# Druk nr 3765

Warszawa, 28 lipca 2015 r.

SEJM
RZECZYPOSPOLITEJ POLSKIEJ
VII kadencja
Marszałek Senatu

Pani
Małgorzata Kidawa-Błońska
Marszałek Sejmu
Rzeczypospolitej Polskiej

*Szanowna Pani Marszałek*

Zgodnie z art. 118 ust. 1 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. mam zaszczyt przekazać Pani Marszałek podjętą przez Senat na 79. posiedzeniu w dniu 24 lipca 2015 r. uchwałę w sprawie wniesienia do Sejmu projektu ustawy

**- o zmianie ustawy o Policji oraz niektórych innych ustaw** wraz z projektem tej ustawy.

Jednocześnie pragnę poinformować, że Senat upoważnił senatora Piotra Zientarskiego do reprezentowania Senatu w dalszych pracach nad tym projektem.

*Z poważaniem*

(-) Bogdan Borusewicz

**U C H W A Ł A**

**S E N A T U  R Z E C Z Y P O S P O L I T E J  P O L S K I E J**

z dnia 24 lipca 2015 r.

**w sprawie wniesienia do Sejmu projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw**

Na podstawie art. 118 ust. 1 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Senat wnosi do Sejmu Rzeczypospolitej Polskiej projekt ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw.

Jednocześnie upoważnia senatora Piotra Zientarskiego do reprezentowania Senatu w pracach nad projektem.

**MARSZAŁEK SENATU**

**Bogdan BORUSEWICZ**

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) podsłuchu rozmów prowadzonych przy użyciu środków technicznych;

2) podsłuchu i podglądzie pomieszczeń i osób poza miejscami publicznymi;

3) kontroli treści korespondencji;

4) nadzorze elektronicznym osób, miejsc i przedmiotów oraz środków transportu;

5) kontroli zawartości przesyłek.”,

---

1) Niniejszą ustawą zmienia się ustawy: 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.

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

„6a. Kontroli operacyjnej nie stanowią czynności, o których mowa w ust. 6 pkt 2 i 4, polegające na:

1) uzyskiwaniu i utrwalaniu obrazu w pomieszczeniach, o których mowa w art. 15 ust. 1 pkt 4a;

2) uzyskiwaniu danych w trybie art. 20c.

6b. Czynności, o których mowa w ust. 6, mogą być realizowane przy użyciu środków technicznych niezbędnych do realizacji celów kontroli operacyjnej.”,

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, jednokrotnie wydać postanowienie o przedłużeniu kontroli operacyjnej, na czas oznaczony jednak nie dłuższy niż 12 miesięcy.”,

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

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

1) zawierają informacje, o których mowa:

a) w art. 178 Kodeksu postępowania karnego,

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

– Komendant Główny Policji, Komendant CBŚP albo komendant wojewódzki Policji nakazuje ich niezwłoczne, komisyjne i protokolarne zniszczenie;

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

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

1) wyrażenie zgody na ich wykorzystanie w postępowaniu karnym, albo
2) wydanie zarządzenia o ich niezwłocznym, komisyjnym i protokolarnym zniszczeniu.

15h. Sąd wydaje postanowienie o stwierdzeniu dopuszczalności wykorzystania w postępowaniu karnym materiałów mogących zawierać informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu, albo zarządza ich zniszczenie, w terminie 14 dni od dnia złożenia wniosku przez prokuratora.

15i. Na postanowienie sądu o stwierdzeniu dopuszczalności wykorzystania w postępowaniu karnym materiałów mogących zawierać informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, prokuratorowi przysługuje zażalenie. Do zażalenia stosuje się odpowiednio przepisy Kodeksu postępowania karnego.

