SEJM
RZECZYPOSPOLITEJ POLSKIEJ
VIII kadencja

Druk nr 154

Warszawa, 23 grudnia 2015 r.

Pan
Marek Kuchciński
Marszałek Sejmu
Rzeczypospolitej Polskiej

Na podstawie art. 118 ust. 1 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. i na podstawie art. 32 ust. 2 regulaminu Sejmu niżej podpisani posłowie wnoszą projekt ustawy:

- o zmianie ustawy o Policji oraz niektórych innych ustaw.

Do reprezentowania wnioskodawców w pracach nad projektem ustawy upoważniamy pana posła Marka Opiołę.

(-) Iwona Ewa Arent; (-) Ryszard Bartosik; (-) Dariusz Bąk; (-) Jerzy Bielecki; (-) Zbigniew Biernat; (-) Przemysław Czarnecki; (-) Jan Duda; (-) Jacek Falfus; (-) Leszek Galemba; (-) Szymon Giżyński; (-) Krzysztof Głuchowski; (-) Jerzy Gosiewski; (-) Teresa Hałas; (-) Grzegorz Janik; (-) Robert Kołakowski; (-) Joanna Kopcińska; (-) Jacek Kurzępa; (-) Marzena Machałek; (-) Jerzy Małecki; (-) Beata Mateusiak-Pielucha; (-) Kazimierz Matuszny; (-) Kazimierz Moskal; (-) Adam Ołdakowski; (-) Jerzy Paul; (-) Marcin Porzucek; (-) Grzegorz Puda; (-) Anna Schmidt-Rodziewicz; (-) Łukasz Schreiber; (-) Czesław Sobierajski; (-) Lech Sprawka; (-) Krzysztof Szulowski; (-) Szymon Szynkowski vel Sęk; (-) Jacek Świat; (-) Robert Telus; (-) Sylwester Tułajew; (-) Piotr Uruski; (-) Jerzy Wilk; (-) Krystyna Wróblewska; (-) Bartłomiej Wróblewski.

Projekt

U S T A W A

z dnia ……

o zmianie ustawy o Policji oraz niektórych innych ustaw[1)]

Art. 1. W ustawie z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2015 r. poz. 355 i 529) wprowadza się następujące zmiany:

1) w art. 19:

a) w ust. 1:

– wprowadzenie do wyliczenia otrzymuje brzmienie:

„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:”,

– pkt 8 otrzymuje brzmienie:

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

b) ust. 6 otrzymuje brzmienie:

„6. Kontrola operacyjna prowadzona jest niejawnie i polega 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;

---

1) Niniejszą ustawą zmienia się ustawy: ustawę z dnia 6 kwietnia 1990 r. o Policji, ustawę z dnia 12 października 1990 r. o Straży Granicznej, ustawę z dnia 28 września 1991 r. o kontroli skarbowej, ustawę z dnia 21 sierpnia 1997 r. – Prawo o ustroju sądów wojskowych, ustawę z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych, ustawę z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych, ustawę z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, ustawę z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, ustawę z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, ustawę z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym oraz ustawę z dnia 27 sierpnia 2009 r. o Służbie Celnej.

4) uzyskiwaniu i utrwalaniu danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych ;

5) uzyskiwaniu dostępu i kontroli zawartości przesyłek.”,

c) po ust. 6 dodaje się ust. 6a i 6b w brzmieniu:

„6a. Kontroli operacyjnej nie stanowią czynności, o których mowa w ust. 6, 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. Realizacja czynności, o których mowa w ust. 6a nie wymaga zgody sądu.”,

d) ust. 9 otrzymuje brzmienie:

„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, wydawać kolejne postanowienie o przedłużeniu kontroli operacyjnej na następujące po sobie okresy, których łączna długość nie może przekraczać 12 miesięcy.”,

e) po ust. 9 dodaje się ust. 9a w brzmieniu:

„9a. Komendant Główny Policji albo Komendant CBŚP może upoważnić swojego zastępcę do składania wniosków, o których mowa w ust. 1, 3, 8 i 9 lub do zarządzania kontroli operacyjnej w trybie ust. 3.”,

f) ust. 12 otrzymuje brzmienie:

„12. Przedsiębiorca telekomunikacyjny, operator pocztowy oraz usługodawca świadczący usługi drogą elektroniczną jest obowiązany do zapewnienia na własny koszt warunków technicznych i organizacyjnych umożliwiających prowadzenie przez Policję kontroli operacyjnej.”,

g) po ust. 15e dodaje się ust. 15f–15j w brzmieniu:

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

1) o których mowa w art. 178 Kodeksu postępowania karnego;

2) o których mowa w art. 178a i art. 180 § 3 Kodeksu postępowania karnego, z wyłączeniem informacji o przestępstwach, o których mowa w art. 240 § 1 Kodeksu karnego;

3) 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, 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) stwierdzenie, które z przekazanych materiałów zawierają informacje, o których mowa w ust. 15f,

2) dopuszczenie do wykorzystania w postępowaniu karnym materiałów zawierających informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego nieobjęte zakazami, określonymi w art. 178, art. 178a i art. 180 § 3 Kodeksu postępowania karnego, z wyłączeniem informacji o przestępstwach, o których mowa w art. 240 § 1 Kodeksu karnego.

15h. Sąd, niezwłocznie po złożeniu wniosku przez prokuratora, wydaje postanowienie o 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, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu, , a także zarządza niezwłoczne zniszczenie materiałów, których wykorzystanie w postępowaniu karnym jest niedopuszczalne.

15i. Na postanowienie sądu w przedmiocie 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, prokuratorowi przysługuje zażalenie. Do zażalenia stosuje się odpowiednio przepisy Kodeksu postępowania karnego.

15j. Organ Policji jest obowiązany do wykonania zarządzenia sądu, o którym mowa w ust. 15h oraz niezwłocznego, komisyjnego i protokolarnego zniszczenia materiałów, których wykorzystanie w postępowaniu karnym jest niedopuszczalne. Organ Policji niezwłocznie informuje prokuratora, o którym mowa w ust. 15g, o zniszczeniu tych materiałów.”,

h) po ust. 16 dodaje się ust. 16a–16d w brzmieniu:

„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. W komórkach organizacyjnych Policji wykonujących zarządzenia w sprawie kontroli operacyjnej można odrębnie rejestrować dane zawarte w dokumentacji z kontroli operacyjnej w zakresie przewidzianym dla prowadzonych przez organy Policji rejestrów, o których mowa w ust. 16a.

16d. Rejestry, o których mowa w ust. 16a-16c, prowadzi się w formie elektronicznej, z zachowaniem przepisów o ochronie informacji niejawnych.”;

i) ust. 20 otrzymuje brzmienie:

„20. Na postanowienia sądu, o których mowa w:

1) ust. 1, 3, 8 i 9 - przysługuje zażalenie organowi Policji, który złożył wniosek o wydanie tego postanowienia;

2) ust. 3 i ust. 15c – przysługuje zażalenie właściwemu prokuratorowi, o którym mowa w ust. 1.

Do zażalenia stosuje się odpowiednio przepisy Kodeksu postępowania karnego.”

2) art. 20c otrzymuje brzmienie:

„Art. 20c. 1. W celu rozpoznawania, zapobiegania, zwalczania, wykrywania albo uzyskania i utrwalenia dowodów przestępstw albo w celu ratowania życia lub zdrowia

ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych, Policja może uzyskiwać dane:

1) określone 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) określone w art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. poz. 1529, z późn. zm.), zwane dalej „danymi pocztowymi”
3) określone w art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422, z późn. zm.), zwane dalej „danymi internetowymi”

– oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.

2. Przedsiębiorca telekomunikacyjny, operator pocztowy lub usługodawca świadczący usługi drogą elektroniczną 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;

3. W przypadku, o którym mowa w ust. 2 pkt 3, udostępnianie danych, o których mowa w ust. 1, odbywa się bez udziału pracowników przedsiębiorcy telekomunikacyjnego, operatora pocztowego lub usługodawcy świadczącego usługi drogą elektroniczną, 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. Komendant Główny Policji, Komendant CBŚP i komendant wojewódzki Policji prowadzi rejestr wystąpień o uzyskanie danych telekomunikacyjnych, pocztowych i internetowych zawierający informacje identyfikujące jednostkę organizacyjną Policji i funkcjonariusza Policji uzyskującego te dane, ich rodzaj, cel uzyskania oraz czas, w którym zostały uzyskane. Rejestr prowadzi się w formie elektronicznej, z zachowaniem przepisów o ochronie informacji niejawnych.

6. Dane, o których mowa w ust. 1, które mają znaczenie dla postępowania karnego Komendant Główny Policji, Komendant CBŚP albo komendant wojewódzki Policji przekazują prokuratorowi właściwemu miejscowo lub rzeczowo. Prokurator podejmuje decyzję o zakresie i sposobie wykorzystania przekazanych danych.

7. Dane, o których mowa w ust. 1, które nie mają znaczenia dla postępowania karnego, podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu.”;

3) po art. 20c dodaje się art. 20ca–20cb w brzmieniu:

„Art. 20ca. 1. Kontrolę nad uzyskiwaniem przez Policję danych telekomunikacyjnych, pocztowych lub internetowych sprawuje sąd okręgowy właściwy dla siedziby organu Policji, któremu udostępniono te dane.

2. Organ Policji, o którym mowa w ust. 1, przekazuje, z zachowaniem przepisów o ochronie informacji niejawnych, sądowi okręgowemu, o którym mowa w ust. 1, 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.

3. W ramach kontroli, o której mowa w ust. 1, sąd okręgowy może zapoznać się z materiałami uzasadniającymi udostępnienie Policji danych telekomunikacyjnych, pocztowych lub internetowych.

4. Sąd okręgowy informuje organ Policji o wyniku kontroli w terminie 30 dni od jej zakończenia.

5. Kontroli, o której mowa w ust. 1, nie podlega uzyskiwanie danych na podstawie art. 20cb ust. 1.

Art. 20cb. 1. W celu rozpoznawania, zapobiegania, zwalczania, wykrywania albo uzyskania i utrwalenia dowodów przestępstw albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych, Policja może uzyskiwać dane:

1) z wykazu, o którym mowa w art. 179 ust. 9 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;
2) o których mowa w art. 161 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne,
3) 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,
4) w przypadku stacjonarnej publicznej sieci telekomunikacyjnej – także nazwę miejscowości oraz ulicy, przy której znajduje się zakończenie sieci, udostępnione użytkownikowi

– oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.

2. Do udostępniania i przetwarzania danych, o których mowa w ust. 1, art. 20c ust. 2–7 stosuje się.”;

4) uchyla się art. 20d;
5) w art. 20da ust. 1 otrzymuje brzmienie:

„1. W celu poszukiwania osób zaginionych Policja może uzyskiwać dane telekomunikacyjne, pocztowe i internetowe oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą; przepisy art. 20c ust. 2-7 stosuje się.”.

Art. 2. W ustawie z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2014 r. poz. 1402, z późn. zm.[2)]) wprowadza się następujące zmiany:

1) w art. 9e:
   a) w ust. 1:
      – pkt 4 otrzymuje brzmienie:

[2)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2014 r. poz. 1055 i 1822 oraz z 2015 r. poz. 529.

„4) określonych w art. 183 § 2, 4 i 5, art. 184 § 1 i 2, art. 263 § 1 i 2, art. 278 § 1, art. 291 § 1 i art. 306 Kodeksu karnego, art. 55 i art. 56 ustawy z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii (Dz. U. z 2012 r. poz. 124 oraz z 2015 r. poz. 28), a także art. 44 i 46a ustawy z dnia 1 lipca 2005 r. o pobieraniu, przechowywaniu i przeszczepianiu komórek, tkanek i narządów (Dz. U. z 2015 r. poz. 793) oraz art. 109 ust. 1 ustawy z dnia 23 lipca 2003 r. o zabytkach i opiece nad zabytkami (Dz. U. z 2014 r. poz. 1446), jeżeli przestępstwa te pozostają w związku z przemieszczaniem przedmiotów przestępstwa przez granicę państwową,”,

– pkt 7 otrzymuje brzmienie:

„7) ściganych na mocy umów międzynarodowych, ratyfikowanych za uprzednią zgodą wyrażoną w ustawie, określonych w polskiej ustawie karnej”,

b) ust. 7 otrzymuje brzmienie:

„7. Kontrola operacyjna prowadzona jest niejawnie i polega 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.”,

c) po ust. 7 dodaje się ust. 7a i 7b w brzmieniu:

„7a. Kontroli operacyjnej nie stanowią czynności, o których mowa w ust. 7, polegające na:

1) uzyskiwaniu i utrwalaniu obrazu w pomieszczeniach, o których mowa w art. 11 ust. 1 pkt 7a;
2) uzyskiwaniu danych w trybie art. 10b.

7b. Realizacja czynności, o których mowa w ust. 7a nie wymaga zgody sądu.”,

d) ust. 10 otrzymuje brzmienie:

„10. 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 Straży Granicznej lub komendanta oddziału Straży Granicznej, złożony po uzyskaniu pisemnej zgody prokuratora, o którym mowa w ust. 1, może, również po upływie okresów, o których mowa w ust. 9, wydawać kolejne postanowienie o przedłużeniu kontroli operacyjnej na następujące po sobie okresy, których łączna długość nie może przekraczać 12 miesięcy.”,

e) po ust. 10 dodaje się ust. 10a w brzmieniu:

„10a. Komendant Główny Straży Granicznej może upoważnić swojego zastępcę do składania wniosków, o których mowa w ust. 1, ust. 4 pkt. 1, ust. 9 i ust. 10 lub do zarządzania kontroli operacyjnej w trybie ust. 4 pkt 1.”,

f) ust. 13 otrzymuje brzmienie:

„13. Przedsiębiorca telekomunikacyjny, operator pocztowy oraz usługodawca świadczący usługi drogą elektroniczną jest obowiązany do zapewnienia na własny koszt warunków technicznych i organizacyjnych umożliwiających prowadzenie przez Straż Graniczną kontroli operacyjnej.”,

g) po ust. 16e dodaje się ust. 16f–16j w brzmieniu:

„16f. W przypadku, gdy zachodzi przypuszczenie, że materiały, o których mowa w ust. 16 mogą zawierać informacje:

1) o których mowa w art. 178 Kodeksu postępowania karnego;

2) o których mowa w art. 178a i art. 180 § 3 Kodeksu postępowania karnego, z wyłączeniem informacji o przestępstwach, o których mowa w art. 240 § 1 Kodeksu karnego;

3) stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego

— Komendant Główny Straży Granicznej lub komendant oddziału Straży Granicznej przekazują prokuratorowi te materiały.

16g. W przypadku, o którym mowa w ust. 16f, prokurator niezwłocznie po otrzymaniu materiałów, kieruje je do sądu, który zarządził kontrolę operacyjną albo wyraził na nią zgodę w trybie określonym w ust. 4, wraz z wnioskiem o:

1) stwierdzenie, które z przekazanych materiałów zawierają informacje, o których mowa w ust. 16f,
2) dopuszczenie do wykorzystania w postępowaniu karnym materiałów zawierających informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego nieobjęte zakazami, określonymi w art. 178, art. 178a i art. 180 § 3 Kodeksu postępowania karnego, z wyłączeniem informacji o przestępstwach, o których mowa w art. 240 § 1 Kodeksu karnego.

16h. Sąd, niezwłocznie po złożeniu wniosku przez prokuratora, wydaje postanowienie o 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, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu, , a także zarządza niezwłoczne zniszczenie materiałów, których wykorzystanie w postępowaniu karnym jest niedopuszczalne.

16i. Na postanowienie sądu w przedmiocie 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, prokuratorowi przysługuje zażalenie. Do zażalenia stosuje się odpowiednio przepisy Kodeksu postępowania karnego.

16j. Organ Straży Granicznej jest obowiązany do wykonania zarządzenia sądu, o którym mowa w ust. 16h oraz niezwłocznego, komisyjnego i protokolarnego zniszczenia materiałów, których wykorzystanie w postępowaniu karnym jest niedopuszczalne. Organ Straży Granicznej niezwłocznie informuje prokuratora, o którym mowa w ust. 16g o zniszczeniu tych materiałów.”,

h) po ust. 17 dodaje się ust. 17a w brzmieniu:

„17a. Sąd okręgowy, Prokurator Generalny, prokurator okręgowy i organ Straży Granicznej prowadzą rejestry: postanowień, pisemnych zgód, wniosków

i zarządzeń dotyczących kontroli operacyjnej. Rejestry prowadzi się w formie elektronicznej, z zachowaniem przepisów o ochronie informacji niejawnych.”,

i) ust. 19 otrzymuje brzmienie:

„19. Na postanowienia sądu, o których mowa w:

1) ust. 1, 4, 9 i 10 - przysługuje zażalenie organowi Straży Granicznej, który złożył wniosek o wydanie tego postanowienia;

2) ust. 4 i ust. 16c – przysługuje zażalenie właściwemu prokuratorowi, o którym mowa w ust. 1.

Do zażalenia stosuje się odpowiednio przepisy Kodeksu postępowania karnego.”;

2) art. 10b otrzymuje brzmienie:

„Art. 10b. 1. W celu rozpoznawania, zapobiegania, zwalczania, wykrywania albo uzyskania i utrwalenia dowodów przestępstw Straż Graniczna może uzyskiwać 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) określone w art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. poz. 1529, z późn. zm.), zwane dalej „danymi pocztowymi”
3) określone w art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422, z późn. zm.), zwane dalej „danymi internetowymi”

– oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.

