b ustawy o ABW) z powodu niedookreśloności pojęcia użytego w treści ustawy o ABW w przepisie art. 5 ust. 1 pkt 2 lit. b. Tu zatem potrzeba zmian legislacyjnych nie jest kwestią swobodnego wyboru ustawodawcy. Zmiana jest bezwzględnie wymagana, jeśli ma dojść do usunięcia stwierdzonego przez Trybunał Konstytucyjny stanu niezgodności inkryminowanych przepisów z ustawą zasadniczą. I w rzeczywistości taką właśnie zmianę proponuje się w ocenianym projekcie. Chodzi o modyfikację przepisu art. 5 ust. 1 pkt 2 ustawy o ABW przez wskazanie w lit. a–g tego przepisu precyzyjnego katalogu przestępstw, które w ramach swych zadań ma rozpoznawać, zapobiegać i wykrywać Agencja Bezpieczeństwa Wewnętrznego. Poprzednie ujęcie tego przepisu (art. 5 ust. 1 pkt 2 lit. b ustawy o ABW), które określało ustawowe zadania Agencji Bezpieczeństwa Wewnętrznego przez odwołanie się do „bliżej nieokreślonych” (por. s. 98 motywów pisemnych wyroku w sprawie K 23/11) przestępstw „godzących w podstawy ekonomiczne państwa”, zostało uznane przez Trybunał za sprzeczne z konstytucyjną zasadą określoności prawa (art. 2 Konstytucji) i zasadą ustawowej formy ograniczeń wolności i praw konstytucyjnych (art. 31 ust. 3

Konstytucji). Niewątpliwie zaproponowane w projekcie nowe ujęcie tego przepisu, eliminujące zakwestionowaną przez Trybunał Konstytucyjny przedmiotową przesłankę „przestępstw godzących w podstawy ekonomiczne państwa” i zastąpienie tego mglistego kryterium ścisłym, taksatywnym wyliczeniem przestępstw, których rozpoznawanie, zapobieganie i wykrywanie leży w ustawowej gestii Agencji Bezpieczeństwa Wewnętrznego czyni zadość wymogom sformułowanym w wyroku Trybunału w sprawie K 23/11, w szczególności zaś postulatowi, by: *ustawowe przesłanki niejawnnej ingerencji [w konstytucyjnie określone wolności i prawa człowieka] możliwe były do ustalenia na podstawie wykładni językowej przepisów ustawy, bez konieczności odwoływania się do wykładni systemowej czy funkcjonalnej* (s. 98 uzasadnienia wyroku Trybunału Konstytucyjnego). Proponowaną zmianę należy zatem ocenić pozytywnie.

5. Podobnie – to znaczy bezwarunkowo – zakwestionował Trybunał Konstytucyjny zgodność przepisów art. 20c ust. 1 o Policji, art. 10b ust. 1 ustawy o SG, art. 36b ust. 1 pkt 1 u.k.s., art. 30 ust. 1 ustawy o ŻW, art. 28 ust. 1 pkt 1 ustawy o ABW, art. 32 ust. 1 pkt 1 ustawy o SKW, art. 18 ust. 1 pkt 1 ustawy o CBA oraz art. 75d ust. 1 ustawy o SC z wzorcami konstytucyjnymi określonymi w przepisach art. 47 i art. 49 Konstytucji w związku z art. 31 ust. 3 Konstytucji. Niezgodność tych przepisów ustawowych z Konstytucją polega na tym, że nie przewidują one mechanizmu niezależnej kontroli udostępniania danych telekomunikacyjnych, o których mowa w art. 180c i art. 180 ustawy z 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. z 2014 r., poz. 243), służbom odpowiedzialnym za zagwarantowanie ochrony porządku publicznego i bezpieczeństwa państwa. Choć Trybunał Konstytucyjny uznał (na tle przeprowadzonego przezeń badania przepisów ustawy o Policji we wskazanym powyżej zakresie), że istnieją pewne ograniczenia dostępu Policji do danych telekomunikacyjnych, to jednak uznał je za „niewystarczające, aby zapobiec nadużyciom” i przyjął, że niezbędne jest zapewnienie „niezależnej kontroli nad pozyskiwaniem danych telekomunikacyjnych” (s. 116 uzasadnienia wyroku). Trybunał Konstytucyjny zwrócił także uwagę, że ani: *zakwestionowany art. 20c ust. 1 ustawy o Policji, ani żaden inny przepis, nie nakłada obowiązku uzyskania zgody sądu (bądź innego organu, który byłby niezależny od organów żądających udostępnienia tych danych lub organów nad nimi nadrzędnych) na udostępnienie Policji danych, o których mowa w art. 180c i art. 180d prawa telekomunikacyjnego*. Wypowiadając się co do konstytucyjności pozostałych ustaw regulujących ustrój i działanie innych niż Policja służb, Trybunał także uznał niekonstytucyjność badanych przepisów i stwierdził stanowczo, że żadna z tych ustaw w zakresie, w którym zezwala na gromadzenie danych telekomunikacyjnych: *nie zawiera (...) minimalnych gwarancji proceduralnych, do których należy konieczność ustanowienia niezależnej kontroli pozyskiwania danych. Stwierdzenie braku tego mechanizmu wystarcza do orzeczenia o niekonstytucyjności zakwestionowanego przepisu* (s. 117–123 uzasadnienia wyroku).