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

15k. W sprawach dotyczących kontroli operacyjnej lub udostępnienia danych telekomunikacyjnych i pocztowych albo wykorzystania materiałów z tych czynności w postępowaniu karnym w odniesieniu do posłów, senatorów i Prezydenta Rzeczypospolitej Polskiej postanowienie wydaje Pierwszy Prezes Sądu Najwyższego.”,

f) po ust. 16 dodaje się ust. 16a–16c 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 ewidencjonować dane zawarte w dokumentacji z kontroli operacyjnej w zakresie przewidzianym dla prowadzonych przez organy Policji rejestrów, o których mowa w ust. 16a.”,

g) po ust. 20 dodaje się ust. 20a–20c w brzmieniu:

„20a. Dokumentację materiałów zgromadzonych podczas stosowania kontroli operacyjnej, stanowią:

1) nośniki, na których utrwalone zostały treści rozmów telefonicznych lub innych przekazów informacji albo treści korespondencji lub zawartość przesyłek;

2) kopie wykonane z nośników, o których mowa w pkt 1;

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

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

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

2) ust. 17 – wraz z tymi materiałami.

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

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

2) pkt 2 i 3 – nie jest sporządzana.”,

h) ust. 21 otrzymuje brzmienie:

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

1) sposób dokumentowania kontroli operacyjnej,
2) sposób przechowywania i przekazywania dokumentacji kontroli operacyjnej,
3) szczegółowy sposób dokumentowania materiałów uzyskanych podczas stosowania kontroli operacyjnej oraz sposób przechowywania, przekazywania oraz przetwarzania i niszczenia tych materiałów i dokumentacji,
4) sposób prowadzenia rejestrów, o których mowa w ust. 16a – 16c,
5) wzory dokumentów wchodzących w zakres dokumentacji kontroli operacyjnej oraz rejestrów, o których mowa w ust. 16a – 16c

– uwzględniając potrzebę zapewnienia niejawnego charakteru podejmowanych czynności i uzyskanych materiałów oraz przejrzystość dokumentacji i rejestrów.”;

2) art. 20c otrzymuje brzmienie:

„Art. 20c. 1. W celu rozpoznawania, zapobiegania, zwalczania, wykrywania albo uzyskania i utrwalenia dowodów przestępstw ściganych z oskarżenia publicznego albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych, Policja może mieć, gdy inne środki okazały się bezskuteczne albo mogą być nieprzydatne, udostępniane dane:

1) o których mowa w art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243, 827 i 1198), zwane dalej „danymi telekomunikacyjnymi”,
2) identyfikujące podmiot korzystający z usług pocztowych w rozumieniu art. 2 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. poz. 1529) oraz dotyczące faktu, okoliczności świadczenia tych usług lub korzystania z nich, zwane dalej „danymi pocztowymi”

– oraz może je przetwarzać.

2. Podmiot prowadzący działalność telekomunikacyjną lub operator świadczący usługi pocztowe udostępnia nieodpłatnie dane, o których mowa w ust. 1:

1) policjantowi wskazanemu w pisemnym wniosku Komendanta Głównego Policji, Komendanta CBŚP, komendanta wojewódzkiego Policji albo osoby przez nich upoważnionej;

2) na ustne żądanie policjanta posiadającego pisemne upoważnienie osób, o których mowa w pkt 1;
3) za pośrednictwem sieci telekomunikacyjnej policjantowi posiadającemu pisemne upoważnienie osób, o których mowa w pkt 1;
4) organowi Policji wskazanemu w postanowieniu sądu wyrażającym zgodę na pozyskanie danych telekomunikacyjnych lub pocztowych, w przypadkach, o których mowa w art. 20ca ust. 1 lub 3.

3. W przypadku, o którym mowa w ust. 2 pkt 3, udostępnianie danych, o których mowa w ust. 1, odbywa się bez udziału pracowników podmiotu prowadzącego działalność telekomunikacyjną lub operatora świadczącego usługi pocztowe, lub przy niezbędnym ich udziale, jeżeli możliwość taka jest przewidziana w porozumieniu zawartym pomiędzy Komendantem Głównym Policji a tym podmiotem.

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

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

5. Materiały uzyskane w wyniku czynności związanych z udostępnieniem danych, o których mowa w ust. 1, które zawierają informacje mające znaczenie dla postępowania karnego Komendant Główny Policji, Komendant CBŚP albo komendant wojewódzki Policji przekazują prokuratorowi właściwemu miejscowo lub rzeczowo.