2. Przedsiębiorca telekomunikacyjny, operator pocztowy lub usługodawca świadczący usługi drogą elektroniczną udostępnia nieodpłatnie dane, o których mowa w ust. 1:

1) funkcjonariuszowi Straży Granicznej wskazanemu w pisemnym wniosku Komendanta Głównego Straży Granicznej lub komendanta oddziału Straży Granicznej albo osoby przez nich upoważnionej,
2) na ustne żądanie funkcjonariusza posiadającego pisemne upoważnienie osób, o których mowa w pkt 1,
3) za pośrednictwem sieci telekomunikacyjnej funkcjonariuszowi posiadającemu pisemne upoważnienie osób, o których mowa w pkt 1,

3. W przypadku, o którym mowa w ust. 2 pkt 3, udostępnianie danych, o których mowa w ust. 1, odbywa się bez udziału pracowników przedsiębiorcy telekomunikacyjnego, operatora pocztowego lub usługodawcy świadczącego usługi drogą elektroniczną, lub przy niezbędnym ich udziale, jeżeli możliwość taka jest przewidziana w porozumieniu zawartym pomiędzy Komendantem Głównym Straży Granicznej a tym podmiotem.

4. Udostępnienie Straży Granicznej 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 Straży Granicznej albo prowadzonych przez nie czynności.

5. Komendant Główny Straży Granicznej i komendant oddziału Straży Granicznej prowadzi rejestr wystąpień o uzyskanie danych telekomunikacyjnych, pocztowych i internetowych zawierający informacje identyfikujące jednostkę organizacyjną Straży Granicznej i funkcjonariusza Straży Granicznej uzyskującego te dane, ich rodzaj, cel uzyskania oraz czas, w którym zostały uzyskane. Rejestr prowadzi się w formie elektronicznej, z zachowaniem przepisów o ochronie informacji niejawnych.

6. Dane, o których mowa w ust. 1, które mają znaczenie dla postępowania karnego, Komendant Główny Straży Granicznej lub komendant oddziału Straży Granicznej przekazują prokuratorowi właściwemu miejscowo lub rzeczowo. Prokurator podejmuje decyzję o zakresie i sposobie wykorzystania przekazanych danych.

7. Dane, o których mowa w ust. 1, które nie mają znaczenia dla postępowania karnego, podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu.

3) po art. 10b dodaje się art. 10ba–10bb w brzmieniu:

„Art.10ba. 1. Kontrolę nad uzyskiwaniem przez Straż Graniczną danych telekomunikacyjnych, pocztowych lub internetowych sprawuje sąd okręgowy właściwy dla siedziby składającego wniosek organu Straży Granicznej.

2. Organ Straży Granicznej, który wystąpił z wnioskiem, przekazuje, z zachowaniem przepisów o ochronie informacji niejawnych, sądowi okręgowemu, o którym mowa w ust. 1, 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.

3. W ramach kontroli, o której mowa w ust. 1, sąd okręgowy może zapoznać się z materiałami uzasadniającymi udostępnienie Straży Granicznej danych telekomunikacyjnych, pocztowych lub internetowych.

4. Sąd okręgowy informuje organ Straży Granicznej o wyniku kontroli w terminie 30 dni od jej zakończenia.

5. Kontroli, o której mowa w ust. 1, nie podlega uzyskiwanie danych na podstawie art. 10bb ust. 1.

Art. 10bb. 1. W celu rozpoznawania, zapobiegania, zwalczania, wykrywania albo uzyskania i utrwalenia dowodów przestępstw Straż Graniczna może uzyskiwać dane:

1) z wykazu, o którym mowa w art. 179 ust. 9 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;
2) o których mowa w art. 161 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne,
3) 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,
4) w przypadku stacjonarnej publicznej sieci telekomunikacyjnej – także nazwę miejscowości oraz ulicy, przy której znajduje się zakończenie sieci, udostępnione użytkownikowi

– oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.

2. Do udostępniania i przetwarzania danych, o których mowa w ust. 1, art. 10b ust. 2–7 stosuje się.”.

Art. 3. W ustawie z dnia 28 września 1991 r. o kontroli skarbowej (Dz. U. z 2015 r. poz. 553 i 788) wprowadza się następujące zmiany:

1) w art. 36b:
   a) ust. 1 otrzymuje brzmienie:

„1. W celu rozpoznawania, zapobiegania, zwalczania, wykrywania albo uzyskania i utrwalenia dowodów przestępstw skarbowych lub przestępstw, o których mowa w art. 2 ust. 1 pkt 14b i art. 36c ust. 1 pkt 3, wywiad skarbowy może uzyskiwać dane:

1) określone 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) określone w art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. poz. 1529, z późn. zm.), zwane dalej „danymi pocztowymi”;
3) określone w art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422, z późn. zm.), zwane dalej „danymi internetowymi”

– oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.”,

b) w ust. 2 wprowadzenie do wyliczenia otrzymuje brzmienie:

„Przedsiębiorca telekomunikacyjny, operator pocztowy lub usługodawca świadczący usługi drogą elektroniczną udostępnia nieodpłatnie dane, o których mowa w ust. 1:”,

c) ust. 3 otrzymuje brzmienie:

„3. W przypadku, o którym mowa w ust. 2 pkt 3, udostępnianie danych, o których mowa w ust. 1, odbywa się bez udziału pracowników przedsiębiorcy telekomunikacyjnego, operatora pocztowego lub usługodawcy świadczącego usługi drogą elektroniczną lub przy niezbędnym ich udziale, jeżeli możliwość taką przewiduje porozumienie zawarte pomiędzy Generalnym Inspektorem Kontroli Skarbowej a tym podmiotem.”,

d) uchyla się ust. 4 i 5;

e) w ust. 6 wprowadzenie do wyliczenia otrzymuje brzmienie:

„Udostępnienie wywiadowi skarbowemu danych, o których mowa w ust. 1, może nastąpić za pośrednictwem sieci telekomunikacyjnej, jeżeli sieć ta zapewnia:”,

f) ust. 7 otrzymuje brzmienie:

„7. Udostępnianie wywiadowi skarbowemu danych, o których mowa w ust. 1, następuje na koszt przedsiębiorcy telekomunikacyjnego, operatora pocztowego lub usługodawcy świadczącego usługi drogą elektroniczną.”,

g) po ust. 7 dodaje się ust. 8 w brzmieniu:

„8. Generalny Inspektor Kontroli Skarbowej prowadzi rejestr wystąpień o uzyskanie danych telekomunikacyjnych, pocztowych i internetowych zawierający informacje identyfikujące jednostkę organizacyjną wywiadu skarbowego i pracownika wywiadu skarbowego uzyskującego te dane, ich rodzaj, cel uzyskania oraz czas, w którym zostały uzyskane. Rejestr prowadzi się w formie elektronicznej, z zachowaniem przepisów o ochronie informacji niejawnych.”;

2) po art. 36b dodaje się art. 36ba–36bb w brzmieniu:

„Art. 36ba. 1. Kontrolę nad uzyskiwaniem przez wywiad skarbowy danych telekomunikacyjnych, pocztowych lub internetowych sprawuje Sąd Okręgowy w Warszawie, zwany dalej „Sądem”.

2. Generalny Inspektor Kontroli Skarbowej przekazuje 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.

3. W ramach kontroli, o której mowa w ust. 1, Sąd może zapoznać się z materiałami uzasadniającymi udostępnienie wywiadowi skarbowemu danych telekomunikacyjnych, pocztowych lub internetowych.

4. Sąd informuje Generalnego Inspektora Kontroli Skarbowej o wyniku kontroli w terminie 30 dni od jej zakończenia.

5. Kontroli, o której mowa w ust. 1, nie podlega uzyskiwanie danych na podstawie art. 36bb ust. 1.

Art. 36bb. 1. W celu rozpoznawania, zapobiegania, zwalczania, wykrywania albo uzyskania i utrwalenia dowodów przestępstw skarbowych lub przestępstw, o których mowa w art. 2 ust. 1 pkt 14b i art. 36c ust. 1 pkt 3, wywiad skarbowy może uzyskiwać dane:

1) z wykazu, o którym mowa w art. 179 ust. 9 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;

2) o których mowa w art. 161 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne,

3) 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,

4) w przypadku stacjonarnej publicznej sieci telekomunikacyjnej – także nazwę miejscowości oraz ulicy, przy której znajduje się zakończenie sieci, udostępnione użytkownikowi

– oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.

2. Do udostępniania i przetwarzania danych, o których mowa w ust. 1, art. 36b ust. 2-3 i ust. 6-7 oraz art. 36d ust. 1 stosuje się.”;

3) w art. 36c:

a) w ust. 1 pkt 5 otrzymuje brzmienie:

„5) ściganych na mocy umów międzynarodowych ratyfikowanych za uprzednią zgodą wyrażoną w ustawie, określonych w polskiej ustawie karnej”,

b) ust. 4 otrzymuje brzmienie:

„4. Kontrola operacyjna prowadzona jest niejawnie i polega 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.”,

c) po ust. 4 dodaje się ust. 4a w brzmieniu:

„4a. Kontroli operacyjnej nie stanowią czynności, o których mowa w ust. 4 pkt 4, polegające na uzyskiwaniu danych w trybie art. 36b. Realizacja tych czynności nie wymaga zgody sądu.”,

d) ust. 7 otrzymuje brzmienie:

„7. W uzasadnionych przypadkach, gdy podczas stosowania kontroli operacyjnej pojawią się nowe okoliczności istotne dla wykrycia przestępstwa lub przestępstwa skarbowego albo ustalenia sprawców i uzyskania dowodów takich przestępstw, Sąd, na pisemny wniosek Generalnego Inspektora Kontroli Skarbowej, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, może, również po upływie okresów, o których mowa w ust. 6, wydawać kolejne postanowienie o przedłużeniu kontroli operacyjnej na następujące po sobie okresy, których łączna długość nie może przekraczać 12 miesięcy.”,

e) po ust. 7 dodaje się ust. 7a w brzmieniu:

„7a. Generalny Inspektor Kontroli Skarbowej może upoważnić swojego zastępcę do składania wniosków, o których mowa w ust. 1, 2, 6 i 7 lub do zarządzania kontroli operacyjnej w trybie ust. 2.”,

f) ust. 10 otrzymuje brzmienie:

„10. Przedsiębiorca telekomunikacyjny, operator pocztowy oraz usługodawca świadczący usługi drogą elektroniczną jest obowiązany do zapewnienia na własny koszt warunków technicznych i organizacyjnych umożliwiających prowadzenie przez wywiad skarbowy kontroli operacyjnej.”,

g) po ust. 13 dodaje się ust. 13a w brzmieniu:

„13a. Sąd, Prokurator Generalny i Generalny Inspektor Kontroli Skarbowej prowadzą odpowiednio rejestry postanowień, pisemnych zgód, zarządzeń i wniosków dotyczących kontroli operacyjnej. Rejestry prowadzi się w formie elektronicznej, z zachowaniem przepisów o ochronie informacji niejawnych.”

h) ust. 14 otrzymuje brzmienie:

„14. Na postanowienia sądu, o których mowa w:

1) ust. 1, 2, 6 i 7 - przysługuje zażalenie Generalnemu Inspektorowi Kontroli Skarbowej;

2) ust. 2 i art. 36d ust. 1c – przysługuje zażalenie Prokuratorowi Generalnemu.

Do zażalenia stosuje się odpowiednio przepisy Kodeksu postępowania karnego.”;

4) w art. 36d:

a) w ust. 1 wprowadzenie do wyliczenia otrzymuje brzmienie:

„Uzyskane w czasie prowadzenia czynności wywiadu skarbowego dane, o których mowa w art. 36b ust. 1, oraz materiały, w tym materiały zgromadzone podczas stosowania kontroli operacyjnej lub niejawnego nadzorowania wytwarzania, przemieszczania, przechowywania i obrotu przedmiotami przestępstwa, które:”,

b) po ust. 1e dodaje się ust. 1f–1i w brzmieniu:

„1f. W przypadku, gdy zachodzi przypuszczenie, że materiały uzyskane w toku kontroli operacyjnej mogą zawierać informacje:

1) o których mowa w art. 178 Kodeksu postępowania karnego;

2) o których mowa w art. 178a i art. 180 § 3 Kodeksu postępowania karnego, z wyłączeniem informacji o przestępstwach, o których mowa w art. 240 § 1 Kodeksu karnego;

3) stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego

— Generalny Inspektor Kontroli Skarbowej przekazuje Prokuratorowi Generalnemu te materiały.

1g. W przypadku, o którym mowa w ust. 1f, Prokurator Generalny niezwłocznie po otrzymaniu materiałów, kieruje je do Sądu, wraz z wnioskiem o:

1) stwierdzenie, które z przekazanych materiałów zawierają informacje, o których mowa w ust. 1f;

2) dopuszczenie do wykorzystania w postępowaniu karnym materiałów zawierających informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego nieobjęte zakazami, określonymi w art. 178, art. 178a i art. 180 § 3 Kodeksu postępowania karnego, z wyłączeniem informacji o przestępstwach, o których mowa w art. 240 § 1 Kodeksu karnego.

1h. Sąd, niezwłocznie po złożenia wniosku przez Prokuratora Generalnego, wydaje postanowienie o dopuszczalności wykorzystania w postępowaniu w sprawie o przestępstwo lub przestępstwo skarbowe materiałów mogących zawierać informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na

podstawie innego dowodu, , a także zarządza niezwłoczne zniszczenie materiałów, których wykorzystanie w postępowaniu karnym jest niedopuszczalne.

1i. Na postanowienie Sądu w przedmiocie 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, Prokuratorowi Generalnemu przysługuje zażalenie. Do zażalenia stosuje się odpowiednio przepisy Kodeksu postępowania karnego.”,

c) ust. 3 otrzymuje brzmienie:

„3. Materiały uzyskane w wyniku czynności podjętych na podstawie art. 36aa ust. 1, art. 36b ust. 1, art. 36c ust. 1 i 2 lub art. 36ca ust. 1, niezawierające dowodów pozwalających na wszczęcie postępowania w sprawie o przestępstwo lub przestępstwo skarbowe, a także materiały uzyskane w wyniku kontroli operacyjnej, o których mowa w ust. 1h, których zniszczenie zarządził Sąd, podlegają niezwłocznemu, komisyjnemu i protokolarnemu zniszczeniu.”,

d) ust. 5 otrzymuje brzmienie:

„5. O wydaniu i wykonaniu zarządzenia dotyczącego zniszczenia materiałów, o których mowa w ust. 3, zgromadzonych na podstawie art. 36b ust. 1, art. 36c ust. 1 i 2 i art. 36ca ust. 1, a także materiałów uzyskanych w wyniku kontroli operacyjnej, o których mowa w ust. 1h, których zniszczenie zarządził Sąd, Generalny Inspektor Kontroli Skarbowej niezwłocznie informuje Prokuratora Generalnego.”.

Art. 4. W ustawie z dnia 21 sierpnia 1997 r. – Prawo o ustroju sądów wojskowych (Dz. U. z 2012 r. poz. 952, z późn. zm.[3)]) po art. 6 dodaje się art. 6a w brzmieniu:

„Art. 6a. Prezesi wojskowych sądów okręgowych właściwych dla siedziby organu wnioskującego o udostępnienie danych, przekazują corocznie Ministrowi Sprawiedliwości informację na temat przetwarzania danych telekomunikacyjnych pocztowych i internetowych, z podziałem na liczbę i rodzaj udostępnianych danych oraz wyników przeprowadzonych kontroli, w terminie do dnia 31 marca roku następującego po roku nią objętym, celem realizacji zadania, o którym mowa w art. 175b § 2 ustawy z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych”.

---

3) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2013 r. poz. 448 i 1247 oraz z 2014 r. poz. 188 i 512.

Art. 5. W ustawie z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych (Dz. U. z 2015 r. poz. 133 i 509) wprowadza się następujące zmiany:

1) w art. 16 w § 4a w pkt 2 kropkę zastępuje się średnikiem i dodaje się pkt 3 w brzmieniu:

„3) kontroli danych telekomunikacyjnych, pocztowych i internetowych – do spraw związanych z kontrolą pozyskiwania danych telekomunikacyjnych, pocztowych i internetowych przez Policję, Agencję Bezpieczeństwa Wewnętrznego, Straż Graniczną, Centralne Biuro Antykorupcyjne, Służbę Celną i wywiad skarbowy.”;

2) tytuł działu IVa otrzymuje brzmienie:

„Przetwarzanie danych osobowych, telekomunikacyjnych, pocztowych i internetowych”;

3) po art. 175a dodaje się art. 175b w brzmieniu:

„Art. 175b § 1. Prezesi sądów okręgowych właściwych dla siedziby organu wnioskującego o udostępnienie danych, przekazują corocznie Ministrowi Sprawiedliwości informację na temat przetwarzania danych telekomunikacyjnych, pocztowych i internetowych, z podziałem na liczbę przypadków udostępnienia danych dla danego rodzaju danych oraz wyników przeprowadzonych kontroli, w terminie do dnia 31 marca roku następującego po roku nią objętym.

§ 2. Minister Sprawiedliwości przedstawia corocznie Sejmowi i Senatowi zagregowaną informację na temat przetwarzania danych telekomunikacyjnych, pocztowych i internetowych oraz wyników przeprowadzonych kontroli, w terminie do dnia 30 czerwca roku następującego po roku nią objętym.”.