Formułując tego rodzaju zarzuty pod adresem obowiązującego systemu kontroli dostępu do danych telekomunikacyjnych lub pocztowych przez służby ochrony porządku prawnego (a ściślej rzecz ujmując: braku jakiegokolwiek systemu kontroli dostępu tych służb do danych telekomunikacyjnych), Trybunał nie wypowiedział się jednak w sposób wiążący odnośnie do tego, jak konkretnie ma wyglądać procedura kontroli dostępu do danych telekomunikacyjnych, formułując jednak w tym zakresie ogólne wskazówki o charakterze standardów minimalnych, które pozwoliłyby ustawodawcy na zaprojektowanie i wprowadzenie do ustawodawstwa mechanizmu kontroli pozyskiwania tych danych zgodnego z Konstytucją (s. 116–117 uzasadnienia wyroku). Z perspektywy tych właśnie wskazówek należy więc dokonać oceny zaproponowanych przez projektodawcę rozwiązań, których celem jest wprowadzenie do ustaw o służbach odpowiednich mechanizmów mających na celu utworzenie systemu kontroli dostępu służb do danych telekomunikacyjnych lub pocztowych.

Zacząć trzeba od zwrócenia uwagi na to, że projektodawca postanowił obciążając korzystanie przez służby z danych telekomunikacyjnych czy pocztowych zasadą subsydiarności. Pozyskiwanie tych danych ma być w myśl projektu tylko wtedy możliwe, jeżeli „inne środki okazały się bezskuteczne albo mogą być nieprzydatne” (projektowany przepis art. 20c ust. 1 ustawy o Policji, analogiczne rozwiązania proponowane w pozostałych ustawach o służbach w przepisach o udostępnianiu danych telekomunikacyjnych i pocztowych). Ta zmiana ma doniosłe znaczenie z punktu widzenia oceny funkcji implementacyjnej ocenianego projektu, bowiem Trybunał Konstytucyjny wyraźnie wskazał w swoim judykacie, że na ocenę znaczenia gwarancji proceduralnych zewnętrznej kontroli nad procesem pozyskiwania danych telekomunikacyjnych (zwłaszcza billingowych i lokalizacyjnych) i pocztowych rzutuje w sposób istotny to, że w obecnie obowiązującym stanie prawnym ustawodawca: *nie uzależniał możliwości żądania danych od okoliczności konkretnej sprawy, rzeczywistego stopnia zagrożenia, a wreszcie – wyczerpania innych, mniej dolegliwych dla jednostki, środków pozyskania informacji* (s. 116 uzasadnienia wyroku). Wprowadzenie więc wymogu subsydiarności sięgania przez służby po dane telekomunikacyjne czy dane pocztowe ma zatem istotne znaczenie z punktu widzenia oceny charakteru niezależnej kontroli dostępu służb do danych telekomunikacyjnych czy danych pocztowych w tym sensie, że kontrola ta niewątpliwie nie musi być aż tak rygorystyczna, jak w sytuacji, gdyby takiego wymogu ustawa nie formułowała.

Opiniowany projekt wprowadza we wszystkich ustawach zakwestionowanych przez Trybunał Konstytucyjny następczy mechanizm sądowej kontroli dostępu służb do danych telekomunikacyjnych i danych pocztowych (por. art. 20cc ustawy o Policji, analogiczne rozwiązania we wszystkich innych ustawach objętych pkt. I.5 sentencji wyroku TK z 30 lipca 2014 r.). Trzeba powiedzieć, że co do zasady jest to mechanizm odpowiadający tym wymogom, które



Trybunał sformułował w motywach orzeczenia w sprawie K 23/11. Wskazując na: *obowiązek zapewnienia niezależnej kontroli pozyskiwania danych telekomunikacyjnych*, Trybunał jednocześnie stwierdził, że: *nie jest wobec tego wykluczone – w odniesieniu do udostępniania danych telekomunikacyjnych w toku czynności operacyjno-rozpoznawczych – wprowadzenie, jako zasady, kontroli następczej*. Sam mechanizm kontroli (jest to właśnie mechanizm opierający się na modelu kontroli następczej), który zaproponował projektodawca w opiniowanym projekcie w poszczególnych ustawach regulujących ustroj i kompetencje służb powołanych do ochrony bezpieczeństwa państwa i porządku publicznego odpowiada co do zasady wymogom orzeczenia w sprawie K 23/11. Nie nasuwa także żadnych zastrzeżeń powierzenie kontroli następczej sądowi. W wyroku w sprawie K 23/11 – stanowiącym w tym zakresie właściwy punkt odniesienia dla projektodawcy i opiniowanego projektu – Trybunał Konstytucyjny przyjął, że mechanizm kontroli niezależnej nad udostępnianiem danych telekomunikacyjnych czy pocztowych wcale nie wymaga tego, 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*. W tym zakresie przewidziany przez projektodawcę model kontroli następczej udostępniania służbom danych telekomunikacyjnych i danych pocztowych należy ocenić jako zgodny ze standardami wynikającymi z judykatu w sprawie K 23/11.

Nie oznacza to jednak jeszcze, że oceniany projekt nie budzi w tym zakresie żadnych wątpliwości.

