Ministerstwo
Spraw Wewnętrznych

Grzegorz Karpiński

Sekretarz Stanu

DPP-OP-0231-1-3/2015

Warszawa, dnia 18 czerwca 2015 r.

S.
Do wiadomości
Członków Komisji

Pan
Michał Seweryński

Przewodniczący Komisji Praw Człowieka,
Praworządności i Petycji Senatu RP

Pan
Piotr Zientarski

Przewodniczący
Komisji Ustawodawczej Senatu RP

Szanowni Panowie Przewodniczący,

W nawiązaniu do ustaleń podjętych na posiedzeniu Komisji Praw Człowieka, Praworządności i Petycji Senatu RP w dniu 19 maja 2015 r. w sprawie rozpatrzenia wskazanych przez Prezesa Najwyższej Izby Kontroli wniosków *de lege ferenda* zawartych w wynikach kontroli NIK *Uzyskiwanie i przetwarzanie przez uprawnione podmioty danych z billingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180 c i d ustawy Prawo telekomunikacyjne* oraz na posiedzeniu Komisji Ustawodawczej Senatu RP w dniu 8 czerwca 2015 r. w sprawie rozpatrzenia wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r. (sygn. akt K 23/11) dotyczącego kontroli operacyjnej stosowanej przez służby policyjne i ochrony państwa uprzejmie informuję, że aktualne pozostaje stanowisko Ministerstwa Spraw Wewnętrznych z dnia 3 kwietnia 2014 r. (znak: DP-I-0232-119/14/ECh), w którym zgłoszono szereg uwag do senackiego *projektu ustawy o zmianie niektórych ustaw w zakresie przepisów dotyczących uzyskiwania i przetwarzania przez uprawnione podmioty danych gromadzonych przez przedsiębiorców telekomunikacyjnych*. Wskazano w nim, iż przyjęcie rozwiązań prawnych przedstawionych w projekcie może mieć negatywny wpływ na dynamikę, a w konsekwencji na skuteczność działań służb, bowiem w istotny sposób wydłużą czas podejmowania działań oraz ograniczą ich zakres. Obecnie, w zdecydowanej większości spraw kryminalnych, wykrycie i zatrzymanie sprawców przestępstw odbywa się z wykorzystaniem danych telekomunikacyjnych. Dane te stanowią również skuteczne narzędzie w poszukiwaniu osób ukrywających się przed organami ścigania. Projektowane ograniczenie możliwości wykorzystania danych telekomunikacyjnych przez służby

ul. Stefana Batorego 5
02-591 Warszawa, Polska
msw.gov.pl

tel. +48 22 601 46 20
fax +48 22 601 39 88

w tych obszarach może w konsekwencji prowadzić do obniżenia poziomu wykrywalności przestępstw, a w skrajnych przypadkach uniemożliwi realizację czynności związanych z wykryciem określonych kategorii przestępstw. Ponadto przyjęcie proponowanych rozwiązań w sposób znaczny zwiększy obciążenie prokuratur oraz sądów wnioskami o dane telekomunikacyjne, rozpatrywanymi w trybie analogicznym do wniosków o kontrolę operacyjną.

Proponowane brzmienie senackich regulacji, nad którymi prace rozpoczęły się przed ogłoszeniem wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r., sygn. akt. K 23/11, jedynie w częściowym zakresie wykonuje przedmiotowy wyrok i w konsekwencji nie w pełni reguluje kwestie związane z kontrolą zewnętrzną nad procesem pozyskiwania danych z bilingów, w tym także pod kątem zasadności ich pozyskiwania oraz nie wprowadza instrumentów gwarantujących niszczenie pozyskanych danych, w sytuacji, gdy nie są one już niezbędne dla prowadzonego postępowania.

Ponadto, w uzasadnieniu wyroku Trybunał Konstytucyjny wskazał dodatkowy obszar zagadnień, które winny zostać doprecyzowane, aby spełniały konstytucyjne przesłanki ograniczenia wolności i praw obywatelskich, w tym m.in. aby określały rodzaje środków niejawnego pozyskiwania informacji, a także rodzaje informacji pozyskiwanych za pomocą poszczególnych środków oraz maksymalny okres prowadzenia czynności operacyjno-rozpoznawczych.

W celu realizacji wytycznych Trybunału Konstytucyjnego, w dniu 8 października 2014 r. powołany został w ramach Kolegium do Służb Specjalnych *Zespół do spraw zmian legislacyjnych wynikających z wyroku Trybunału Konstytucyjnego K23/11 z dnia 30 lipca 2014 r.*, w skład którego weszli m.in. przedstawiciele podmiotów uprawnionych do stosowania kontroli operacyjnej lub pozyskiwania danych telekomunikacyjnych oraz przedstawiciele administracji rządowej. Opracowywane przez stronę rządową propozycje rozwiązań zmierzających do wykonania ww. wyroku TK, zarówno w zakresie postulatów zawartych w jego sentencji jak i w uzasadnieniu, mogą zapewnić w pełni jego realizację, tym bardziej, że rekomendowane przez Najwyższą Izbę Kontroli wnioski *de lege ferenda* wpisują się w postulaty Trybunału Konstytucyjnego.