Art. 6. W ustawie z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. z 2013 r. poz. 568 i 628 oraz z 2014 r. poz. 1055) wprowadza się następujące zmiany:

1) art. 30 otrzymuje brzmienie:

„Art. 30. 1. W celu rozpoznawania, zapobiegania, zwalczania, wykrywania przestępstw, w tym przestępstw skarbowych albo uzyskania i utrwalenia dowodów przestępstw popełnionych przez osoby, o których mowa w art. 3 ust. 2 pkt 1, 3, 4, 5 i 6 albo w celu ratowania życia lub zdrowia ludzkiego bądź do wsparcia działań poszukiwawczych i ratowniczych Żandarmeria Wojskowa może uzyskiwać dane:

1) określone 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) określone w art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. poz. 1529, z późn. zm.), zwane dalej „danymi pocztowymi”;
3) określone w art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422, z późn. zm.), zwane dalej „danymi internetowymi”,

– oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.

2. Przedsiębiorca telekomunikacyjny, operator pocztowy lub usługodawca świadczący usługi drogą elektroniczną udostępnia nieodpłatnie dane, o których mowa w ust. 1:

1) żołnierzowi Żandarmerii Wojskowej wskazanemu w pisemnym wniosku Komendanta Głównego Żandarmerii Wojskowej lub komendanta oddziału Żandarmerii Wojskowej albo osoby przez nich upoważnionej;
2) na ustne żądanie żołnierza Żandarmerii Wojskowej posiadającego pisemne upoważnienie osób, o których mowa w pkt 1;
3) za pośrednictwem sieci telekomunikacyjnej żołnierzowi Żandarmerii Wojskowej posiadającemu pisemne upoważnienie osób, o których mowa w pkt 1;

3. W przypadku, o którym mowa w ust. 2 pkt 3, udostępnianie danych, o których mowa w ust. 1, odbywa się bez udziału pracowników przedsiębiorcy telekomunikacyjnego, operatora pocztowego lub usługodawcy świadczącego usługi drogą elektroniczną, lub przy ich niezbędnym współudziale, jeżeli możliwość taką przewiduje porozumienie zawarte pomiędzy Komendantem Głównym Żandarmerii Wojskowej a tym podmiotem.

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

1) wykorzystywane sieci i system teleinformatyczny zapewniają:
   a) możliwość ustalenia osoby uzyskującej dane, ich rodzaju oraz czasu, w którym zostały uzyskane,
   b) zabezpieczenie techniczne i organizacyjne uniemożliwiają osobie nieuprawnionej dostępu do danych;
2) jest to uzasadnione specyfiką lub zakresem zadań wykonywanych przez jednostki organizacyjne Żandarmerii Wojskowej albo prowadzonych przez nie czynności.

5. Komendant Główny Żandarmerii Wojskowej i komendant oddziału Żandarmerii Wojskowej prowadzą rejestr wystąpień o uzyskanie danych telekomunikacyjnych,

pocztowych i internetowych zawierający informacje identyfikujące jednostkę organizacyjną Żandarmerii Wojskowej i żołnierza Żandarmerii Wojskowej uzyskującego te dane, ich rodzaj, cel uzyskania oraz czas, w którym zostały uzyskane. Rejestr prowadzi się w formie elektronicznej, z zachowaniem przepisów o ochronie informacji niejawnych.

6. Dane, o których mowa w ust. 1, które mają znaczenie dla postępowania karnego Komendant Główny Żandarmerii Wojskowej lub komendant oddziału Żandarmerii Wojskowej przekazują prokuratorowi właściwemu miejscowo lub rzeczowo. Prokurator podejmuje decyzję o zakresie i sposobie wykorzystania przekazanych danych.

7. Dane, o których mowa w ust. 1, które nie mają znaczenia dla postępowania karnego, podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu.”;

2) po art. 30a dodaje się art. 30b–30c w brzmieniu:

„Art. 30b. 1. Kontrolę nad uzyskiwaniem przez Żandarmerię Wojskową danych telekomunikacyjnych, pocztowych lub internetowych sprawuje wojskowy sąd okręgowy właściwy dla siedziby organu Żandarmerii Wojskowej, któremu udostępniono te dane.

2. Organ Żandarmerii Wojskowej, o którym mowa w ust. 1, przekazuje, z zachowaniem przepisów o ochronie informacji niejawnych, sądowi okręgowemu, o którym mowa w ust. 1, w okresach półrocznych, sprawozdanie obejmujące:

1) liczbę przypadków pozyskania 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 do wsparcia działań poszukiwawczych i ratowniczych.

3. W ramach kontroli, o której mowa w ust. 1, wojskowy sąd okręgowy może zapoznać się z materiałami uzasadniającymi udostępnienie Żandarmerii Wojskowej danych telekomunikacyjnych, pocztowych lub internetowych.

4. Wojskowy sąd okręgowy informuje organ Żandarmerii Wojskowej o wyniku kontroli w terminie 30 dni od jej zakończenia.

5. Kontroli, o której mowa w ust. 1, nie podlega uzyskiwanie danych na podstawie art. 30c ust. 1.

Art. 30c. 1. W celu rozpoznawania, zapobiegania, zwalczania, wykrywania przestępstw, w tym przestępstw skarbowych albo uzyskania i utrwalenia dowodów

przestępstw popełnionych przez osoby, o których mowa w art. 3 ust. 2 pkt 1, 3, 4, 5 i 6 albo w celu ratowania życia lub zdrowia ludzkiego bądź do wsparcia działań poszukiwawczych i ratowniczych, Żandarmeria Wojskowa może uzyskiwać dane:

1) z wykazu, o którym mowa w art. 179 ust. 9 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;
2) o których mowa w art. 161 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne,
3) 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,
4) w przypadku stacjonarnej publicznej sieci telekomunikacyjnej – także nazwę miejscowości oraz ulicy, przy której znajduje się zakończenie sieci, udostępnione użytkownikowi

– oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.

2. Do udostępniania i przetwarzania danych, o których mowa w ust. 1, art. 30 ust. 2–7 stosuje się.”;

3) w art. 31:

a) ust. 1 otrzymuje brzmienie:

„1. Przy wykonywaniu czynności operacyjno–rozpoznawczych, podejmowanych przez Żandarmerię Wojskową w granicach zadań określonych w art. 4 ust. 1 oraz w stosunku do osób wskazanych w art. 3 ust. 2 pkt 1, 3, 5 i 6, w celu zapobieżenia, wykrycia, ustalenia sprawców oraz uzyskania i utrwalenia dowodów, umyślnych przestępstw ściganych z oskarżenia publicznego:

1) przeciwko pokojowi i ludzkości,
2) przeciwko Rzeczypospolitej Polskiej, z wyjątkiem przestępstw określonych w art. 127–132 Kodeksu karnego,
3) przeciwko życiu, określonych w art. 148–150 Kodeksu karnego,
4) określonych w art. 140, art. 156 § 1 i 3, art. 163 § 1 i 3, art. 164 § 1, art. 165 § 1 i 3, art. 166, art. 167, art. 171 § 1, art. 173 § 1 i 3, art. 189, art. 189a, art. 200, art. 200a, art. 202 § 3 i 4, art. 211a, art. 223, art. 228 § 1 i 3–5, art. 229 § 1 i 3–5, art. 230 § 1, art. 230a § 1, art. 231 §1 i 2, art. 232, art. 245, art. 246, art. 252 § 1–3, art. 258, art. 263 § 1 i 2, art. 265, art. 269, art. 280–

282, art. 285 § 1, art. 286 § 1 i 2, art. 299 § 1–6, art. 305, art. 310 § 1, 2 i 4, art. 339 § 2, art. 345 § 2 i 3 oraz art. 358 § 2 Kodeksu karnego,

5) skarbowych, jeżeli wartość przedmiotu czynu lub uszczuplenie należności publicznoprawnej przekraczają pięćdziesięciokrotną wysokość najniższego wynagrodzenia za pracę określonego na podstawie odrębnych przepisów,

6) określonych w art. 8 ustawy z dnia 6 czerwca 1997 r. – Przepisy wprowadzające Kodeks karny (Dz. U. Nr 88, poz. 554, z późn. zm.),

7) określonych w art. 43–44 ustawy z dnia 1 lipca 2005 r. o pobieraniu, przechowywaniu i przeszczepianiu komórek, tkanek i narządów (Dz. U. z 2015 r. poz. 793),

8) określonych w art. 53 ust. 1, art. 55 ust. 1, art. 56 ust. 1, art. 58 ust. 1, art. 59 ust. 1 oraz art. 62 ust. 1 ustawy z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii (Dz. U. z 2012 r. poz. 124 oraz z 2015 r. poz. 28),

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

– gdy inne środki okazały się bezskuteczne albo będą nieprzydatne, wojskowy sąd okręgowy, na pisemny wniosek Komendanta Głównego Żandarmerii Wojskowej, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, lub na pisemny wniosek komendanta oddziału Żandarmerii Wojskowej, złożony po uzyskaniu zgody Komendanta Głównego Żandarmerii Wojskowej i pisemnej zgody właściwego wojskowego prokuratora okręgowego, może, w drodze postanowienia, zarządzić kontrolę operacyjną.”,

b) ust. 7 otrzymuje brzmienie:

„7. Kontrola operacyjna prowadzona jest niejawnie i polega 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.”,

c) po ust. 7 dodaje się ust. 7a w brzmieniu:

„7a. Kontroli operacyjnej nie stanowią czynności, o których mowa w ust. 7 pkt 4, polegające na uzyskiwaniu danych w trybie art. 30. Realizacja tych czynności nie wymaga zgody sądu.”,

d) ust. 10 otrzymuje brzmienie:

„10. 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, wojskowy sąd okręgowy właściwy miejscowo ze względu na siedzibę wnioskującego organu Żandarmerii Wojskowej, na pisemny wniosek Komendanta Głównego Żandarmerii Wojskowej lub komendanta oddziału Żandarmerii Wojskowej, złożony po uzyskaniu pisemnej zgody Komendanta Głównego Żandarmerii Wojskowej oraz właściwego prokuratora wojskowego, może, również po upływie okresów, o których mowa w ust. 9, wydawać kolejne postanowienie o przedłużeniu kontroli operacyjnej na następujące po sobie okresy, których łączna długość nie może przekraczać 12 miesięcy.”,

e) po ust. 10 dodaje się ust. 10a w brzmieniu:

„10a. Komendant Główny Żandarmerii Wojskowej może upoważnić swojego zastępcę do składania wniosków, o których mowa w ust. 1, ust. 4 pkt. 1, ust. 9 i ust. 10 lub do zarządzania kontroli operacyjnej w trybie ust. 4 pkt 1.”,

f) ust. 13 otrzymuje brzmienie:

„13. Przedsiębiorca telekomunikacyjny, operator pocztowy oraz usługodawca świadczący usługi drogą elektroniczną jest obowiązany do zapewnienia na własny koszt warunków technicznych i organizacyjnych umożliwiających prowadzenie przez Żandarmerię Wojskową kontroli operacyjnej.”,

g) po ust. 16e dodaje się ust. 16f–16j w brzmieniu:

„16f. W przypadku, gdy zachodzi przypuszczenie, że materiały, o których mowa w ust. 16 mogą zawierać informacje:

1) o których mowa w art. 178 Kodeksu postępowania karnego;

2) o których mowa w art. 178a i art. 180 § 3 Kodeksu postępowania karnego, z wyłączeniem informacji o przestępstwach, o których mowa w art. 240 § 1 Kodeksu karnego;

3) stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego

— Komendant Główny Żandarmerii Wojskowej lub komendant oddziału Żandarmerii Wojskowej przekazują prokuratorowi wojskowemu te materiały.

16g. W przypadku, o którym mowa w ust. 16f, prokurator wojskowy niezwłocznie po otrzymaniu materiałów, kieruje je do sądu, który zarządził kontrolę operacyjną albo wyraził na nią zgodę w trybie określonym w ust. 4, wraz z wnioskiem o:

1) stwierdzenie, które z przekazanych materiałów zawierają informacje, o których mowa w ust. 16f,
2) dopuszczenie do wykorzystania w postępowaniu karnym materiałów zawierających informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego nieobjęte zakazami, określonymi w art. 178, art. 178a i art. 180 § 3 Kodeksu postępowania karnego, z wyłączeniem informacji o przestępstwach, o których mowa w art. 240 § 1 Kodeksu karnego.

16h. Sąd, niezwłocznie po złożeniu wniosku przez prokuratora wojskowego, wydaje postanowienie o 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, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu , a także zarządza niezwłoczne zniszczenie materiałów, których wykorzystanie w postępowaniu karnym jest niedopuszczalne,.

16i. Na postanowienie sądu w przedmiocie 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, prokuratorowi wojskowemu przysługuje zażalenie. Do zażalenia stosuje się odpowiednio przepisy Kodeksu postępowania karnego.

16j. Organ Żandarmerii Wojskowej jest obowiązany do wykonania zarządzenia sądu, o którym mowa w ust. 16h oraz niezwłocznego, komisyjnego i protokolarnego zniszczenia materiałów, których wykorzystanie w postępowaniu

karnym jest niedopuszczalne. Organ Żandarmerii Wojskowej niezwłocznie informuje prokuratora, o którym mowa w ust. 16g o zniszczeniu tych materiałów.

h) po ust. 17 dodaje się ust. 17a w brzmieniu:

„17a. Wojskowy sąd okręgowy, Prokurator Generalny, wojskowy prokurator okręgowy i organ Żandarmerii Wojskowej prowadzą rejestry: postanowień, pisemnych zgód, wniosków i zarządzeń dotyczących kontroli operacyjnej oraz centralny rejestr kontroli operacyjnych. Rejestry prowadzi się w formie elektronicznej, z zachowaniem przepisów o ochronie informacji niejawnych.”

i) ust. 19 otrzymuje brzmienie:

„19. Na postanowienia sądu, o których mowa w:

1) ust. 1, 4, 9 i 10 - przysługuje zażalenie organowi Żandarmerii Wojskowej, który złożył wniosek o wydanie tego postanowienia;

2) ust. 4 i ust. 16c – przysługuje zażalenie właściwemu prokuratorowi, o którym mowa w ust. 1.

Do zażalenia stosuje się odpowiednio przepisy Kodeksu postępowania karnego.”.

Art. 7. W ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2015 r., poz. 1929[j)]) wprowadza się następujące zmiany:

1) w art. 19 ust. 2 otrzymuje brzmienie:

„2. Szefowie Agencji mogą upoważnić podległych funkcjonariuszy do załatwiania spraw w ich imieniu w określonym zakresie, z wyjątkiem spraw, o których mowa w art. 29-31, a także art. 27 z wyłączeniem upoważnienia dla zastępcy Szefa ABW, w zakresie określonym w art. 27 ust. 9a.”;

2) w art. 27:

a) ust. 1 otrzymuje brzmienie:

„1. Sąd, na pisemny wniosek Szefa ABW, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, może, w drodze postanowienia, zarządzić kontrolę operacyjną — gdy inne środki okazały się bezskuteczne albo będą nieprzydatne — przy wykonywaniu czynności operacyjno-rozpoznawczych, podejmowanych przez ABW w celu rozpoznawania, zapobiegania i wykrywania przestępstw, o których mowa w:

1) art. 5 ust. 1 pkt 2 lit. a, c, d, e;

2) rozdz. 35-37 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. Nr 88, poz. 553, z późn. zm.) oraz rozdz. 6 i 7 ustawy z dnia 10 września 1999 r. – Kodeks karny skarbowy (Dz. U. z 2013 r. poz. 186, z późn. zm.) — jeżeli godzą w podstawy ekonomiczne państwa

— oraz w celu uzyskania i utrwalenia dowodów tych przestępstw i ścigania ich sprawców.

b) ust. 6 otrzymuje brzmienie:

„6. Kontrola operacyjna prowadzona jest niejawnie i polega 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.”,

c) po ust. 6 dodaje się ust. 6a w brzmieniu:

„6a. Kontroli operacyjnej nie stanowią czynności, o których mowa w ust. 6 pkt 4, polegające na uzyskiwaniu danych w trybie art. 28. Realizacja tych czynności nie wymaga zgody sądu.”,

d) ust. 9 otrzymuje brzmienie:

„9. W uzasadnionych przypadkach, gdy podczas stosowania kontroli operacyjnej pojawią się nowe okoliczności istotne dla zapobieżenia lub wykrycia przestępstwa albo ustalenia sprawcy i uzyskania dowodów przestępstwa, sąd, o którym mowa w ust. 2, na pisemny wniosek Szefa ABW, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, może wydawać, również po upływie okresów, o których mowa w ust. 8, kolejne postanowienie o przedłużeniu kontroli operacyjnej na następujące po sobie okresy, z których żaden nie może trwać dłużej niż 12 miesięcy.”,

e) po ust. 9 dodaje się ust. 9a w brzmieniu:

9a. Szef ABW może upoważnić swojego zastępcę do składania wniosków, o których mowa w ust. 1, 3, 8 i 9 lub do zarządzania kontroli operacyjnej w trybie ust. 3.”,

f) ust. 11a otrzymuje brzmienie:

„11a. Na postanowienia Sądu, o których mowa w:

1) ust. 1, 3, 8 i 9 - przysługuje zażalenie Szefowi ABW;

2) ust. 3 i ust. 15c – przysługuje zażalenie Prokuratorowi Generalnemu.

Do zażalenia stosuje się odpowiednio przepisy Kodeksu postępowania karnego.”

g) ust. 12 otrzymuje brzmienie:

„12. Przedsiębiorca telekomunikacyjny, operator pocztowy oraz usługodawca świadczący usługi drogą elektroniczną jest obowiązany do zapewnienia na własny koszt warunków technicznych i organizacyjnych umożliwiających prowadzenie przez ABW kontroli operacyjnej.”,

h) po ust. 15g dodaje się ust. 15h–15l w brzmieniu:

„15h. W przypadku, gdy zachodzi przypuszczenie, że materiały, o których mowa w ust. 15, mogą zawierać informacje:

1) o których mowa w art. 178 Kodeksu postępowania karnego;

2) o których mowa w art. 178a i art. 180 § 3 Kodeksu postępowania karnego, z wyłączeniem informacji o przestępstwach, o których mowa w art. 240 § 1 Kodeksu karnego;

3) stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego

— Szef ABW przekazuje Prokuratorowi Generalnemu te materiały.