6. Materiały uzyskane w wyniku czynności związanych z udostępnieniem danych, o których mowa w ust. 1, które nie zawierają informacji mających znaczenie dla postępowania karnego, podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu.

7. Dane, o których mowa w ust. 1, przetwarza się przez okres, w którym są one niezbędne do realizacji ustawowych zadań, przy czym, nie rzadziej niż co 3 lata, dokonuje się weryfikacji potrzeby dalszego ich przetwarzania.

8. W przypadku gdy w wyniku weryfikacji ustalono, że dalsze przetwarzanie danych, o których mowa w ust. 1, nie jest niezbędne dla realizacji ustawowych zadań, dane te oraz materiały, o których mowa w ust. 6, niezwłocznie, nie później jednak niż w terminie 14 dni od dnia zakończenia weryfikacji, niszczy komisja powołana przez Komendanta Głównego Policji lub osobę przez niego upoważnioną. Z czynności komisji sporządza się protokół.”;

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

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

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

3. Sąd okręgowy wydaje postanowienie o stwierdzeniu dopuszczalności wykorzystania w postępowaniu karnym materiałów zawierających dane, o których mowa ust. 1, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu, albo zarządza ich komisyjne i protokolarne zniszczenie, w terminie 14 dni od dnia złożenia wniosku przez prokuratora.

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

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

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

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

4. Sąd okręgowy wydaje postanowienie w przedmiocie zgody na pozyskanie danych i ich wykorzystanie w postępowaniu karnym gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu.

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

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

1) wydania zarządzenia o ich niezwłocznym, komisyjnym i protokolarnym zniszczeniu – w przypadku gdy dane te zostały przekazane;
2) poinformowania podmiotu prowadzącego działalność telekomunikacyjną lub operatora świadczącego usługi pocztowe o braku zgody na ich przekazanie – w przypadku gdy dane te nie zostały przekazane.

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

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

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

2. Organ Policji, o którym mowa w ust. 1, przekazuje sądowi okręgowemu, o którym mowa w ust. 1, raz na 6 miesięcy, sprawozdanie obejmujące:

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

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

4. W przypadku stwierdzenia przez sąd okręgowy braku podstaw do pozyskania danych telekomunikacyjnych lub pocztowych, zgromadzone dane podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu. Przepis art. 20c ust. 8 stosuje się odpowiednio.

5. O zarządzeniu zniszczenia danych organ Policji jest obowiązany do niezwłocznego poinformowania sądu okręgowego, o którym mowa w ust. 1.

Art. 20cd. 1. W celu zapobiegania lub wykrywania przestępstw Policja może mieć udostępniane dane abonamentowe:

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

– oraz może je przetwarzać.

2. Do udostępniania danych, o których mowa w ust. 1, art. 20c ust. 2–8 stosuje się.”;

4) uchyla się art. 20d;

5) w art. 20da ust. 1 otrzymuje brzmienie:

„1. W celu poszukiwania osób zaginionych Policja może mieć:

1) udostępniane dane, o których mowa w art. 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne,

2) udostępniane dane pocztowe

– oraz może je przetwarzać; przepisy art. 20c ust. 2, 3, 4 i 5 stosuje się.”.

**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:

„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) podsłuchu rozmów prowadzonych przy użyciu środków technicznych;

2) podsłuchu i podglądzie pomieszczeń i osób poza miejscami publicznymi;

3) kontroli treści korespondencji;

4) nadzorze elektronicznym osób, miejsc i przedmiotów oraz środków transportu,

---

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

5) 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 pkt 2 i 4, 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. Czynności, o których mowa w ust. 7, mogą być realizowane przy użyciu środków technicznych niezbędnych do realizacji celów kontroli operacyjnej.”,

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, jednokrotnie wydać postanowienie o przedłużeniu kontroli operacyjnej na czas oznaczony jednak nie dłuższy niż 12 miesięcy.”,

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

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

1) zawierają informacje:

a) w art. 178 Kodeksu postępowania karnego,

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

– Komendant Główny Straży Granicznej lub komendant oddziału Straży Granicznej nakazują ich niezwłoczne, komisyjne i protokolarne zniszczenie;

2) mogą zawierać informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, Komendant Główny Straży Granicznej lub komendant oddziału Straży Granicznej przekazują prokuratorowi te materiały.

