RZECZNIK PRAW OBYWATELSKICH

Adam Bodnar

Warszawa, 18 lutego 2016 r.

II.519.109.2015.KŁS/VV/AG

Trybunał Konstytucyjny

Warszawa

Na podstawie art. 191 ust. 1 pkt 1 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78, poz. 483 ze zm.) oraz art. 16 ust. 2 pkt 2 ustawy z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich (Dz. U. z 2014 r., poz. 1648 ze zm.)

wnoszę o

stwierdzenie niezgodności:

I.

- art. 19 ust. 9 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2015 r., poz. 355 ze zm.);
- art. 9e ust. 10 ustawy z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2014 r., poz. 1402 ze zm.);
- art. 36c ust. 7 ustawy z dnia 28 września 1991 r. o kontroli skarbowej (Dz. U. z 2015 r., poz. 553 ze zm.);

– art. 31 ust. 10 ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organizacjach porządkowych (Dz. U. z 2013 r., poz. 568 ze zm.);
– art. 17 ust. 9 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. z 2014 r., poz. 1411 ze zm.)

– w zakresie, w jakim umożliwiają przedłużenie kontroli operacyjnej na następujące po sobie okresy, których łączna długość nie może przekraczać 12 miesięcy, co w konsekwencji oznacza możliwość prowadzenia kontroli operacyjnej przez 18 miesięcy – z art. 2, art. 47, art. 49, art. 51 ust. 2 w zw. z art. 31 ust. 3 Konstytucji RP;

II.

– art. 19 ust. 15h ustawy z dnia 6 kwietnia 1990 r. o Policji;
– art. 9e ust. 16h ustawy z dnia 12 października 1990 r. o Straży Granicznej;
– art. 36d ust. 1h ustawy z dnia 28 września 1991 r. o kontroli skarbowej;
– art. 31 ust. 16h ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych;
– art. 27 ust. 15j ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu;
– art. 31 ust. 14h ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego;
– art. 17 ust. 15h ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym

– w zakresie, w jakim posługuje się nieostrym kryterium „dobra wymiaru sprawiedliwości” i nie określa wagi okoliczności, która ma być ustalona na podstawie materiałów mogących zawierać informacje, o których mowa w art. 178a, art. 180 § 2 i art. 180 § 3 Kodeksu postępowania karnego – z art. 2 Konstytucji RP, z art. 42 ust. 2, art. 47, art. 49, art. 51 ust. 2 w

zw. z art. 31 ust. 3 Konstytucji RP oraz z art. 6 Konwencji o ochronie praw człowieka i podstawowych wolności;

III.

- art. 20c ust. 1 oraz art. 20cb ust. 1 ustawy z dnia 6 kwietnia 1990 r. o Policji,
- art. 10b ust. 1 oraz art. 10bb ust. 1 ustawy z dnia 12 października 1990 r. o Straży Granicznej,
- art. 36b ust. 1 oraz art. 36bb ust. 1 ustawy z dnia 28 września 1991 r. o kontroli skarbowej,
- art. 30 ust. 1 oraz art. 30c ust. 1 ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych,
- art. 28 ust. 1 oraz art. 28b ust. 1 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu,
- art. 32 ust. 1 oraz art. 32b ust. 1 ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego,
- art. 18 ust. 1 oraz art. 18b ust. 1 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym,
- art. 75d ust. 1 oraz art. 75db ust. 1 ustawy z dnia 27 sierpnia 2009 r. o Służbie Celnej,

z art. 2, 30, 47, 49, 51 ust. 2 w zw. z art. 31 ust. 3 Konstytucji, art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności oraz art. 7 i 8 w zw. z art. 52 ust. 1 Karty Praw Podstawowych UE

IV.

- art. 20c ust. 3 w zw. z art. 20c ust. 2 ustawy o Policji,
- art. 10b ust. 3 w zw. z art. 10b ust. 2 ustawy o Straży Granicznej,
- art. 36b ust. 3 w zw. z art. 36b ust. 2 ustawy o kontroli skarbowej,

– art. 30 ust. 3 w zw. z art. 30 ust. 2 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych,

– art. 28 ust. 3 w zw. z art. 28 ust. 2 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu,

– art. 32 ust. 3 w zw. z art. 32 ust. 2 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego,

– art. 18 ust. 3 w zw. z art. 18 ust. 2 ustawy o Centralnym Biurze Antykorupcyjnym,

– art. 75d ust. 3 w zw. z art. 75d ust. 2 ustawy o Służbie Celnej

z art. 2, art. 20 oraz z art. 47 i art. 51 ust. 2 w zw. z art. 31 ust. 3 Konstytucji RP.

V.

– art. 20ca ustawy o Policji,

– art. 10ba ustawy o Straży Granicznej,

– art. 36ba ustawy o kontroli skarbowej,

– art. 30b ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych,

– art. 28a ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu,

– art. 32a ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego,

– art. 18a ustawy o Centralnym Biurze Antykorupcyjnym

– art. 75da ustawy o Służbie Celnej

– w zakresie, w jakim nie przewidują wprowadzenia mechanizmu niezależnej realnej kontroli udostępniania danych – z art. 2, 47, 51 ust. 2 w zw. z art. 31 ust. 3 Konstytucji, art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności oraz art. 7 i 8 w zw. z art. 52 ust. 1 Karty Praw Podstawowych UE.

VI.

– art. 20c ustawy o Policji,

– art. 10b ustawy o Straży Granicznej,

– art. 36b ustawy o kontroli skarbowej,

– art. 30 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych,

– art. 28 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu,

– art. 32 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego,

– art. 18 ustawy o Centralnym Biurze Antykorupcyjnym,

– art. 75d ustawy o Służbie Celnej

– w zakresie, w jakim przepisy te nie wskazują kategorii osób, których dane mogą być pozyskiwane w sposób określony w ustawach, nie regulują obowiązków informacyjnych wobec osób, których dane były pozyskiwane oraz nie określają czasu, przez który uprawnione podmioty mogą przetwarzać pozyskane dane – z art. 2, 30, 47, 49, 51 ust. 2, 3 i 4 w zw. z art. 31 ust. 3 Konstytucji, z art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności oraz art. 7 i 8 w zw. z art. 52 ust. 1 Karty Praw Podstawowych UE

VII.

– art. 28 ust. 7 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu

– art. 32 ust. 9 ustawy o Służbie Kontrwywiadu Wojskowego

– w zakresie, w jakim nie przewidują zniszczenia wszelkich innych danych telekomunikacyjnych, pocztowych i internetowych niż tylko tych, niemających znaczenia dla prowadzonego postępowania karnego – z art. 51 ust. 2 Konstytucji w zw. z art. 31 ust. 3 Konstytucji, art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności oraz art. 7 i 8 w zw. z art. 52 ust. 1 Karty Praw Podstawowych UE.

VIII.

Art. 13 oraz art. 16 ustawy z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw (Dz. U. z 2016 r., poz. 147)

– w zakresie, w jakim nakazują stosować przepisy, które przestały obowiązywać na mocy wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r., sygn. K 23/11 – z art. 2 oraz z art. 190 ust. 1 i 3 Konstytucji RP.

UZASADNIENIE

Ustawa z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw (Dz. U. z 2016 r., poz. 147), która wprowadziła do porządku prawnego większość przepisów kwestionowanych w niniejszym wniosku, wykonuje – w opinii projektodawców – wyrok Trybunału Konstytucyjnego z dnia 30 lipca 2014 r., sygn. K 23/11. W wyroku tym Trybunał Konstytucyjny orzekł o niezgodności z Konstytucją RP szeregu przepisów regulujących stosowanie kontroli operacyjnej przez służby policyjne i służby specjalne. W ocenie Rzecznika Praw Obywatelskich przepisy będące przedmiotem niniejszego wniosku nie tylko nie realizują przywołanego wyroku Trybunału Konstytucyjnego, ale w poważnym zakresie naruszają konstytucyjne prawa i wolności człowieka oraz standardy wyznaczone w prawie międzynarodowym.

Nie ma wątpliwości, że kontrola operacyjna jest narzędziem stosowanym przez służby specjalne na całym świecie. Umożliwia ona realne prowadzenie czynności, do których te służby zostały powołane. Trudne, jeżeli nie niemożliwe, byłoby zapewnienie bezpieczeństwa państwu i jego obywatelom bez dopuszczenia korzystania z tajnych technik operacyjnych. Nie można zapominać, że środowiska przestępcze co do zasady nie posługują się metodami jawnymi, przewidywalnymi, korzystającymi ze środków ogólnodostępnych i wykorzystywanych w działalności legalnej. Próba zapewnienia skutecznej ochrony przed działalności przestępczą, polegająca na wykorzystaniu tylko metod jawnych, byłaby z góry skazana na niepowodzenie. Jest to tym bardziej oczywiste, jeżeli weźmie się pod uwagę

występujące współcześnie główne źródła zagrożeń dla bezpieczeństwa. Działania terrorystów na taką skalę nie byłyby możliwe bez korzystania z nowych technologii, zwłaszcza z Internetu i innych technik telekomunikacyjnych. Zrozumiałe jest, że skuteczna walka z tymi zjawiskami wymaga nie tylko korzystania z tych kanałów informacyjnych, ale także uzyskania dostępu do informacji wymienianych przez osoby prowadzące działalność grożącą bezpieczeństwu. Rzecznik Praw Obywatelskich nie kwestionuje – co do zasady – możliwości, a nawet potrzeby stosowania kontroli operacyjnej. Co więcej, zauważa, że niejednokrotnie to właśnie stosowanie czynności z zakresu kontroli operacyjnej może przysłużyć się do ochrony wolności i praw człowieka.

Służby policyjne i służby specjalne w państwie demokratycznym nakierowane są na zapewnienie państwu i jego obywatelom bezpieczeństwa, a więc ochrony przed zagrożeniem wewnętrznym i zewnętrznym. Bezpieczeństwo jest niewątpliwie dobrem ulokowanym wysoko w hierarchii dóbr prawem chronionych. Słusznie wskazuje się w doktrynie, że bezpieczeństwo jest pewnym stanem „dającym jednostce poczucie pewności elementarnej wartości, jaką jest istnienie oraz gwarancję zachowania i ciągłości tegoż istnienia, umożliwia dalszy rozwój i doskonalenie się" (M. Ławrynowicz-Mikłaszewicz, *Bezpieczeństwo jako prawo człowieka w kontekście stosowania środków przymusu bezpośredniego i broni palnej przez uprawnione podmioty*, „Przegląd Prawniczy, Ekonomiczny i Społeczny" 2014, nr 4, s. 64). Nie można jednak zapominać, że czynności operacyjno-rozpoznawcze w swojej istocie w sposób poważny ingerują w fundamentalne wolności i prawa człowieka. Nie zawsze i nie w każdym zakresie ingerencja taka może być usprawiedliwiona bezpieczeństwem. Bezpieczeństwo jest bez wątpienia jednym z ważniejszych dóbr prawnych, niemniej nie jedynym. Nie ma też ono charakteru bezwzględnego, co oznacza, że może podlegać ograniczeniom wynikającym z kolizji z innymi dobrami. Innymi słowy, działania nakierowane na ochronę bezpieczeństwa obywateli nie mogą w sposób nieograniczony ingerować w inne dobra prawne, w tym

zwłaszcza w wolności i prawa człowieka. Zbyt duży zakres dopuszczalnej ingerencji prowadziłby niewątpliwie do ryzyka poważnych nadużyć polegających na wykorzystywaniu szerokich uprawnień przez organy państwa w celu realizacji dobra nie tyle wspólnego, co bardziej partykularnego.

Instrumentarium prawne, którym obudowana jest kontrola operacyjna, musi być konstruowane w oparciu o świadome i pogłębione studium kolizji dóbr chronionych, w tym wypadku dóbr najważniejszych dla wspólnoty politycznej, sięgających godności człowieka, dobra wspólnego i zasady demokratycznego państwa prawnego (na te dylematy zwraca uwagę M. Safjan, w: M. Safjan, *Wyzwania dla państwa prawa*, Warszawa 2007, s. 61-62). Organy ochrony praw człowieka, w tym Rzecznik Praw Obywatelskich, powołane są do prowadzenie szczególnie intensywnej kontroli, weryfikującej czy granica proporcjonalności stosowania czynności operacyjno-rozpoznawczych w państwie demokratycznym nie została naruszona. Ograniczenia nakładane na służby policyjne i służby specjalne mogą skutkować w jakimś stopniu zwiększeniem ryzyka niebezpieczeństwa, niemniej daleko idące ograniczenie tego ryzyka byłoby możliwe tylko poprzez budowanie państwa omnipotentnego, a więc ostatecznie totalitarnego.

Należy zauważyć, że omawiane przepisy nie dotyczą problematyki czynności operacyjno-rozpoznawczych prowadzonych w ramach procesu karnego, w sposób uregulowany w Kodeksie postępowania karnego. Kwestionowane przepisy są raczej przejawem czegoś, co Dobrosława Szumiło-Kulczycka określa jako erozję utrwalonego schematu stosowania omawianych tutaj czynności. Głównym przejawem tej erozji jest porzucenie przekonania, że „jedną z różnic między czynnościami operacyjno-rozpoznawczymi a procesowymi jest niedopuszczalność bezpośredniego wykorzystania w procesie materiałów pozyskanych przy zastosowaniu tych pierwszych" (D. Szumiło-Kulczycka, *Czynności operacyjno-rozpoznawcze i ich relacje do procesu karnego*, Warszawa 2012, s. 17). W konsekwencji, przepisy będące

przedmiotem wniosku regulują czynności wyjęte z reżimu procedury karnej, mogące prowadzić do wszczęcia postępowania karnego, ale nie pociągające za sobą takiej konieczności. W literaturze podkreśla się, że czynności operacyjne pełnią rolę subsydiarną względem procesu karnego, wyprzedzają postępowanie przygotowawcze, dostarczając uzasadnienia do wszczęcia postępowania przygotowawczego (K. Eichstaedt, *Zarządzenie przez sąd kontroli operacyjnej w ujęciu procesowym*, „Prokuratura i Prawo" 2003, nr 9, s. 28).

Kontrola operacyjna ma charakter niejawny i może polegać na:

1) uzyskiwaniu i utrwalaniu treści rozmów prowadzonych przy użyciu środków technicznych, w tym za pomocą sieci telekomunikacyjnych;
2) uzyskiwaniu i utrwalaniu obrazu lub dźwięku osób z pomieszczeń, środków transportu lub miejsc innych niż miejsca publiczne;
3) uzyskiwaniu i utrwalaniu treści korespondencji, w tym korespondencji prowadzonej za pomocą środków komunikacji elektronicznej;
4) uzyskiwaniu i utrwalaniu danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych;
5) uzyskiwaniu dostępu i kontroli zawartości przesyłek.

Ustawodawca zakresem ustawy z dnia 15 stycznia 2106 r. o zmianie ustawy o Policji oraz niektórych innych ustaw objął nie tylko czynności z zakresu kontroli operacyjnej, ale także uzyskiwanie danych, niestanowiących treści odpowiednio, przekazu telekomunikacyjnego, przesyłki pocztowej albo przekazu w ramach usługi świadczonej drogą elektroniczną, zwanych danymi internetowymi, danymi telekomunikacyjnymi i danymi pocztowymi. Ten zakres nowelizacji budzi szczególne wątpliwości natury konstytucyjnej.