15i. W przypadku, o którym mowa w ust. 15h, Prokurator Generalny 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) stwierdzenie, które z przekazanych materiałów zawierają informacje, o których mowa w ust. 15h,

2) dopuszczenie do wykorzystania w postępowaniu karnym materiałów zawierających informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania

karnego nieobjęte zakazami, określonymi w art. 178, art. 178a i art. 180 § 3 Kodeksu postępowania karnego, z wyłączeniem informacji o przestępstwach, o których mowa w art. 240 § 1 Kodeksu karnego.

15j. Sąd, niezwłocznie po złożeniu wniosku przez Prokuratora Generalnego, wydaje postanowienie o 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, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu , a także zarządza niezwłoczne zniszczenie materiałów, których wykorzystanie w postępowaniu karnym jest niedopuszczalne.

15k. Na postanowienie sądu w przedmiocie 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, Prokuratorowi Generalnemu przysługuje zażalenie. Do zażalenia stosuje się odpowiednio przepisy Kodeksu postępowania karnego.

15l. Szef ABW jest obowiązany do wykonania zarządzenia sądu, o którym mowa w ust. 15j oraz niezwłocznego, komisyjnego i protokolarnego zniszczenia materiałów, których wykorzystanie w postępowaniu karnym jest niedopuszczalne. Szef ABW niezwłocznie informuje Prokuratora Generalnego o zniszczeniu tych materiałów.”,

i) po ust. 16a dodaje się ust. 16b–16d w brzmieniu:

„16b. Sąd, Prokurator Generalny oraz Szef ABW prowadzą rejestry: postanowień, zarządzeń i wniosków dotyczących kontroli operacyjnej.

16c. Szef ABW prowadzi odrębne rejestry wniosków do Sądu o zezwolenie na zachowanie materiałów zgromadzonych podczas stosowania kontroli operacyjnej istotnych dla bezpieczeństwa państwa, zarządzeń o zniszczeniu materiałów zgromadzonych podczas stosowania kontroli operacyjnej oraz zawiadomień Prokuratora Generalnego o wydaniu przez Szefa ABW i wykonaniu zarządzenia o zniszczeniu materiałów z kontroli operacyjnej.

16d. Rejestry, o których mowa w ust. 16b i 16c, prowadzi się w formie elektronicznej, z zachowaniem przepisów o ochronie informacji niejawnych.”;

3) w art. 28:

a) ust. 1 otrzymuje brzmienie:

„1. ABW może uzyskiwać niezbędne do realizacji zadań, o których mowa w art. 5 ust. 1, dane:

1) określone 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) określone w art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. poz. 1529, z późn. zm.), zwane dalej „danymi pocztowymi”,

3) określone w art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422, z późn. zm.), zwane dalej „danymi internetowymi”,

b) w ust. 2 wprowadzenie do wyliczenia otrzymuje brzmienie:

„Przedsiębiorca telekomunikacyjny, operator pocztowy lub usługodawca świadczący usługi drogą elektroniczną udostępnia nieodpłatnie dane, o których mowa w ust. 1, odpowiednio:”,

c) ust. 3 otrzymuje brzmienie:

„3. W przypadku, o którym mowa w ust. 2 pkt 3, udostępnianie danych, o których mowa w ust. 1, odbywa się bez udziału pracowników przedsiębiorcy telekomunikacyjnego, operatora pocztowego lub usługodawcy świadczącego usługi drogą elektroniczną, lub przy ich niezbędnym współudziale, jeżeli możliwość taką przewiduje porozumienie zawarte pomiędzy Szefem ABW a tym podmiotem.”,

d) dodaje się ust. 5–7 w brzmieniu:

„5. Szef ABW prowadzi rejestr wystąpień o uzyskanie danych telekomunikacyjnych, pocztowych i internetowych zawierający informacje identyfikujące jednostkę organizacyjną ABW i funkcjonariusza ABW uzyskującego te dane, ich rodzaj, cel uzyskania oraz czas, w którym zostały uzyskane. Rejestr prowadzi się w formie elektronicznej, z zachowaniem przepisów o ochronie informacji niejawnych.

6. Dane, o których mowa w ust. 1, które mają znaczenie dla postępowania karnego Szef ABW przekazuje Prokuratorowi Generalnemu. Prokurator Generalny podejmuje decyzję o zakresie i sposobie wykorzystania przekazanych danych.

7. Dane, o których mowa w ust. 1,, które nie mają znaczenia dla postępowania karnego albo nie są istotne dla bezpieczeństwa państwa, podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu.”;

4) po art. 28 dodaje się art. 28a–28b w brzmieniu:

„Art. 28a. 1. Kontrolę nad uzyskiwaniem przez ABW danych telekomunikacyjnych, pocztowych lub internetowych sprawuje Sąd Okręgowy w Warszawie.

2. Szef ABW przekazuje, z zachowaniem przepisów o ochronie informacji niejawnych, sądowi, o którym mowa w ust. 1, 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.

3. W ramach kontroli, o której mowa w ust. 1, sąd może zapoznać się z materiałami uzasadniającymi udostępnienie ABW danych telekomunikacyjnych, pocztowych lub internetowych.

4. Sąd, o którym mowa w ust. 1, informuje Szefa ABW o wyniku kontroli w terminie 30 dni od jej zakończenia.

5. Kontroli, o której mowa w ust. 1, nie podlega uzyskiwanie danych na podstawie art. 28d ust. 1.

Art. 28d. 1. W celu realizacji zadań, o których mowa w art. 5 ust. 1, ABW może uzyskiwać dane:

1) z wykazu, o którym mowa w art. 179 ust. 9 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne
2) o których mowa w art. 161 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne,
3) 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,
4) w przypadku stacjonarnej publicznej sieci telekomunikacyjnej – także nazwę miejscowości oraz ulicy, przy której znajduje się zakończenie sieci, udostępnione użytkownikowi

– oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.

2. Do udostępniania i przetwarzania danych, o których mowa w ust. 1, art. 28 ust. 2–7 stosuje się.”.

Art. 8. W ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422) w art. 18 ust. 6 otrzymuje brzmienie:

„6. Usługodawca nieodpłatnie udostępnia dane, o których mowa w ust. 1-5, organom państwa uprawnionym na podstawie odrębnych przepisów na potrzeby prowadzonych przez nie postępowań.”.

Art. 9. W ustawie z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243, 827 i 1198) uchyla się art. 180g.

Art. 10. W ustawie z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. z 2014 r. poz. 253, 502 i 1055) wprowadza się następujące zmiany:

1) w art. 20 ust. 2 otrzymuje brzmienie:

„2. Szefowie SKW i SWW mogą upoważnić podległych żołnierzy zawodowych lub funkcjonariuszy do załatwiania spraw w ich imieniu w określonym zakresie, z zastrzeżeniem, że upoważnienie Szefa SKW nie może obejmować spraw, o których mowa w art. 29 ust. 3, art. 33 ust. 1 i art. 34 ust. 1, a także art. 31 z wyłączeniem upoważnienia zastępcy Szefa SKW w zakresie określonym w art. 31 ust. 7a.”;

2) w art. 31:

a) ust. 1 otrzymuje brzmienie:

„1. Przy wykonywaniu czynności operacyjno–rozpoznawczych, podejmowanych przez SKW w celu realizacji zadań określonych w art. 5 ust. 1 pkt 1, 5, 7 i 8 oraz ust. 2, gdy inne środki okazały się bezskuteczne albo będą nieprzydatne, sąd, na pisemny wniosek Szefa SKW, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, może, w drodze postanowienia, zarządzić kontrolę operacyjną.”,

b) ust. 4 otrzymuje brzmienie:

„4. Kontrola operacyjna prowadzona jest niejawnie i polega 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.”,

c) po ust. 4 dodaje się ust. 4a w brzmieniu:

„4a. Kontroli operacyjnej nie stanowią czynności, o których mowa w ust. 4 pkt 4, polegające na uzyskiwaniu danych w trybie art. 32. Realizacja tych czynności nie wymaga zgody sądu.”,

d) ust. 7 otrzymuje brzmienie:

„7. W uzasadnionych przypadkach, gdy podczas stosowania kontroli operacyjnej pojawią się nowe okoliczności istotne dla zapobieżenia lub wykrycia przestępstwa albo ustalenia sprawcy i uzyskania dowodów przestępstwa, sąd, o którym mowa w ust. 2, na pisemny wniosek Szefa SKW, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, może wydawać, również po upływie okresów, o których mowa w ust. 6, kolejne postanowienie o przedłużeniu kontroli operacyjnej na następujące po sobie okresy, z których żaden nie może trwać dłużej niż 12 miesięcy.”,

e) po ust. 7 dodaje się ust. 7a w brzmieniu:

„7a. Szef SKW może upoważnić swojego zastępcę do składania wniosków, o których mowa w ust. 1, 3, 6 i 7 lub do zarządzania kontroli operacyjnej w trybie ust. 3.”,

f) ust. 11 otrzymuje brzmienie:

„11. Przedsiębiorca telekomunikacyjny, operator pocztowy oraz usługodawca świadczący usługi drogą elektroniczną jest obowiązany do zapewnienia na własny koszt warunków technicznych i organizacyjnych umożliwiających prowadzenie przez SKW kontroli operacyjnej.”,

g) po ust. 14e dodaje się ust. 14f–14j w brzmieniu:

„14f. W przypadku, gdy zachodzi przypuszczenie, że materiały, o których mowa w ust. 14 mogą zawierać informacje:

1) o których mowa w art. 178 Kodeksu postępowania karnego;
2) o których mowa w art. 178a i art. 180 § 3 Kodeksu postępowania karnego, z wyłączeniem informacji o przestępstwach, o których mowa w art. 240 § 1 Kodeksu karnego;
3) stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego

— Szef SKW przekazuje Prokuratorowi Generalnemu te materiały.

14g. W przypadku, o którym mowa w ust. 14f, Prokurator Generalny 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) stwierdzenie, które z przekazanych materiałów zawierają informacje, o których mowa w ust. 14f,
2) dopuszczenie do wykorzystania w postępowaniu karnym materiałów zawierających informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego nieobjęte zakazami, określonymi w art. 178, art. 178a i art. 180 § 3 Kodeksu postępowania karnego, z wyłączeniem informacji o przestępstwach, o których mowa w art. 240 § 1 Kodeksu karnego.

14h. Sąd, niezwłocznie po złożenia wniosku przez Prokuratora Generalnego, wydaje postanowienie o 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, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu , a także zarządza niezwłoczne zniszczenie materiałów, których wykorzystanie w postępowaniu karnym jest niedopuszczalne.

14i. Na postanowienie sądu w przedmiocie 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, Prokuratorowi Generalnemu przysługuje zażalenie. Do zażalenia stosuje się odpowiednio przepisy Kodeksu postępowania karnego.

14j. Szef SKW jest obowiązany do wykonania zarządzenia sądu, o którym mowa w ust. 14h oraz niezwłocznego, komisyjnego i protokolarnego zniszczenia materiałów, których wykorzystanie w postępowaniu karnym jest niedopuszczalne. Szef SKW niezwłocznie informuje Prokuratora Generalnego o zniszczeniu tych materiałów.”,

h) po ust. 15a dodaje się ust. 15b w brzmieniu:

„15b. Sąd, Prokurator Generalny i Szef SKW prowadzą rejestry wniosków, zarządzeń, zgód i postanowień dotyczących kontroli operacyjnej. Rejestry prowadzi się w formie elektronicznej, z zachowaniem przepisów o ochronie informacji niejawnych.”

i) ust. 10 otrzymuje brzmienie:

„11a. Na postanowienia sądu, o których mowa w:

1) ust. 1, 3, 6 i 7 - przysługuje zażalenie Szefowi SKW;

2) ust. 3 i ust. 14c – przysługuje zażalenie Prokuratorowi Generalnemu.

Do zażalenia stosuje się odpowiednio przepisy Kodeksu postępowania karnego.”;

3) w art. 32:

a) ust. 1 otrzymuje brzmienie:

„1. SKW może uzyskiwać niezbędne do realizacji zadań, o których mowa w art. 5 dane:

1) określone 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) określone w art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. poz. 1529, z późn. zm.), zwane dalej „danymi pocztowymi”.

3) określone w art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422, z późn. zm.), zwane dalej „danymi internetowymi”

— oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.”

b) w ust. 2 wprowadzenie do wyliczenia otrzymuje brzmienie:

„Przedsiębiorca telekomunikacyjny, operator pocztowy lub usługodawca świadczący usługi drogą elektroniczną udostępnia nieodpłatnie dane, o których mowa w ust. 1:”

c) ust. 3-5 otrzymują brzmienie:

„3. O udostępnieniu danych w trybie określonym w ust. 2 pkt 2 przedsiębiorca telekomunikacyjny, operator pocztowy lub usługodawca świadczący usługi drogą elektroniczną informuje niezwłocznie Szefa SKW.

4. Przedsiębiorca telekomunikacyjny, operator pocztowy oraz usługodawca świadczący usługi drogą elektroniczną są obowiązani udostępnić dane, o których mowa w ust. 1, funkcjonariuszom wskazanym we wniosku.

5. W przypadku, o którym mowa w ust. 2 pkt 3, udostępnianie danych, o których mowa w ust. 1, odbywa się bez udziału pracowników przedsiębiorcy telekomunikacyjnego, operatora pocztowego lub usługodawcy świadczącego usługi drogą elektroniczną przy niezbędnym ich współudziale, jeżeli możliwość taką przewiduje porozumienie zawarte pomiędzy Szefem SKW a tym podmiotem.”,

d) w ust. 6 wprowadzenie do wyliczenia otrzymuje brzmienie:

„Udostępnienie SKW danych telekomunikacyjnych, pocztowych lub internetowych może nastąpić za pośrednictwem sieci telekomunikacyjnej, jeżeli:”,

e) dodaje się ust. 7–9 w brzmieniu:

„7. Szef SKW prowadzi rejestr wystąpień o uzyskanie danych telekomunikacyjnych, pocztowych i internetowych zawierający informacje identyfikujące jednostkę organizacyjną SKW i funkcjonariusza SKW uzyskującego te dane, ich rodzaj, cel uzyskania oraz czas, w którym zostały uzyskane. Rejestr prowadzi się w formie elektronicznej, z zachowaniem przepisów o ochronie informacji niejawnych.

8. Dane, o których mowa w ust. 1, które mają znaczenie dla postępowania karnego Szef SKW przekazuje Prokuratorowi Generalnemu. Prokurator Generalny podejmuje decyzję o zakresie i sposobie wykorzystania przekazanych danych.

9. Dane, o których mowa w ust. 1, które nie mają znaczenia dla postępowania karnego albo nie są istotne dla obronności Państwa, podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu.”

4) po art. 32 dodaje się art. 32a–32b w brzmieniu:

Art. 32a. 1. Kontrolę nad uzyskiwaniem przez SKW danych telekomunikacyjnych, pocztowych lub internetowych sprawuje Wojskowy Sąd Okręgowy w Warszawie.

2. Szef SKW przekazuje, z zachowaniem przepisów o ochronie informacji niejawnych, sądowi, o którym mowa w ust. 1, 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.

3. W ramach kontroli, o której mowa w ust. 1, sąd może zapoznać się z materiałami uzasadniającymi udostępnienie SKW danych telekomunikacyjnych, pocztowych lub internetowych.

4. Sąd o którym mowa w ust. 1, informuje Szefa SKW o wyniku kontroli w terminie 30 dni od jej zakończenia.

5. Kontroli, o której mowa w ust. 1, nie podlega uzyskiwanie danych na podstawie art. 32b ust. 1.

Art. 32b. 1. W celu realizacji zadań, o których mowa w art. 5, SKW może uzyskiwać dane:

1) z wykazu, o którym mowa w art. 179 ust. 9 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;
2) o których mowa w art. 161 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne,
3) 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,
4) w przypadku stacjonarnej publicznej sieci telekomunikacyjnej – także nazwę miejscowości oraz ulicy, przy której znajduje się zakończenie sieci, udostępnione użytkownikowi

– oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.