Po pierwsze, kontrolę przednią projektodawca zarezerwował wyłącznie dla tych układów, w których dane telekomunikacyjne albo dane pocztowe dotyczą „bezpośrednio osoby wykonującej zawód lub funkcję, o których mowa w art. 180 § 2 k.p.k.” (projektowany przepis art. 20cb ust. 1 ustawy o Policji i inne analogiczne rozwiązania w opiniowanym projekcie dotyczące pozostałych ustaw o służbach). To słuszne rozwiązanie, w każdym razie niewątpliwie zgodne z orzeczeniem Trybunału Konstytucyjnego. Podkreślono w nim bowiem wyraźnie, że kontrola następcza nie zawsze będzie właściwym rozwiązaniem legislacyjnym z punktu widzenia należytego wyważenia między wartościami w postaci – z jednej strony – efektywnej walki służb odpowiedzialnych za bezpieczeństwo państwa i porządek publiczny z zagrożeniami, z drugiej zaś – z ochroną takich konstytucyjnie chronionych dóbr prawnych, jak prawo do tajemnicy komunikowania się czy tajemnice zawodowe gwarantujące należyte wykonywanie zawodów zaufania publicznego. Dostęp do danych telekomunikacyjnych osób wykonujących zawody zaufania publicznego lub sytuacje, w których „nie ma konieczności pilnego działania służb”, to zdaniem Trybunału Konstytucyjnego „argumenty za wprowadzeniem kontroli przedniej w pewnych wypadkach” (s. 116–117 uzasadnienia wyroku). Szkopuł jed-

nak w tym, że projektodawca z nieznanych względów postanowił wprowadzić sądową kontrolę uprzednią wyłącznie w sytuacjach, gdy pozyskiwanie danych telekomunikacyjnych lub danych pocztowych dotyczy „bezpośrednio osoby wykonującej zawód lub funkcję, o której mowa w art. 180 k.p.k.” (por. proponowane przez projekt brzmienie art. 20cb ust. 1 ustawy o Policji i analogiczne rozwiązania w innych ustawach o służbach), pomijając drugi z układów, o których mowa w orzeczeniu Trybunału w sprawie K 23/11, to jest sytuacje, w których pozyskiwanie danych telekomunikacyjnych czy pocztowych nie ma wcale charakteru pilnego. Lojalnie jednak trzeba także przyznać, że Trybunał w tym zakresie nie wypowiedział się mimo wszystko kategorycznie i nie postawił kropki na „i”, pozostawiając te kwestie „odpowiedniemu wyważeniu przez ustawodawcę”.

Znacznie więcej zastrzeżeń budzi sam mechanizm kontroli następczej przewidziany dla udostępniania danych telekomunikacyjnych i danych pocztowych służbom i ich funkcjonariuszom. Powstaje bowiem pytanie, czy mechanizm ten może być skuteczny, czy też jest – być może – wyłącznie instytucją o charakterze iluzorycznym. Odpowiadając na to pytanie, należy powiedzieć, że koncepcja sądowej kontroli następczej przyjęta przez projektodawcę w istocie ma wyłącznie fasadowy charakter. Trzeba bowiem podkreślić, że z naruszeniem ustawy przy pozyskiwaniu danych telekomunikacyjnych lub pocztowych (stwierdzenie przez sąd „braku podstaw do pozyskania danych telekomunikacyjnych lub pocztowych”) nie wiąże się żadna sankcja, która byłaby w stanie w sposób realny wpłynąć na ograniczenie czy zapobieżenie nieproporcjonalnym i nadmiernym ingerencjom w sferę prywatności jednostki czy sferę objętą tajemnicą komunikowania się. Wbrew pozorom nie jest wcale taką sankcją niezwłoczne i protokolarne zniszczenie przez Policję czy inną służbę zgromadzonych danych telekomunikacyjnych czy pocztowych w związku z decyzją sądu sprawującego kontrolę następczą (art. 20cc ust. 4 ustawy o Policji, podobne rozwiązania w pozostałych ustawach zmienianych opiniowanym projektem). Z formalnego punktu widzenia przewidziany przez projektodawcę mechanizm kontroli następczej jest zgodny z minimalnymi standardami przewidzianymi w wytycznych sformułowanych przez Trybunał Konstytucyjny w tej sprawie uzasadnienia, w której sąd konstytucyjny zajmował się zagadnieniem wprowadzenia odpowiedniego mechanizmu kontroli pozyskiwania danych telekomunikacyjnych i danych pocztowych (pkt 10.4.4. motywów pisemnych wyroku). Z materialnego punktu widzenia jednak kontrola ta nie może zostać uznana za spełniającą pokładane w niej nadzieje. W założeniu przecież sankcja tego rodzaju, jaką jest zniszczenie materiałów pozyskanych przez Policję i pokrewne służby, ma mieć charakter prewencyjny. Tego celu jednak sankcja polegająca na obowiązku zniszczenia materiałów w postaci uzyskanych danych telekomunikacyjnych czy danych pocztowych nie jest w stanie skutecznie zrealizować, jeżeli uprzednio dane te pozostawały przez dłuższy czas do dyspozycji służby i jej