Działania prowadzone w ramach szeroko rozumianej kontroli operacyjnej, a więc także zbieranie danych telekomunikacyjnych, internetowych i pocztowych, mają charakter niejawny.

Podkreślić należy, że z jednej strony niejawność prowadzonych czynności determinuje ich skuteczność, jednakże z drugiej strony ogranicza jednostce możliwość realizacji ochrony swoich praw i wolności zagwarantowanych w Konstytucji RP, albowiem obywatel nie ma wiedzy, że organy państwa ingerowały w jego prawa i wolności. Jak zauważono w wyroku Trybunału Konstytucyjnego z dnia 12 grudnia 2005 r.: „Istotną cechą czynności operacyjnych jest również ich poufny lub tajny charakter (T. Hanausek, *Kryminalistyka. Zarys wykładu*, Kraków 1998, s. 130), co stanowi przesłankę skuteczności, ale jednocześnie powoduje, że zainteresowany, nie wiedząc o prowadzonej wobec niego kontroli operacyjnej, nie jest w stanie, z przyczyn czysto faktycznych, uruchomić procedur i gwarancji, których wykorzystanie jest zależne od jego wiedzy i inicjatywy" (wyrok TK z 12 grudnia 2005 r., sygn. K 32/04).

Poszczególne trybunały wypracowały minimalne wymagania, jakie łącznie muszą spełniać przepisy ograniczające wolności i prawa, regulujące czynności operacyjno-rozpoznawcze. Ilustrując to stwierdzenie przykładami, Rzecznik Praw Obywatelskich pragnie odnieść się do orzecznictwa ETPC, który wielokrotnie podkreślał, że ingerencję w życie prywatne i korespondencję stanowią nie tylko indywidualne środki niejawnej kontroli skierowane przeciwko oznaczonym podmiotom, ale też strategiczny monitoring połączeń i pozyskiwanie związanych z tym danych osobowych komunikujących się podmiotów. Kwestia ta była rozpatrywana w sprawie *Weber* i *Saravia przeciwko Niemcom*, w której zakwestionowano niemieckie przepisy regulujące strategiczny monitoring połączeń telekomunikacyjnych, polegający na utrwalaniu rozmów telefonicznych nieoznaczonego kręgu rozmówców, a następnie identyfikowaniu, za pomocą słów kluczy, informacji zawartych w tych rozmowach, które mogą potencjalnie identyfikować sprawców przestępstw lub plany ich popełnienia (orzeczenie ETPC z 29 czerwca 2006 r. w sprawie *Weber i Saravia*, sprawa nr 54934/00). W ocenie ETPC doszło do ingerencji w „tajemnicę telekomunikacyjną" (ang. secrecy of telecomunications) chronioną przez art. 8 EKPC. W świetle orzecznictwa ETPC

ingerencją w sferę prywatności jednostki jest też gromadzenie i przechowywanie danych na temat jednostek przez służby państwowe, niezależnie od sposobu, w jaki zostały zgromadzone (zob. orzeczenia ETPC z 4 maja 2000 r. w sprawie *Rotaru p. Rumunii*, skarga nr 28341/95, § 43-44 uzasadnienia oraz 2 września 2010 r. w sprawie *Uzun p. Niemcom*, § 46 uzasadnienia). ETPC zwracał więc uwagę, że wystarczające dla stwierdzenia ingerencji w prawo zagwarantowane przez art. 8 EKPC jest zgromadzenie danych o jednostkach, bez względu na to, w jaki sposób będą one w przyszłości wykorzystane. Tym niemniej ETPC nie zanegował w ogóle dopuszczalności niejawnego pozyskiwania informacji o osobach przez władze publiczne, lecz wręcz wskazywał na ich niezbędność, jako narzędzia umożliwiającego efektywne zagwarantowanie bezpieczeństwa oraz ochronę instytucji demokratycznego państwa przed wyrafinowanymi formami zagrożeń, zwłaszcza szpiegostwem czy terroryzmem (zob. m.in. orzeczenie ETPC z 6 września 1978 r. w sprawie *Klass i inni przeciwko Niemcom*, sprawa nr 5029/71).

Należy jednocześnie podkreślić, że również Trybunał Konstytucyjny, jak i Trybunał Sprawiedliwości Unii Europejskiej (TSUE) nie zanegowały konieczności przyznania właściwym organom kompetencji do pozyskiwania wiedzy, zbierania i gromadzenia informacji o obywatelach w sposób niejawny (zob. przykładowo wyrok TK z 30 lipca 2014 r. o sygn. akt K 23/11 czy też wyrok TSUE z 8 kwietnia 2014 r. w połączonych sprawach C-293/12 *Digital Rights Ireland* i C-594/12 *Kärtner Landesregierung i in.*; orzeczenie ETPC z 29 czerwca 2006 r. w sprawie *Weber i Saravia* p. *Niemcom*, sprawa nr 54934/00 albo ostatnio z 4 grudnia 2015 r. w sprawie *Zakharov* p. *Rosji*, sprawa nr 14881/03).

Omawiając problematykę poruszaną w niniejszym wniosku należy odwołać się także do prawa Unii Europejskiej, a zwłaszcza do postanowień Karty Praw Podstawowych UE, która w art. 7 statuuje prawo do prywatności, natomiast w art. 8 wyodrębnia prawo do ochrony danych osobowych. Zgodnie z art. 52 ust. 1 KPP UE wszelkie ograniczenia w korzystaniu z praw i

wolności uznanych w Karcie muszą być przewidziane ustawą i szanować istotę tych praw i wolności. Z zastrzeżeniem zasady proporcjonalności, ograniczenia mogą być wprowadzone wyłącznie wtedy, gdy są konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób. Prawo do ochrony danych osobowych jest również chronione w Unii Europejskiej na mocy art. 16 Traktatu o funkcjonowaniu Unii Europejskiej.

Należy podkreślić, że zastosowanie Karty Praw Podstawowych Unii Europejskiej w niniejszej sprawie musi uwzględniać treść jej art. 51 ust. 1, zgodnie z którym postanowienia Karty mają zastosowanie do państw członkowskich wyłącznie w zakresie, w jakim stosują one prawo Unii. Państwa te szanują zatem prawa, przestrzegają zasad i popierają ich stosowanie zgodnie ze swoimi uprawnieniami i w poszanowaniu kompetencji Unii powierzonych jej w traktatach. W omawianym przypadku KPP UE znajduje zastosowanie ze względu na obowiązywanie następujących dyrektyw, które mają zastosowanie w odniesieniu do ograniczenia praw dotyczących prawa do prywatności, zwłaszcza w zakresie danych telekomunikacyjnych i danych internetowych:

- dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej, Dz. Urz. WE L 201 z 31.7.2002, s. 37 ze zm.), w szczególności jej art. 15 ust. 1 w zw. z art. 5,
- dyrektywy 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym, Dz. Urz. WE L 178 z 17.7.2000, s. 1 ze zm.), w szczególności jej art. 3 ust. 4 w zw. z art. 3 ust. 1,

– dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dz. Urz. L 281 z 23.11.1995, s. 31), w szczególności jej art. 1 i art. 7.

Ustawodawca zobligowany był zatem do przeanalizowania zgodności ustawy z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw, wprowadzającej zakwestionowane we wniosku zmiany, pod kątem zgodności z przepisami ww. dyrektyw, w szczególności w kontekście proporcjonalności ograniczeń w prawie do prywatności i prawie do ochrony danych osobowych. Konieczność zweryfikowania proponowanych regulacji pod kątem ich przydatności i niezbędności wynika zatem również z prawa Unii Europejskiej.

Uwzględniając dotychczasowe ustalenia Trybunału Konstytucyjnego, ETPC, a także TSUE dotyczące przepisów regulujących niejawne pozyskiwanie przez władze publiczne w demokratycznym państwie prawa informacji o jednostkach, możliwe jest zestawienie minimalnych wymagań, jakie muszą spełniać przepisy ograniczające konstytucyjne wolności i prawa. Takiego zestawienia dokonał m.in. Trybunał Konstytucyjny w wyroku z 30 lipca 2014 r. w sprawie K 23/11. Przypomnieć należy w szczególności te z nich, które bezpośrednio odnoszą się do zakwestionowanych przepisów ustawy o Policji oraz pozostałych wskazanych ustaw i które następnie powołane zostaną w dalszej części wniosku Rzecznika. W szczególności:

1) nie można gromadzić, przechowywać oraz przetwarzać danych dotyczących osób bez wyraźnej i precyzyjnej podstawy ustawowej;
2) należy określić precyzyjnie organy państwa upoważnione do przeprowadzania kontroli operacyjnej;

3) przepisy powinny precyzyjnie określać przesłanki stosowania czynności operacyjno-rozpoznawczych oraz ograniczać ją tylko do wykrywania poważnych przestępstw oraz do zapobiegania im;
4) należy wskazać nie tylko środki niejawnego pozyskiwania informacji, ale także rodzaje informacji gromadzonych za pomocą poszczególnych środków;
5) czynności z zakresu kontroli operacyjnej i inne czynności polegające na gromadzeniu danych powinny być subsydiarnym środkiem pozyskiwania informacji lub dowodów;
6) ustawa powinna określać maksymalny okres prowadzenia czynności operacyjno-rozpoznawczych, który nie powinien naruszać zasady konieczności wynikającej z zasady proporcjonalności (art. 31 ust. 3 Konstytucji RP);
7) należy precyzyjnie unormować w ustawie procedurę zarządzania czynności operacyjno-rozpoznawczych, w tym powinien znaleźć się obowiązek pozyskania zgody niezależnego organu na niejawne pozyskiwanie informacji;
8) konieczne jest precyzyjne określenie w ustawie zasad postępowania z materiałami zgromadzonymi w toku czynności operacyjno-rozpoznawczych;
9) należy zagwarantować bezpieczeństwo zgromadzonych danych;
10) konieczne jest unormowanie procedury następczego informowania jednostek o niejawnym pozyskaniu informacji na ich temat, a także wprowadzenie procedury zaskarżania czynności operacyjno-rozpoznawczych.

Już po dokonaniu powyższego zestawienia ogłoszone zostały kolejne wyroki TSUE i ETPC, które dotyczyły problematyki masowego gromadzenia informacji. W tym kontekście należy przywołać wyrok TSUE z 6 października 2015 r. w sprawie C-362/14 w sprawie *Maximillian Schrems*, gdzie TSUE co prawda dokonał oceny ważności konkretnej decyzji Komisji Europejskiej, tym niemniej odniósł się do problemu braku środków prawnych przysługujących obywatelowi w przypadku przekazywania jego danych do państwa trzeciego,

nawet w celach związanych z ochroną bezpieczeństwa publicznego, w którym nie są spełnione minimalne wymogi związane z ochroną danych osobowych. Unieważniona decyzja nie określała żadnych ograniczeń w zakresie dostępu amerykańskich organów publicznych do danych osobowych przekazywanych na jej podstawie. TSUE w szczególności wyjaśnił, że uregulowanie umożliwiające organom publicznym uzyskanie powszechnego dostępu do treści wiadomości elektronicznych należy uznać za naruszenie zasadniczej istoty prawa podstawowego do poszanowania życia prywatnego (pkt 94 wyroku TSUE w sprawie C-362/14 *Maximillian Schrems*).

Rzecznik Praw Obywatelskich pragnie również zwrócić uwagę na sprawę, którą rozstrzygnął Europejski Trybunał Praw Człowieka w dniu 4 grudnia 2015 r. (*Zakharov* p. *Rosji*, skarga nr 47413/06). ETPC uznał w swoim wyroku, że doszło do naruszenia art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności, a system niejawnej kontroli rozmów telefonicznych z telefonów komórkowych obowiązujący w Rosji narusza prawo do poszanowania życia prywatnego i korespondencji. Chociaż skarżący nie wykazał, by jego rozmowy były podsłuchiwane lub by operatorzy przekazywali jego dane nieuprawnionym osobom, to jednak ETPC postanowił o przeprowadzeniu abstrakcyjnej analizy tego prawa. Z wyroku wynika, że ETPC zwrócił w szczególności uwagę na naruszenie standardów konwencyjnych poprzez brak jakiegokolwiek sprecyzowania okoliczności, w jakich organy władzy mogą podsłuchiwać rozmowy obywateli, brak prawnego nakazu zakończenia podsłuchu, gdy ustały przesłanki uzasadniające jego stosowanie, brak uregulowania procedur przechowywania i niszczenia zarejestrowanych danych, co w praktyce oznaczało bezterminowe przechowywanie takich danych, brak procedur zezwalania na prowadzenie niejawnej kontroli, nieuregulowanie zasad nadzoru nad prowadzeniem takiej kontroli, wreszcie brak uregulowania zasad informowania obywateli o prowadzeniu kontroli oraz środkach prawnych przysługującym obywatelom w razie podsłuchiwania ich telefonów komórkowych.

Ponadto, w nieostatecznym jeszcze wyroku w sprawie *Szabó* i *Vissy* przeciwko Węgrom (wyrok z 12 stycznia 2016 r., skarga 37138/14) ETPC uznał, że naturalną odpowiedzią władz państwowych na zjawisko terroryzmu i przestępczości jest podejmowanie działań, również o charakterze prewencyjnym, zmierzających do jego zwalczania, w szczególności poprzez masowe monitorowanie środków komunikacji. Trybunał podniósł jednak zastrzeżenia co do tego, czy w przepisach krajowych przewidziano gwarancje, które byłyby wystarczająco precyzyjne, efektywne i zrozumiałe w odniesieniu do zarządzania, wykonywania i realizacji wskazanych uprawnień. W szczególności Trybunał dostrzegł, że przepisy węgierskie:

- nie określają kategorii osób, które mogłyby podlegać niejawnemu nadzorowi, w szczególności nie wymagają wskazania żadnego związku z zagrożeniem terrorystycznym,
- służby, które żądają zezwolenia od Ministra Sprawiedliwości na dokonanie podsłuchu, nie muszą uzasadnić w żaden szczegółowy sposób, by zbieranie takich informacji było konieczne, co – zdaniem Trybunału – może z łatwością prowadzić do nadużyć,
- niewystarczająco precyzyjnie określają maksymalny okres trwania nadzoru, co w efekcie może prowadzić do tego, że nie będzie on ograniczony czasowo w żaden sposób,
- nie przewidziano żadnych środków prawnych przysługujących osobom, których komunikacja była nadzorowana – w szczególności za właściwy środek nadzoru Trybunał nie uznał obowiązku przedstawiania raportu w odstępach półrocznych komisji parlamentarnej.

Wyrok ten w chwili złożenia niniejszego wniosku w Trybunale Konstytucyjnym nie jest jeszcze ostateczny, tym niemniej potwierdza kierunek rozważań przyjmowanych przez ETPC i ugruntowuje dotychczasową linię orzeczniczą.