2. Do udostępniania i przetwarzania danych, o których mowa w ust. 1, art. 32 ust. 2–9 stosuje się.”.

Art. 11. W ustawie z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. z 2014 r. poz. 1411 i 1822) wprowadza się następujące zmiany:

1) w art. 10 ust. 2 otrzymuje brzmienie:

„2. Szef CBA może upoważnić podległych funkcjonariuszy do załatwiania spraw w jego imieniu w określonym zakresie, z wyjątkiem spraw, o których mowa w art. 19 i 23, a także art. 17 z wyłączeniem upoważnienia dla zastępcy Szefa CBA, w zakresie określonym w art. 17 ust. 9a.”;

2) w art. 17:

a) w ust. 1 pkt 1 otrzymuje brzmienie:

„1) określonych w art. 228-231, 250a, 258, 286, 296-297, 299, 305, 310 § 1, 2 i 4 ustawy z dnia 6 czerwca 1997 r. - Kodeks karny,”,

b) ust. 5 otrzymuje brzmienie:

„5. Kontrola operacyjna prowadzona jest niejawnie i polega 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.”,

c) po ust. 5 dodaje się ust. 5a w brzmieniu:

„5a. Kontroli operacyjnej nie stanowią czynności, o których mowa w ust. 5 pkt 4, polegające na uzyskiwaniu danych w trybie art. 18. Realizacja tych czynności nie wymaga zgody sądu.”,

d) ust. 9 otrzymuje brzmienie:

„9. W uzasadnionych przypadkach, gdy podczas stosowania kontroli operacyjnej pojawią się nowe okoliczności istotne dla zapobieżenia lub wykrycia przestępstwa albo ustalenia sprawcy i uzyskania dowodów przestępstwa, sąd, o którym mowa w ust. 2, na pisemny wniosek Szefa CBA, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, może wydawać, również po upływie

okresów, o których mowa w ust. 8, kolejne postanowienie o przedłużeniu kontroli operacyjnej na następujące po sobie okresy, których łączna długość nie może przekraczać 12 miesięcy.”,

e) po ust. 9 dodaje się ust. 9a w brzmieniu:

„9a. Szef CBA może upoważnić swojego zastępcę do składania wniosków, o których mowa w ust. 1, 3, 8 i 9 lub do zarządzania kontroli operacyjnej w trybie ust. 3.”,

f) ust. 12 otrzymuje brzmienie:

„12. Przedsiębiorca telekomunikacyjny, operator pocztowy oraz usługodawca świadczący usługi drogą elektroniczną jest obowiązany do zapewnienia na własny koszt warunków technicznych i organizacyjnych umożliwiających prowadzenie przez CBA kontroli operacyjnej.”,

g) po ust. 15e dodaje się ust. 15f–15j w brzmieniu:

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

1) o których mowa w art. 178 Kodeksu postępowania karnego;

2) o których mowa w art. 178a i art. 180 § 3 Kodeksu postępowania karnego, z wyłączeniem informacji o przestępstwach, o których mowa w art. 240 § 1 Kodeksu karnego;

3) stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego

— Szef CBA przekazuje Prokuratorowi Generalnemu te materiały.

15g. W przypadku, o którym mowa w ust. 15f, Prokurator Generalny 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) stwierdzenie, które z przekazanych materiałów zawierają informacje, o których mowa w ust. 15f,

2) dopuszczenie do wykorzystania w postępowaniu karnym materiałów zawierających informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego nieobjęte zakazami, określonymi w art. 178, art. 178a i art. 180 § 3

Kodeksu postępowania karnego, z wyłączeniem informacji o przestępstwach, o których mowa w art. 240 § 1 Kodeksu karnego.

15h. Sąd, niezwłocznie po złożeniu wniosku przez Prokuratora Generalnego, wydaje postanowienie o 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, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu , a także zarządza niezwłoczne zniszczenie materiałów, których wykorzystanie w postępowaniu karnym jest niedopuszczalne.

15i. Na postanowienie sądu w przedmiocie 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, Prokuratorowi Generalnemu przysługuje zażalenie. Do zażalenia stosuje się odpowiednio przepisy Kodeksu postępowania karnego.

15j. Szef CBA jest obowiązany do wykonania zarządzenia sądu, o którym mowa w ust. 15h oraz niezwłocznego, komisyjnego i protokolarnego zniszczenia materiałów, których wykorzystanie w postępowaniu karnym jest niedopuszczalne. Szef CBA niezwłocznie informuje Prokuratora Generalnego o zniszczeniu tych materiałów.”,

h) ust. 17 otrzymuje brzmienie:

„17. Na postanowienia sądu, o których mowa w:

1) ust. 1, 3, 8 i 9 - przysługuje zażalenie Szefowi CBA;

2) ust. 3 i ust. 15c – przysługuje zażalenie Prokuratorowi Generalnemu.

Do zażalenia stosuje się odpowiednio przepisy Kodeksu postępowania karnego.”,

i) po ust. 17 dodaje się ust. 17a w brzmieniu:

„17a. Sąd, Prokurator Generalny i Szef CBA prowadzą rejestry, odpowiednio: postanowień, zarządzeń i wniosków dotyczących kontroli operacyjnej. Rejestry prowadzi się w formie elektronicznej, z zachowaniem przepisów o ochronie informacji niejawnych.”;

3) w art. 18:

a) ust. 1 otrzymuje brzmienie:

„1. CBA może uzyskiwać niezbędne do realizacji zadań, o których mowa w art. 2, dane:

1) określone 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) określone w art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. poz. 1529, z późn. zm.), zwane dalej „danymi pocztowymi”,

3) określone w art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422, z późn. zm.), zwane dalej „danymi internetowymi”

— oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.”,

b) w ust. 2 wprowadzenie do wyliczenia otrzymuje brzmienie:

„Przedsiębiorca telekomunikacyjny, operator pocztowy lub usługodawca świadczący usługi drogą elektroniczną udostępnia nieodpłatnie dane, o których mowa w ust. 1:”

c) ust. 3 otrzymuje brzmienie:

„3. W przypadku, o którym mowa w ust. 2 pkt 3, udostępnianie danych, o których mowa w ust. 1, odbywa się bez udziału pracowników przedsiębiorcy telekomunikacyjnego, operatora pocztowego lub usługodawcy świadczącego usługi drogą elektroniczną lub przy niezbędnym ich współudziale, jeżeli możliwość taką przewiduje porozumienie zawarte pomiędzy Szefem CBA a tym podmiotem.”,

d) dodaje się ust. 5–7 w brzmieniu:

„5. Szef CBA prowadzi rejestr wystąpień o uzyskanie danych telekomunikacyjnych, pocztowych i internetowych zawierający informacje identyfikujące jednostkę organizacyjną CBA i funkcjonariusza CBA uzyskującego te dane, ich rodzaj, cel uzyskania oraz czas, w którym zostały uzyskane. Rejestr prowadzi się w formie elektronicznej, z zachowaniem przepisów o ochronie informacji niejawnych.

6. Dane, o których mowa w ust. 1, które mają znaczenie dla postępowania karnego Szef CBA przekazuje Prokuratorowi Generalnemu. Prokurator Generalny podejmuje decyzję o zakresie i sposobie wykorzystania przekazanych danych.

7. Dane, o których mowa w ust. 1, które nie mają znaczenia dla postępowania karnego, podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu.”;

4) po art. 18 dodaje się art. 18a–18b w brzmieniu:

Art. 18a. 1. Kontrolę nad uzyskiwaniem przez CBA danych telekomunikacyjnych, pocztowych lub internetowych sprawuje Sąd Okręgowy w Warszawie.

2. Szef CBA przekazuje, z zachowaniem przepisów o ochronie informacji niejawnych, sądowi, o którym mowa w ust. 1, 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.

3. W ramach kontroli, o której mowa w ust. 1, sąd może zapoznać się z materiałami uzasadniającymi udostępnienie CBA danych telekomunikacyjnych, pocztowych lub internetowych.

4. Sąd, o którym mowa w ust. 1, informuje Szefa CBA o wyniku kontroli w terminie 30 dni od jej zakończenia.

5. Kontroli, o której mowa w ust. 1, nie podlega uzyskiwanie danych na podstawie art. 18b ust. 1.

Art. 18b. 1. W celu realizacji zadań, o których mowa w art. 2, CBA może uzyskiwać dane:

1) z wykazu, o którym mowa w art. 179 ust. 9 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;
2) o których mowa w art. 161 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne,
3) 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,

4) w przypadku stacjonarnej publicznej sieci telekomunikacyjnej – także nazwę miejscowości oraz ulicy, przy której znajduje się zakończenie sieci, udostępnione użytkownikowi

– oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.

2. Do udostępniania i przetwarzania danych, o których mowa w ust. 1, art. 18 ust. 2–7 stosuje się.”.

Art. 12. W ustawie z dnia 27 sierpnia 2009 r. o Służbie Celnej (Dz. U. z 2013 r. poz. 1404, z późn. zm.[4)]) wprowadza się następujące zmiany:

1) w art. 75d:

a) ust. 1 otrzymuje brzmienie:

„1. W celu rozpoznawania, zapobiegania, zwalczania, wykrywania albo uzyskania i utrwalenia dowodów przestępstw skarbowych, o których mowa w rozdziale 9 Kodeksu karnego skarbowego, Służba Celna może uzyskiwać dane:

1) określone 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) określone w art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422, z późn. zm.), zwane dalej „danymi internetowymi”,

— oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.”,

b) w ust. 2 wprowadzenie do wyliczenia otrzymuje brzmienie:

„Przedsiębiorca telekomunikacyjny lub usługodawca świadczący usługi drogą elektroniczną udostępnia nieodpłatnie dane telekomunikacyjne lub internetowe:”,

c) ust. 3 otrzymuje brzmienie:

„3. W przypadku, o którym mowa w ust. 2 pkt 3, udostępnianie danych telekomunikacyjnych lub internetowych odbywa się bez udziału pracowników przedsiębiorcy telekomunikacyjnego lub usługodawcy świadczącego usługi drogą elektroniczną lub przy niezbędnym ich udziale, jeżeli możliwość taka jest przewidziana w porozumieniu zawartym między Szefem Służby Celnej a tym podmiotem.”,

d) w ust. 4 wprowadzenie do wyliczenia otrzymuje brzmienie”

---

4) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2014 r. 486, 1055, 1215, 1395 i 1662 oraz z 2015 r. poz. 211 i 671.

„Udostępnienie danych telekomunikacyjnych lub internetowych może nastąpić za pośrednictwem sieci telekomunikacyjnej, jeżeli:”,

e) ust. 5 otrzymuje brzmienie:

„5. Dane telekomunikacyjne lub internetowe, które mają znaczenie dla postępowania karnego lub postępowania karnego skarbowego, Szef Służby Celnej albo dyrektor izby celnej przekazuje prokuratorowi właściwemu ze względu na siedzibę organu przekazującego. Prokurator podejmuje decyzję o zakresie i sposobie wykorzystania przekazanych danych”,

f) dodaje się ust. 6–7 w brzmieniu:

„6. Dane telekomunikacyjne lub internetowe, które nie mają znaczenia dla postępowania karnego lub postępowania karnego skarbowego, podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu.

7. Szef Służby Celnej i dyrektor izby celnej prowadzi rejestr wystąpień o uzyskanie danych telekomunikacyjnych i internetowych zawierający informacje identyfikujące jednostkę organizacyjną Służby Celnej i funkcjonariusza uzyskującego te dane, ich rodzaj, cel uzyskania oraz czas, w którym zostały uzyskane. Rejestr prowadzi się w formie elektronicznej, z zachowaniem przepisów o ochronie informacji niejawnych.”;

2) po art. 75d dodaje się art. 75da–75db w brzmieniu:

Art. 75da. 1. Kontrolę nad uzyskiwaniem przez Służbę Celną danych telekomunikacyjnych i internetowych sprawuje sąd okręgowy właściwy dla siedziby organu Służby Celnej, któremu udostępniono te dane.

2. Organ Służby Celnej, o którym mowa w ust. 1, przekazuje, z zachowaniem przepisów o ochronie informacji niejawnych, sądowi okręgowemu, o którym mowa w ust. 1, w okresach półrocznych, sprawozdanie obejmujące:

1) liczbę przypadków pozyskania w okresie sprawozdawczym danych telekomunikacyjnych lub internetowych oraz rodzaj tych danych;

2) kwalifikacje prawne czynów w związku z zaistnieniem których wystąpiono o dane telekomunikacyjne lub internetowe.

3. W ramach kontroli, o której mowa w ust. 1, sąd okręgowy może zapoznać się z materiałami uzasadniającymi udostępnienie Służbie Celnej danych telekomunikacyjnych lub internetowych.

4. Sąd, o którym mowa w ust. 1, informuje Szefa Służby Celnej o wyniku kontroli w terminie 30 dni od jej zakończenia.

5. Kontroli, o której mowa w ust. 1, nie podlega uzyskiwanie danych na podstawie art. 75db ust. 1.

Art. 75db. 1. W celu rozpoznawania, zapobiegania, zwalczania, wykrywania albo uzyskania i utrwalenia dowodów przestępstw skarbowych, o których mowa w rozdziale 9 Kodeksu karnego skarbowego Służba Celna może uzyskiwać dane:

1) z wykazu, o którym mowa w art. 179 ust. 9 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne
2) o których mowa w art. 161 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne,
3) 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,
4) w przypadku stacjonarnej publicznej sieci telekomunikacyjnej – także nazwę miejscowości oraz ulicy, przy której znajduje się zakończenie sieci, udostępnione użytkownikowi

– oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.

2. Do udostępniania i przetwarzania danych, o których mowa w ust. 1, art. 75d ust. 2–7 stosuje się.”.

Art. 13. Do kontroli operacyjnej, która była prowadzona przed dniem wejścia w życie ustawy i nie została zakończona do tego czasu, stosuje się przepisy dotychczasowe.

Art. 14. 1. Jeżeli wniosek o zarządzenie kontroli operacyjnej, o której mowa w 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 i art. 31 ust. 10 ustawy z dnia z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych, w dotychczasowym brzmieniu, został złożony przed dniem wejścia w życie niniejszej ustawy, kontrola ta jest zarządzana w trybie określonym w tych przepisach, w brzmieniu nadanym niniejszą ustawą.

2. Po zakończeniu kontroli operacyjnej, o której mowa w art. 12, wskutek upływu terminu może zostać jednokrotnie zarządzona kontrola operacyjna na podstawie 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 i art. 31 ust. 10 ustawy z dnia z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych, w brzmieniu nadanym niniejszą ustawą.

Art. 15. Do postępowań w sprawie udostępniania danych, o których mowa w art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne oraz danych identyfikujących podmiot korzystający z usług pocztowych oraz dotyczących faktu, okoliczności świadczenia usług pocztowych lub korzystania z tych usług, wszczętych i niezakończonych przed dniem wejścia w życie niniejszej ustawy, oraz do zgromadzonych danych stosuje się przepisy dotychczasowe.

Art. 16. 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, niezakończonej do dnia wejścia w życie niniejszej ustawy, stosuje się przepisy dotychczasowe.

Art. 17. Ustawa wchodzi w życie z dniem 7 lutego 2016 r.

UZASADNIENIE

1. Cel projektowanej ustawy

Projektowana ustawa o zmianie ustawy o Policji oraz niektórych innych ustaw ma na celu dostosowanie systemu prawa do wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r. (sygn. akt K 23/11), stwierdzającego niezgodność wybranych przepisów: ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2015 r. poz. 355 , z późn. zm.), ustawy z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2014 r. poz. 1402, z późn. zm.), ustawy z dnia 28 września 1991 r. o kontroli skarbowej (Dz. U. z 2015 r. poz. 553, z późn. zm.), ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. z 2013 r. poz. 568, z późn. zm.), ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2015 r., poz. 1929), ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. z 2014 r. poz. 253, z późn. zm.), ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. z 2014 r. poz. 1411, z późn. zm.) oraz ustawy
z dnia 27 sierpnia 2009 r. o Służbie Celnej (Dz. U. z 2015 r. poz. 990, z późn. zm.), z Konstytucją Rzeczypospolitej Polskiej. Sentencja rozstrzygnięcia została ogłoszona dnia 6 sierpnia 2014 r. w Dz. U. poz. 1055.

2. Przedmiot i istota wypowiedzi Trybunału Konstytucyjnego.

Trybunał Konstytucyjny na wniosek Rzecznika Praw Obywatelskich oraz Prokuratora Generalnego zbadał konstytucyjność przepisów ustaw zawierających regulacje dotyczące kontroli operacyjnej, pozyskiwania danych telekomunikacyjnych, ochrony tajemnicy zawodowej w toku kontroli operacyjnej oraz niszczenia zbędnych danych telekomunikacyjnych w ustawach, o których mowa w pkt 1.

Zgodnie z sentencją orzeczenia:

1) art. 27 ust. 1 w związku z art. 5 ust. 1 pkt 2 lit. b ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, zwanej dalej „ustawą o ABW oraz AW" jest niezgodny z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji RP;

2) art. 20c ust. 1 ustawy o Policji, art. 10b ust. 1 ustawy o Straży Granicznej, zwanej dalej „ustawą o SG", art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej, art. 30 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, zwanej dalej „ustawą o ŻW", art. 28 ust. 1 pkt 1 ustawy o ABW oraz AW, art. 32 ust. 1 pkt 1 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, zwanej dalej „ustawą o SKW oraz SWW", art. 18 ust. 1 pkt 1 ustawy o Centralnym Biurze Antykorupcyjnym, zwanej dalej „ustawą o CBA", art. 75d ust. 1 ustawy o Służbie Celnej, zwanej dalej „ustawą o SC" – przez to, że nie przewidują niezależnej kontroli udostępniania danych telekomunikacyjnych, 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), są niezgodne z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji RP;

3) art. 19 ustawy o Policji, art. 9e ustawy o SG, art. 36c ustawy o kontroli skarbowej, art. 31 ustawy o ŻW, art. 27 ustawy o ABW oraz AW, art. 31 ustawy o SKW oraz SWW, art. 17 ustawy o CBA – w zakresie, w jakim nie przewidują gwarancji niezwłocznego, komisyjnego i protokolarnego zniszczenia materiałów zawierających informacje objęte zakazami dowodowymi, co do których sąd nie uchylił tajemnicy zawodowej bądź uchylenie było niedopuszczalne, są niezgodne z art. 42 ust. 2, art. 47, art. 49, art. 51 ust. 2 i art. 54 ust. 1 w związku z art. 31 ust. 3 Konstytucji RP;

4) art. 28 ustawy o ABW oraz AW, art. 32 ustawy o SKW oraz SWW, art. 18 ustawy o CBA – w zakresie, w jakim nie przewidują zniszczenia danych niemających znaczenia dla prowadzonego postępowania, są niezgodne z art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji RP;

5) art. 75d ust. 5 ustawy o SC w zakresie, w jakim zezwala na zachowanie materiałów innych, niż zawierające informacje mające znaczenie dla postępowania w sprawach wykroczeń skarbowych lub przestępstw skarbowych określonych w rozdziale 9 ustawy z dnia 10 września 1999 r. – Kodeks karny skarbowy (Dz. U. z 2013 r. poz. 186, z późn. zm.), jest niezgodny z art. 51 ust. 4 Konstytucji RP.