funkcjonariuszy. Charakter danych telekomunikacyjnych zbieranych w trybie i na zasadach przewidzianych w przepisie art. 20c ust. 2 pkt 1–3 ustawy o Policji (i analogicznych przepisów innych ustaw ustrojowych służb objętych wyrokiem Trybunału Konstytucyjnego z 30 lipca 2014 r.) ma bowiem to do siebie, że ich zniszczenie w przeważającej liczbie przypadków nie będzie miało najmniejszego praktycznego znaczenia dla pracy służb. Tym samym trudno zakładać, że przewidziana przez projektodawcę konstrukcja następczej sądowej kontroli pozyskiwania danych odniesie jakiegokolwiek skutek poza symbolicznym. Trzeba wszak uwzględnić to, że w rachubę wchodzi tutaj przecież wyłącznie tzw. metadane telekomunikacyjne, a zatem tego rodzaju dane, które umożliwiają ustalenie zakończenia sieci telekomunikacyjnego urządzenia końcowego lub użytkownika końcowego inicjującego połączenie (albo do którego kierowane jest połączenie), określenie daty i godziny połączenia oraz czasu jego trwania, rodzaju połączenia i lokalizacji telekomunikacyjnego urządzenia końcowego. Wartość tych danych dla służb polega na tym, że pozwalają im na precyzyjne ustalenie szeroko rozumianej konfiguracji „siatki personalnej” osoby czy osób będących przedmiotem zainteresowania operacyjnego służb (z jakimi abonentami, kiedy i w przybliżeniu z jakiego miejsca łączył się czy łączyły się określone numery telefonów). Walor tych danych dla postępowania karnego jest trudny do przecenienia. Nawet, jeżeli nie da się ich bezpośrednio wykorzystać w postępowaniu karnym (z uwagi na decyzję sądu o ich zniszczeniu), to i tak samo niezakłócone dysponowanie tymi danymi przez służby pozwala z reguły bez większego trudu na ich „przekonwertowanie” na dowody możliwe do procesowego wykorzystania w przyszłym czy aktualnie toczącym się postępowaniu karnym. Dane te pozwalają bowiem na rekonstrukcję prawdopodobnych kontaktów danej osoby (nawet, jeżeli na tej tylko podstawie nie jest możliwe kategoryczne ustalenie, kto personalnie korzystał z danego aparatu telefonicznego przypisanego do określonego numeru telefonicznego) i umożliwiają w razie potrzeby ułożenie planu postępowania przygotowawczego, włącznie – na przykład – z ustaleniem potencjalnej listy osób, które należy przesłuchać, oraz złożenia wniosku w trybie przepisu art. 237 § 1 Kodeksu postępowania karnego o sądowe zarządzenie kontroli i utrwalania treści rozmów telefonicznych w celu wykrycia i uzyskania dowodów dla toczącego się postępowania lub zapobieżenia popełnieniu nowego przestępstwa. Krótko mówiąc, stwierdzenie przez sąd właściwy do przeprowadzenia kontroli następczej pozyskiwania danych telekomunikacyjnych przez służby, że brak było podstaw do pozyskania danych telekomunikacyjnych lub danych pocztowych, nie ma wcale aż tak dużego znaczenia z punktu widzenia zagwarantowania należytego przestrzegania przez Policję i podobne służby lub formacje wymogów prawnych w zakresie korzystania z danych telekomunikacyjnych z uwagi na sankcję, która nie ma prawie żadnego waloru prewencyjnego, zapobiegającego pokusie korzystania z konstytucyjnie wrażliwych danych pozyskanych sprzecznie z przepisami prawa.

Reasumując powyższe rozważania, trzeba powiedzieć, że przewidziany przez opiniowany projekt tryb kontroli pozyskiwania danych telekomunikacyjnych z uwagi na rodzaj przewidzianej w projekcie sankcji ma przeważnie symboliczne znaczenie i nie uzasadnia przekonania, że zastosowanie tej sankcji może mieć jakikolwiek skutek prewencyjny.

6. Na dwie jeszcze bardzo istotne sprawy należy zwrócić uwagę w tym kontekście. Iluzoryczność następczej kontroli sądowej wynika także z zaproponowanego przez projektodawcę sposobu prowadzenia tej kontroli, a konkretnie ze sposobu określenia podstawy informacyjnej udostępnianej sądowi dla przeprowadzenia tej kontroli. Projektodawca postanowił oprzeć model prowadzenia sądowej kontroli następczej nie na kontroli konkretnych spraw, lecz na przygotowywanym przez same służby materiale o dość ogólnikowym charakterze sprawozdawczym, obejmującym między innymi takie informacje, jak liczba przypadków pozyskania danych telekomunikacyjnych, podstawa prawna pozyskania danych telekomunikacyjnych czy rodzaje przestępstw, w związku z zaistnieniem których wystąpiono o dane telekomunikacyjne lub pocztowe (por. art. 20cc ust. 2 ustawy o Policji w ujęciu projektu, podobne regulacje przewidziane we wszystkich innych ustawach o służbach ochrony porządku publicznego objętych tekstem projektu). Szkopeł jednak w tym, że dane te (statystyczny materiał sprawozdawczy zestawiany przez służby dla sądu lub sądów właściwych do przeprowadzania kontroli następczej) nie tylko mogą okazać się zbyt wąte dla dokonania rzetelnej kontroli następczej legalności, ale wręcz z samego założenia są niewystarczającą podstawą dla dokonania tego typu kontroli, stanowiąc, jak powiedziano, wyłącznie nader ogólnikowe zestawienie statystyczne, mające bardzo ograniczoną wartość dla sądu w toku postępowania kontrolnego. Jeżeli kontrola następcza ma mieć rzeczywiście efektywny charakter, to musi bazować na szczegółowym badaniu wszystkich przypadków pozyskiwania danych telekomunikacyjnych, a nie na analizie opracowania o charakterze statystycznym. Wprawdzie projektodawca wyposażył sąd właściwy do przeprowadzenia kontroli następczej w wyjątkowe prawo do: *zapoznania się z materiałami uzasadniającymi udostępnienie Policji danych telekomunikacyjnych lub pocztowych oraz materiałami uzyskanymi w wyniku podjętych czynności* (por. art. 20cc ust. 3 ustawy o Policji w ujęciu projektu, analogiczne regulacje przewidziane we wszystkich innych ustawach o służbach ochrony porządku publicznego objętych projektem), ale i tak będzie to oznaczało konieczność albo losowego (przesiewowego) wyboru spraw poddawanych kontroli sądowej, albo – jeżeli kontrola ta miałaby mieć charakter pełny i rzetelny – poddaniu kontroli „wszystkich” przypadków pozyskiwania danych telekomunikacyjnych czy pocztowych przez służby (nie wiadomo jednak, czy to z kolei byłoby w ogóle realne, zważywszy na skończone jednak zasoby kadrowe sądów powołanych do przeprowadzania tej kontroli, jak i na nieznaną jeszcze wolumen przypadków pozyskiwania danych telekomunikacyjnych