Ocena konstytucyjności zakwestionowanych przepisów ustaw musi zostać poprzedzona również rozważaniami na temat możliwości skontrolowania przez Trybunał braku regulacji i zakwalifikowania tego braku jako zaniechania lub pominięcia ustawodawczego. Zdaniem

Trybunału Konstytucyjnego, zaniechanie ustawodawcze (tzw. luka w prawie) polega na niewydaniu aktu ustawodawczego, choćby obowiązek jego wydania wynikał z norm konstytucyjnych (por. orzeczenie TK z dnia 3 grudnia 1996 r. o sygn. K 25/95). W przyjętym przez Trybunał ujęciu kognicji tego sądu, brak jest kompetencji do orzekania o zaniechaniu ustawodawcy, czyli wtedy, gdy określone zagadnienie zostało pozostawione w całości poza regulacją prawną. Z kolei pominięcie ustawodawcze polega na przyjęciu uregulowania niepełnego – w akcie prawnym wydanym i obowiązującym prawodawca reguluje jakieś zagadnienie w sposób niepełny, fragmentaryczny. W takim wypadku, dopuszczalna jest kontrola regulacji niepełnej, mającej z punktu widzenia zasad konstytucyjnych zbyt wąski zakres zastosowania lub z uwagi na cel i przedmiot regulacji pomijającej treści istotne (tak TK w wyroku z dnia 13 czerwca 2011 r. o sygn. SK 41/09). Jak zauważył Trybunał, „zarzut niekonstytucyjności może więc dotyczyć zarówno tego, co ustawodawca w danym akcie unormował, jak i tego, co w akcie tym pominął, choć postępując zgodnie z Konstytucją powinien był unormować (wyrok o sygn. K 25/95). Wskazany wyżej podział na niepodlegające kontroli Trybunału zaniechanie prawodawcze, a badane przez sąd konstytucyjny uregulowanie niepełne znalazł odzwierciedlenie w wielu orzeczeniach TK (np. wyrok z dnia 6 maja 1998 r. o sygn. K 37/97, wyrok z dnia 24 października 2001 r. o sygn. SK 22/01, wyrok z dnia 19 maja 2003 r. o sygn. K 39/01 czy wyrok z dnia 9 grudnia 2008 r. o sygn. SK 43/07).

Powyższe argumenty stały się podstawą oceny znowelizowanych przepisów przeprowadzonej przez Rzecznika Praw Obywatelskich. W pozostałym zakresie przepisy regulujące kontrolę operacyjną zostały zaskarżone przez Rzecznika Praw Obywatelskich wnioskiem z dnia 4 grudnia 2015 r. (sygn. akt K 32/15). Mimo nowelizacji przepisów regulujących kontrolę operacyjną, zarzuty pierwszy i trzeci podniesione we wniosku z 4 grudnia 2015 r. pozostają aktualne. Zarzut drugi wymagał korekty, dlatego został uwzględniony w niniejszym wniosku.

I. Niezgodność art. 19 ust. 9 ustawy z dnia 6 kwietnia 1990 r. o Policji; art. 9e ust. 10 ustawy z dnia 12 października 1990 r. o Straży Granicznej; art. 36c ust. 7 ustawy z dnia 28 września 1991 r. o kontroli skarbowej; art. 31 ust. 10 ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organizacjach porządkowych; art. 17 ust. 9 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym – w zakresie, w jakim umożliwiają przedłużenie kontroli operacyjnej na następujące po sobie okresy, których łączna długość nie może przekraczać 12 miesięcy, co w konsekwencji oznacza możliwość prowadzenia kontroli operacyjnej przez 18 miesięcy – z art. 2, art. 47, art. 49, art. 51 ust. 2 w zw. z art. 31 ust. 3 Konstytucji RP.

Przepisy kwestionowane w tej części wniosku regulują problematykę czasu trwania kontroli operacyjnej. Zmienione przepisy ustawy o Policji, o Straży Granicznej, o kontroli skarbowej, o Żandarmerii Wojskowej i wojskowych organizacjach porządkowych, o Centralnym Biurze Antykorupcyjnym przewidują, że kontrola operacyjna może być przedłużana ponad podstawowy okres jej trwania, jeżeli podczas stosowania kontroli operacyjnej pojawiły się nowe okoliczności istotne dla zapobieżenia lub wykrycia przestępstwa albo ustalenia sprawców i uzyskania dowodów przestępstwa. W takich przypadkach sąd może wydawać kolejne postanowienia o przedłużeniu kontroli operacyjnej na następujące po sobie okresy, których łączna długość nie może przekraczać 12 miesięcy.

W ocenie Rzecznika Praw Obywatelskich przepisy ustalające czas trwania kontroli operacyjnej są niezgodne z art. 2, art. 47, art. 49, art. 51 ust. 2 w zw. z art. 31 ust. 3 Konstytucji RP.

Możliwość nieproporcjonalnie długotrwałego stosowania kontroli operacyjnej w pierwszej kolejności narusza zasadę demokratycznego państwa prawnego, a przede wszystkim

wynikającą z niej zasadę zaufania obywateli do państwa oraz zasadę praworządności. Jak wywiódł Trybunał Konstytucyjny: „(...) zasada zaufania do państwa i stanowionego przez nie prawa opiera się na wymaganiu pewności prawa, a więc takim zespole cech przysługujących prawu, które zapewniają jednostce bezpieczeństwo prawne; umożliwiają jej decydowanie o swoim postępowaniu na podstawie pełnej znajomości przesłanek działania organów państwowych oraz konsekwencji prawnych, jakie jej działania mogą pociągnąć za sobą" (wyrok TK z 14 czerwca 2000 r., P 3/00). Zasady zaufania do państwa nie można pojmować tylko w sposób formalny, rozumiany jako poprawne proceduralnie uchwalenie przepisów, ich opublikowanie, niezależnie od ich treści. Aspekt materialny działalności prawodawczej, uwzględniający zakres działalności normatywnej ustawodawcy, jego treść oraz relację podejmowanych rozstrzygnięć do standardów demokratycznego państwa prawnego, ma fundamentalne znaczenie z perspektywy obywatela i jego stosunku do państwa. Nie bez przyczyny zasadę tę nazywa się inaczej zasadą lojalności państwa wobec obywateli. Na aspekt materialny zasady zaufania obywateli do państwa wskazuje *expressis verbis* Wojciech Sokolewicz: „Zasada zaufania (lojalności) odnosi się nie tylko do trybu i formy stanowionego prawa. Cały proces stosowania prawa, począwszy od wykładni, powinien odbywać się w zgodności z tą zasadą" (W. Sokolewicz, *Komentarz do art. 2*, [w:] L. Garlicki (red.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, t. V Warszawa 2007, s. 34. Por. też wyrok TK z 27 listopada 1997 r., U 11/97). Jak się wydaje, zasadę zaufania obywateli do państwa należy pojmować jeszcze szerzej. Składa się na nią nie tylko właściwy formalnie proces stanowienia prawa, wprowadzenie *vacatio legis* i stabilność prowadzonej wykładni. Zasadę lojalności urzeczywistnia się już na etapie kształtowania treści przepisów. Nie sposób utrzymać relację zaufania i lojalności, jeżeli państwo kształtuje swoje kompetencje w sposób poważnie ingerujący w wolności i prawa obywateli, nie wskazując granic korzystania z tych kompetencji, lub wyznaczając granice przekraczające zasadę proporcjonalności. Problem ten

jest zauważalny w kontekście wskazywanym w niniejszym wniosku. Przekazanie obywatelom komunikatu, że mogą być inwigilowani przez służby policyjne i służby państwowe przez osiemnaście miesięcy z pewności nie buduje relacji zaufania między państwem i obywatelami. Zasadniczy wpływ na problemy w tej relacji ma także to, że obywatel nie zostanie, choćby następczo, poinformowany o prowadzonych wobec niego czynnościach kontroli operacyjnej. Informacja nie zostanie przekazana nawet wtedy, gdy nie wykryto żadnych okoliczności mogących uzasadniać pierwotne podejrzenia, które spowodowały złożenie wniosku do sądu i rozpoczęcie kontroli operacyjnej. Trybunał Konstytucyjny w wyroku z 30 lipca 2014 r. dopuścił zróżnicowanie standardów przeprowadzania kontroli operacyjnej, zwłaszcza jeżeli prowadzona jest ona przez służby odpowiadające za bezpieczeństwo państwa. Nie oznacza to jednak, że państwo może zupełnie porzucić wynikający ze standardów praw człowieka wymóg określenia maksymalnego okresu prowadzenia czynności operacyjno-rozpoznawczych wobec jednostek. Okres ten mógłby być dłuższy niż w przypadku pozostałych służb, ale powinien być określony.

Biorąc powyższe pod uwagę, w przekonaniu Rzecznika Praw Obywatelskich określony w przepisach czas prowadzenia czynności z zakresu kontroli operacyjnej przekracza ramy konieczne w demokratycznym państwie prawa.

Możliwość stosowania kontroli operacyjnej przez tak długi okres budzi poważne wątpliwości z perspektywy wolności i praw człowieka. Konieczne jest zatem zrekonstruowanie katalogu dóbr, w które ustawodawca ingeruje, a także kolidujących z nimi dóbr mogących uzasadniać wprowadzoną regulację. Ostateczne rozstrzygnięcie tak ukształtowanej kolizji jest możliwe na podstawie art. 31 ust. 3 Konstytucji, a więc z wykorzystaniem zasady proporcjonalności.

W pierwszej kolejności narzucającym się wzorcem kontroli jest prawo do prywatności. Zgodnie z art. 47 Konstytucji RP, każdy ma prawo do ochrony prawnej życia prywatnego,

rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym. W literaturze podnosi się, że prawnej ochronie podlegają wszystkie aspekty życia jednostki w obszarach wskazanych w art. 47 Konstytucji RP. Prawo do prywatności było wielokrotnie wzorcem kontroli w postępowaniach przed Trybunałem Konstytucyjnym, także w sprawach dotyczących zbierania i przetwarzania informacji o osobie. W wyroku z 20 stycznia 2015 r. Trybunał Konstytucyjny zauważył, że: „Stanowiąc jeden z podstawowych elementów aksjologii demokratycznego państwa prawnego, konstytucyjna ochrona prywatności to w szczególności możność samodzielnego decydowania o ujawnianiu innym podmiotom informacji dotyczących własnej osoby, a także sprawowania kontroli nad tymi informacjami, nawet jeżeli znajdują się w posiadaniu innych osób (autonomia informacyjna jednostki) oraz możność samostanowienia o swym życiu osobistym w aspekcie przedmiotowym, podmiotowym oraz czasowym (autonomia decyzyjna jednostki). W sferze autonomii informacyjnej normy konstytucyjne gwarantują jednostce ochronę przed pozyskiwaniem, przetwarzaniem, przechowywaniem i ujawnieniem, w sposób naruszający reguły przydatności, niezbędności i proporcjonalności sensu stricto, informacji m.in. o: a) stanie zdrowia (cyt. wyroki o sygn. U 5/97; U 3/01); b) sytuacji majątkowej (cyt. wyroki o sygn. K 21/96; K 41/02); c) sytuacji rodzinnej (cyt. wyroki o sygn. SK 40/01; K 20/03); d) przeszłości politycznej lub społecznej (cyt. wyroki o sygn. K 24/98; K 7/01; K 31/04); e) nazwisku lub wizerunku (cyt. wyrok o sygn. K 17/05; K 25/09) lub f) innych informacji niezbędnych dla działań organów władzy publicznej (cyt. wyroki o sygn. K 4/04; K 45/02; K 54/07; K 33/08). W sferze autonomii decyzyjnej normy konstytucyjne gwarantują jednostce ochronę przed - dokonaną z naruszeniem reguły przydatności, niezbędności i proporcjonalności sensu stricto - ingerencją w decyzje jednostki m.in. o: a) własnym życiu lub zdrowiu (cyt. wyrok o sygn. SK 48/05; K 16/10); b) kształtowaniu życia rodzinnego (cyt. wyroki o sygn. K 1/98; K 18/02); c) wychowaniu dzieci zgodnie z własnymi przekonaniami (m.in cyt. wyrok o sygn. U 10/07); d)

urodzeniu dziecka (por. wyrok o sygn. K 26/96)" (wyrok TK z 20 stycznia 2015 r., K 39/12). W świetle tego rozstrzygnięcia nie można mieć wątpliwości, że autonomia informacyjna oraz autonomia decyzyjna jednostki muszą być wzięte pod uwagę podczas oceny zgodności kwestionowanych przepisów z Konstytucją RP. Jest też w zasadzie oczywiste, że czynności z zakresu kontroli operacyjnej ingerują w tak zrekonstruowaną autonomię człowieka, zakorzenioną w zasadzie ukonstytuowanej w art. 47 Konstytucji RP.

Prawo do prywatności było także jednym z podstawowych wzorców kontroli w postępowaniu zakończonym wyrokiem Trybunału Konstytucyjnego z 30 lipca 2014 r. W świetle tego rozstrzygnięcia należy stwierdzić, że niedopuszczalne jest domniemywanie kompetencji władzy publicznej w obszarze ingerencji w prywatność jednostki. Do powstrzymania się od takiej ingerencji zobowiązane są nie tylko organy państwa, ale także podmioty prywatne. Konstatacja Trybunału Konstytucyjnego nie pozostawia żadnych wątpliwości: „(...) pozyskiwanie informacji o życiu prywatnym jednostek przez organy władzy publicznej, zwłaszcza niejawnie, musi być ograniczone do koniecznych sytuacji, dopuszczalnych w demokratycznym państwie wyłącznie dla ochrony konstytucyjnie uznanych wartości i zgodnie z zasadą proporcjonalności. Warunki gromadzenia i przetwarzania tych danych przez władze publiczne muszą być unormowane w ustawie w sposób jak najbardziej przejrzysty, wykluczający arbitralność i dowolność ich stosowania" (wyrok TK z 30 lipca 2014 r., K 23/11; por. też wyrok SN z dnia 25 czerwca 2015 r., sygn. V CSK 507/14, Legalis nr 1337785).

Rekonstruując wzorzec z art. 47 Konstytucji RP nie sposób nie odnieść się do art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności, który statuuje co następuje: „1. Każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji. 2. Niedopuszczalna jest ingerencja władzy publicznej w korzystanie z tego prawa, z wyjątkiem przypadków przewidzianych przez ustawę i

koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności innych osób". Przepis ten był wielokrotnie przedmiotem rozważań prowadzonych przez Europejski Trybunał Praw Człowieka, także w kontekście problematyki czynności operacyjno-rozpoznawczych. W wyroku z dnia 28 czerwca 2007 r. Trybunał stwierdził, że prawo do prywatności oraz klauzula z art. 8 § 2 EKPC wymaga, aby ewentualne ograniczenia prywatności polegające na prowadzeniu wobec jednostki czynności operacyjno-rozpoznawczych wynikały z przepisów jasnych, precyzyjnych, dostępnych jednostce. Nadto, ramy prowadzonej kontroli powinny być rozsądne (wyrok ETPC z 28 czerwca 2007 r. w sprawie *The Association for European Integration and Human Rights i Ekimdzhiev p. Bułgarii,* nr 62540/00). Trybunał w tym wyroku wskazał *expressis verbis*, że przepisy muszą określać czas trwania inwigilacji (por. też inne wyroki dotyczące kontroli operacyjnej i retencji danych: wyr. ETPC z 4 maja 2000 r. w sprawie *Rotaru p. Rumunii,* nr 28341/95; wyr. ETPC z 16 lutego 2000 r., w sprawie *Amann p. Szwajcarii,* nr 27798/95). Europejski Trybunał Praw Człowieka w wyroku z 21 czerwca 2011 r. wyeksplikował, że „życie prywatne to także działalność o charakterze zawodowym, albowiem zasięg interakcji z innymi ludźmi nawet w publicznym kontekście może w sobie skrywać życie prywatne (wyrok ETPC z 21 czerwca 2011 r. w sprawie *Shimovolos p. Rosji,* nr 30194/09). Nie sposób nie odnieść się także do art. 17 Międzynarodowego Paktu Praw Obywatelskich i Politycznych. Komitet Praw Człowieka ONZ wielokrotnie odwoływał się do tego wzorca, wskazując na nieprawidłowości w zakresie prowadzonych przez państwa czynności operacyjno-rozpoznawczych (por. opinie dotyczące sprawozdań przedkładanych przez państwa na podstawie art. 40 MPPOiP: USA – opinia z 18 grudnia 2006 r., sygn. CCPR/C/USA/CO/3/Rev.1, pkt 21; Holandii – opinia z 25 kwietnia 2009 r., sygn.