W dotychczasowym orzecznictwie Trybunał Konstytucyjny kilkukrotnie wypowiadał się w sprawie konstytucyjności przepisów regulujących czynności operacyjno-rozpoznawcze prowadzące do ingerencji w sferę prywatności jednostek i tajemnicę komunikowania się. Trybunał nie podważył dopuszczalności ich stosowania w demokratycznym państwie prawa. Przeciwnie, wyraźnie podkreślił, że niejawne pozyskiwanie przez organy władzy publicznej informacji o obywatelach, w toku kontroli operacyjnej ukierunkowanej na zapobieganie przestępstwom, ich wykrywanie oraz zwalczanie, jest nieodzowne. Jawność tych czynności powodowałaby bowiem ich nieskuteczność, a to z kolei rzutowałoby na poziom bezpieczeństwa państwa i jego obywateli. Ocena ta wynikała z dostrzeżenia specyfiki działalności przestępczej i coraz trudniejszych warunków zapewnienia bezpieczeństwa spowodowanych zagrożeniem terroryzmem, zorganizowaną przestępczością czy wykorzystywaniem przez przestępców nowych technologii w celu komunikowania się między sobą i popełniania rozmaitych przestępstw (np. komputerowych).

Trybunał Konstytucyjny generalnie aprobował powierzenie kompetencji w zakresie prowadzenia czynności operacyjno-rozpoznawczych nie tylko Policji, Agencji Bezpieczeństwa Wewnętrznego czy Centralnemu Biuru Antykorupcyjnemu, ale również organom kontroli skarbowej, które odpowiadają m.in. za zwalczanie negatywnych zjawisk w postaci niewywiązywania się z obowiązków daninowych wobec Państwa, prowadzenia nieujawnionej działalności gospodarczej, prania pieniędzy, niedozwolonego wykorzystywania powiązań kapitałowych między podmiotami.

Trybunał wielokrotnie wskazywał ustawodawcy warunki, jakie muszą spełniać normy prawne regulujące niejawne pozyskiwanie przez służby policyjne i służby ochrony państwa informacji na temat jednostek.

Zdaniem Trybunału, ograniczenia w korzystaniu z konstytucyjnych wolności i praw muszą być precyzyjne unormowanie w ustawie. Chodzi jednak nie tylko o formalne umiejscowienie przepisu ograniczającego w akcie normatywnym o randze co najmniej ustawy, ale również o „jakość" tego unormowania, które musi zapewniać przewidywalność rozstrzygnięć organów władzy publicznej wobec jednostek. Ustawowa forma ograniczeń prawa do ochrony prywatności (art. 47 Konstytucji RP), wolności i ochrony tajemnicy komunikowania się (art. 49 Konstytucji RP) oraz autonomii informacyjnej (art. 51 ust. 1 Konstytucji RP) wynika bezpośrednio z art. 31 ust. 3 Konstytucji RP, a zapewnienie dostatecznej określoności przepisów także z zasady demokratycznego państwa prawa (art. 2 Konstytucji RP).

Trybunał w uzasadnieniu do wyroku przywołał minimalne standardy ustawowej regulacji czynności operacyjno-rozpoznawczych (niejawnego pozyskiwania przez władze publiczne informacji o jednostkach).

Według Trybunału, po pierwsze, ustawa ma precyzować przedmiotowe przesłanki zarządzenia takich czynności. Aby zachować standard konstytucyjny, nie wystarcza odwołanie się do ogólnych zagrożeń dóbr prawnie chronionych, zwłaszcza przez zwroty niedookreślone. Ustawodawca zobowiązany jest zdefiniować zamknięty i możliwie wąski katalog poważnych przestępstw, uzasadniających tego rodzaju ingerencję w status jednostki. Nie jest wykluczone zastosowanie innych technik legislacyjnych (np. odwołanie się do konkretnych rozdziałów lub ustaw), jednakże w każdym wypadku powinno być możliwe zrekonstruowanie sytuacji, w których niejawne pozyskiwanie informacji przez organy państwa jest dopuszczalne. Precyzyjne ustawowe uregulowanie przedmiotowych przesłanek dopuszczalności kontroli operacyjnej i pozyskiwania danych telekomunikacyjnych, jest tym bardziej konieczne, ponieważ w istocie to same służby – działając w ramach ich ustawowych zadań – definiują zagrożenia, którym mają następnie zapobiegać.

Po drugie, niezbędne jest sprecyzowanie sposobu niejawnego wkroczenia w sferę prywatności jednostki. Nie jest przy tym konieczne wskazanie w przepisach prawa konkretnych środków techniki operacyjnej ani tym bardziej zdefiniowanych ich parametrów. Mając na uwadze zróżnicowane środki odpowiadające obecnym formom techniki i w efekcie m.in. możliwością komunikowania się, które stosowane są przez organy państwa w pracy operacyjno-rozpoznawczej, ustawowy ich katalog musiałby być rozbudowany, a co za tym idzie norma prawna musiałaby być kazuistyczna. Z punktu widzenia zasady określoności prawa istotne jest natomiast sprecyzowanie w przepisach prawa zamkniętego rodzajowo katalogu środków i metod działania, za pomocą których władze publiczne mogą w sposób niejawny gromadzić informacje o jednostkach. Raz jeszcze należy podkreślić, że nie chodzi o wskazanie parametrów technicznych, ale rodzajowych nazw poszczególnych środków i informacji możliwych do pozyskania za ich pomocą. Zamknięty katalog rodzajów środków technicznych służących do niejawnego pozyskiwania informacji i dowodów ogranicza arbitralność organów państwa. Ponadto umożliwia sprawowanie efektywnej kontroli nad

niejawną działalnością operacyjno-rozpoznawczą w zakresie wykorzystywanych metod pozyskiwania informacji o osobie.

Według Trybunału, najbardziej pożądanym rozwiązaniem z konstytucyjnego punktu widzenia jest uregulowanie rodzajów środków służących niejawnemu pozyskiwaniu informacji o jednostkach w ustawie. Precyzyjne określenie tej kwestii przez ustawodawcę nie tylko wiąże się z realizacją zasady określoności prawa wynikającą z art. 2 Konstytucji RP, ale przede wszystkim z tą częścią art. 31 ust. 3 Konstytucji RP, która przewiduje obowiązek unormowania ograniczeń w korzystaniu z wolności i praw konstytucyjnych w „ustawie", będącej aktem normatywnym pochodzącym od przedstawicielskiego organu Narodu – Sejmu (art. 4 w zw. z art. 104 ust. 1 Konstytucji RP).

Po trzecie, ustawa ma precyzować maksymalny czas prowadzenia niejawnych czynności, po upływie którego dalsze ich prowadzenie jest już niedopuszczalne. Termin ten ma określić ustawodawca tak, aby umożliwiał osiągnięcie konstytucyjnie uzasadnionego celu. Nie może być to jednak termin ani nadmiernie długi, ani zbyt krótki, który nie pozwala na efektywną pracę operacyjno-rozpoznawczą. Ustawodawca musi mieć także na uwadze, że w demokratycznym państwie prawa nie jest dopuszczalne – nawet za zgodą sądu i w sytuacji podejrzenia popełnienia nawet poważnych przestępstw – prowadzenie czynności operacyjno-rozpoznawczych bezterminowo, choćby miało się to wiązać z bezpowrotną utratą dowodów.

Po czwarte, w ustawie ma być uregulowana procedura zarządzania czynności operacyjno-rozpoznawczych, włączywszy w to powierzenie kompetencji do zarządzania tych czynności, a także badanie ich legalności przez zewnętrzny i niezależny od organów władzy wykonawczej podmiot, najlepiej przez sąd. Ustawa ma wskazywać podstawowe elementy proceduralne, zasady wykorzystywania zgromadzonych materiałów oraz przesłanki czy tryb ich niszczenia. Z punktu widzenia ochrony konstytucyjnych wolności i praw niezbędne jest zobowiązanie organów wnoszących o zarządzenie kontroli operacyjnej do wskazania określonego w prawie środka pozyskiwania informacji i dowodów w konkretnej sprawie oraz nałożenie na organy zarządzające takie czynności obowiązku wyrażenia zgody na konkretny rodzaj środka, służącego pozyskiwaniu informacji.

Po piąte, ustawa musi precyzyjnie wskazywać zakres wykorzystania danych pozyskanych w toku czynności operacyjno-rozpoznawczych, a zwłaszcza wykorzystanie ich w procesie karnym jako materiałów dowodowych. Ustawa ma także określać postępowanie z materiałami, które podlegają niezwłocznemu, protokolarnemu i komisyjnemu zniszczeniu, z uwagi na ich zbędność lub nieprzydatność.

Trybunał Konstytucyjny w uzasadnieniu wyroku stwierdził ponadto, iż niejawne pozyskiwanie informacji o jednostkach w toku czynności operacyjno-rozpoznawczych powinno być środkiem subsydiarnym, czyli stosowanym, gdy inne rozwiązania są nieprzydatne lub nieskuteczne. W obecnym stanie prawym zasada subsydiarności obowiązuje w odniesieniu do kontroli operacyjnej – sąd może zarządzić kontrolę operacyjną, gdy inne środki okazały się bezskuteczne albo będą nieprzydatne.

Z przesłanką subsydiarności wiąże się wprowadzenie proceduralnego wymogu, którym jest kontrola niejawnego pozyskiwaniem informacji o osobach przez niezależny od rządu organ państwa. Pożądane jest powierzenie kompetencji w tym zakresie niezależnym i niezawisłym sądom, dającym rękojmię odpowiednio wysokiego stopnia wiedzy i doświadczenia życiowego. Z punktu widzenia Konstytucji sądowa kontrola nad czynnościami operacyjno-rozpoznawczymi jest rozwiązaniem optymalnym. Nie jest jednak bezwzględnie konieczna. Kompetencje tego rodzaju mogą zostać też powierzone innym organom państwa, których status ustrojowy i zakres ustawowych kompetencji gwarantuje efektywną, niezależną i profesjonalną kontrolę nad służbami policyjnymi i ochrony państwa.

Odnosząc się do zagadnienia określenia w ustawie zasad postępowania z materiałami zgromadzonymi w toku czynności operacyjno-rozpoznawczych, Trybunał zauważył, że ustawa musi precyzyjnie wskazywać zakres wykorzystania danych pozyskanych w toku czynności operacyjno-rozpoznawczych, a zwłaszcza wykorzystania ich w procesie karnym jako materiałów dowodowych. Ustawa ma także określać postępowanie z materiałami, które podlegają niezwłocznemu, protokolarnemu i komisyjnemu zniszczeniu z uwagi na ich zbędność lub nieprzydatność.

W wyroku o sygn. akt K 32/04 Trybunał zaznaczył: „w demokratycznym państwie prawnym nie jest konieczne przechowywanie informacji na temat obywateli uzyskanych w toku czynności operacyjnych ze względu na potencjalną przydatność tych informacji". Może to być stosowane tylko w związku z konkretnym postępowaniem, prowadzonym na podstawie ustawy dopuszczającej ograniczenie wolności ze względu na bezpieczeństwo państwa i porządek publiczny (wyrok TK z 12 grudnia 2005 r., sygn. akt K 32/04, cz. III, pkt 4.7). TK nie wyklucza zróżnicowania ochrony prawnej prywatności jednostek z uwagi na ich status obywatelski, jakkolwiek nie może być ono traktowane jako zasada, a w każdym wypadku – nie może prowadzić do arbitralnego różnicowania podmiotów tych konstytucyjnych wolności oraz praw, których sam ustrojodawca nie scharakteryzował jako obywatelskich.

Od tak ujętej zasady jednakowej ochrony dopuszczalne może być wprowadzenie w ustawie wyjątków odnoszących się do cudzoziemców, którzy podlegają polskiemu prawu. Powyższe założenie nie wyklucza dopuszczalności odmiennego określenia przesłanek pozyskiwania danych i postępowania z nimi w stosunku do osób niepodlegających polskiemu prawu (np. danych pozyskiwanych przez służby wywiadu o działalność obcych podmiotów za granicą), chociaż w każdym wypadku takie działania władz publicznych muszą mieścić się w ramach standardów państwa prawnego.

Trybunał w wyroku podniósł również kwestię ochrony tajemnicy zawodowej i wskazał, że jednym z instrumentów ochrony zaufania jest tajemnica zawodowa i gwarancje jej poszanowania w postępowaniach sądowych. Zaliczają się do nich m.in. bezwarunkowe i warunkowe zakazy dowodowe w postępowaniu karnym.

Nie jest wykluczone umożliwienie służbom policyjnym i służbom ochrony państwa pozyskania informacji o charakterze poufnym, przekazywanym podmiotom wykonującym zawody zaufania publicznego. Zważywszy na znaczenie nowych technologii w efektywnej walce z zagrożeniami, zdaniem Trybunału Konstytucyjnego, ogólne wyłączenie spod kontroli

operacyjnej podmiotów zobowiązanych w ustawie do zachowania tajemnicy zawodowej, a nawet wyłączenie informacji uznawanych za stanowiące tajemnicę zawodową, jako bezwzględnie niedopuszczalnych do pozyskania w tym trybie, prowadziłoby do istotnych utrudnień w gromadzeniu materiału dowodowego niektórych rodzajów przestępstw, popełnianych np. z wykorzystaniem nowych technologii.

Zdaniem Trybunału, punkt ciężkości przesuwa się więc na zapewnienie stosownych gwarancji proceduralnych, eliminujących nieuprawnione pozyskanie przez służby policyjne oraz służby ochrony państwa informacji, które – z uwagi na ich treść i okoliczności przekazania – powinny podlegać ochronie prawnej. Modelowym rozwiązaniem tego konfliktu dóbr jest przewidziany w art. 180 § 2 k.p.k. mechanizm zwolnienia z tajemnicy zawodowej przez sąd, jeżeli jest to konieczne dla dobra wymiaru sprawiedliwości, zaś dana okoliczność nie może zostać wykazana w inny sposób, niełamiący tajemnicy zawodowej. W ocenie Trybunału, zbliżone w swej istocie rozwiązania legislacyjne powinny dotyczyć również ochrony tajemnicy zawodowej w trakcie czynności operacyjno-rozpoznawczych, w tym kontroli operacyjnej. Nie ma żadnych uzasadnionych podstaw, by na tym etapie postępowania stosować łagodniejsze standardy niż przewidziane w postępowaniu karnym. Przeciwnie, standardy te – z uwagi na niejawność kontroli oraz jej ponadprocesowy charakter – powinny być co najmniej zbieżne ze standardami w postępowaniu karnym.

Trybunał zauważa potrzebę poinformowania jednostki o podjętych wobec niej działaniach operacyjno-rozpoznawczych oraz pozyskaniu informacji na jej temat, i to bez względu na to, czy były to osoby podejrzane o naruszenie prawa, czy osoby postronne, które przypadkowo stały się obiektem kontroli. Trybunał ma świadomość, że w pewnych sytuacjach może być również uzasadnione odstąpienie od wspomnianego obowiązku informacyjnego. Dotyczy to w szczególności takich sytuacji, gdy dane zostały pozyskane wyłącznie przypadkowo i nie podlegają dalszej analizie, czy też gdy pozyskano dane dostępne w publicznych rejestrach. Kwestie te musi rozstrzygnąć ustawodawca. Wprowadzenie obowiązku informowania osób w zakresie wskazanym przez Trybunał niesie za sobą szereg konsekwencji. W szczególności wiązałoby się to z naruszeniem podstawowych zasad na podstawie których funkcjonują służby i poważnie mogłoby zaważyć, nie tylko na skutecznym działaniu służb, ale także mogłoby zagrozić bezpieczeństwu Sił Zbrojnych RP oraz osób, które w sposób niejawny udzielają pomocy służbom. W praktyce wiązałyby się z tym m.in. trudności w ustaleniu danych osób z uwagi na znaczną skalę używania tzw. telefonów pre–paid. Ponadto obowiązek informowania pozostawałby w sprzeczności z ustawowym wymogiem ochrony form i metod czynności operacyjno-rozpoznawczych oraz faktu ich prowadzenia.

Jednym z wymagań, które powinny spełniać przepisy ustawowe upoważniające służby do pozyskiwania danych telekomunikacyjnych, jest wykreowanie mechanizmu niezależnej kontroli. Skoro pozyskiwanie tych danych dokonuje się w sposób niejawny, bez wiedzy i woli podmiotów, o których informacje są gromadzone, a zarazem przy ograniczonej kontroli społeczeństwa, brak niezależnej kontroli organów państwa nad tym procesem stwarza ryzyko nadużyć. Wymóg unormowania w ustawie proceduralnych mechanizmów przeciwdziałających arbitralności podczas pozyskiwania danych telekomunikacyjnych jest tym silniejszy, im szerszy jest zakres kompetencji organów państwa do niejawnego

pozyskiwania informacji. W takiej sytuacji tym większe znaczenie ma ustanowienie gwarancji proceduralnych zewnętrznej kontroli procesu pozyskiwania danych telekomunikacyjnych, zwłaszcza bilingowych i lokalizacyjnych. TK nie przesądza jak dokładnie ma wyglądać procedura dostępu do danych telekomunikacyjnych, a w szczególności, czy konieczne ma być w odniesieniu do każdego rodzaju zatrzymywanych danych, o których mowa w art. 180c i 180d prawa telekomunikacyjnego, uzyskanie zgody na ich udostępnienie. Zdaniem Trybunału, nie jest wykluczone wprowadzenie, jako zasady, kontroli następczej. Niemniej, zgodnie z konstytucyjną zasadą sprawności działania instytucji publicznych, należy wykreować mechanizm, który umożliwi służbom odpowiedzialnym za bezpieczeństwo państwa i porządek publiczny efektywną walkę z zagrożeniami. Trybunał Konstytucyjny nie wymaga jednocześnie by kontrolę udostępniania danych telekomunikacyjnych sprawowały sądy. Konieczne jest natomiast, by był to organ niezależny od rządu i niepozostający z funkcjonariuszami pozyskującymi dane w bezpośredniej lub pośredniej relacji zwierzchności.