Założeniem projektodawcy jest również, w miarę możliwości, ujednolicenie regulacji w stosunku do wszystkich służb posiadających uprawnienie do pozyskiwania i przetwarzania danych telekomunikacyjnych. Ponadto, projekt uwzględni kwestię *dyrektywy 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniającej dyrektywę 2002/58/WE*, która w konsekwencji spowodowała utratę mocy podstawy prawnej dla funkcjonowania sprawozdawczości w zakresie udostępnionych danych telekomunikacyjnych. Projekt uwzględni również obszar związany z uzyskiwaniem danych od podmiotów świadczących usługi pocztowe na podstawie ustawy z dnia 23 listopada 2012 r. – *Prawo pocztowe* (Dz. U. poz. 1529), tj. wniosków kierowanych do operatorów pocztowych o ujawnienie danych dotyczących osób korzystających z usług pocztowych oraz danych dotyczących faktu i okoliczności świadczenia lub korzystania z tych usług. Projektodawca zamierza włączyć do materii ustawowej wybrane przepisy rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 10 czerwca 2011 r. *w sprawie sposobu dokumentowania prowadzonej przez Policję kontroli operacyjnej, przechowywania i przekazywania wniosków, zarządzeń i materiałów uzyskanych podczas stosowania tej kontroli, a także przetwarzania i niszczenia tych materiałów* (Dz. U. Nr 122,

poz. 697, z późn. zm.) dotyczące prowadzenia przez poszczególne organy rejestrów wniosków i zarządzeń kontroli operacyjnej.

Na przykładzie przepisów ustawy o Policji, uprzejmie przedstawiam Panom Przewodniczącym wypracowane dotychczas propozycje zmian przepisów, które mogą stanowić model legislacyjnych rozwiązań w przypadku projektowania przepisów dla innych służb uprawnionych do pozyskiwania i przetwarzania danych telekomunikacyjnych:

1. **Wprowadzenie uprzedniej i następczej kontroli udostępniania danych telekomunikacyjnych, a także danych uzyskiwanych od podmiotów świadczących usługi pocztowe na podstawie *ustawy z dnia 23 listopada 2012 r. - Prawo pocztowe (Dz. U. poz. 1529).***

1.1. Dookreślenie przepisów dotyczących udostępniania danych telekomunikacyjnych.

Wychodząc naprzeciw postulatowi TK określoności prawa, proponuje się dookreślenie przesłanek pozyskiwania danych telekomunikacyjnych oraz uwzględnienie w przepisie danych, które na podstawie obowiązującego art. 20d ust. 3 *ustawy o Policji* są udostępniane na wniosek organu Policji przez podmioty uprawnione do świadczenia usług pocztowych, na podstawie *ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe*. Dotyczy to wniosków kierowanych do operatorów pocztowych o ujawnienie danych dotyczących osób korzystających z usług pocztowych oraz danych dotyczących faktu i okoliczności świadczenia lub korzystania z tych usług.

Art. 20c. *1. W celu rozpoznawania, zapobiegania, zwalczania, wykrywania albo uzyskania i utrwalenia dowodów przestępstw ściganych z oskarżenia publicznego albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych, Policja może mieć udostępniane dane:*
1) o których mowa w art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243, 827 i 1198), zwane dalej „danymi telekomunikacyjnymi";
2) identyfikujące podmiot korzystający z usług pocztowych w rozumieniu art. 2 ustawy z dnia 23 listopada 2012 r. - Prawo pocztowe (Dz. U. poz. 1529) oraz dotyczące faktu, okoliczności świadczenia tych usług lub korzystania z nich, zwane dalej „danymi pocztowymi"
- oraz może je przetwarzać.

Powyższa konstrukcja przepisu doprecyzowuje jednocześnie przesłanki pozyskiwania tego rodzaju danych.

Uzasadnionym jest również doprecyzowanie zakresu udostępnianych danych o „dane pocztowe" na potrzeby czynności związanych z poszukiwaniem osób zaginionych.

Art. 20da ust.1. *W celu poszukiwania osób zaginionych Policja może mieć:*
1) udostępniane dane, o których mowa w art. 180d ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne;
2) udostępniane dane pocztowe
- oraz może je przetwarzać; przepisy art. 20c ust. 2, 3, 4 i 5 stosuje się.".

W stosunku do powyżej określonych danych proponuje się, aby organem wyznaczonym do sprawowania kontroli był właściwy sąd okręgowy.