CCPR/C/NLD/CO/4, pkt 15; Szwecji – opinia z 7 maja 2009 r., sygn. CCPR/C/SWE/CO/6, pkt 18; Franci – opinia z 17 kwietnia 2015 r., sygn. CCPR/C/FRA/CO/5, pkt 13).

Mając powyższe na względzie, Rzecznik Praw Obywatelskich nie ma wątpliwości, że przepisy kwestionowane w niniejszym wniosku stanowią ingerencję w prawa rekonstruowane z art. 47 Konstytucji RP i z art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności.

Przepisy będące przedmiotem zarzutu budzą także poważne wątpliwości w świetle art. 49 Konstytucji RP, który stanowi, że: „Zapewnia się wolność i ochronę tajemnicy komunikowania się. Ich ograniczenie może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej określony". Wolność komunikowania się już w swojej istocie zawiera poufność polegającą na „zakazie zmuszania adresatów do ujawniania treści otrzymywanych przekazów, jak i na zakazie adresowanym do wszystkich innych podmiotów, łącznie z organami władzy publicznej, podejmowania prób poinformowania się o tych treściach bez zgody adresata. Co więcej, obejmuje również poufność co do faktu, że jest się w ogóle adresatem określonych przekazów" (P. Sarnecki, *Komentarz do art. 49,* [w:] L. Garlicki (red.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, t. III, Warszawa 2003, s. 3). Wolność i poufność komunikowania się jest blisko związana z godnością człowieka, określającą go jako autonomiczny podmiot prawa, z istoty korzystający ze swojej wolności i wchodzący w relacje z innymi ludźmi. Stosowanie czynności z zakresu kontroli operacyjnej ingeruje w wolność i poufność komunikowania się. Ustalenie, że jest to dobro bardzo zbliżone do godności człowieka, silnie w niej zakorzenione, pozwala twierdzić, że jakakolwiek ingerencja musi być solidnie uzasadniona i umocowana w innym dobru ulokowanym wysoko w konstytucyjnej hierarchii dóbr chronionych. Takie warunki muszą spełniać także przepisy regulujące czas trwania kontroli operacyjnej. Im dłuższy okres dopuszczalnego prowadzenia takich czynności, tym silniejsze musi być uzasadnienie odwołujące się do konstytucyjnego systemu dóbr.

Zdaniem Rzecznika Praw Obywatelskich długie osiemnastomiesięczne okresy prowadzenia kontroli przez ww. służby stanowią naruszenie art. 49 Konstytucji RP.

Kolejnym wzorcem kontroli jest art. 51 ust. 2 Konstytucji RP, który zakazuje pozyskiwania, gromadzenia i udostępniania innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym. Przepis ten jest naturalną konsekwencją prawa do prywatności (P. Sarnecki, *Komentarz do art. 51*, [w:] L. Garlicki (red.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, t. III, Warszawa 2003, s. 2). Trudności może wywoływać ustalenie kryteriów pozwalających na selekcję danych, które są „niezbędne w demokratycznym państwie prawnym". W literaturze proponuje się następującą dyrektywę interpretacyjną: „jeżeli zakres podobnych systemów informacyjnych staje się dla wygody administracji zbyt szeroki (inwigilacja <<na wszelki wypadek>> szerszych grup społecznych, jednolite <<konto informacyjne>> obywatela powstające z integracji setek danych administracyjnych z różnych dziedzin) lub szczegółowość danych prowadzi do tworzenia <<profilów osobowych>> (uproszczonej informatycznej charakterystyki jednostki), czy wreszcie dochodzi do ukrytego lub jawnego oznaczenia obywateli za pomocą numerów identyfikacyjnych nie o charakterze porządkowym, lecz znaczącym, mamy do czynienia z przypadkiem wykraczania poza to, co niezbędne w demokratycznym państwie prawnym" (I. Lipowicz, [w:] J. Boć, *Konstytucje Rzeczypospolitej Polskiej oraz komentarz do Konstytucji RP z 1997 r.*, Wrocław 1998, s. 99). Badając niezbędność w państwie demokratycznym należy także wziąć pod uwagę przewidziany w przepisach czas trwania czynności z zakresu kontroli operacyjnej. Nie wydaje się uzasadnione przyjęcie, że w świetle art. 51 ust. 2 Konstytucji RP możliwie jest prowadzenie kontroli operacyjnej bez rozsądnych granic czasowych. W przekonaniu Rzecznika Praw Obywatelskich kryterium rozsądnych granic czasowych, wynikającego z art. 51 ust. 2 Konstytucji RP, nie spełniają przepisy ustaw wskazanych w petitum wniosku.

Ingerencję w wolności i prawa człowieka i obywatela, rekonstruowane z art. 47, 49 i 51 ust. 2 Konstytucji RP, należy zbadać w świetle kryteriów wynikających z art. 31 ust. 3 Konstytucji RP statuującego zasadę proporcjonalności. Jak wielokrotnie wskazywał Trybunał Konstytucyjny w orzecznictwie, zawarta w art. 31 ust. 3 Konstytucji zasada proporcjonalności wymaga po pierwsze, aby ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw wprowadzane były w formie ustawy, co wyklucza normowanie ich w aktach niższej rangi. Po drugie zaś zasada ta w aspekcie materialnym dopuszcza ustanawianie tylko takich ograniczeń, które nie naruszają istoty danej wolności lub prawa podmiotowego i tylko wtedy, gdy istnieje konieczność ich wprowadzenia w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia, moralności publicznej, albo wolności i praw innych osób. Co istotne, zakres ograniczeń powinien być proporcjonalny, tzn. konieczny dla realizacji określonego celu. W związku z tym rekonstruuje się trzy kryteria: przydatności, konieczności i proporcjonalności sensu stricto przyjmowanych ograniczeń. Ingerencja taka jest zatem dopuszczalna, jeżeli jest w stanie doprowadzić do zamierzonych przez nią skutków, jest niezbędna dla ochrony interesu publicznego, z którym jest powiązana, a jej efekty pozostają w odpowiedniej proporcji do ciężarów nakładanych przez nią na obywatela (zob. m.in. wyrok TK z 3 czerwca 2008 r., sygn. K 42/07, wyrok TK z 29 września 2008 r., sygn. SK 52/05; por. też K. Wojtyczek, *Zasada proporcjonalności jako granica prawa karania*, [w:] A. Zoll (red.), *Racjonalna reforma prawa karnego*, Warszawa 2001, s. 297; M. Piechowiak, *Klauzula limitacyjna a nienaruszalność praw i godności*, „Przegląd Sejmowy" 2009, nr 2, s. 56–57; A. Stępkowski, *Zasada proporcjonalności w europejskiej kulturze prawnej*, Warszawa 2010, s. 194; A. Zoll, *Konstytucyjne aspekty prawa karnego*, [w:] T. Bojarski (red.), *Źródła prawa karnego. System Prawa Karnego*, t. 2, Warszawa 2011, s. 237–241).

Z uwagi na to, że każda regulacja dotycząca działań władzy publicznej w obszarze czynności operacyjno-rozpoznawczych prowadzi do ograniczeń w korzystaniu z wolności i praw, ustawodawca karny powinien wykazać w każdym przypadku, że proponowane rozstrzygnięcie normatywne spełnia kryteria testu proporcjonalności. Ustawodawca powinien w pierwszej kolejności ustalić cel proponowanej normy, wykazać jej konieczność w świetle zamierzonego celu, jej przydatność w jego osiągnięciu, a w końcu przeprowadzić test preferencji implikowany przez kolizję między dobrem, które chce chronić, a dobrem powiązanym z prawami i wolnościami, które planowana regulacja narusza.

Na ustawodawcy spoczywa ciężar dowodu wykazania, że przepis ingerujący w prawa i wolności człowieka spełnia kryteria wynikające z zasady proporcjonalności. W ocenie Rzecznika Praw Obywatelskich przepisy kwestionowane w tej części wniosku, w zakresie, w jakim ustalają czas trwania kontroli operacyjnej łącznie na osiemnaście miesięcy nie spełniają kryterium konieczności. Także zasada proporcjonalności *sensu stricto* będzie zachowana tylko, gdy ingerencja w prawa i wolności będzie odbywała się w rozsądnych ramach czasowych. Trudno jest przyjąć, że służby policyjne i służby specjalne potrzebują aż osiemnastu miesięcy na zebranie materiałów uzasadniających wszczęcie postępowania karnego. Należy pamiętać, że Kodeks postępowania karnego także przewiduje możliwość stosowania środków z zakresu kontroli operacyjnej, prowadzonej już jednak w sposób obudowany gwarancjami procesowymi, w reżimie procedury karnej.

W przekonaniu Rzecznika niezgodne z Konstytucją są również art. 27 ust. 9 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2015 r., poz. 1929 ze zm.) i art. 31 ust. 7 ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. z 2014 r., poz. 253 ze zm.) w zakresie, w jakim nie wyznaczają górnej granicy czasu trwania kontroli operacyjnej.

Problematyka ta stała się przedmiotem zaskarżenia we wniosku Rzecznika do Trybunału Konstytucyjnego z dnia 4 grudnia 2015 r. (sygn. akt K 32/15).

II. Niezgodność art. 19 ust. 15h ustawy z dnia 6 kwietnia 1990 r. o Policji; art. 9e ust. 16h ustawy z dnia 12 października 1990 r. o Straży Granicznej; art. 36d ust. 1h ustawy z dnia 28 września 1991 r. o kontroli skarbowej; art. 31 ust. 16h ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych; art. 27 ust. 15j ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu; art. 31 ust. 14h ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego; art. 17 ust. 15h ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym – w zakresie, w jakim posługuje się nieostrym kryterium „dobra wymiaru sprawiedliwości" i nie określa wagi okoliczności, która ma być ustalona na podstawie materiałów mogących zawierać informacje, o których mowa w art. 178a, art. 180 § 2 i art. 180 § 3 Kodeksu postępowania karnego – z art. 2 Konstytucji RP, z art. 42 ust. 2, art. 47, art. 49, art. 51 ust. 2 w zw. z art. 31 ust. 3 Konstytucji RP oraz z art. 6 Konwencji o ochronie praw człowieka i podstawowych wolności;

Zaskarżone w tej części przepisy przewidują mechanizm nakładający na sądy obowiązek wydania postanowienia w przedmiocie dopuszczenia do wykorzystania w postępowaniu karnym materiałów zawierających informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 k.p.k., nieobjęte zakazami określonymi w art. 178a i art. 180 § 3 k.p.k. z wyłączeniem informacji o przestępstwach, o których mowa w art. 240 § 1 k.k., zawsze wtedy, gdy jest to niezbędne ze względu na dobro wymiaru sprawiedliwości, a okoliczność ta nie może być ustalona na podstawie innego dowodu. Wydanie takiego postanowienia następuje na podstawie złożonego przez prokuratora

bądź Prokuratora Generalnego (w zależności od faktyczno-prawnego układu konkretnego przypadku) wniosku o dopuszczenie do wykorzystania w postępowaniu karnym ww. materiałów.

W kontekście uregulowań będących przedmiotem niniejszego zarzutu, w pierwszej kolejności należy zaznaczyć, że dotychczas nie wykształciła się utrwalona i jednolita praktyka judykatury w zakresie stosowania kontroli operacyjnej wobec osób zobowiązanych do zachowania tajemnicy zawodowej. Brak jest także jednolitych zasad postępowania z materiałami zawierającymi informacje objęte tajemnicą zawodową. Z praktyki orzeczniczej wynika, że sądy często nawet nie rozważały, czy osoby poddane kontroli operacyjnej nie są objęte zakazami dowodowymi. Takie wnioski płyną m.in. z pisma z 19 grudnia 2013 r. skierowanego przez Trybunał Konstytucyjny do prezesów wszystkich sądów apelacyjnych, a także do prezesów sądów okręgowych mających siedzibę w miastach będących siedzibą apelacji (pkt 3.11.1 wyroku TK z dnia 30 lipca 2014 r., K 23/11).

Ponadto w cytowanym orzeczeniu Trybunał zwrócił uwagę na konieczność wprowadzenia wymogu uprzedniego uzyskania zgody na pozyskiwanie danych telekomunikacyjnych osób zobowiązanych do zachowania tajemnicy zawodowej. Zgodnie ze wskazaniami Trybunału konieczne jest wprowadzenie regulacji umożliwiających udostępnianie takich danych służbom policyjnym i organom ochrony państwa dopiero po udzieleniu zgody na udostępnienie przez niezależny organ.

Regulacje wskazane w przedmiotowym zarzucie stanowią jedną z najdalej idących oraz najbardziej dotkliwych form ingerencji w wolności i prawa jednostki. Dotykają bowiem materii szczególnie wrażliwej, związanej z działalnością zawodową jednostki. O wyjątkowym charakterze informacji związanych z działalnością zawodową lub piastowaniem określonej funkcji przesądza fakt, że owe wiadomości dotykają przeważnie interesów majątkowych oraz prywatnych o dużym znaczeniu dla funkcjonowania i bezpieczeństwa szerokich grup

jednostek. Ponadto, nawet w sytuacji, gdy wiadomości te mają znaczenie jedynie dla pojedynczych podmiotów, często są relewantne w zakresie kwestii fundamentalnych dla ich funkcjonowania, takich jak ochrona życia prywatnego i interesów majątkowych, odpowiedzialność karna oraz cywilna.

Wskazane w niniejszym zarzucie regulacje przewidują obowiązek dopuszczenia do wykorzystania w postępowaniu karnym przez sąd materiałów objętych tajemnicą zawodową lub związanych z pełnioną funkcją. Takie dopuszczenie powinno nastąpić zawsze, gdy jest to konieczne ze względu na dobro wymiaru sprawiedliwości, o ile dana okoliczność nie może być ustalona na podstawie innego dowodu.

Identycznym kryterium posługuje się art. 180 § 2 k.p.k. przewidujący możliwość przesłuchania osób obowiązanych do zachowania tajemnicy notarialnej, adwokackiej, radcy prawnego, doradcy podatkowego, lekarskiej, dziennikarskiej lub statystycznej. Między tymi regulacjami występuje jednak fundamentalna różnica polegająca na tym, że o ile w przypadku art. 180 § 2 k.p.k. to dopiero sąd decyduje o dopuszczalności ingerencji w tajemnicę zawodową w celu wykorzystania określonych wiadomości na potrzeby postępowania karnego, o tyle w przypadku mechanizmu przewidzianego w przepisach skarżonej ustawy, sąd decyduje nie o uchyleniu owej tajemnicy, lecz jedynie o dopuszczalności wykorzystania na potrzeby postępowania karnego pewnych wiadomości uprzednio uzyskanych wskutek naruszenia tajemnicy zawodowej. Uzyskanie informacji objętych tajemnicą może nastąpić bowiem bez szczególnej zgody sądu, a rezultaty takiej inwigilacji mające znaczenie dla powstania odpowiedzialności karnej są jedynie wtórnie „legalizowane” przez sąd poprzez ich dopuszczenie do wykorzystania w postępowaniu karnym. Ponadto skarżone przepisy – w przeciwieństwie do art. 180 k.p.k. – nie przewidują żadnej możliwości zaskarżenia decyzji sądu w przedmiocie dopuszczenia dowodów na podstawie informacji objętych tajemnicą jawną i zawodową.