3. Różnice między dotychczasowym a projektowanym stanem prawnym

Projektowana ustawa, realizując ściśle sentencję wspomnianego wyroku Trybunału Konstytucyjnego z 30 lipca 2014 r. o sygn. K 23/11, uwzględnia ponadto zasadniczą część sformułowanych przez Trybunał w uzasadnieniu do tego wyroku minimalnych wymagań, jakie łącznie powinny spełniać przepisy ustaw normujących niejawne pozyskiwanie przez władze publiczne w demokratycznym państwie prawa informacji o osobach; w projekcie uregulowano zatem następujące zagadnienia.

3.1. Przesłanki stosowania kontroli operacyjnej i dostępu do danych telekomunikacyjnych.

W uzasadnieniu do wyroku o sygn. K 23/11 Trybunał Konstytucyjny zwrócił uwagę na niedookreślony ustawowy katalog sytuacji uzasadniających zarządzenie kontroli operacyjnej w toku czynności operacyjno-rozpoznawczych prowadzonych przez Policję, Straż Graniczną, wywiad skarbowy, Żandarmerię Wojskową, Służbę Kontrwywiadu Wojskowego i Agencję Bezpieczeństwa Wewnętrznego w odniesieniu do „przestępstw ściganych na mocy umów i porozumień międzynarodowych", „przestępstw godzących w bezpieczeństwo państwa", „podstawy ekonomiczne państwa", czy „bezpieczeństwo Sił Zbrojnych, jednostek organizacyjnych MON i państw zapewniających wzajemność". Co prawda zakwestionowane przed Trybunałem przepisy zawierające przytoczone określenia (pkt 1 wyroku o sygn. K 23/11) zostały uznane za warunkowo zgodne z Konstytucją, jednak w uzasadnieniu do wyroku Trybunał zauważył, że obowiązujące przepisy nie precyzują, o jakie dokładnie przestępstwa chodzi ani w jakich dokładnie aktach normatywnych są ujęte. Mając na uwadze powyższe, w projektowanych: art. 19 ust. 1 pkt 8 ustawy o Policji, art. 9e ust. 1 pkt 7 ustawy o SG, art. 36c ust. 1 pkt 5 ustawy o kontroli skarbowej, art. 31 ust. 1 pkt 9 ustawy o ŻW, 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.

Ponadto w projektowanym:

– art. 9e ust. 1 pkt 4 ustawy o SG, doprecyzowano katalog przestępstw pozostających w związku z przekraczaniem granicy państwowej lub przemieszczaniem przez granicę państwową towarów oraz wyrobów akcyzowych podlegających obowiązkowi oznaczania znakami akcyzy, jak również przedmiotów określonych w przepisach o broni, amunicji oraz o materiałach wybuchowych, a także o przeciwdziałaniu narkomanii;

– art. 27 ust. 1 ustawy o ABW i AW (zmienianym art. 7 pkt 1 lit. a projektu) doprecyzowano katalog przestępstw, do których rozpoznawania, zapobiegania i zwalczania ABW może stosować kontrolę operacyjną. Doprecyzowanie ma na celu wykonanie pkt 1 wyroku Trybunału w sprawie K 23/11 i zostało ujęte poprzez określenie, na podstawie systematyki Kodeksu karnego, zamkniętego katalogu rodzajów przestępstw stanowiących odpowiednik zakwestionowanego przez Trybunał pojęcia „przestępstw godzących w podstawy ekonomiczne państwa”;

– art. 31 ust. 1 ustawy o ŻW sformułowano zamknięty katalog przestępstw, w odniesieniu do których może zostać zarządzona kontrola operacyjna na wniosek szefa tej służby.

Ponadto, w celu uniknięcia ewentualnego podważania zebranego podczas kontroli operacyjnej materiału dowodowego w projekcie zaproponowano, by jako organ uprawniony do wnioskowania o zarządzanie kontroli operacyjnej, o zarządzenie kontroli operacyjnej w przypadkach niecierpiących zwłoki oraz do wnioskowania o przedłużenie kontroli operacyjnej, występował obok Szefa CBA również upoważniony jego zastępca. W powyższy sposób doprecyzowano także odpowiednie przepisy pozostałych ustaw.

Odnosząc się do postępowania w sprawie zainicjowanej wnioskiem Prokuratora Generalnego, dotyczącej zgodności z art. 2 *Konstytucji Rzeczypospolitej Polskiej* przepisów, które pomijają prokuratora, jako podmiot uprawniony do zainicjowania postępowania odwoławczego od postanowienia sądu w przedmiocie kontroli operacyjnej (sygn. akt K 32/15), w projekcie zaproponowano uwzględnienie powyższego postulatu. Uwzględnienie polega na wprowadzeniu do projektu odpowiedniego przepisu zmieniającego, który przewiduje uprawnienie dla prokuratora w zakresie zażalenia na postanowienie sądu w przedmiocie kontroli operacyjnej.

Kierując się potrzebami uporządkowania katalogu danych uzyskiwanych przez uprawnione służby od przedsiębiorców prowadzących działalność w szeroko rozumianej sferze komunikacji, a także ujednolicenia sformułowań używanych w ustawach dotyczących różnych służb, w projektowanej ustawie:

1) zamiast dotychczasowego opisowego ujęcia informacji „identyfikujących podmiot korzystający z usług pocztowych oraz dotyczących faktu, okoliczności świadczenia usług pocztowych lub korzystania z tych usług” wprowadzono pojęcie „danych pocztowych” definiowane poprzez odesłanie do art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. poz. 1529, z późn. zm.);

2) doprecyzowano istniejący na gruncie ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2013 r., poz. 1422, z późn. zm.) obowiązek usługodawcy świadczącego usługi drogą elektroniczną udzielania informacji o danych, o których mowa w art. 18 ust. 1-5 tej ustawy, organom państwa na potrzeby prowadzonych przez nie postępowań (art. 18 ust. 6 ww. ustawy); doprecyzowanie polega na podmiotowym związaniu treści uprawnienia do pozyskiwania tych danych z organami państwa konkretnie wskazanymi w ustawach zmienianych projektem niniejszej ustawy;

3) doprecyzowując przepisy ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne określono zamknięty katalog danych o osobach będących w posiadaniu przedsiębiorców telekomunikacyjnych (innych niż dane telekomunikacyjne), które uprawnione służby mogą uzyskiwać w celu zapobiegania lub wykrywania przestępstw.

W powyższy sposób doprecyzowano przepisy ustaw dotyczące wszystkich służb uprawnionych do pozyskiwania ww. danych.

W zakresie udostępnienia danych wskazano, iż dane telekomunikacyjne, pocztowe oraz internetowe mogą być udostępniane tylko w celu realizacji konkretnych zadań określonych w ustawie regulującej działalność uprawnionej służby, przy czym wyznaczenie zakresu tych zadań zostało każdorazowo dostosowane do specyfiki działania danej służby.

3.2. Rodzaje środków niejawnego pozyskiwania informacji.

W aktualnym stanie prawnym właściwym dla wszystkich ustaw dotyczących służb uprawnionych do stosowania tego środka pozyskiwania informacji kontrola operacyjna prowadzona jest niejawnie i polega na:

1) kontrolowaniu treści korespondencji;

2) kontrolowaniu zawartości przesyłek;

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

Wychodząc naprzeciw sformułowanym w uzasadnieniu do wyroku o sygn. K 23/11 oczekiwaniom Trybunału, odnośnie sprecyzowania w przepisach prawa zamkniętego rodzajowo katalogu środków i metod działania, za pomocą których władze publiczne mogą w sposób niejawny gromadzić informacje o osobach, ustawodawca odpowiednio w art. 19 ust. 6 i 6a ustawy o Policji, art. 9e ust. 7 i 7a ustawy o SG, art. 36c ust. 4 i 4a ustawy o kontroli skarbowej, art. 31 ust. 7 i 7a ustawy o ŻW, art. 27 ust. 6 i 6a ustawy o ABW oraz AW, art. 31 ust. 4 i 4a ustawy o SKW oraz SWW oraz w art. 17 ust. 5 i 5a ustawy o CBA określił wyczerpująco i jednolicie dla wszystkich uprawnionych służb sposoby prowadzenia kontroli operacyjnej, wraz z niezbędnymi wyłączeniami. Zgodnie z projektem, kontrola operacyjna prowadzona jest niejawnie i polega 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 dostępu i kontroli zawartości przesyłek;

5) uzyskiwaniu i utrwalaniu danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych.

3.3. Okres prowadzenia kontroli operacyjnej.

W obecnym stanie prawnym przepisy nie ograniczają maksymalnego czasu prowadzenia kontroli operacyjnej. Istniejące rozwiązania prawne (zasadniczo jednolite dla wszystkich uprawnionych służb) przewidują, że kontrolę operacyjną zarządza właściwy dla danej służby sąd na okres nie dłuższy niż 3 miesiące. Niemniej sąd ten może, na pisemny wniosek szefa służby, złożony po uzyskaniu pisemnej zgody właściwego prokuratora, wydać postanowienie o jednorazowym jej przedłużeniu na okres nie dłuższy niż kolejne 3 miesiące, jeżeli nie ustały przyczyny tej kontroli. Ponadto, 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, właściwy sąd, na pisemny wniosek szefa służby, złożony po uzyskaniu pisemnej zgody właściwego prokuratora, może wydać postanowienie o prowadzeniu kontroli operacyjnej przez czas oznaczony również po upływie ww. okresów.

Realizując postulat Trybunału Konstytucyjnego, dotyczący sprecyzowania w ustawie maksymalnego czasu prowadzenia niejawnych czynności, po upływie których dalsze ich prowadzenie jest już niedopuszczalne, projektodawca, odpowiednio w projektowanym art. 19 ust. 9 ustawy o Policji, art. 9e ust. 10 ustawy o SG, art. 36c ust. 7 ustawy o kontroli skarbowej oraz art. 31 ust. 10 ustawy o ŻW, art. 17 ust. 9 ustawy o CBA określił jednoznacznie maksymalny okres stosowania kontroli operacyjnej. Powyższe zmienione przepisy przewidują, że po upływie okresów, na które została zarządzona kontrola operacyjna, tj. nie dłużej niż 3 miesiące – pierwsze postanowienie sądu, nie dłużej niż kolejne 3 miesiące – jednorazowe przedłużenie kontroli operacyjnej postanowieniem sądu, możliwe będzie, na podstawie postanowienia sądu, przedłużenie, po upływie ww. dwóch okresów, prowadzenia kontroli operacyjnej na kolejne następujące po sobie okresy, jednak łączny okres przedłużenia stosowania przez te służby kontroli operacyjnej (nie licząc dwóch pierwszych przedłużeń) nie może przekroczyć 12 miesięcy. Tym samym całkowity czas prowadzenia przez ww. służby kontroli operacyjnej w danej sprawie (łącznie ze wszystkimi przedłużeniami) nie będzie mógł przekroczyć 18 miesięcy.

Ze względu na specyfikę zadań realizowanych przez służby specjalne wykonujące działania w zakresie kontrwywiadu, ograniczenia powyższe nie zostały wprowadzone w odniesieniu do kontroli operacyjnej stosowanej przez te służby. W projektowanych art. 27 ust. 9 ustawy o ABW i AW i art. 31 ust. 7 ustawy o SKW i SWW określono, że jeżeli w trakcie stosowania kontroli operacyjnej pojawią się nowe okoliczności istotne dla zapobieżenia lub wykrycia przestępstwa albo ustalenia sprawcy i uzyskania dowodów przestępstwa, kontrola operacyjna może być przedłużana na następujące po sobie okresy, z których żaden nie może trwać dłużej niż 12 miesięcy. O przedłużeniu kontroli, każdorazowo będzie decydować sąd, który wydał zgodę na jej prowadzenie, co zapewni kontrolę niezależnego organu nad prawidłowością działań podejmowanych przez te służby. Przyjęcie takiego rozwiązania w odniesieniu do służb specjalnych realizujących zadania kontrwywiadowcze i antyterrorystyczne jest niezbędne w perspektywie bieżących zagrożeń bezpieczeństwa, m.in. w kontekście przyjmowanego obecnie *modus operandi* sprawców takich przestępstw jak przestępstwa o charakterze terrorystycznym, sabotaż, czy szpiegostwo, wykorzystujących tzw. „uśpione ogniwo". Trybunał wskazał, że nie jest wykluczone zróżnicowanie intensywności ochrony prywatności, autonomii informacyjnej oraz tajemnicy komunikowania się z uwagi na to, czy dane o osobach pozyskują służby wywiadowcze i zajmujące się ochroną bezpieczeństwa państwa, czy też czynią to służby policyjne. Specyfika działalności służb informacyjno–wywiadowczych oraz związany z tym relatywnie wąsko określony zakres ich ustawowych zadań, może uzasadniać odmienne ustalenie zasad prowadzenia takich czynności i wykorzystywania zgromadzonych materiałów, od reguł obowiązujących pozostałe organy państwa, a zwłaszcza służby policyjne, mające szeroki zakres działania. Takie zróżnicowanie zasad prowadzenia czynności operacyjno-rozpoznawczych nie uchyla oczywiście wymogu przestrzegania zasady proporcjonalności.

Warto w tym miejscu zwrócić uwagę, że projektowane określenie maksymalnego czasu prowadzenia kontroli operacyjnej pozostaje w zbieżności z regulacją art. 180a ust.1 pkt 1 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, przewidującą obowiązek operatorów publicznej sieci telekomunikacyjnej oraz dostawców publicznie dostępnych usług telekomunikacyjnych zatrzymywania i przechowywania, na własny koszt, danych, o których mowa w art. 180c ustawy, przez okres 12 miesięcy, licząc od dnia połączenia lub nieudanej próby połączenia. Oceny zasadności przechowywania przez okres 12 miesięcy danych telekomunikacyjnych należy dokonać przez pryzmat możliwości ich skutecznego wykorzystania w realizowanych działaniach operacyjno-rozpoznawczych. Należy podkreślić, iż w ramach rozpoznawania, zapobiegania i wykrywania przestępstw, w tym w szczególności o charakterze szpiegowskim, terrorystycznym, czy udziału w zorganizowanej grupie lub związku przestępczym, ważną rolę odgrywa praca analityczna. Uzyskanie informacji o określonej, niezgodnej z prawem działalności, uruchamia proces analityczny, którego jednym z ważnych celów jest wykazanie genezy rozpoznawanych powiązań przestępczych. Powyższe pozwala (np. w przypadku przestępstwa szpiegostwa) na określenie potencjalnych szkód wyrządzonych taką działalnością. Priorytetową rolę w tym zakresie odgrywają dane telekomunikacyjne, pozwalające niejednokrotnie na wychwycenie okresu nawiązania współpracy w ramach niezgodnej z prawem działalności. Dane telekomunikacyjne pozwalają również we właściwy sposób zaplanować kolejne – niejednokrotnie złożone – czynności

operacyjno-rozpoznawcze w celu neutralizacji istniejących zagrożeń. Trybunał formułując postulat skrócenia okresu przechowywania danych telekomunikacyjnych, wskazał na dane statystyczne, w świetle których większość przypadków udostępniania danych mieściła się w okresie pierwszych 6 miesięcy przechowywania. Nawet, jeżeli w późniejszym okresie obserwowane jest zmniejszenie liczby udostępnianych danych, pamiętać jednak należy, że również w późniejszych etapach prowadzenia sprawy, pozyskane dane mogą być istotne dla sprawy i skutecznie wykorzystane.

Podkreślenia wymaga także, że okres przechowywania danych telekomunikacyjnych przez operatorów został już skrócony z 24 do 12 miesięcy (ustawa z dnia 16 listopada 2012 r. o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw, Dz. U. poz. 1445), która obowiązuje od 21 stycznia 2013 r. Podobny termin zatrzymywania danych obowiązuje w większości państw członkowskich Unii Europejskiej.

3.4. Zasady i procedury dotyczące weryfikacji i niszczenia danych telekomunikacyjnych, pocztowych i internetowych zbędnych dla prowadzonego postępowania.

W celu wykonania pkt 8 i 9 wyroku Trybunału Konstytucyjnego w sprawie K 23/11 stwierdzającego niezgodność przepisów ustawy o ABW i AW, ustawy SKW i SWW oraz ustawy CBA, w zakresie w jakim nie przewidują zniszczenia danych telekomunikacyjnych i pocztowych niemających znaczenia dla prowadzonego postępowania, w projekcie ustawy wprowadzono ujednolicone dla wszystkich służb procedury postępowania z tymi danymi. Zgodnie z projektowanymi: art. 20c ustawy o Policji, art. 10b ustawy o SG, art. 36ba ustawy o kontroli skarbowej, art. 30 ustawy o ŻW, art. 28 ustawy o ABW oraz AW, art. 32 ustawy o SKW oraz SWW, art. 18 ustawy o CBA oraz art. 75d ustawy o SC, dane telekomunikacyjne i pocztowe, które mają znaczenie dla postępowania karnego, przekazywane są właściwemu prokuratorowi, który podejmuje decyzję o zakresie i sposobie wykorzystania przekazanych danych. Materiały, które nie mają znaczenia dla prowadzonego postępowania mają podlegać niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu. Te same zasady będą miały zastosowanie również w postępowaniu z danymi internetowymi.