przez służby). Po drugie – nie tylko nie jest jasne to, w jakim trybie i na jakich zasadach (czy są to przepisy postępowania karnego czy też – być może – przepisy postępowania administracyjnego) ma być przez sąd prowadzona kontrola następcza, o której mowa w opiniowanym projekcie, ale przede wszystkim nie jest jasne, czym (jakim rozstrzygnięciem) ma się skończyć przeprowadzona przez sąd kontrola. Wydaje się, że w przypadku oceny „negatywnej” (ustalenie przez sąd w toku kontroli następczej braku podstaw do pozyskania danych telekomunikacyjnych, por. art. 20cc ust. 4 ustawy o Policji w brzmieniu przewidzianym przez projekt i analogiczne przepisy pozostałych ustaw w wersji proponowanej przez projekt) konieczne będzie wydanie rozstrzygnięcia o zarządzeniu zniszczenia pozyskanych danych telekomunikacyjnych (podjęcie takiej decyzji będzie zresztą zawsze wymagało od sądu – jak już powiedziano powyżej – sięgnięcia do konkretnych materiałów związanych z pozyskiwaniem danych telekomunikacyjnych lub sądowych). Co jednak w przypadku porzestania na badaniu przez sąd tylko samego „suchego” sprawozdania statystycznego przedstawiającego jedynie bardzo ogólny obraz liczbowy pozyskiwania przez powołane do tego służby danych telekomunikacyjnych (do czego wszakże sąd zdaje się mieć uprawnienie na podstawie projektowanych przepisów). Zakładając, że wyłącznie na podstawie tych danych sprawozdawczych miałby sąd sprawujący kontrolę następczą dokonać oceny przestrzegania prawa przez służby (co wydaje się wysoce nieracjonalne, ale na co projekt niewątpliwie zezwala), to nasuwa się wówczas pytanie, czy sąd jest zobowiązany do wydania w tym przedmiocie jakiejś decyzji (rozstrzygnięcia) „pozytywnej” i jaka ma być ewentualna forma i treść tej decyzji.

Wszystkie wyżej powołane okoliczności przemawiają za konkluzją, że charakter podstawy informacyjnej (zestawienie statystyczne) przeprowadzanej przez sąd kontroli następczej pozyskiwania przez Policję i inne służby danych telekomunikacyjnych lub pocztowych może doprowadzić do tego, że kontrola ta będzie miała tylko iluzoryczny charakter. W dodatku opiniowany projekt w zakresie następczej sądowej procedury kontrolnej cechuje zdecydowane niedopracowanie normatywne. W szczególności nie wiadomo, czy w razie ograniczenia się tylko do kontroli opartej na sprawozdaniu statystycznym sporządzanym przez służby i pozytywnej oceny tego sprawozdania, sąd powołany do przeprowadzania kontroli następczej będzie zobowiązany do wydania jakiegokolwiek decyzji. Nie jest jasne także, jaka ma być forma procesowa i treść tej decyzji.

7. Przechodząc od oceny regulacji związanej z ochroną danych objętych tajemnicami zawodowymi oraz zakazami dowodowymi, Trybunał Konstytucyjny zakwestionował w sposób bezwarunkowy (pkt I.6 sentencji orzeczenia w sprawie K 23/11) zgodność przepisów art. 19 o Policji, art. 9e ustawy o SG, art. 36c u.k.s., art. 31 ustawy o ŻW, art. 27 ustawy o ABW, art. 31 ustawy o SKW, art. 17 ustawy o CBA z wzorcami konstytucyjnymi określonymi w przepisach

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. Oceniając zakwestionowane rozwiązania (a raczej zupełny brak odpowiednich rozwiązań prawnych), Trybunał stwierdził między innymi, że: *mankamentem konstytucyjnym art. 19 ustawy o Policji jest niezagwarantowanie w ustawie, że w sytuacji uzasadnionego podejrzenia, że zgromadzone materiały zawierają informacje objęte tajemnicą zawodową i z tego powodu wymagają szczególnej ochrony, nastąpi dodatkowa weryfikacja tych materiałów przez sąd i ewentualne zwolnienie z tajemnicy zawodowej, zanim zostaną przekazane funkcjonariuszom służb bądź prokuratorowi (s. 131 uzasadnienia wyroku)*. „Wyjątkowo negatywnie” ustosunkował się Trybunał do braku rozwiązań w odniesieniu do tych tajemnic zawodowych, które z uwagi na ich znaczenie dla urzeczywistnienia takich wartości, jak prawo do obrony oraz wolność prasy – powinny podlegać szczególnej ochronie przed ujawnianiem ich treści służbom stosującym kontrolę operacyjną (s. 132 uzasadnienia wyroku).