Rozwiązanie przyjęte wskutek nowelizacji ustawy o Policji oraz niektórych innych ustaw zdaje się naruszać w sposób rażący wyrażoną w art. 2 zasadę demokratycznego państwa prawnego. Jakkolwiek uregulowanie przewidziane w art. 180 § 2 k.p.k. przewiduje pewien mechanizm łagodzący ingerencję w tajemnicę zawodową poprzez uprzednią kontrolę zasadności takiej ingerencji przez sąd, już na gruncie tego przepisu w nauce prawa karnego podniesiono wiele wątpliwości. W literaturze wielokrotnie wskazywano, że znaczenie społeczne tajemnicy, o której mowa w 180 § 2 k.p.k. wymaga wprowadzenia dodatkowych kryteriów podkreślających wagę i istotność informacji ujawnionych w procesie karnym (D. Gruszecka, *Komentarz do art. 180 Kodeksu postępowania karnego* [w:] *Kodeks postępowania karnego. Komentarz,* Warszawa 2015, s. 420).

W tym kontekście decyzja ustawodawcy o wprowadzeniu abstrakcyjnej wartości w postaci dobra wymiaru sprawiedliwości jako kryterium dopuszczalności wykorzystania w postępowaniu karnym informacji uzyskanych za pomocą naruszenia tajemnicy zawodowej powinna budzić duży niepokój. Zagrożenie dla ochrony praw i wolności jednostki potęguje dodatkowo fakt, że ustawodawca nie zdecydował się na dokładniejsze określenie wagi okoliczności, która ma być ustalona na podstawie materiałów mogących zawierać informacje, o których mowa w art. 178a, art. 180 § 2 i art. 180 § 3 k.p.k.

Obecny stan prawny zdaje się stwarzać pole do nieskrępowanej ograniczeniami formalnymi dowolności w zakresie ingerencji w informacje objęte tajemnica zawodową podmiotów obdarzonych wysokim zaufaniem ze strony społeczeństwa. Tymczasem Trybunał Konstytucyjny w wyroku z dnia 30 lipca 2014 r. (K 23/11) wyraźnie wskazał, że zbieranie informacji niejawnych może być uzasadnione tylko na potrzeby pociągnięcia do odpowiedzialności karnej za poważne przestępstwa i zagrożenia dla bezpieczeństwa państwa. Podobne stanowisko zaprezentował także Trybunał Sprawiedliwości Unii Europejskiej w wyroku z 8 kwietnia 2014 r. (C-293/12). W szeregu orzeczeń na podobne stanowisko w

zakresie niekonstytucyjności formułowania przesłanek określających dopuszczalną ingerencję w zakresie przekazywania danych w sposób zbyt ogólny i abstrakcyjny stanęła najnowsza judykatura wielu sądów konstytucyjnych państw członkowskich Unii Europejskiej (por. wyrok Sądu Konstytucyjnego Bułgarii z dnia 12 marca 2015 r., (8/2014); wyrok Sądu Konstytucyjnego Rumunii z 8 grudnia 2009 r. (Nr 1258); w tym duchu także wyrok Federalnego Sądu Konstytucyjnego Niemiec z 2 marca 2010 r. (sygn. 1 BvR 256/08); wyrok Trybunału Konstytucyjnego Austrii (sygn. G 47/2012, G 59/2012, G 62/2012, G 70/2012, G 71/2012). Niedookreśloność wagi okoliczności, która ma być ustalona na podstawie materiałów mogących zawierać informacje objęte tajemnicą zawodową oraz abstrakcyjność pojęcia „dobro wymiaru sprawiedliwości" naruszają w sposób rażący konstytucyjną zasadę zaufania do państwa. Omawiane uregulowania nie przewidują bowiem żadnych mechanizmów zabezpieczających ich prawa i wolności. Istota czynności operacyjno-rozpoznawczych przekreśla możliwość informowania osób będących obiektem takich działań i właśnie dlatego podstawowym obowiązkiem państwa w tym zakresie jest ustanowienie sprawnego mechanizmu swoistej samokontroli jego organów i ochrony jednostki przed działaniami inwigilacyjnymi. Skoro ingerencja w prawa i wolności jednostki *ex definitione* ma się odbywać bez jej wiedzy, to rolą państwa jako gwaranta przestrzegania jej praw i wolności jest ustanowienie kontrolnego mechanizmu za pomocą organu niezależnego od innych podmiotów państwa zainteresowanych uzyskaniem informacji wskutek inwigilacji.

Wykorzystanie na potrzeby postępowania karnego informacji objętych tajemnicą zawodową na podstawie wyjątkowo nieostrych kryteriów staje się szczególnie niebezpieczne z punktu widzenia ochrony praw i wolności jednostki w zakresie informacji objętych tajemnicą zawodową niektórych zawodów prawniczych. Mechanizm pozyskiwania takich informacji za pomocą czynności operacyjno-rozpoznawczych prowadzonych w stosunku do adwokatów oraz radców prawnych może prowadzić do rażącego naruszenia jednego z fundamentalnych praw

jednostki w państwie prawa, jakim jest prawo do obrony (art. 42 ust. 2 Konstytucji RP). W świetle art. 6 ust. 1 ustawy z dnia 26 maja 1982 r. – Prawo o adwokaturze (t.j. Dz.U. z 2015 r., poz. 615): „Adwokat obowiązany jest zachować w tajemnicy wszystko, o czym dowiedział się w związku z udzielaniem pomocy prawnej". Z kolei zgodnie z art. 3 ust. 3 ustawy z dnia 6 lipca 1982 r. – O radcach prawnych (t.j. Dz.U z 2015 r., poz. 507): „Radca prawny jest obowiązany zachować w tajemnicy wszystko, o czym dowiedział się w związku z udzieleniem pomocy prawnej". Ze względu na fundamentalne znaczenie tajemnicy adwokackiej oraz radcowskiej dla sytuacji prawnej osób, których bezpośrednio dotyczą informacje objęte tajemnicą, konieczne jest wprowadzenie szczegółowo określonych wymagań co do trybu oraz przesłanek uchylenia obowiązku zachowania takiej tajemnicy. Tymczasem procedura przewidziana w art. 19 ust. 15h ustawy o Policji, art. 9e ust. 16h ustawy o Straży Granicznej, art. 36d ust. 1h ustawy o kontroli skarbowej, art. 31 ust. 16h ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 27 ust. 15j ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 31 ust. 14h ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego oraz w art. 17 ust. 15h ustawy o Centralnym Biurze Antykorupcyjnym zdaje się nie spełniać żadnego z wyżej wymienionych wymogów. Sama ingerencja w tajemnicę zawodową odbywa się bowiem w warunkach braku jakiegokolwiek mechanizmu kontrolnego. Równie niepokojący jest fakt, że weryfikacja możliwości wykorzystania informacji objętych tajemnicą zawodową na potrzeby postępowania karnego odbywa się na podstawie nieostrego kryterium dobra wymiaru sprawiedliwości. Abstrakcyjność tego kryterium sprawia, że sąd, rozstrzygając w przedmiocie dopuszczalności wykorzystania takich informacji zobowiązany jest do każdorazowego ważenia dwóch wartości – jednostkowego prawa do obrony oraz kolektywnego dobra wymiaru sprawiedliwości. Pomijając trafność kolektywistyczno-obiektywnego ujęcia dobra wymiaru sprawiedliwości, można przypuszczać, że kolizja ww. dóbr niemalże zawsze powinna być rozstrzygnięta na

korzyść dobra ponadindywidualnego mającego znaczenie dla sprawnego funkcjonowania całego aparatu państwowego. Dobro wymiaru sprawiedliwości, bowiem to wszelkie możliwe układy sytuacyjne o charakterze prawnym oraz faktycznym, które w jakikolwiek sposób mogą przyczynić się do realizacji podstawowych zadań i celów stawianych wymiarowi sprawiedliwości. W tym kontekście nie powinno ulegać wątpliwości, że rozstrzygając w przedmiocie dopuszczalności wykorzystania na potrzeby postępowania karnego informacji objętych tajemnicą adwokacką lub radcowską, sąd będzie musiał odmówić pierwszeństwa interesowi jednostkowemu w imię dobra wymiaru sprawiedliwości będącego jednym z aspektów abstrakcyjnego dobra wspólnego. Wyjątkowo ogólne ujmowanie dóbr prawnych o charakterze kolektywnym, których nie da się przyporządkować chociażby bliżej określonego zbioru konkretnych wartości jest zjawiskiem wyjątkowo niebezpiecznym, prowadzącym do przekreślenia istoty dóbr indywidualnie ujmowanych za pomocą mechanizmów urealniających ich przestrzeganie. Tak więc skarżone regulacje prowadzą sądy do prostej alternatywy – albo dopuścić do wykorzystania w postępowaniu karnym materiały zawierające informację objęte tajemnica zawodową, albo podważyć znaczenie prawidłowego funkcjonowania całego wymiaru sprawiedliwości i przyznać pierwszeństwu jednostkowemu prawu do obrony przysługującemu każdej jednostce (o ile, rzecz jasna, okoliczność nie może być ustalona na podstawie innego dowodu). Tymczasem samo dobro wymiaru sprawiedliwości zawiera przecież prawo do obrony jednostki jako jeden z warunków rzetelnego procesu stojącego u fundamentów dobra wymiaru sprawiedliwości.

Niedookreśloność przesłanek, spełnienie których powoduje powstanie po stronie sądu obowiązku niezwłocznego dopuszczenia do wykorzystania w postępowaniu karnym materiałów zawierających informacje stanowiące tajemnice związane z wykonywanie zawodu lub funkcji stanowi także naruszenie konstytucyjnie zagwarantowanego każdej jednostce prawa do ochrony życia prywatnego (art. 47 Konstytucji RP). Nie ma także wątpliwości, że

podnoszona w tym zakresie niedookreśloność przesłanek powoduje naruszenie art. 49 i 51 ust. 2 Konstytucji RP. Trybunał Konstytucyjny wyraźnie podkreślił, że konstytucyjną ochroną wynikającą z art. 47, art. 49 i art. 51 Konstytucji RP objęte są „wszelkie sposoby przekazywania wiadomości, w każdej formie komunikowania się, bez względu na fizyczny ich nośnik (np. rozmowy osobiste i telefoniczne, korespondencja pisemna, faks, wiadomości tekstowe i multimedialne, poczta elektroniczna). Ochrona konstytucyjna obejmuje nie tylko treść wiadomości, ale także wszystkie okoliczności procesu porozumiewania się, do których zaliczają się dane osobowe uczestników tego procesu, informacje o wybieranych numerach telefonów, przeglądanych stronach internetowych, dane obrazujące czas i częstotliwość połączeń, czy umożliwiające lokalizację geograficzną uczestników rozmowy, wreszcie dane o numerze IP czy numerze IMEI” (wyrok TK z 30 lipca 2014 r. o sygn. akt K 23/11). W tym samym wyroku Trybunał Konstytucyjny podkreślił również wyraźnie, że w ramach konstytucyjnie gwarantowanej wolności człowieka i jego autonomii informacyjnej mieści się również ochrona przed niejawnym monitorowaniem jednostki.

III. Niezgodność art. 20c ust. 1 oraz art. 20cb ust. 1 ustawy z dnia 6 kwietnia 1990 r. o Policji, art. 10b ust. 1 oraz art. 10bb ust. 1 ustawy z dnia 12 października 1990 r. o Straży Granicznej, art. 36b ust. 1 oraz art. 36bb ust. 1 ustawy z dnia 28 września 1991 r. o kontroli skarbowej, art. 30 ust. 1 oraz art. 30c ust. 1 ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28 ust. 1 oraz art. 28b ust. 1 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 32 ust. 1 oraz art. 32b ust. 1 ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, art. 18 ust. 1 oraz art. 18b ust. 1 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym, art. 75d ust. 1 oraz art. 75db ust. 1

ustawy z dnia 27 sierpnia 2009 r. o Służbie Celnej z art. 2, 30, 47, 49, 51 ust. 2 w zw. z art. 31 ust. 3 Konstytucji, art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności oraz art. 7 i 8 w zw. z art. 52 ust. 1 Karty Praw Podstawowych UE

Uchwalona w dniu 15 stycznia 2016 r. ustawa o zmianie ustawy o Policji dokonała zmian w art. 20c ust. 1 ustawy o Policji, art. 10b ust. 1 ustawy o Straży Granicznej, art. 36b ust. 1 ustawy o kontroli skarbowej, art. 30 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28 ust. 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 32 ust. 1 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, art. 18 ust. 1 ustawy o Centralnym Biurze Antykorupcyjnym oraz art. 75d ust. 1 ustawy o Służbie Celnej.

W brzmieniu obowiązującym po nowelizacji ustawy o Policji, na podstawie art. 20c ust. 1 ustawodawca przyznał Policji prawo do uzyskiwania danych niestanowiących treści odpowiednio, przekazu telekomunikacyjnego, przesyłki pocztowej albo przekazu w ramach usługi świadczonej drogą elektroniczną, a także do przetwarzania tych danych bez wiedzy i zgody osoby, której dotyczą. Prawo to przyznane zostało w celu zapobiegania lub wykrywania przestępstw albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych. Dane, do których uzyskiwania i przetwarzania zyskała dostęp Policja określone są odpowiednio w:

- art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243 ze zm., dalej jako: Prawo telekomunikacyjne) – tzw. „dane telekomunikacyjne”,
- art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. poz. 1529 oraz z 2015 r. poz. 1830, dalej jako: Prawo pocztowe) – tzw. „dane pocztowe”,

– art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422 orz z 2015 r. poz. 1844, dalej jako: uśude) – tzw. „dane internetowe”.

Analogiczne uprawnienia do uzyskiwania i przetwarzania danych uzyskały pozostałe służby:

– Straż Graniczna – w celu zapobiegania lub wykrywania przestępstw (art. 10b ust. 1 ustawy o Straży Granicznej),
– wywiad skarbowy – w celu zapobiegania lub wykrywania przestępstw skarbowych lub przestępstw, o których mowa w art. 2 ust. 1 pkt 14b i art. 36c ust. 1 pkt 3 ustawy o kontroli skarbowej (art. 36b ust. 1 ustawy o kontroli skarbowej),
– Żandarmeria Wojskowa – w celu zapobiegania lub wykrywania przestępstw, w tym przestępstw skarbowych, popełnionych przez osoby, o których mowa w art. 3 ust. 1 pkt 1, 3, 4, 5 i 6 albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych (art. 30 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych),
– Agencja Bezpieczeństwa Wewnętrznego – do realizacji zadań, o których mowa w art. 5 ust. 1 (art. 28 ust. 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu),
– Służba Kontrwywiadu Wojskowego – do realizacji zadań, o których mowa w art. 5 (art. 32 ust. 1 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego),
– Centralne Biuro Antykorupcyjne – do realizacji zadań, o których mowa w art. 2 (art. 18 ust. 1 ustawy o Centralnym Biurze Antykorupcyjnym),
– Służba Celna – w celu zapobiegania lub wykrywania przestępstw skarbowych, o których mowa w rozdziale 9 Kodeksu karnego skarbowego (art. 75d ust. 1 ustawy o Służbie Celnej).