Trybunał Konstytucyjny nie przesądził jak dokładnie ma wyglądać procedura kontroli dostępu do danych telekomunikacyjnych, niemniej wskazał, że konieczne jest, aby kontrolę sprawował organ niezależny od rządu i niepozostający z funkcjonariuszami pozyskującymi dane w bezpośredniej lub pośredniej relacji zwierzchności. W ocenie Trybunału, powierzenie kompetencji kontrolnych niezależnym i niezawisłym sądom, dałoby rękojmię odpowiednio wysokiego stopnia wiedzy i doświadczenia życiowego. Z punktu widzenia Konstytucji, sądowa kontrola nad czynnościami operacyjno-rozpoznawczymi jest rozwiązaniem optymalnym.

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

W powyższym kontekście proponuje się wprowadzenie modelu mieszanego sądowej kontroli pozyskiwania oraz wykorzystania przez organy danych telekomunikacyjnych. Co do zasady, projekt określa tryb kontroli następczej w stosunku do wszystkich zgromadzonych materiałów, w których takie dane były pozyskiwane. Natomiast w odniesieniu do materiałów mogących zawierać informacje stanowiące tajemnice związane z wykonywaniem zawodu zaufania publicznego projekt przewiduje mechanizm kontroli uprzedniej. Rozwiązanie to realizuje cytowane powyżej postulaty TK zawarte w uzasadnieniu wyroku.

Istotnym elementem konstrukcji mechanizmu kontroli następczej jest gwarancja autonomii sądów w wyborze kryteriów przyjmowanych do typowania spraw w określeniu zakresu jej przeprowadzania.

1.2. Kontrola uprzednia.

Kontrola uprzednia byłaby prowadzona w przypadkach, gdy z materiałów zgromadzonych w sprawie będzie wynikać, że zawierają one informacje stanowiące tajemnice związane z wykonywaniem zawodu

lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego. O wykorzystaniu tych materiałów w postępowaniu karnym albo ich zniszczeniu decydowałby właściwy sąd okręgowy. Jeżeli w toku czynności zostanie ustalone, że konieczne jest pozyskanie danych dotyczących bezpośrednio osoby wykonującej zawód zaufania publicznego, właściwy organ będzie występował do sądu okręgowego o zgodę na udostępnienie tych danych i wykorzystanie w postępowaniu karnym. Projekt przewiduje też, że w sytuacjach niecierpiących zwłoki (m.in. zagrożenie dla życia lub zdrowia), właściwy organ będzie mógł wystąpić o udostępnienie danych, zwracając się jednocześnie do sądu o wydanie postanowienia w tej sprawie.

Art. 20ca. *1. Jeżeli z materiałów sprawy, o których mowa w art. 20c ust. 5[1)], wynika, że zawierają one dane dotyczące bezpośrednio osoby wykonującej zawód lub funkcję, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, Komendant Główny Policji, Komendant CBŚP albo komendant wojewódzki Policji przekazują prokuratorowi te materiały.*

2. W przypadku, o którym mowa w ust. 1, prokurator niezwłocznie po otrzymaniu materiałów kieruje je do właściwego miejscowo sądu okręgowego, wraz z wnioskiem o wyrażenie zgody na ich wykorzystanie w postępowaniu karnym.

3. Sąd okręgowy wydaje postanowienie o stwierdzeniu dopuszczalności wykorzystania w postępowaniu karnym materiałów zawierających dane, o których mowa ust. 1, albo zarządza ich komisyjne i protokolarne zniszczenie, w terminie 14 dni od dnia złożenia wniosku przez prokuratora.

4. O wykonaniu zarządzenia dotyczącego zniszczenia materiałów zawierających dane, o których mowa w ust. 1, organ Policji jest obowiązany do niezwłocznego poinformowania sądu okręgowego.

Art. 20cb*. 1. Jeżeli z materiałów sprawy wynika, że konieczne jest pozyskanie danych telekomunikacyjnych lub pocztowych dotyczących bezpośrednio osoby wykonującej zawód lub funkcję, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, Komendant Główny Policji, Komendant CBŚP albo komendant wojewódzki Policji występują do właściwego miejscowo sądu okręgowego z pisemnym wnioskiem o wyrażenie, w drodze postanowienia, zgody na pozyskanie tych danych i ich wykorzystanie w postępowaniu karnym.*

2. Wniosek, o którym mowa w ust. 1, przedstawia się wraz z materiałami uzasadniającymi potrzebę wykorzystania danych, o których mowa w ust. 1.