Opiniowany projekt ustawy stanowi również odpowiedź na tę część orzeczenia Trybunału Konstytucyjnego, wprowadzając w bardzo szerokim zakresie instrumenty prawne związane z objęciem szczególnymi gwarancjami owoców czynności operacyjno-rozpoznawczych w postaci materiałów czy danych objętych tajemnicami zawodowymi. Generalnie zaproponowane przez projektodawcę rozwiązania zasługują na aprobatę i należy implemmentować wskazania sformułowane w wyroku w sprawie K 23/11.

8. Zasadnicze zastrzeżenia budzi jednak to, że materiały operacyjne obejmujące tajemnice zawodowe mogą nigdy nie dotrzeć do prokuratora i – dalej – do sądu w ramach przewidzianego przez projekt systemu nadzoru, bo o tym, czy dane materiały zostaną poddane kontroli sądowej decydują same służby (por. projektowany art. 15f ust. 2 ustawy o Policji, analogiczne rozwiązania w innych ustawach ustrojowych służb objętych projektem). Sam prokurator odgrywa w tym procesie małą rolę, jest bowiem zależny od oceny podjętej przez służbę i w pewnym sensie związany oceną funkcjonariuszy (art. 15g ustawy o Policji, który nie pozostawia mu w tym zakresie większej swobody).

Sposób zaproponowanego w projekcie normatywnego ukształtowania kontroli sądowej nad niejawnymi ingerencjami w obszar objęty tajemnicą zawodową budzi potrójne zastrzeżenia. Po pierwsze, chodzi o to, że – jak już powiedziano wyżej – nadzór ten może zostać uruchomiony wyłącznie w wypadku dokonania określonej oceny zgromadzonego materiału przez samą służbę (projektowany art. 15f ust. 2 ustawy o Policji i inne zbieżne rozwiązania przewidziane w projekcie), która przecież właśnie dokonuje ingerencji w materię potencjalnie chronioną tajemnicą zawodową i jest immanentnie zainteresowa-

na jej dowodowym czy operacyjnym wykorzystaniem. Po drugie, istotne jest to, że sama tajemnica zawodowa to zagadnienie nader delikatne i oddzielenie tego, co jest nią objęte, od tego, co nie jest nią objęte, nie jest wcale łatwym zagadnieniem, szczególnie wówczas, gdy takiej oceny dokonuje podmiot bezpośrednio zainteresowany w wykorzystaniu określonej treści. Po trzecie wreszcie, zanim materiały operacyjne zostaną poddane następczej kontroli sprawowanej przez sąd (jeżeli w ogóle takiej kontroli zostaną poddane) służby i tak mogą te materiały eksploatować dla swoich potrzeb (zresztą podobnie ma się sprawa z informacjami objętymi bezwarunkowymi zakazami dowodowymi – por. w tym względzie projektowany przepis art. 15f ust. 1 ustawy o Policji i inne analogiczne rozwiązania przewidziane w ustawach o służbach objętych projektem oraz następczym nadzorem sądowym nad danymi telekomunikacyjnymi czy pocztowymi dotyczącymi bezpośrednio osoby wykonującej zawód lub funkcję, o której mowa w art. 180 § k.p.k. – por. w tym zakresie proponowane przez projekt brzmienie art. 20ca ustawy o Policji i analogiczne rozwiązania przewidziane w innych ustawach o służbach). Dostrzegł to ryzyko także Trybunał w swoim orzeczeniu (s. 131). Wydaje się jednak, że wyrażony w wyroku w sprawie K 23/11 pogląd, że: *jest [ono] poważne, aczkolwiek nie na tyle, aby usprawiedliwiać zupełne wyłączenie określonej grupy podmiotów – również obrońców i dziennikarzy – spod kontroli operacyjnej*, jest nie tylko przesadnie optymistyczny, ale może wręcz doprowadzić do całkowitej erozji funkcji ochronnej jaką pełni tajemnica zawodowa.

Wszystkie powyższe okoliczności razem wzięte wybitnie potęgują ryzyko nadużyć w zakresie ochrony tajemnicy zawodowej przed ingerencją w toku kontroli operacyjnej i uzasadniają konkluzję, że standard nadzoru sądowego dla pozyskanych operacyjnie danych objętych tajemnicami zawodowymi przewidziany w projekcie nie może być oceniony pozytywnie. Trybunał stwierdził w orzeczeniu z 30 lipca 2014 r., że: *to do ustawodawcy należy wprowadzenie rozwiązań prawnych, które zapobiegą ryzyku [zapoznania się przez funkcjonariuszy służb informacjami stanowiącymi tajemnice zawodowe i] wykorzystaniu informacji wymagających ochrony lub przynajmniej zminimalizują to ryzyko*. Projekt nie zapobiega temu ryzyku, a wątpliwie jest także to, czy je „przynajmniej minimalizuje”.