Ponadto, zgodnie z art. 20cb ust. 1 ustawy o Policji, a także odpowiednio art. 10bb ust. 1 ustawy o SG, art. 36bb ust. 1 ustawy o kontroli skarbowej, art. 30c ust. 1 ustawy o Żandarmerii

Wojskowej i wojskowych organach porządkowych, art. 28b ust. 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 32b ust. 1 ustawy o Służbie Kontrwywiadu Wojskowego i Służbie Wywiadu Wojskowego, art. 75db ust. 1 ustawy o Służbie Celnej, służby będą uprawnione do pozyskiwania – w celu zapobiegania lub wykrywania przestępstw albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych (z odpowiednimi modyfikacjami w poszczególnych ustawach):

- z wykazu, o którym mowa w art. 179 ust. 9 Prawa telekomunikacyjnego – czyli z elektronicznego wykazu abonentów, użytkowników lub zakończeń sieci, z uwzględnieniem danych uzyskiwanych przy zawarciu umowy,
- o których mowa w art. 161 Prawa telekomunikacyjnego – dane dotyczące użytkownika, do których przetwarzania uprawniony jest dostawca publicznie dostępnych usług telekomunikacyjnych (dane osobowe),
- w przypadku użytkownika, który nie jest osobą fizyczną numer zakończenia sieci oraz siedzibę lub miejsce wykonywania działalności gospodarczej, firmę lub nazwę i formę organizacyjną tego użytkownika, w przypadku stacjonarnej publicznej sieci telekomunikacyjnej – także nazwę miejscowości oraz ulicy, przy której znajduje się zakończenie siedzi, udostępnione użytkownikowi.

Analizując wskazane przepisy ustaw należy rozpocząć od stwierdzenia, że w art. 20c ust. 1 o Policji (oraz analogicznie w pozostałych przepisach wskazanych ustaw) nie są spełnione kryteria uzasadniające ograniczenie praw i wolności obywatelskich, wynikających z Konstytucji, co podaje w wątpliwość zgodność art. 20c ust. 1 ustawy o Policji oraz pozostałych wskazanych przepisów z art. 2, 30, 47, 49, 51 ust. 2 Konstytucji w zw. z art. 31 ust. 3 oraz art. 8 EKPC i art. 7 i 8 w zw. z art. 52 ust. 1 KPP UE.

Jak wskazano wyżej, ustawa o Policji przewiduje dopuszczalność uzyskiwania danych telekomunikacyjnych, danych pocztowych i danych internetowych do celów określonych w zakwestionowanych przepisach. Tym samym celom ma służyć pozyskiwanie danych, określonych w art. 20cb ust. 1 ustawy o Policji.

Analizując katalog przestępstw, w przypadku których dopuszczalne jest uzyskiwanie i przetwarzanie tych danych w odniesieniu do poszczególnych służb wyraźnie widać, że jest on nadmiernie szeroki, co wskazuje na przekroczenie granic, o których mowa w art. 31 ust. 3 Konstytucji, art. 8 ust. 2 EKPC oraz art. 52 ust. 1 KPP UE. W art. 20c ust. 1 ustawy o Policji nie wskazano poszczególnych typów czynów zabronionych pod groźbą kary, lecz użyto ogólnego określenia „przestępstwa". Oznacza to możliwość uzyskiwania przez Policję danych w odniesieniu do wszystkich czynów zabronionych spełniających znamiona przestępstwa. Tym samym stanowić to będzie nadmierną ingerencję w prawo do prywatności i w prawo do ochrony danych osobowych, a także naruszenie zasady autonomii informacyjnej, wyrażone w art. 47, 49 oraz 51 ust. 2 Konstytucji, przez co naruszona jest również zasada godności człowieka, określona w art. 30 Konstytucji.

Z podobnych względów, za niezgodne ze wskazanymi wyżej wzorcami konstytucyjnymi oraz wzorcami określonymi w ratyfikowanych umowach międzynarodowych należy uznać:

- art. 10b ust. 1 i art. 10bb ust. 1 ustawy o Straży Granicznej, zawierający ogólne określenie „przestępstwa",
- art. 36b ust. 1 i art. 36bb ust. 1 ustawy o kontroli skarbowej, zawierający bardzo ogólne odniesienie do przestępstw skarbowych,
- art. 30 ust. 1 i art. 30c ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, zawierający odesłanie do przestępstw, w tym przestępstw skarbowych,
- art. 28 ust. 1 i art. 28b ust. 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, zawierający odesłanie do zadań określonych w art. 5 ust. 1 ustawy o Agencji

Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu; należy przy tym podkreślić, że odesłanie to oznacza, że Agencja Bezpieczeństwa Wewnętrznego będzie mogła uzyskiwać dane nie tylko w celu rozpoznawania, zapobiegania i wykrywania przestępstw, lecz także w celu realizacji pozostałych ustawowo określonych jej zadań, takich jak: rozpoznawanie, zapobieganie i zwalczanie zagrożeń godzących w bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny; uzyskiwanie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć istotne znaczenie dla ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego; podejmowanie innych działań określonych w odrębnych ustawach i umowach międzynarodowych,

- art. 32 ust. 1 i art. 32b ust. 1 ustawy o Służbie Kontrwywiadu Wojskowego i Służbie Wywiadu Wojskowego, odsyłający do zadań określonych w art. 5 ustawy o Służbie Kontrwywiadu Wojskowego i Służbie Wywiadu Wojskowego; odesłanie to oznacza, że Służba Kontrwywiadu Wojskowego będzie mogła uzyskiwać dane nie tylko w celu rozpoznawania, zapobiegania i wykrywania określonych przestępstw, lecz również w celu realizacji pozostałych ustawowo określonych jej zadań, takich jak podejmowanie działań przewidzianych dla Służby Kontrwywiadu Wojskowego w innych ustawach, a także umowach międzynarodowych, którymi RP jest związana;
- art. 18 ust. 1 i art. 18b ust. 1 ustawy o Centralnym Biurze Antykorupcyjnym, umożliwiający uzyskiwanie danych do realizacji zadań, określonych w art. 2 ustawy o Centralnym Biurze Antykorupcyjnym. Odesłanie to oznacza, że Centralne Biuro Antykorupcyjne będzie mogło uzyskiwać dane nie tylko w celu rozpoznawania, zapobiegania i wykrywania przestępstw określonych w ustawie, lecz również w celu realizacji pozostałych ustawowo określonych jego zadań, takich jak prowadzenie działalności analitycznej dotyczącej zjawisk występujących w obszarze właściwości Centralnego Biura Antykorupcyjnego oraz

podejmowanie innych działań określonych w odrębnych ustawach i umowach międzynarodowych;

– art. 75d ust. 1 i art. 75db ust. 1 ustawy o Służbie Celnej, zawierający odesłanie do przestępstw skarbowych, o którym mowa w rozdziale 9 Kodeksu karnego skarbowego. Należy zaznaczyć, że wskazane przepisy rozdziału 9 określają przestępstwa skarbowe i wykroczenia skarbowe przeciwko organizacji gier hazardowych. Analiza wykazu przestępstw określonych w przepisach tego rozdziału prowadzi do wniosku, że co najmniej część z tych przestępstw nie spełnia kryterium „wystarczająco poważnych".

Użyte w tych przepisach pojęcia nie tylko nie są precyzyjne, ale przede wszystkim nie spełniają wskazanego wyżej kryterium jasności przepisów. Tak ujęty cel gromadzenia i przetwarzania danych może bowiem oznaczać w istocie brak selektywności zarówno na etapie rozpoczęcia pozyskiwania danych internetowych, czyli możliwości uzyskiwania przez służby danych w postępowaniach w sprawie bliżej nieokreślonych czynów zabronionych, bez względu na ich szkodliwość społeczną. Oznacza ponadto, że nie zagwarantowano, by gromadzenie i przetwarzanie danych internetowych było subsydiarnym środkiem pozyskiwania informacji lub dowodów o jednostkach. Brak subsydiarności proponowanych przepisów otwiera możliwość wykorzystywania danych telekomunikacyjnych, pocztowych i internetowych nie tylko wówczas, gdy jest to rzeczywiście konieczne do wykrywania lub zapobiegania przestępstwom, ale także wtedy gdy jest to po prostu najprostsze i najwygodniejsze (zob. wyrok TK w sprawie K 32/04 lub K 54/07). W powiązaniu z przepisami dotyczącymi kontroli sądowej, o czym jeszcze będzie mowa w dalszej części wniosku, należy wyraźnie stwierdzić, że sądy nie będą mogły ocenić, na ile sięgnięcie w określonej sytuacji po dane było rzeczywiście niezbędne i należycie uzasadnione, co dodatkowo osłabia poziom ochrony prywatności jednostek. Do tej kwestii odniósł się również Trybunał Konstytucyjny w wyroku w sprawie K 23/11 wskazując, że „niejawne pozyskiwanie informacji o jednostkach w toku czynności operacyjno-

rozpoznawczych musi być środkiem subsydiarnym, czyli stosowanym wówczas, gdy inne rozwiązania są nieprzydatne lub nieskuteczne".

Na konieczność precyzyjnego uregulowania zakresu przestępstw, w przypadku których dopuszczalne jest sięganie po dane, wskazywały również trybunały: ETPC i TSUE, interpretując przepisy EKPC i KPP UE. W szczególności, we wspomnianych sprawach *Zakharov przeciwko Rosji* ETPC wskazał, że przesłanką uzasadniającą stwierdzenie naruszenia art. 8 EKPC jest m.in. brak sprecyzowania jakichkolwiek okoliczności, w których organy mogą prowadzić inwigilację obywateli. Z kolei w sprawie C-293/12 i C-594/12 Digital Rights Ireland TSUE, stwierdzając nieważność dyrektywy retencyjnej 2006/24/WE w związku z naruszeniem wymogu proporcjonalności przy ingerencji w prawo do prywatności i prawo do ochrony danych osobowych uznał, że nie wystarczy samo odniesienie się do „poważnych przestępstw" by uznać przesłanki wskazane w art. 52 ust. 1 KPP UE za spełnione i uzasadniające ingerencję w określone wyżej prawa.

Wskazane przepisy ustaw są zatem niezgodne z art. 30, 47, 49, 51 ust. 2 w zw. z art. 31 ust. 3 Konstytucji, a także z art. 8 EKPC oraz 7 i 8 w zw. z art. 52 ust. 2 KPP UE.

Ponadto, wskazane przepisy ustaw naruszają również art. 30, 47, 49, 51 ust. 2 Konstytucji w zw. z art. 2 Konstytucji statuującym zasadą ochrony zaufania do państwa i stanowionego przez nie prawa, a także zasadę określoności przepisów prawa poprzez odwołanie się do definicji pojęcia „dane internetowe", które nie jest jasne i precyzyjne, a tym samym zaskarżone przepisy naruszają wymóg przewidywalności przepisów ograniczających prawo do prywatności, prawo do ochrony danych osobowych oraz zasadę autonomii informacyjnej jednostki. W szczególności wskazać należy, że pojęcie „danych internetowych" definiowane jest poprzez odwołanie się do art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r., poz. 1422 ze zm.). Pojęcie to obejmuje zatem:

1) dane osobowe usługobiorcy niezbędne do nawiązania, ukształtowania treści, zmiany lub rozwiązania stosunku prawnego, między innymi nazwisko i imiona usługobiorcy, numer ewidencyjny PESEL, lub – gdy numer ten nie został nadany – numer paszportu, dowodu osobistego lub innego dokumentu potwierdzającego tożsamość, adres zameldowania na pobyt stały, adres do korespondencji, dane służące do weryfikacji podpisu elektronicznego usługobiorcy, adresy elektroniczne usługobiorcy;
2) inne dane niezbędne ze względu na właściwość świadczonej usługi lub sposób jej rozliczenia;
3) inne dane dotyczące usługobiorcy, które nie są niezbędne do świadczenia usługi drogą elektroniczną, przekazane za zgodą usługobiorcy;
4) tzw. dane eksploatacyjne, charakteryzujące sposób korzystania z usługi świadczonej drogą elektroniczną, w tym oznaczenia identyfikujące usługobiorcę, oznaczenia identyfikujące zakończenie sieci telekomunikacyjnej lub system teleinformatyczny, z którego korzystał usługobiorca, informacje o rozpoczęciu, zakończeniu oraz zakresie każdorazowego korzystania z usługi świadczonej drogą elektroniczną, informacje o skorzystaniu przez usługobiorcę z usług świadczonych drogą elektroniczną.

Rzecznik Praw Obywatelskich pragnie podkreślić, że wymienione w tym przepisie kategorie danych są określone bardzo ogólnie, co może powodować niejasności i prowadzić do zbyt szerokiego pojmowania tych pojęć, a w efekcie do nadmiernej ingerencji w prawa podstawowe. Przypomnieć należy, że prawo określające granice ingerencji państwa w prawa człowieka i obywatela musi spełniać wymogi jakościowe, być dostępne oraz przewidywalne dla jednostek – z prawa muszą wynikać okoliczności i warunki, w których władze publiczne będą sięgać po określone dane. Precyzja regulacji prawnej ma zapobiegać ryzyku arbitralności działań, z natury rzeczy pozostających poza zasięgiem kontroli publicznej. Niejasności

związane z zakresem danych internetowych, które mogą być gromadzone przez służby, powoduje, że nie można uznać, by spełniony był wymóg precyzyjności prawa.

Trzeba również podkreślić, że wskazany szeroki zakres informacji, do których będą mieć dostęp służby, będzie pozwalał na szerokie i precyzyjne odtworzenie różnych aspektów życia prywatnego. Może również prowadzić do budowania profilu osobowego osób uczestniczących w procesie komunikacji, a co za tym idzie – do ustalenia ich trybu życia, przynależności do organizacji społecznych czy politycznych, osobistych upodobań czy skłonności osób poddanych obserwacji. Uzyskiwanie i przetwarzanie danych internetowych nie będzie też miało związku z żadnym toczącym się postępowaniem.

IV. Niezgodność art. 20c ust. 3 w zw. z art. 20c ust. 2 ustawy o Policji, art. 10b ust. 3 w zw. z art. 10b ust. 2 ustawy o Straży Granicznej, art. 36b ust. 3 w zw. z art. 36b ust. 2 ustawy o kontroli skarbowej, art. 30 ust. 3 w zw. z art. 30 ust. 2 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28 ust. 3 w zw. z art. 28 ust. 2 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 32 ust. 3 w zw. z art. 32 ust. 2 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, art. 18 ust. 3 w zw. z art. 18 ust. 2 ustawy o Centralnym Biurze Antykorupcyjnym, art. 75d ust. 3 w zw. z art. 75d ust. 2 ustawy o Służbie Celnej z art. 2, art. 20 oraz z art. 47 i art. 51 ust. 2 w zw. z art. 31 ust. 3 Konstytucji RP.