Należy również zaznaczyć, że pomimo niewykluczenia przez Trybunał możliwości zróżnicowania ochrony prawnej prywatności jednostek z uwagi na ich status obywatelski, poprzez dopuszczenie wprowadzenia w ustawie wyjątków odnoszących się do cudzoziemców, polegających na odmiennym określeniu przesłanek pozyskiwania danych i postępowania z nimi w stosunku do tych osób, w projekcie ustawy nie zdecydowano się na wprowadzenie rozwiązań pozwalających na przechowywanie danych telekomunikacyjnych, pocztowych i internetowych dotyczących cudzoziemców, które są nieprzydane w prowadzonym postępowaniu.

3.5. Organy oraz procedura kontroli pozyskiwania danych telekomunikacyjnych, pocztowych i internetowych.

W odróżnieniu od regulacji odnoszących się do udostępniania danych telekomunikacyjnych i pocztowych, obowiązujące przepisy przewidują wzmocniony nadzór prokuratorski i sądowy nad prowadzeniem kontroli operacyjnej przez uprawnione służby. Nadzór ten sprawowany

jest od początkowej fazy uzyskiwania zgody na jej prowadzenie (kontrola operacyjna może być zarządzona lub przedłużona przez sąd, po uzyskaniu wcześniejszej zgody prokuratora), poprzez obowiązek informowania prokuratora o przebiegu i wynikach tej kontroli, zasady i procedury wykorzystania materiałów z kontroli operacyjnej w prowadzonych postępowaniach karnych oraz niszczenia tych materiałów, a skończywszy na obowiązkach informacyjnych wobec Sejmu i Senatu. Realizując pkt 5 wyroku Trybunału Konstytucyjnego w sprawie K 23/11, stwierdzający niezgodność z Konstytucją RP obecnych uregulowań nieprzewidujących niezależnej kontroli udostępniania danych telekomunikacyjnych, o których mowa w art. 180c i 180d ustawy – Prawo telekomunikacyjne, w projekcie ustawy zaproponowano, aby podmiotem uprawnionym do kontroli uzyskiwania danych telekomunikacyjnych został: sąd okręgowy właściwy dla siedziby podmiotu uprawnionego do złożenia wniosku – w odniesieniu do Policji, Straży Granicznej i Służby Celnej, wojskowy sąd okręgowy właściwy dla siedziby organu Żandarmerii Wojskowej, Sąd Okręgowy w Warszawie – w odniesieniu do organu kontroli skarbowej, Agencji Bezpieczeństwa Wewnętrznego i Centralnego Biura Antykorupcyjnego oraz Wojskowy Sąd Okręgowy w Warszawie – w odniesieniu do Służby Kontrwywiadu Wojskowego.

Jednocześnie na uprawnione formacje został nałożony obowiązek przekazywania określonemu powyżej sądowi, raz na 6 miesięcy, sprawozdań obejmujących: liczbę przypadków pozyskania w okresie sprawozdawczym danych telekomunikacyjnych, pocztowych lub internetowych oraz ich rodzaj; rodzaje przestępstw, w związku z zaistnieniem których wystąpiono o dane telekomunikacyjne, pocztowe lub internetowe; liczbę przypadków, ze wskazaniem ich podziału na rodzaje spraw, w których wystąpiono o dane. W ramach kontroli, sąd okręgowy może zapoznać się z materiałami uzasadniającymi udostępnienie danych. Sąd informuje szefa służby o wyniku kontroli w terminie 30 dni od jej zakończenia.

Z uwagi na konieczność opracowania kompleksowego ujęcia materii, obok danych telekomunikacyjnych, kontrolą sądową objęto również proces udostępniania uprawnionym służbom danych pocztowych, określonych na podstawie ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. z 2012 r. poz. 1529) oraz tzw. danych internetowych, określonych w art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422). Pomimo, że pkt 5 wyroku Trybunału o sygn. K 23/11 nie obejmuje swoim zakresem danych uzyskiwanych na podstawie prawa pocztowego oraz danych uzyskiwanych na podstawie ustawy o świadczeniu usług drogą elektroniczną, powyższe rozszerzenie zakresu przedmiotowego kontroli znajduje uzasadnienie w tym, że działalność służb w tych obszarach w podobnym stopniu ingeruje w prawa i wolności obywatelskie jak proces pozyskiwania danych telekomunikacyjnych. Projekt przewiduje również takie same przesłanki udostępniania, procedury weryfikacji oraz niszczenia udostępnianych służbom danych pocztowych oraz danych o których mowa w ustawie o świadczeniu usług drogą elektroniczną, zbędnych dla prowadzonego postępowania. Skorelowanie regulacji prawnych w stosunku do wszystkich obszarów danych dotyczących sfery komunikacji między osobami stanowi rozwiązanie systemowe służące pogłębieniu zaufania obywateli do organów państwowych.

3.6. Zasady postępowania z materiałami, które mogą zawierać informacje objęte tajemnicą zawodową (notarialną, adwokacką, radcy prawnego, doradcy podatkowego, lekarską, dziennikarską lub statystyczną), albo są objęte zakazami dowodowymi.

Kierując się potrzebą wykonania pkt 6 wyroku Trybunału Konstytucyjnego o sygn. K 23/11 odnoszącego się do niekonstytucyjności przepisów regulujących kontrolę operacyjną, ze względu na brak regulacji przewidującej gwarancję niezwłocznego, komisyjnego i protokolarnego zniszczenia materiałów zawierających informacje objęte zakazami dowodowymi, co do których sąd nie uchylił tajemnicy zawodowej, bądź uchylenie było niedopuszczalne, w poszczególnych ustawach pragmatycznych wprowadzono zasady postępowania z materiałami uzyskanymi w ramach czynności operacyjno-rozpoznawczych, które mogą zawierać informacje objęte tajemnicą zawodową. W projektowanych: art. 19 ust. 15f–15j ustawy o Policji, art. 9e ust. 16f–16j ustawy o SG, art. 36d ust. 1f–1i ustawy o kontroli skarbowej, art. 31 ust. 16f–16j ustawy o ŻW, art. 27 ust. 15h–15l ustawy o ABW i AW, art. 31 ust. 14f–14j ustawy o SKW i SWW, art. 17 ust. 15f–15j ustawy o CBA, zaproponowano, aby w przypadku, w którym będzie zachodzić przypuszczenie, że materiały uzyskane w wyniku kontroli operacyjnej będą zawierać informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 k.p.k. (tajemnicy notarialnej, adwokackiej, radcy prawnego, doradcy podatkowego, lekarskiej, dziennikarskiej lub statystycznej) albo zawierać informacje, o których mowa w art. 178, art. 178a albo art. 180 § 3 k.p.k., szef służby przekaże je właściwemu prokuratorowi . Prokurator następnie kieruje je niezwłocznie do sądu, który zarządził kontrolę operacyjną wraz z wnioskiem o: stwierdzenie, które z przekazanych materiałów zawierają informacje, o których mowa w przytoczonych przepisach k.p.k., a także dopuszczenie do wykorzystania w postępowaniu karnym materiałów zawierających informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego nieobjęte zakazami, określonymi w art. 178, art. 178a i art. 180 § 3 k.p.k., z wyłączeniem informacji o przestępstwach, o których mowa w art. 240 § 1 k.k. Sąd wydając postanowienie o dopuszczenie do wykorzystania w postępowaniu karnym tych materiałów będzie obowiązany kierować się tymi samymi przesłankami, o których mowa w art. 180 § 2 k.p.k. tj. dobrem wymiaru sprawiedliwości oraz faktem, że okoliczność nie może być ustalona na podstawie innego dowodu. Sąd ma też zarządzać zniszczenie materiałów, których wykorzystanie w postępowaniu karnym jest niedopuszczalne. Na postanowienie sądu o stwierdzeniu dopuszczalności wykorzystania w postępowaniu karnym tych materiałów prokuratorowi będzie przysługiwało zażalenie. O wykonaniu zarządzenia dotyczącego zniszczenia materiałów, szef uprawnionej służby niezwłocznie informuje prokuratora.

3.7. Nowelizacja ustawy – Prawo telekomunikacyjne.

W projektowanej ustawie zawarto przepis (art. 8) uchylający art. 180g ustawy z dnia 16 lipca 2014 r. – Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243, 827 i 1198).

Konieczność uchylenia tego przepisu wynika z wyroku Trybunału Sprawiedliwości Unii Europejskiej z dnia 8 kwietnia 2014 r. (sprawy połączone C–293/12 i C–594/12). 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 zawarty w art. 180g ustawy obowiązek przekazywania przez przedsiębiorców telekomunikacyjnych Prezesowi Urzędu Komunikacji Elektronicznej informacji wskazanych w art. 180g ust. 1 i następnie obowiązek przekazywania tych informacji przez Prezesa UKE Komisji Europejskiej.

W zamian za uchylone regulacje, w celu zapewnienia opinii publicznej niezbędnych informacji, w projekcie ustawy przewidziano natomiast obowiązek corocznego przedstawiania Sejmowi i Senatowi przez Ministra Sprawiedliwości, zagregowanej informacji na temat przetwarzania danych telekomunikacyjnych oraz wyników przeprowadzonych kontroli, w terminie do dnia 30 czerwca roku następującego po roku nią objętym (art. 5 pkt 3 projektu).

3.8. Nowelizacja ustawy o świadczeniu usług drogą elektroniczną.

W projektowanej ustawie wprowadzono przepis dotyczący art. 18 ust. 6 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422), który reguluje zagadnienie braku odpłatności za dane otrzymywane od usługodawców świadczących usługi drogą elektroniczną.

3.9. Przepisy przejściowe.

Wobec faktu odroczenia w wyroku o sygn. K 23/11 utraty mocy obowiązującej zakwestionowanych przez Trybunał przepisów projektodawca przyjął jako zasadę, że ustanowione w projekcie unormowania dotyczące postępowania z materiałami kontroli operacyjnej oraz danymi telekomunikacyjnymi i pocztowymi powinny znaleźć zastosowanie we wskazanych obszarach w ramach postępowań wszczynanych po wejściu w życie projektowanej ustawy.

Mając na uwadze powyższe projekt w art. 13 przewiduje, że do kontroli operacyjnej, która była prowadzona przed dniem wejścia w życie projektowanej ustawy i nie została zakończona do tego czasu stosuje się przepisy dotychczasowe, natomiast w art. 15 dotyczącym postępowań w sprawie udostępniania danych telekomunikacyjnych oraz danych identyfikujących podmiot korzystający z usług pocztowych, które były wszczęte przed dniem wejścia w życie projektowanej ustawy i nie zostały zakończone do tego czasu, a także danych telekomunikacyjnych i pocztowych uzyskanych w tych postępowaniach stwierdza się, że do tych postępowań i zgromadzonych danych stosuje się przepisy dotychczasowe.

W związku z przewidzianym w projekcie ograniczeniem maksymalnego czasu trwania kontroli operacyjnej zarządzanej na wniosek właściwego organu Policji, Straży Granicznej, kontroli skarbowej i Żandarmerii Wojskowej w art. 14 projektu zawarto regulację, zgodnie z którą wniosek tych służb o zarządzenie kontroli operacyjnej w dotychczasowym brzmieniu, złożony przed dniem wejścia w życie niniejszej ustawy, stanowi podstawę do zarządzenia

przez sąd kontroli w trybie określonym w tych przepisach, w brzmieniu nadanym projektowaną ustawą. Po zakończeniu powyższej kontroli operacyjnej wskutek upływu terminu może zostać jednokrotnie zarządzona kontrola operacyjna według zasad określonych projektowaną ustawą.

W związku z doprecyzowaniem katalogu przestępstw uprawniających ABW do wnioskowania o zarządzenie kontroli operacyjnej w projekcie zawarto przepis przejściowy (art. 16) przewidujący, że do prowadzonej przez ABW kontroli operacyjnej wszczętej i niezakończonej przed dniem wejścia w życia przedmiotowej ustawy, stosuje się przepisy dotychczasowe. Przepis ten obejmuje także przedłużenia kontroli operacyjnej, o których mowa w ust. 8 i 9 obecnej ustawy o ABW, a trwające w chwili wejścia w życie ustawy nowelizującej. A zatem przedłużenia kontroli operacyjnej, o których mowa w ust. 8 i 9 obecnej ustawy o ABW będą się odbywać na podstawie dotychczasowych przepisów.

4. Wstępna ocena skutków regulacji

Projekt uwzględnia stanowisko Trybunału Konstytucyjnego w odniesieniu do: przepisów regulujących zakres przesłanek prowadzenia kontroli operacyjnej i udostępniania danych telekomunikacyjnych, ochrony tajemnicy zawodowej w toku realizowanych czynności, niszczenia zbędnych danych telekomunikacyjnych, określenia zakresu i trybu kontroli nad pozyskiwaniem danych telekomunikacyjnych, określenia środków niejawnego pozyskiwania informacji o jednostkach, określenia maksymalnego okresu prowadzenia kontroli operacyjnej, podawania do publicznej wiadomości informacji o danych telekomunikacyjnych pozyskiwanych przez uprawnione służby. Ponadto wprowadzone zostały takie same gwarancje ochrony prawnej w stosunku do uzyskiwanych przez uprawnione służby danych telekomunikacyjnych, pocztowych oraz „danych internetowych”.

Wobec tego podstawowym skutkiem projektu będzie urzeczywistnienie zasad i gwarancji konstytucyjnych w sposób wskazany przez Trybunał Konstytucyjny. Można oczekiwać, że wejście w życie projektowanej regulacji będzie sprzyjać budowaniu zaufania jednostek do działań o charakterze niejawnym podejmowanych przez służby policyjne oraz służby ochrony państwa, w szczególności poprzez zwiększenie przejrzystości przepisów oraz określenie precyzyjnych procedur obowiązujących w omawianym obszarze funkcjonowania Państwa.

Projekt oddziałuje na:

1) sądy okręgowe i wojskowe sądy okręgowe, w zakresie jakim nadaje uprawnienie kontrolne nad uzyskiwaniem przez właściwe służby danych telekomunikacyjnych, pocztowych i „danych internetowych”. W ramach przyznanych uprawnień sądy będą mogły zapoznawać się z materiałami uzasadniającymi wystąpienia o dane telekomunikacyjne, pocztowe, internetowe oraz z materiałami uzyskanymi w wyniku podjętych przez służby czynności;

2) funkcjonariuszy Policji, Straży Granicznej, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego, Centralnego Biura Antykorupcyjnego, Służby Celnej, wywiadu skarbowego i żołnierzy Żandarmerii Wojskowej prowadzących czynności

operacyjno-rozpoznawcze oraz mających dostęp do danych telekomunikacyjnych, pocztowych i „danych internetowych", poprzez wprowadzenie nowego trybu uzyskiwania tych danych, tj. przekazywania ich do organu kontrolnego oraz wprowadzenia trybu niszczenia zbędnych danych;

3) osoby objęte tajemnicą notarialną, adwokacką, radcy prawnego, doradcy podatkowego, lekarską, dziennikarską lub statystyczną, w zakresie zapewnienia procedur gwarantujących ochronę prawną pochodzących od nich informacji, które z uwagi na ich treść i okoliczności przekazania winny takiej ochronie podlegać

4) przedsiębiorców telekomunikacyjnych i Prezesa Urzędu Komunikacji Elektronicznej poprzez zniesienie obowiązku przekazywania informacji wskazanych w art. 180g ust. 1 ustawy – Prawo telekomunikacyjne i następnie obowiązku ich przekazywania przez Prezesa UKE do Komisji Europejskiej;

5) obywateli, którym projekt zapewnia zwiększenie ochrony konstytucyjnych wolności i praw.

Proponowana nowelizacja może przyczynić się do wzrostu wydatków z budżetu państwa związanego z nałożonym na sądy okręgowe zadaniem kontroli pozyskiwania przez uprawnione służby danych telekomunikacyjnych, pocztowych i „danych internetowych" (art. 5 projektu). Jednakże, w chwili obecnej, nie jest możliwe szczegółowe wyliczenie kosztów funkcjonowania takiej kontroli, gdyż to prezesi sądów okręgowych będą podejmować autonomiczne decyzje w zakresie wewnętrznej organizacji sądów (możliwość tworzenia w strukturze sądów wydziałów do spraw kontroli danych telekomunikacyjnych, pocztowych i internetowych) oraz liczby i zakresu podejmowanych czynności kontrolnych, z czym związane mogą być zmiany w obsadzie etatowej sądów.

Nie przewiduje się natomiast zwiększenia wydatków w budżetach uprawnionych służb związanych z wprowadzeniem dodatkowych procedur kontroli sądowej informacji objętych tajemnicą wykonywanego zawodu lub funkcji, zawartych w materiałach z kontroli operacyjnej.

W związku z planowanym zniesieniem obowiązku przekazywania informacji wskazanych w art. 180g ustawy – Prawo telekomunikacyjne i następnie obowiązku ich przekazywania przez Prezesa UKE do Komisji Europejskiej (art. 8 projektu) powinien nastąpić nieznaczny spadek wydatków w budżecie Prezesa UKE. Wskutek likwidacji tego obowiązku zmniejszeniu ulegnie także liczba obciążeń administracyjnych nałożonych na przedsiębiorców telekomunikacyjnych, co spowoduje niewielki spadek kosztów ich działalności.

Projektowana ustawa nie spowoduje skutków finansowych dla pozostałych jednostek sektora finansów publicznych, w tym jednostek samorządu terytorialnego.

5. Wstępna opinia o zgodności z prawem Unii Europejskiej

Zakres przedmiotowy projektowanej ustawy nie jest sprzeczny z prawem Unii Europejskiej.