Podkreślić należy wreszcie, że także sam proces sądowego nadzoru nad wykorzystaniem owoców kontroli operacyjnej obejmujących informacje stanowiące tajemnice zawodowe budzi istotne zastrzeżenia. To niekwestionowana przez nikogo prawda (podkreśla to zresztą również sam Trybunał Konstytucyjny w wyroku w sprawie K 23/11), że tajemnica zawodowa wcale nie służy przedstawicielom określonego zawodu. Jednak wydaje się, że to w dobrze pojętym interesie przedstawicieli zawodu, który został przez ustawodawcę „objęty” tajemnicą zawodową, leży zapobieganie bezzasadnym naruszeniom ingerencji w materię chronioną tajemnicą zawodową. Istotną słabością wprowadzanego

przez projektodawcę mechanizmu ochrony przed bezprawnymi naruszeniami sfery chronionej tajemnicą zawodową jest również to, że w procesie tym odgrywa nadmierną, wręcz kluczową rolę, podmiot zainteresowany w jak najwęższym interpretowaniu granicy tajemnicy zawodowej (same służby), a osoby, których kontakty są objęte ochroną tajemnicy zawodowej, nie tylko nie mają możliwości kwestionowania decyzji zapadających w tym postępowaniu, ale nie mogą się też nigdy dowiedzieć o tym, że tajemnica zawodowa została naruszona (chyba że już *post factum* w toku postępowania karnego). W związku z tym niezbędne jest zatem wprowadzenie do przewidzianego przez ustawodawcę mechanizmu nadzoru nad kontrolą operacyjną, podczas której gromadzi się materiały objęte tajemnicą zawodową takich rozwiązań, które uczyniłyby ten nadzór bardziej obiektywnym. Wybór określonego rozwiązania należy oczywiście do ustawodawcy. Być może dobrym wyjściem byłoby rozważenie nadania w postępowaniu dotyczącym nadzoru nad operacyjną ingerencją w materię objętą tajemnicą zawodową uprawnień procesowych organom samorządu zawodowego lub ich przedstawicielom, skoro to właśnie do tych organów należy konstytucyjne zadanie sprawowania pieczy nad należyтым wykonywaniem zawodów zaufania publicznego w granicach interesu publicznego i dla jego ochrony (art. 17 ust. 1 Konstytucji).

9. W wielu miejscach orzeczenia w sprawie K 23/11 Trybunał Konstytucyjny podkreślał, że najlepszym organem kontroli nad ingerencją w sferę objętą konstytucyjnie chronionym prawem do prywatności czy tajemnicą komunikowania się jest co do zasady sąd. Projektodawca w zasadzie respektuje ten postulat. Projekt zmierza jednak w kierunku „rozproszenia” bezpośredniego nadzoru (następczego i uprzedniego) nad korzystaniem z danych telekomunikacyjnych i danych pocztowych. Chodzi o to, że nadzór ten będą sprawowały różne sądy okręgowe (sąd okręgowy właściwy dla siedziby organu Policji, Straży Granicznej i Służby Celnej uprawnionego do złożenia wniosku w przypadku Policji, Straży Granicznej i Służby Celnej, wojskowy sąd okręgowy właściwy dla siedziby organu Żandarmerii Wojskowej, w odniesieniu do kontroli skarbowej, Agencji Bezpieczeństwa Wewnętrznego i Centralnego Biura Antykorupcyjnego Sąd Okręgowy w Warszawie, a w odniesieniu do Służby Kontrwywiadu Wojskowego Wojskowy Sąd Okręgowy w Warszawie). Doszło zatem do recypowania dotychczasowego modelu właściwości sądów przewidzianego dla sądowego nadzoru nad kontrolą operacyjną prowadzoną przez służby. To rozwiązanie budzi jednak zastrzeżenia, w szczególności w świetle akcentowanej w orzeczeniu w sprawie K 23/11 (s. 166 uzasadnienia wyroku) niejawności orzeczeń wydawanych w sprawach kontroli operacyjnej, braku ich uzasadniania oraz braku kontroli tych orzeczeń z punktu widzenia ich jednolitości przez Prezesa Sądu Okręgowego w Warszawie. Należy zatem postulować wprowadzenie właściwości centralnej (jeden sąd dla wszystkich spraw objętych ustawami o służbach). Umożliwiłoby to wypracowanie jednolitego orzecznictwa w tych sprawach.



Z tych samych względów niezbędne wydaje się także wyraźne wprowadzenie obowiązku uzasadniania postanowień sądu wydawanych w sprawach nadzoru nad kontrolą operacyjną czy pozyskiwaniem danych telekomunikacyjnych przez służby, co przesądziłoby ewentualnie pojawiające się wątpliwości co do konieczności uzasadniania tych orzeczeń. Brak uzasadnień tych orzeczeń nie tylko jest sprzeczny z jakimikolwiek standardami procesowymi, ale faktycznie uniemożliwia jakąkolwiek realną weryfikację zasadności formalnej i merytorycznej orzekania w przedmiocie wniosków o zarządzenie kontroli operacyjnej (czy uruchomienia dostępu do danych telekomunikacyjnych).