Kolejne wątpliwości co do zgodności przyjętych przepisów z art. 2, art. 20 oraz z art. 47 i art. 51 ust. 2 w zw. z art. 31 ust. 3 Konstytucji RP nasuwają te przepisy, które dotyczą zawierania przez przedsiębiorców telekomunikacyjnych, operatorów pocztowych czy usługodawców świadczących usługi drogą elektroniczną porozumień z właściwymi organami

służb (Komendantem Głównym Policji oraz odpowiednio innymi w przypadku pozostałych służb).

W szczególności podkreślić należy, że art. 20c ust. 3 ustawy o Policji (i odpowiednio pozostałe przepisy) nie określa przesłanek zawarcia porozumienia, co może oznaczać w praktyce ograniczenie swobody przedsiębiorcy co do odmowy zawarcia porozumienia. Przepisy wszystkich wymienionych ustaw wyraźnie wskazują, że udostępnianie danych ma się odbywać nieodpłatnie, co może prowadzić do ingerencji w zasadę swobody działalności gospodarczej, wyrażoną w art. 20 Konstytucji poprzez ograniczenie możliwości swobodnego podejmowania działań faktycznych i prawnych, mieszczących się w ramach prowadzonej działalności gospodarczej. W odniesieniu do zasady wolności gospodarczej, wynikającej z art. 20 Konstytucji, Trybunał Konstytucyjny podkreślał wielokrotnie, że chodzi o działalność jednostek (osób fizycznych) oraz instytucji „niepaństwowych" (czy też – szerzej ujmując – niepublicznych), które mają prawo samodzielnego decydowania o udziale w życiu gospodarczym, zakresie i formach tego udziału, w tym możliwie swobodnego podejmowania różnych działań faktycznych i prawnych, mieszczących się w ramach prowadzenia działalności gospodarczej (por. wyrok TK o sygn. akt K 33/03).

Dodać również należy, że porozumienia spowodują budowę stałej infrastruktury, tzw. stałych łącz, dzięki którym funkcjonariusze służb, bez udziału pracowników usługodawcy lub przy niezbędnym ich udziale, będą mogli w dowolnym zakresie pozyskiwać dane wskazane w ustawach nowelizowanych przez ustawę z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw. Przepisy pozwalające na nieograniczone w praktyce zbieranie danych internetowych, bez następczego informowania osoby, których zbierane dane dotyczyły, stanowią naruszenie tak fundamentalnych zasad, jak zasada demokratycznego państwa prawnego, godność człowieka i wynikające z niej prawo do prywatności, wolność i ochrona tajemnicy komunikowania się czy w końcu ochrona informacji o sobie. Taki stan prawny

stanowi niewątpliwe naruszenie art. 47 i art. 51 ust. 2 Konstytucji RP. Umożliwienie służbom policyjnym i służbom specjalnym utrzymywanie stałej infrastruktury prowadzącej do permanentnego zbierania danych internetowych, telekomunikacyjnych i pocztowych prowadzi do trwałego zagrożenia prawa do prywatności oraz prawa do ochrony danych osobowych. Trudno bowiem twierdzić, że prywatność i dane osobowe są chronione w sytuacji, gdy bez ściśle określonych przesłanek i bez realnej kontroli mogą być pobierane przez funkcjonariuszy służb. Niemożliwe jest wykazanie konieczności i proporcjonalności takich regulacji. Cele założone tutaj przez ustawodawcę, w zakresie w jakim są one legitymizowane zasadą przydatności wynikającą z art. 31 ust. 3 Konstytucji RP, mogą być z pewnością realizowane w sposób znacznie mniej dotkliwy dla obywateli i odpowiadający standardom konstytucyjnym, w tym zwłaszcza wynikającym z wzorców kontroli powołanych w tej części wniosku.

Trzeba również podkreślić, że obowiązki nałożone na przedsiębiorców telekomunikacyjnych, operatorów pocztowych oraz usługodawców świadczących usługi drogą elektroniczną, będą w praktyce dotyczyć wyłącznie przedsiębiorców mających siedzibę na terenie Rzeczypospolitej Polskiej (art. 3 ustawy o świadczeniu usług drogą elektroniczną). Fakt, że obowiązki określone w ustawie dotyczyć będą wyłącznie ograniczonego kręgu podmiotów, nie umniejsza wagi zarzutów podniesionych przez Rzecznika Praw Obywatelskich. Wręcz przeciwnie, pozwala na stwierdzenie, że taka regulacja może prowadzić do sytuacji, w której niemożliwe będzie w ogóle sięgnięcie po dane posiadane przez przedsiębiorców z siedzibą poza terytorium RP lub będzie się odbywać w ogóle bez żadnej podstawy prawnej. To oznacza, że proponowane rozwiązania mogą nie stanowić efektywnego środka zapobiegania i zwalczania przestępczości.

W tym stanie rzeczy przepisy te naruszają standardy z art. 2, art. 20 oraz z art. 47 i art. 51 ust. 2 w zw. z art. 31 ust. 3 Konstytucji RP.

V. Niezgodność art. 20ca ustawy o Policji, art. 10ba ustawy o Straży Granicznej, art. 36ba ustawy o kontroli skarbowej, art. 30b ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28a ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 32a ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, art. 18a ustawy o Centralnym Biurze Antykorupcyjnym, art. 75da ustawy o Służbie Celnej – w zakresie, w jakim nie przewidują wprowadzenia mechanizmu niezależnej realnej kontroli udostępniania danych – z art. 2, 47, 51 ust. 2 w zw. z art. 31 ust. 3 Konstytucji, art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności oraz art. 7 i 8 w zw. z art. 52 ust. 1 Karty Praw Podstawowych UE.

Ustawa o zmianie ustawy o Policji dodała również w ww. ustawach przepis, regulujący zasady sprawowania przez sąd okręgowy kontroli nad uzyskiwaniem przez Policję i inne służby danych telekomunikacyjnych, pocztowych lub internetowych. Są to – odpowiednio: art. 20ca ustawy o Policji, art. 10ba ustawy o Straży Granicznej, art. 36ba ustawy o kontroli skarbowej, art. 30b ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28a ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 32a ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, art. 18a ustawy o Centralnym Biurze Antykorupcyjnym oraz art. 75da ustawy o Służbie Celnej. Zgodnie z tymi przepisami, kontrolę nad uzyskiwaniem przez daną służbę danych telekomunikacyjnych, pocztowych lub internetowych sprawować ma sąd okręgowy właściwy dla siedziby organu Policji (i odpowiednio innych służb, z wyjątkiem Żandarmerii Wojskowej, w przypadku której kontrolę sprawuje wojskowy sąd okręgowy właściwy ze względu na siedzibę organu Żandarmerii Wojskowej oraz Agencji Bezpieczeństwa Wewnętrznego i Centralnego Biura Antykorupcyjnego w przypadku której sądem właściwym jest Sąd Okręgowy w Warszawie, a także Służby Kontrwywiadu Wojskowego w przypadku której

sądem właściwym jest Wojskowy Sąd Okręgowy w Warszawie), któremu udostępniono te dane. Właściwy organ Policji (i odpowiednio innych służb) ma obowiązek przekazywać, z zachowaniem przepisów o ochronie informacji niejawnych, właściwemu sądowi, w okresach półrocznych, sprawozdanie obejmujące:

1) liczbę przypadków pozyskania w okresie sprawozdawczym danych telekomunikacyjnych, pocztowych lub internetowych oraz rodzaj tych danych,
2) kwalifikacje prawne czynów, w związku z zaistnieniem których wystąpiono o dane telekomunikacyjne, pocztowe lub internetowe, albo informacje o pozyskaniu danych w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych.

W ramach kontroli sąd okręgowy może zapoznać się z materiałami uzasadniającymi udostępnienie Policji (i odpowiednio pozostałym służbom) danych telekomunikacyjnych, pocztowych lub internetowych. Sąd okręgowy informuje organ Policji (i odpowiednio pozostałych służb) o wyniku kontroli w terminie 30 dni od jej zakończenia. Dodatkowo przepisy określają przypadek, kiedy uzyskiwanie danych nie podlega kontroli sądu (dane zbierane na podstawie art. 20cb ustawy o Policji i odpowiednio przepisów pozostałych ustaw).

Wskazane w ustawach procedury kontrolne budzą poważne wątpliwości Rzecznika Praw Obywatelskich. Kwestia zapewnienia realnej uprzedniej kontroli sądowej była przedmiotem rozważań Trybunału Sprawiedliwości UE w połączonych sprawach C-293/12 i C-594/12, gdzie TSUE stwierdził wyraźnie – analizując przepisy dyrektywy 2006/24/WE – że nie przewidziała ona uprzedniej kontroli sądu lub niezależnego organu administracyjnego, który pilnowałby, aby udostępnianie i wykorzystywanie danych ograniczało się do przypadków, gdy jest to ściśle konieczne do realizacji zamierzonego celu oraz orzekały lub decydowały wyłącznie na uzasadniony wniosek przedstawiony w kontekście postępowań mających na celu zapobieganie, wykrywanie lub ściganie przestępstw. Brak uprzedniej kontroli sądu lub niezależnego organu

TSUE uznał za nieuzasadnioną ingerencję w prawa podstawowe ustanowione w art. 7 i 8 KPP UE.

Z kolei Trybunał Konstytucyjny, orzekając w sprawie K 23/11 w odniesieniu do danych telekomunikacyjnych stwierdził wyraźnie, że ogólny standard konstytucyjny nie przesądza, jak dokładnie ma wyglądać procedura dostępu do danych telekomunikacyjnych, a w szczególności czy konieczne ma być w odniesieniu do każdego rodzaju zatrzymywanych danych, o których mowa w art. 180c i art. 180d prawa telekomunikacyjnego uzyskanie zgody na ich udostępnienie. Nie wszystkie dane tego rodzaju powodują taką samą intensywność ingerencji w wolności i prawa człowieka. Zdaniem Trybunału, „nie jest wobec tego wykluczone – w odniesieniu do udostępniania danych telekomunikacyjnych w toku czynności operacyjno-rozpoznawczych – wprowadzenie, jako zasady, kontroli następczej. Regulując ten mechanizm, ustawodawca powinien uwzględnić m.in. specyfikę działania i ustawowy zakres zadań poszczególnych służb, sytuacje niecierpiące zwłoki, w których szybkie pozyskanie danych telekomunikacyjnych może być niezbędne do zapobieżenia popełnieniu przestępstwa lub jego wykrycia. Zgodnie z konstytucyjną zasadą sprawności działania instytucji publicznych (wstęp do Konstytucji) należy wykreować mechanizm, który umożliwiłby służbom odpowiedzialnym za bezpieczeństwo państwa i porządek publiczny efektywną walkę z zagrożeniami. Trybunał dostrzega jednak argumenty za wprowadzeniem kontroli uprzedniej w pewnych wypadkach. W szczególności chodzić może o dostęp do danych telekomunikacyjnych osób wykonujących zawody zaufania publicznego lub jeśli nie ma koniecznego pilnego działania służb. Kwestie te musi jednak odpowiednio wyważyć ustawodawca”.

W przepisach dotyczących poszczególnych służb wskazuje się na właściwość sądu okręgowego (lub odpowiednio innych sądów) w tzw. trybie następczym. Kontrola ta ma polegać na analizie półrocznych sprawozdań przedkładanych sądom przez służby. Należy podkreślić, że w przypadku zakwestionowanych we wniosku ustaw ustawodawca nie podjął się

żadnego wyważenia potrzeby wprowadzenia uprzedniej kontroli, a ponadto – w odniesieniu do kontroli następczej – skonstruował ją w ten sposób, że w praktyce może mieć ona charakter iluzoryczny. Sprawozdania służb kierowane co pół roku do właściwego sądu w oparciu o przepisy o ochronie informacji niejawnych nie będą stanowiły informacji publicznej, chociaż będą zawierały informacje dotyczące liczby przypadków pozyskania w okresie sprawozdawczym danych telekomunikacyjnych, pocztowych lub internetowych oraz rodzaj tych danych, a także kwalifikacji prawnej czynów, w związku z zaistnieniem których wystąpiono o dane. Przeprowadzenie czynności kontrolnych przez sąd będzie mieć charakter fakultatywny, a nie obligatoryjny. Ponadto, sąd po przeprowadzeniu kontroli będzie mógł jedynie poinformować kontrolowaną służbę o wynikach kontroli, ale nie będzie mógł zarządzić zniszczenia zgromadzonych danych.

Wydaje się, że przy dużej skali pozyskiwanych danych oraz stosunkowo dużym odstępie czasowym, kontrola ta może mieć w istocie charakter iluzoryczny i nie spełniać wymogów wynikających z Konstytucji RP, a także ze wskazanych umów międzynarodowych. Zaproponowana forma kontroli jest zatem niewystarczająca. Kontrola następcza nie powinna być stosowana domyślnie, lecz może być dopuszczalna jedynie wyjątkowo, w sytuacjach, w których zachodzi potrzeba natychmiastowego działania służb. Zakwestionowane przepisy ustaw w żadnym przypadku nie przewidują przeprowadzenia kontroli uprzedniej. Dzięki takiemu mechanizmowi przypadki sięgania po dane mogłyby podlegać rzetelnej ocenie pod względem spełniania kryteriów niezbędności, adekwatności i celowości. Podkreślenia wymaga, że zgodnie z art. 51 ust. 2 Konstytucji RP, władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym. Przewidziana forma kontroli nie gwarantuje w sposób realny przestrzegania tych zasad, a przede wszystkim nie blokuje możliwości pozyskiwania danych nawet wtedy, gdyby miało ono nastąpić z naruszeniem tychże zasad.

Należy również dodać, że zgodnie z art. 20ca ust. 5 ustawy o Policji (i odpowiednio w przypadku pozostałych służb) żadnej kontroli nie podlega uzyskiwanie danych, pozyskiwanych na podstawie art. 20cb ust. 1 ustawy o Policji. Należy w tym miejscu wskazać, że ustawa o Policji i analogicznie pozostałe ustawy spod jakiejkolwiek kontroli wyłączają pozyskiwanie danych nie tylko określonych w art. 179 ust. 9 Prawa telekomunikacyjnego, ale również całego art. 161 Prawa telekomunikacyjnego, co znacząco poszerza zakres dostępu do danych wyłączonych spod jakiejkolwiek kontroli. W szczególności art. 161 ust. 3 Prawa telekomunikacyjnego zawiera odniesienie do bliżej nieokreślonych „innych danych".

VI. Niezgodność art. 20c ustawy o Policji, art. 10b ustawy o Straży Granicznej, art. 36b ustawy o kontroli skarbowej, art. 30 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 32 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, art. 18 ustawy o Centralnym Biurze Antykorupcyjnym, art. 75d ustawy o Służbie Celnej – w zakresie, w jakim przepisy te nie wskazują kategorii osób, których dane mogą być pozyskiwane w sposób określony w ustawach, nie regulują obowiązków informacyjnych wobec osób, których dane były pozyskiwane oraz nie określają czasu, przez który uprawnione podmioty mogą przetwarzać pozyskane dane – z art. 2, 30, 47, 49, 51 ust. 2, 3 i 4 w zw. z art. 31 ust. 3 Konstytucji, art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności oraz art. 7 i 8 w zw. z art. 52 ust. 1 Karty Praw Podstawowych UE

Zastrzeżenia Rzecznika Praw Obywatelskich budzi również fakt pominięć ustawodawczych, czyli spraw, które nie zostały (a powinny) być uregulowane w ustawie.