3. W przypadkach niecierpiących zwłoki, jeżeli mogłoby to spowodować zagrożenie życia lub zdrowia, możliwość utraty informacji, zatarcie lub zniszczenie dowodów przestępstwa, organ Policji może wystąpić do podmiotu prowadzącego działalność telekomunikacyjną lub pocztową o przekazanie danych, o których mowa w ust. 1, zwracając się jednocześnie do właściwego miejscowo sądu okręgowego z pisemnym wnioskiem o wyrażenie zgody w drodze postanowienia w tej sprawie.

4. Na postanowienie sądu o odmowie uwzględnienia wniosku przysługuje zażalenie organowi Policji, który złożył wniosek o wydanie tego postanowienia. Do zażalenia stosuje się odpowiednio przepisy Kodeksu postępowania karnego.

5. W przypadku nieuwzględnienia zażalenia organ Policji, który wystąpił o przekazanie danych, o których mowa w ust. 1, jest zobowiązany do:

1) wydania zarządzenia o ich niezwłocznym, komisyjnym i protokolarnym zniszczeniu – w przypadku gdy dane te zostały przekazane;

[1)] W obowiązującym brzmieniu *ustawy o Policji*, odpowiednikiem przywołanego ustępu 5 jest ustęp 6 przepisu art. 20c – przyp. Ministerstwa Spraw Wewnętrznych.

2) poinformowania podmiotu prowadzącego działalność telekomunikacyjną lub pocztową o braku zgody na ich przekazanie – w przypadku gdy dane te nie zostały przekazane.

1.3. Kontrola następcza.

Organy pozyskujące dane, byłyby zobligowane raz na 6 miesięcy przekazywać sprawozdanie zawierające informacje, w oparciu, o które zostanie przeprowadzona kontrola następcza, według kryteriów oraz w zakresie autonomicznie wybranym przez sąd. W przypadku stwierdzenia przez sąd braku podstaw do pozyskania tych danych, będą one podlegały zniszczeniu.

Art. 20cc. *1. Kontrolę nad uzyskiwaniem przez Policję danych telekomunikacyjnych lub pocztowych sprawuje sąd okręgowy właściwy dla siedziby organu Policji, któremu udostępniono te dane.*
2. Organ Policji, o którym mowa w ust. 1, przekazuje sądowi okręgowemu, o którym mowa w ust. 1, raz na 6 miesięcy, sprawozdanie obejmujące:
1) liczbę i rodzaj pozyskanych danych telekomunikacyjnych i pocztowych;
2) podstawę prawną pozyskania danych telekomunikacyjnych i pocztowych;
3) rodzaje przestępstw, w związku z zaistnieniem których wystąpiono o dane telekomunikacyjnych i pocztowych;
4) liczbę przypadków, ze wskazaniem ich podziału na rodzaje spraw, w których wystąpiono o dane telekomunikacyjne i pocztowe.
3. W ramach kontroli, o której mowa w ust. 1, sąd okręgowy może zapoznać się z materiałami uzasadniającymi udostępnienie Policji danych telekomunikacyjnych lub pocztowych oraz materiałami uzyskanymi w wyniku podjętych czynności.
4. W przypadku stwierdzenia przez sąd okręgowy braku podstaw do pozyskania danych telekomunikacyjnych lub pocztowych, zgromadzone dane podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu. Przepis art. 20c ust. 8 stosuje się odpowiednio.
5. O zarządzeniu zniszczenia danych organ Policji jest obowiązany do niezwłocznego poinformowania sądu okręgowego, o którym mowa w ust. 1.

2. Wprowadzenie przepisów zapewniających ochronę informacji, których źródłem są osoby lub podmioty wykonujące zawody zaufania publicznego oraz gwarancję niezwłocznego i protokolarnego zniszczenia materiałów objętych zakazami dowodowymi.

Proponuje się nałożenie na służby obowiązku wskazywania prokuratorowi, że materiały zgromadzone w toku kontroli operacyjnej mogą zawierać informacje stanowiące tajemnice związane z wykonywaniem zawodu zaufania publicznego. O dalszym wykorzystaniu albo zniszczeniu tych materiałów decydowałby sąd, który zarządził stosowanie kontroli operacyjnej.

Art. 19.

15h. Sąd wydaje postanowienie o stwierdzeniu dopuszczalności wykorzystania w postępowaniu karnym materiałów mogących zawierać informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, albo zarządza ich zniszczenie, w terminie 14 dni od dnia złożenia wniosku przez prokuratora.

15i. O wykonaniu zarządzenia dotyczącego zniszczenia informacji stanowiących tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, organ Policji jest obowiązany do niezwłocznego poinformowania prokuratora, o którym mowa w ust. 15g.

Art. 20cb.

6. W przypadku gdy zgromadzone w trybie określonym w ust. 1 lub 3 dane telekomunikacyjne lub pocztowe, nie zawierają informacji mających znaczenie dla prowadzonego postępowania karnego organ Policji, który wnioskował o ich udostępnienie, zarządza ich niezwłoczne, komisyjne i protokolarne zniszczenie.