W uzasadnieniu projektu podaje się zresztą przykłady państw, gdzie funkcjonują centralne organy zajmujące się w określonym zakresie weryfikacją ingerencji w sferę prywatności przez służby, np. Dania czy Wielka Brytania (s. 10–11 uzasadnienia projektu). Scentralizowanie sądowej kontroli nad wnioskami służb o zezwolenie na prowadzenie czynności ingerujących w konstytucyjnie chronioną sferę prywatności jednostek ma niewątpliwą przewagę nad rozproszeniem tej działalności.

W tym kontekście należy jeszcze zwrócić uwagę na wyodrębnienie przez projekt kontroli nad czynnościami operacyjno-rozpoznawczymi prowadzonymi wobec posłów, senatorów i Prezydenta Rzeczypospolitej lub pozyskiwania danych telekomunikacyjnych lub pocztowych posłów, senatorów lub Prezydenta Rzeczypospolitej Polskiej. Projekt przewiduje, że organem właściwym do podejmowania decyzji w tych sprawach (projektowany przepis art. 15k ustawy o Policji i analogiczne rozwiązania w innych ustawach o służbach) będzie sprawował Pierwszy Prezes Sądu Najwyższego. Po pierwsze, projektowana regulacja wykracza poza problematykę, która była przedmiotem wyroku Trybunału Konstytucyjnego. Po drugie, zastrzeżenia budzi odmienny tryb rozstrzygania w tych sprawach i organ, któremu zostały powierzone te zadania (organ niesądowy – Pierwszy Prezes Sądu Najwyższego). Nie przewidział też projektodawca żadnego trybu zażalenia. Nie wydaje się, żeby tych decyzji nie mógł podejmować jeden i ten sam wyspecjalizowany organ o charakterze sądowym, tj. Sąd Okręgowy w Warszawie.

## Wnioski

1. Większość rozwiązań zaproponowanych w opiniowanym projekcie ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw ściśle koresponduje z ustaleniami dokonanyymi w wyroku Trybunału Konstytucyjnego z 30 lipca 2014 r. (sygn. akt K 23/11) i zasługuje na aprobatę.

2. Przewidziany przez opiniowany projekt tryb kontroli pozyskiwania przez Policję i inne bliźniacze służby państwowe danych telekomunikacyjnych lub pocztowych z uwagi na rodzaj przewidzianej w projekcie sankcji ma włas-

ciwie tylko symboliczne znaczenie i nie uzasadnia przekonania, że zastosowanie tej sankcji może mieć jakikolwiek skutek prewencyjny.

3. Charakter merytoryczny podstawy informacyjnej (zestawienie statystyczne) przeprowadzanej przez sąd kontroli następczej pozyskiwania przez Policję i inne służby danych telekomunikacyjnych lub pocztowych może prowadzić do tego, że kontrola ta będzie miała tylko iluzoryczny charakter.

4. Opiniowany projekt w zakresie następczej sądowej procedury kontrolnej nad pozyskiwaniem danych telekomunikacyjnych i pocztowych cechuje zdecydowane niedopracowanie normatywne. W szczególności nie wiadomo, czy w razie ograniczenia się tylko do kontroli opartej na sprawozdaniu statystycznym sporządzanym przez służby i pozytywnej oceny tego sprawozdania, sąd powołany do przeprowadzania kontroli następczej będzie zobowiązany do wydania jakiegokolwiek decyzji. Nie jest także jasne, jaka powinna być forma i treść tej decyzji.

5. Przewidziany przez projekt proces sądowego nadzoru nad wykorzystaniem wyników kontroli operacyjnej obejmujących informacje stanowiące tajemnice zawodowe budzi bardzo poważne zastrzeżenia. Po pierwsze, dlatego, że nadzór ten może zostać uruchomiony wyłącznie w wypadku dokonania określonej oceny zgromadzonego materiału przez służbę, która sama ingeruje w materię potencjalnie chronioną tajemnicą zawodową i jest immanentnie zainteresowana jej dowodowym czy operacyjnym wykorzystaniem. Po drugie, dlatego, że sama tajemnica zawodowa to zagadnienie nader delikatne i oddzielenie tego, co jest nią objęte, od tego, co nie jest nią objęte, nie zawsze będzie łatwe. Szczególnie wtedy, gdy takiej oceny dokonuje podmiot bezpośrednio zainteresowany w wykorzystaniu określonej treści. Po trzecie wreszcie, istotne jest to, że zanim materiały operacyjne zostaną poddane kontroli sprawowanej przez sąd służby i tak mogą te materiały eksploatować dla swoich potrzeb.

6. Należy postulować wprowadzenie sądowej właściwości scentralizowanej dla wszystkich spraw objętych ustawami o służbach i związanych z prowadzeniem następczego bądź uprzedniego nadzoru nad kontrolą operacyjną lub pozyskiwaniem przez Policję i inne podobne służby danych telekomunikacyjnych lub danych pocztowych.

7. Kontrolę nad czynnościami operacyjno-rozpoznawczymi prowadzonymi wobec posłów, senatorów i Prezydenta Rzeczypospolitej lub pozyskiwaniem danych telekomunikacyjnych lub pocztowych posłów, senatorów i Prezydenta Rzeczypospolitej Polskiej powinien prowadzić sąd, a nie organ o charakterze niesądowym.