W szczególności, w wyroku w sprawie K 23/11 Trybunał Konstytucyjny podkreślił, że niejawne pozyskiwanie przez organy władzy publicznej informacji o jednostce wymaga zachowania daleko idących gwarancji proceduralnych – przede wszystkim ma istnieć obowiązek poinformowania jednostki o podjętych wobec niej działaniach operacyjno-rozpoznawczych oraz pozyskaniu informacji na jej temat, bez względu na to, czy były to osoby podejrzane o naruszenie prawa, czy osoby postronne, które przypadkowo stały się obiektem kontroli. Ma to szczególne znaczenie w odniesieniu do osób, wobec których nie zapadł wyrok lub którym nie zostały oficjalnie postawione zarzuty, jak również osób trzecich, których pozyskanie danych dotyczyło bezpośrednio. W opinii Trybunału, ustawodawca powinien zagwarantować późniejsze poinformowanie o tym fakcie, gdyż powiadomienie jednostki na etapie wykonywania działań operacyjno-rozpoznawczych i gromadzenia informacji narażałoby te działania na nieskuteczność. Na konieczność ustanowienia takiego obowiązku informacyjnego zwracał już uwagę TK w postanowieniu z 25 stycznia 2006 r. o sygn. S 2/06. Zapewnienie informacji jest też przesłanką skorzystania przez jednostki z wynikającego z art. 51 ust. 3 Konstytucji prawa dostępu do urzędowych dokumentów i zbiorów danych. Jak zauważył Trybunał, pominięcie poinformowania o zebraniu o jednostkach informacji przez władze publiczne samo w sobie stanowi naruszenie art. 51 ust. 3 i 4 Konstytucji. Skoro jednostka nie wie o zebraniu na jej temat określonych informacji, nie dysponuje możliwością uzyskania dostępu do nich i nie może żądać ich sprostowania lub usunięcia na warunkach określonych w art. 51 ust. 4 Konstytucji.

Zakwestionowane ustawy nie zakładają istnienia żadnej procedury, w wyniku której o pozyskiwaniu danych retencyjnych, pocztowych czy internetowych kiedykolwiek dowiedziałby się podmiot, którego dane były przetwarzane. W przekonaniu Rzecznika Praw Obywatelskich, obywatel powinien mieć prawo do podjęcia stosownych środków prawnych w zakresie działań prowadzonych względem niego, również w odniesieniu do informacji

gromadzonych przez właściwe służby. Jest to również wymóg jasno określony przez Trybunał Konstytucyjny (postanowienie z 25 stycznia 2006 r. o sygn. akt S 2/06).

Co więcej, projektodawca nie przewidział żadnych przepisów określających szczegółowo kategorie podmiotów, wobec których mogą być podejmowane czynności operacyjno-rozpoznawcze.

Wreszcie, ustawy nie określają okresu, przez który uprawnione podmioty mogą przetwarzać pozyskane dane telekomunikacyjne, pocztowe i internetowe. Stoi to w sprzeczności z wyrażoną w art. 26 ust. 1 pkt 4 ustawy o ochronie danych osobowych zasadą ograniczenia czasowego, zgodnie z którą dane mogą być przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania. Ustawa przewiduje jedynie, że dane, które nie mają znaczenia dla postępowania karnego, podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu. Nie został natomiast uregulowany sposób postępowania z danymi, które dla określonego postępowania miały znaczenie i zostały w nim wykorzystane, a tym kwestia weryfikacji potrzeby ich dalszego przetwarzania. O ile do czasu przechowywania danych włączonych w akta postępowania odnosić się będą przepisy szczególne, o tyle brak jest regulacji określających okres retencji danych przetwarzanych w systemach prowadzonych przez Policję i poszczególne służby. W praktyce może prowadzić to do nieuzasadnionego, bezterminowego przechowywania danych. Okres przetwarzania danych telekomunikacyjnych, pocztowych i internetowych powinien zatem być określony w sposób precyzyjny tak, aby wyeliminować ryzyko nadużyć, istniejące wobec faktu, że nie przewidziano zewnętrznej kontroli niezbędności dalszego przetwarzania danych do realizacji ustawowych zadań.

Powyższe pominięcia ustawodawcze polegają na przyjęciu uregulowania niepełnego w powyżej wskazanym zakresie. Zdaniem Rzecznika, kwestie te powinny zostać uregulowane w art. 20c ustawy o Policji oraz w odpowiednich przepisach pozostałych ustaw. Z tego względu

należy uznać, że niepełne uregulowanie zagadnienia, dotykającego podstawowych praw i wolności człowieka, powinno stać się również przedmiotem kontroli z punktu widzenia zasad konstytucyjnych.

VII. Niezgodność art. 28 ust. 7 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 32 ust. 9 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego – w zakresie, w jakim nie przewidują zniszczenia wszelkich innych danych telekomunikacyjnych, pocztowych i internetowych niż tylko tych, niemających znaczenia dla prowadzonego postępowania karnego – z art. 51 ust. 2 Konstytucji w zw. z art. 31 ust. 3 Konstytucji, art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności oraz art. 7 i 8 w zw. z art. 52 ust. 1 Karty Praw Podstawowych UE.

Dodane ustawą o zmianie ustawy o Policji art. 28 ust. 7 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu oraz art. 32 ust. 9 ustawy o Służbie Kontrwywiadu Wojskowego i Służbie Wywiadu Wojskowego nie przewidują zniszczenia wszelkich innych danych telekomunikacyjnych, pocztowych i internetowych niż tylko tych niemających znaczenia dla prowadzonego postępowania karnego. Ustawa zezwala na zachowanie danych, określonych jako „istotne dla bezpieczeństwa państwa" (w przypadku Agencji Bezpieczeństwa Wewnętrznego) oraz „istotne dla obronności Państwa" (w przypadku Służby Kontrwywiadu Wojskowego).

Trybunał Konstytucyjny w wyroku w sprawie K 23/11 w punkcie I ppkt 8 wyraźnie stwierdził, że art. 28 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, a także art. 32 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego w zakresie, w jakim nie przewidują zniszczenia danych niemających znaczenia

dla prowadzonego postępowania, są niezgodne z art. 51 ust. 2 w zw. z art. 31 ust. 3 Konstytucji. Przyjęta ustawa nie usunęła tego zastrzeżenia. W tym świetle Rzecznik Praw Obywatelskich nie ma wątpliwości, że wykazane tutaj pominięcie jest niezgodne z Konstytucją.

VIII. Niezgodność art. 13 oraz art. 16 ustawy z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw (Dz. U. z 2016 r., poz. 147) – w zakresie, w jakim nakazują stosować przepisy, które przestały obowiązywać na mocy wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r., sygn. K 23/11 – z art. 2 oraz z art. 190 ust. 1 i 3 Konstytucji RP.

W ustawie z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw przewidziano przepisy przejściowe, które w pewnym zakresie utrzymują w mocy przepisy dotychczasowe. Zgodnie z art. 13 ustawy: „Do kontroli operacyjnej, która była prowadzona przed dniem wejścia w życie ustawy i nie została zakończona do tego czasu, stosuje się przepisy dotychczasowe". Podobną konstrukcję przewidziano w art. 16 ustawy: „Do kontroli operacyjnej prowadzonej na podstawie art. 27 ust. 1 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu w brzmieniu dotychczasowym, w celu realizacji zadań określonych w art. 5 ust. 1 pkt 2 lit. b tej ustawy, niezakończonej do dnia wejścia w życie niniejszej ustawy, stosuje się przepisy dotychczasowe". Konstrukcja tych przepisów może wskazywać, że ustawodawca – w zakresie w nich wskazanym – chce utrzymać w mocy przepisy, które zostały uznane za niezgodne z Konstytucją RP i przestały obowiązywać na mocy wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r., sygn. K 23/11. Wskazuje na to zakres ustawy z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw. Przepisy tej ustawy – jak wskazywano w uzasadnieniu do projektu ustawy – mają na celu wykonanie ww. wyroku Trybunału Konstytucyjnego. Tym samym,

należy uznać, że wprowadzając odwołanie do „przepisów dotychczasowych” ustawodawca ma na myśli przepisy uznane przez Trybunał za niezgodne z Konstytucją RP. Wnioskowanie to znajduje pokrycie w uzasadnieniu do projektu ustawy (Uzasadnienie do projektu ustawy, druk sejmowy nr 154, s. 15-16). W ocenie Rzecznika Praw Obywatelskich przepisy te są niezgodne z art. 2 oraz z art. 190 ust. 2 i 3 Konstytucji RP.

Trudno znaleźć uzasadnienie prawne dla utrzymania w mocy przepisów, których domniemanie konstytucyjności zostało prawomocnie obalone przez Trybunał Konstytucyjny. Konstrukcja prawna przyjęta przez ustawodawcę niewątpliwie narusza zasadę przyzwoitej legislacji, zasadę zaufania obywatela do państwa i zasadę pewności prawa. Jak się wydaje skutki wyroku Trybunału Konstytucyjnego o niezgodności przepisu z Konstytucją RP są dwojakie. Po pierwsze, przepis ten formalnie jest usuwany z obrotu prawnego, niezwłocznie po ogłoszeniu wyroku lub – w razie odroczenia utraty mocy obowiązującej – w terminie wskazanym w orzeczeniu Trybunału Konstytucyjnego. Po drugie, ogłaszając niezgodność przepisu z Konstytucją RP, Trybunał jednocześnie orzeka niejako o niezgodności danej normy prawnej z ustawą zasadniczą. Nie tylko przepis jest niekonstytucyjny, ale także normy, które są z niego interpretowane. Tak rozumiany skutek orzeczenia prowadzi do ograniczenia kompetencji ustawodawcy w zakresie prawodawstwa w obszarze objętym wyrokiem Trybunału Konstytucyjnego. Oczywiste jest, że ustawodawca nie może uchwalić przepisu o tej samej treści, która została uznana za niezgodną z ustawą zasadniczą. Ustawodawca jednak nie tylko nie może uchwalić przepisu o tej samej treści, ale także przepisu o innej treści, z którego można wyinterpretować tylko normę o treści uznanej wcześniej za niekonstytucyjną. Innymi słowy, efektem jest derogacja nie tylko przepisu, ale także norm prawnych. W świetle zasady przyzwoitej legislacji należy zatem pamiętać, że uchwalanie norm – nawet przy zmianie językowego brzmienia przepisów – wcześniej uznanych za niezgodne z Konstytucją, narusza zasadę demokratycznego państwa prawnego. W kontekście art. 13 i 16 ustawy z dnia 15

stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw, naruszenie zasady przyzwoitej legislacji jest bardziej oczywiste. Nie próbując nawet zmieniać brzmienia przepisów uznanych za niezgodne z ustawą zasadniczą, utrzymuje się je w mocy, uchybiając w ten sposób wyrokowi Trybunału Konstytucyjnego. W świetle tej zasady, przepis uznany za niezgodny z Konstytucją RP nie tylko formalnie, ale nawet materialnie nie może funkcjonować w obrocie prawnym.

Powyższa konstatacja znajduje dodatkowe uzasadnienie w zasadzie pewności prawa. W orzecznictwie oraz w literaturze wskazuje się, że pewność prawa ma być gwarancją stabilności porządku prawnego, a nadto dawać obywatelowi pewność pozwalającą na kształtowanie swoich spraw życiowych (W. Sokolewicz, *Komentarz do art. 2*, [w:] L. Garlicki (red.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, t. V Warszawa 2007, s. 36; por. też wyrok TK z 15 czerwca 2000 r., P 3/00). Niewątpliwie uprawnione jest przekonanie obywatela o możliwości uznania za nieobowiązujące tych przepisów, które Trybunał Konstytucyjny uznał za niezgodne z Konstytucją RP i jednocześnie upłynął termin odraczający utratę ich mocy. Decyzja ustawodawcy o utrzymaniu takich przepisów w mocy powoduje zachwianie bezpieczeństwa prawnego. Uderza ona także w zasadę zaufania obywateli do państwa, zwłaszcza w kontekście art. 190 ust. 1 i 3 Konstytucji RP.

Zgodnie z art. 190 ust. 1 Konstytucji RP: „Orzeczenia Trybunału Konstytucyjnego mają moc powszechnie obowiązującą i są ostateczne". Jak statuuje art. 190 ust. 3 Konstytucji RP: „Orzeczenie Trybunału Konstytucyjnego wchodzi w życie z dniem ogłoszenia, jednak Trybunał Konstytucyjny może określić inny termin utraty mocy obowiązującej aktu normatywnego. Termin ten nie może przekroczyć osiemnastu miesięcy, gdy chodzi o ustawę, a gdy chodzi o inny akt normatywny – dwunastu miesięcy (...)". Przepisy te nie pozostawiają żadnych wątpliwości. Zabieg ustawodawcy prowadzący do utrzymania w mocy przepisów obowiązujących przed wejściem w życie ustawy z dnia 15 stycznia 2016 r. o zmianie ustawy o

Policji oraz niektórych innych ustaw, uznanych przez Trybunał Konstytucyjny za niezgodne z Konstytucją RP, narusza zasadę ostateczności i powszechnej mocy obowiązującej wyroków Trybunału Konstytucyjnego. Przeprowadzone tutaj wnioskowanie znajduje potwierdzenie w wyroku Naczelnego Sądu Administracyjnego z 31 stycznia 2014 r., w którym zauważono, że: „Z art. 190 ust. 3 Konstytucji można wyprowadzić wniosek, że skoro Konstytucja wyjątkowo tylko zezwala na obowiązywanie niezgodnego z nią aktu prawnego, to regułą jest jego nieobowiązywanie, a więc niestosowanie" (wyrok NSA z 31 stycznia 2014 r., sygn. II FSK 2752/13).

Instytucja odroczenia utraty mocy obowiązującej przez przepis stosowana jest przez Trybunał Konstytucyjny po to, aby dać odpowiedniemu organowi państwa czas na wykonanie wyroku, a więc na wprowadzenie stosownych zmian prawnych. Jest to sytuacja wyjątkowa, albowiem w systemie prawnym obowiązuje przepis, którego niezgodność z ustawą zasadniczą została prawomocnie potwierdzona. Ustawodawca, nie czekając na upływ terminu odroczenia, powinien niezwłoczne dostosować stan prawny do wymogów ustawy zasadniczej. Konstruując przepisy przejściowe w takich sytuacjach należy pamiętać o *ratio legis* instytucji odroczenia utraty mocy obowiązującej. Rzecznik Praw Obywatelskich nie widzi podstaw do zaniechania stosowania przepisów nowych także do kontroli operacyjnej, która była prowadzona przed dniem wejścia w życie kwestionowanej ustawy i nie została zakończona do tego czasu.

W tym stanie rzeczy zaskarżone w tej części przepisy są niezgodne z art. 2 oraz z art. 190 ust. 1 i 3 Konstytucji RP.

Mając na względzie powyższe, a zwłaszcza doniosłość wykazanych wątpliwości odnośnie zgodności zaskarżonych przepisów z Konstytucją RP, nie mam wątpliwości, że

zaskarżone przepisy stanowią poważne zagrożenie dla najważniejszych wolności i praw człowieka. Wobec tego, wnoszę o orzeczenie jak w petitum.