7. O wydaniu i wykonaniu zarządzenia dotyczącego zniszczenia danych telekomunikacyjnych lub pocztowych, o którym mowa w ust. 5 pkt 1 i ust. 6, organ Policji jest obowiązany do niezwłocznego poinformowania sądu okręgowego.

W sytuacji, gdy zaistnieje przypuszczenie, że materiały uzyskane w wyniku kontroli operacyjnej zawierają informacje objęte zakazami dowodowymi, o których mowa w art. 178 Kodeksu postępowania karnego, tj. dotyczące faktów, o których obrońca lub adwokat dowiedział się udzielając porady prawnej lub prowadząc sprawę, albo faktów, o których dowiedział się duchowny przy spowiedzi, proponuje się, aby właściwy organ wnioskujący o zarządzenie kontroli operacyjnej nakazywał niezwłoczne, komisyjne i protokolarne ich zniszczenie.

Art. 19.

15f. W przypadku gdy zachodzi przypuszczenie, że materiały, o których mowa w ust. 15:

1) zawierają informacje, o których mowa w art. 178 Kodeksu postępowania karnego - Komendant Główny Policji, Komendant CBŚP albo komendant wojewódzki Policji nakazuje ich niezwłoczne, komisyjne i protokolarne zniszczenie;

2) mogą zawierać informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, Komendant Główny Policji, Komendant CBŚP albo komendant wojewódzki Policji przekazuje prokuratorowi te materiały.

15g. W przypadku, o którym mowa w ust. 15f pkt 2, prokurator niezwłocznie po otrzymaniu materiałów, kieruje je do sądu, który zarządził kontrolę operacyjną albo wyraził na nią zgodę w trybie określonym w ust. 3, wraz z wnioskiem o:

1) wyrażenie zgody na ich wykorzystanie w postępowaniu karnym, albo

2) wydanie zarządzenia o ich niezwłocznym, komisyjnym i protokolarnym zniszczeniu.

W odniesieniu do informacji zgromadzonych w wyniku udostępnienia danych telekomunikacyjnych i „pocztowych", stanowiących tajemnice związane z wykonywaniem zawodu zaufania publicznego, zastosowanie będzie miała procedura opisana w pkt 1 (kontrola uprzednia).

3. **Wprowadzenie jednolitych rozwiązań w zakresie weryfikacji oraz niszczenia zbędnych danych telekomunikacyjnych i „pocztowych".**

Materiały uzyskane w związku z udostępnieniem danych, które nie zawierają informacji mających znaczenie dla postępowania karnego lub nie są istotne dla bezpieczeństwa państwa podlegałyby niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu.

Art. 20c.

6. Materiały uzyskane w wyniku czynności związanych z udostępnieniem danych telekomunikacyjnych lub pocztowych, które nie zawierają informacji mających znaczenie dla postępowania karnego, podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu.

Pozostałe dane przetwarzane byłyby przez okres, w którym są niezbędne do realizacji zadań, przy czym nie rzadziej niż co 5 lat, należałoby weryfikować potrzebę ich przetwarzania. W przypadku uznania, że dalsze przetwarzanie danych nie jest niezbędne, materiały te należałoby niezwłocznie zniszczyć.

Art. 20c.

7. Dane telekomunikacyjne lub pocztowe przetwarza się przez okres, w którym są one niezbędne do realizacji ustawowych zadań, przy czym, nie rzadziej niż co 5 lat, dokonuje się weryfikacji potrzeby dalszego ich przetwarzania.

8. W przypadku gdy w wyniku weryfikacji ustalono, że dalsze przetwarzanie danych telekomunikacyjnych lub pocztowych nie jest niezbędne dla realizacji ustawowych zadań, dane te oraz materiały, o których mowa w ust. 6, niezwłocznie, nie później jednak niż w terminie 14 dni od dnia zakończenia weryfikacji, niszczy komisja powołana przez Komendanta Głównego Policji lub osobę przez niego upoważnioną. Z czynności komisji sporządza się protokół.

4. **Określenie rodzajów przestępstw, w odniesieniu do których możliwe jest pozyskiwanie informacji o osobach w ramach kontroli operacyjnej.**

W obowiązującej regulacji doprecyzowano, że kontrola operacyjna może zostać zarządzona w odniesieniu do przestępstw ściganych na mocy umów międzynarodowych ratyfikowanych za uprzednią zgodą wyrażoną w ustawie, określonych w polskiej ustawie karnej.

Art. 19. *1. Przy wykonywaniu czynności operacyjno-rozpoznawczych, podejmowanych przez Policję w celu zapobieżenia, wykrycia, ustalenia sprawców, a także uzyskania i utrwalenia dowodów ściganych z oskarżenia publicznego, umyślnych przestępstw:*

(...)

8) ściganych na mocy umów międzynarodowych ratyfikowanych za uprzednią zgodą wyrażoną w ustawie, określonych w polskiej ustawie karnej.

Ponadto określono rodzaje przestępstw, w związku z którymi może zostać zarządzona kontrola operacyjna (dotyczy to w szczególności Żandarmerii Wojskowej, Agencji Bezpieczeństwa Wewnętrznego i Straży Granicznej).

W odniesieniu do danych telekomunikacyjnych i „pocztowych" doprecyzowano przesłanki ich udostępniania (przykładowo w Policji - w celu rozpoznawania, zapobiegania, zwalczania, wykrywania albo uzyskania i utrwalenia dowodów przestępstw ściganych z oskarżenia publicznego albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych). Propozycja uregulowania trybu ich pozyskiwania została omówiona w pkt 1.

5. Określenie rodzajów środków niejawnego pozyskiwania informacji, a także rodzajów informacji pozyskiwanych za pomocą poszczególnych środków.

Jak wskazuje w uzasadnieniu do wyroku TK, nie jest konieczne wskazanie w przepisach prawa konkretnych środków techniki operacyjnej ani tym bardziej zdefiniowanie jej parametrów. Z punktu widzenia zasady określoności prawa istotne jest natomiast sprecyzowanie w przepisach prawa zamkniętego rodzajowo katalogu środków i metod działania, za pomocą których może być prowadzona kontrola operacyjna. Zgodnie z projektowaną propozycją, kontrola operacyjna polegałaby na: podsłuchu rozmów prowadzonych przy użyciu środków technicznych, podsłuchu i podglądzie pomieszczeń i osób poza miejscami publicznymi, kontroli treści korespondencji, nadzorze elektronicznym osób, miejsc i przedmiotów oraz środków transportu. W projekcie wymienia się jednocześnie jakie czynności nie stanowią kontroli operacyjnej.

Art. 19.

6. Kontrola operacyjna prowadzona jest niejawnie i polega na:
1) podsłuchu rozmów prowadzonych przy użyciu środków technicznych;
2) podsłuchu i podglądzie pomieszczeń i osób poza miejscami publicznymi;
3) kontroli treści korespondencji;
4) nadzorze elektronicznym osób, miejsc i przedmiotów oraz środków transportu.",
6a. Kontroli operacyjnej nie stanowią czynności, o których mowa w ust. 6 pkt 2 i 4, polegające na:
1) uzyskiwaniu i utrwalaniu obrazu w pomieszczeniach, o których mowa w art. 15 ust. 1 pkt 4a;
2) uzyskiwaniu danych w trybie art. 20c.
6b. Czynności, o których mowa w ust. 6, mogą być realizowane przy użyciu środków technicznych niezbędnych do realizacji celów kontroli operacyjnej.

Projektodawca określając katalog środków i metod działania stosowanych w toku kontroli operacyjnej enumeratywnie wskazał również, co stanowi dokumentację materiałów uzyskanych w toku przeprowadzenia przedmiotowej kontroli. Ma to na celu wykluczenie na etapie stosowania prawa ewentualnych wątpliwości mogących powstać podczas niszczenia zgromadzonych materiałów, którego tryb został dookreślony w przepisie.

***20a.** Dokumentację materiałów zgromadzonych podczas stosowania kontroli operacyjnej, stanowią:*
1) nośniki, na których utrwalone zostały treści rozmów telefonicznych lub innych przekazów informacji albo treści korespondencji lub zawartość przesyłek;
2) kopie wykonane z nośników, o których mowa w pkt 1;

3) dokumenty sporządzone na podstawie informacji utrwalonych na nośnikach i kopiach, o których mowa w pkt 1 i 2.

20b. *Dokumentacja materiałów zgromadzonych podczas stosowania kontroli operacyjnej podlega protokolarnemu i komisyjnemu zniszczeniu w przypadku, o którym mowa w:*

1) ust. 15 - niezwłocznie po przekazaniu materiałów, które dokumentuje, prokuratorowi;

2) ust. 17 - wraz z tymi materiałami.

20c. *W przypadku, o którym mowa w ust. 15f, dokumentacja materiałów zgromadzonych podczas stosowania kontroli operacyjnej, o której mowa w ust. 20a:*

1) pkt 1 - podlega komisyjnemu, protokolarnemu zniszczeniu wraz z materiałami, które dokumentuje, albo niezwłocznie po przekazaniu tych materiałów prokuratorowi;

2) pkt 2 i 3 - nie jest sporządzana.",

6. Określenie maksymalnego okresu prowadzenia czynności operacyjno – rozpoznawczych.

W odniesieniu do służb policyjnych proponuje się, aby maksymalny okres stosowania kontroli operacyjnej trwał 18 miesięcy. Trybunał zwrócił uwagę, że specyfika działalności służb informacyjno-wywiadowczych oraz związany z tym relatywnie wąsko określony zakres ich ustawowych zadań, może uzasadniać ustalenie zasad prowadzenia takich czynności i wykorzystywania zgromadzonych materiałów, od reguł obowiązujących pozostałe organy państwa, a zwłaszcza służby policyjne, mające szeroki zakres działań. Ze względu na specyfikę zadań realizowanych przez służby specjalne, ograniczenia takie nie zostały wprowadzone w tych formacjach. Wskazano natomiast, że kontrola operacyjna może być przedłużana na następujące po sobie okresy, z których żaden nie może trwać dłużej niż 12 miesięcy.

Art. 19.

9. W uzasadnionych przypadkach, gdy podczas stosowania kontroli operacyjnej pojawią się nowe okoliczności istotne dla zapobieżenia lub wykrycia przestępstwa albo ustalenia sprawców i uzyskania dowodów przestępstwa, sąd okręgowy, na pisemny wniosek Komendanta Głównego Policji, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, może, również po upływie okresów, o których mowa w ust. 8, jednokrotnie wydać postanowienie o przedłużeniu kontroli operacyjnej, na czas oznaczony jednak nie dłuższy niż 12 miesięcy.

7. Nałożenie obowiązku podawania do publicznej wiadomości informacji dotyczących udostępnionych danych telekomunikacyjnych.

Proponuje się wprowadzenie obowiązku corocznego przekazywania przez Ministra Sprawiedliwości Sejmowi i Senatowi zagregowanych informacji na temat przetwarzania danych telekomunikacyjnych oraz wyników przeprowadzonych kontroli udostępniania tych danych.

Ponadto, w projekcie proponuje się uwzględnienie zmiany *ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243, z późn. zm.).* Konieczność nowelizacji w tym zakresie wynika z wyroku Trybunału Sprawiedliwości UE z dnia 8 kwietnia 2014 r. Trybunał w przedmiotowym wyroku stwierdził nieważność *dyrektywy 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie*

dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniającej dyrektywę 2002/58/WE. W konsekwencji powyższego, utracił podstawę prawną obowiązek przekazywania przez przedsiębiorców telekomunikacyjnych Prezesowi Urzędu Komunikacji Elektronicznej informacji na temat ilości danych telekomunikacyjnych przekazywanych służbom i następnie obowiązek przekazywania tych informacji przez Prezesa UKE Komisji Europejskiej.

8. Przeniesienie do materii ustawowej kwestii uregulowanych w rozporządzeniu oraz dostosowanie obowiązujących przepisów.

Proponuje się włączenie do materii ustawowej przepisów rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 10 czerwca 2011 r. *w sprawie sposobu dokumentowania prowadzonej przez Policję kontroli operacyjnej, przechowywania i przekazywania wniosków, zarządzeń i materiałów uzyskanych podczas stosowania tej kontroli, a także przetwarzania i niszczenia tych* dotyczące prowadzenia przez poszczególne organy rejestrów wniosków i zarządzeń kontroli operacyjnej. Taki zabieg legislacyjny podyktowany jest potrzebą stworzenia kompleksowych regulacji na poziomie ustawowym, adekwatnym do przedmiotu regulacji, który związany jest ze sferą praw i wolności obywatelskich.

Art.19.

16a. Sąd okręgowy, Prokurator Generalny, prokurator okręgowy i organ Policji prowadzą rejestry: postanowień, pisemnych zgód, wniosków i zarządzeń dotyczących kontroli operacyjnej.
16b. Komendant Główny Policji może prowadzić rejestr centralny wniosków i zarządzeń dotyczących kontroli operacyjnej organów Policji, w zakresie przewidzianym dla prowadzonych przez nie rejestrów.
16c. Organ Policji może odrębnie ewidencjonować dane zawarte w dokumentacji z kontroli operacyjnej, w zakresie przewidzianym dla prowadzonych przez organy Policji rejestrów, o których mowa w ust. 16a.

Projekt w sposób komplementarny wprowadza zmiany obowiązujących przepisów ustawowych dotyczących pozyskiwania i przetwarzania danych telekomunikacyjnych i „pocztowych" oraz odnoszących się do prowadzenia kontroli operacyjnej, czego konsekwencją jest nadanie wybranym przepisom nowego brzmienia.

Art. 20c.

2. 2. Podmiot prowadzący działalność telekomunikacyjną lub operator świadczący usługi pocztowe udostępnia nieodpłatnie dane, o których mowa w ust. 1:
1) policjantowi wskazanemu w pisemnym wniosku Komendanta Głównego Policji, Komendanta CBŚP, komendanta wojewódzkiego Policji albo osoby przez nich upoważnionej;
2) na ustne żądanie policjanta posiadającego pisemne upoważnienie osób, o których mowa w pkt 1;
3) za pośrednictwem sieci telekomunikacyjnej policjantowi posiadającemu pisemne upoważnienie osób, o których mowa w pkt 1;
4) organowi Policji wskazanemu w postanowieniu sądu wyrażającym zgodę na pozyskanie danych telekomunikacyjnych lub pocztowych, w przypadkach, o których mowa w art. 20ca ust. 1 lub 3.
3. W przypadku, o którym mowa w ust. 2 pkt 3, udostępnianie danych, o których mowa w ust. 1, odbywa się bez udziału pracowników podmiotu prowadzącego działalność telekomunikacyjną lub pocztową,

lub przy niezbędnym ich udziale, jeżeli możliwość taka jest przewidziana w porozumieniu zawartym pomiędzy Komendantem Głównym Policji a tym podmiotem.

4. Udostępnienie Policji danych, o których mowa w ust. 1, może nastąpić za pośrednictwem sieci telekomunikacyjnej jeżeli:

1) wykorzystywane sieci telekomunikacyjne zapewniają:

a) możliwość ustalenia osoby uzyskującej dane, ich rodzaju oraz czasu, w którym zostały uzyskane,

b) zabezpieczenie techniczne i organizacyjne uniemożliwiające osobie nieuprawnionej dostęp do danych;

2) jest to uzasadnione specyfiką lub zakresem zadań wykonywanych przez jednostki organizacyjne Policji albo prowadzonych przez nie czynności.

5. Materiały uzyskane w wyniku czynności związanych z udostępnieniem danych telekomunikacyjnych lub pocztowych, które zawierają informacje mające znaczenie dla postępowania karnego Komendant Główny Policji, Komendant CBŚP albo komendant wojewódzki (Stołeczny) Policji przekazują prokuratorowi właściwemu miejscowo lub rzeczowo.

Projektowana nowelizacja przepisów przewiduje również nadanie nowego brzmienia przepisu zawierającego upoważnienie dla ministra właściwego do spraw wewnętrznych, który wraz z ministrem właściwym do spraw łączności określi w drodze rozporządzenia sposób dokumentowania kontroli operacyjnej oraz pozostałych kwestii dotyczących jej rejestrów i przechowywania dokumentacji zgromadzonych materiałów uzyskanych podczas kontroli operacyjnej.

Art. 19.

21. Minister właściwy do spraw wewnętrznych, w porozumieniu z Ministrem Sprawiedliwości oraz ministrem właściwym do spraw łączności, określi, w drodze rozporządzenia:

1) sposób dokumentowania kontroli operacyjnej,

2) sposób przechowywania i przekazywania dokumentacji kontroli operacyjnej,

3) szczegółowy sposób dokumentowania materiałów uzyskanych podczas stosowania kontroli operacyjnej oraz sposób przechowywania, przekazywania oraz niszczenia tych materiałów i dokumentacji,

4) sposób prowadzenia rejestrów, o których mowa w ust. 16a - 16c,

5) wzory dokumentów wchodzących w zakres dokumentacji kontroli operacyjnej oraz rejestrów, o których mowa w ust. 16a - 16c

- uwzględniając potrzebę zapewnienia niejawnego charakteru podejmowanych czynności i uzyskanych materiałów oraz przejrzystość dokumentacji i rejestrów.

Konsekwencją dookreślenia przepisów dotyczących udostępniania danych telekomunikacyjnych, o którym mowa w pkt 1.1., tzn. uwzględnienie w przepisie danych, które na podstawie obowiązującego art. 20d ust. 3 *ustawy o Policji* są udostępniane na wniosek organu Policji przez podmioty uprawnione do świadczenia usług pocztowych, będzie uchylenie obowiązującego przepisu art. 20d *ustawy o Policji*.

Reasumując, w opinii Ministerstwa Spraw Wewnętrznych, w celu zachowania zasady proporcjonalności pomiędzy ochroną praw i wolności obywatelskich a zapewnieniem skutecznych i szybkich działań służb bezpieczeństwa i porządku publicznego, zasadne jest, aby dalsze prace nad wykonaniem wyroku Trybunału Konstytucyjnego sygn. akt K 23/11 oraz realizacją wniosków *de lege ferenda* NIK prowadzone

były przez stronę rządową. Wydaje się, że na obecnym zaawansowanym etapie prac nad rządowym projektem, proces dostosowania projektu senackiego do postulatów zawartych w wyroku Trybunału Konstytucyjnego nie znajduje uzasadnienia.

Z wyrazami szacunku

Mariusz Kamiński

ul. Stefana Batorego 5
02-591 Warszawa, Polska
msw.gov.pl

tel. +48 22 601 46 20
fax +48 22 601 39 88