16g. W przypadku, o którym mowa w ust. 16f pkt 2, prokurator niezwłocznie po otrzymaniu materiałów, kieruje je do sądu, który zarządził kontrolę operacyjną albo wyraził na nią zgodę w trybie określonym w ust. 4, wraz z wnioskiem o:

1) wyrażenie zgody na ich wykorzystanie w postępowaniu karnym, albo
2) wydanie zarządzenia o ich niezwłocznym, komisyjnym i protokolarnym zniszczeniu.

16h. Sąd wydaje postanowienie o stwierdzeniu dopuszczalności wykorzystania w postępowaniu karnym materiałów mogących zawierać informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu, albo zarządza ich zniszczenie, w terminie 14 dni od dnia złożenia wniosku przez prokuratora.

16i. Na postanowienie sądu o stwierdzeniu dopuszczalności wykorzystania w postępowaniu karnym materiałów mogących zawierać informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, prokuratorowi przysługuje zażalenie. Do zażalenia stosuje się odpowiednio przepisy Kodeksu postępowania karnego.

16j. O wykonaniu zarządzenia dotyczącego zniszczenia informacji stanowiących tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, organ Straży Granicznej jest obowiązany do niezwłocznego poinformowania prokuratora, o którym mowa w ust. 16g.

16k. W sprawach dotyczących kontroli operacyjnej lub udostępnienia danych telekomunikacyjnych i pocztowych albo wykorzystania materiałów z tych czynności w postępowaniu karnym w odniesieniu do posłów, senatorów i Prezydenta Rzeczypospolitej Polskiej postanowienie wydaje Pierwszy Prezes Sądu Najwyższego.”,

f) 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.”,

g) po ust. 19 dodaje się ust. 19a–19c w brzmieniu:

„19a. Dokumentację materiałów zgromadzonych podczas stosowania kontroli operacyjnej, stanowią:

1) nośniki, na których utrwalone zostały treści rozmów telefonicznych lub innych przekazów informacji albo treści korespondencji lub zawartość przesyłek;
2) kopie wykonane z nośników, o których mowa w pkt 1;
3) dokumenty sporządzone na podstawie informacji utrwalonych na nośnikach lub ich kopiach, o których mowa w pkt 1 i 2.

19b. Dokumentacja materiałów zgromadzonych podczas stosowania kontroli operacyjnej podlega protokolarnemu i komisyjnemu zniszczeniu w przypadku, o którym mowa w:

1) ust. 16 – niezwłocznie po przekazaniu materiałów, które dokumentuje, prokuratorowi;
2) ust. 18 – wraz z tymi materiałami.

19c. W przypadku, o którym mowa w ust. 16f, dokumentacja materiałów zgromadzonych podczas stosowania kontroli operacyjnej, o której mowa w ust. 19a:

1) pkt 1 – podlega komisyjnemu, protokolarnemu zniszczeniu wraz z materiałami, które dokumentuje, albo niezwłocznie po przekazaniu tych materiałów prokuratorowi;
2) pkt 2 i 3 – nie jest sporządzana.”,

h) ust. 20 otrzymuje brzmienie:

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

1) sposób dokumentowania kontroli operacyjnej,
2) sposób przechowywania i przekazywania dokumentacji kontroli operacyjnej,
3) szczegółowy sposób dokumentowania materiałów uzyskanych podczas stosowania kontroli operacyjnej oraz sposób przechowywania, przekazywania oraz przetwarzania i niszczenia tych materiałów i dokumentacji,
4) sposób prowadzenia rejestrów, o których mowa w ust. 17a,

5) wzory dokumentów wchodzących w zakres dokumentacji kontroli operacyjnej oraz rejestrów, o których mowa w ust. 17a

– uwzględniając potrzebę zapewnienia niejawnego charakteru podejmowanych czynności i uzyskanych materiałów oraz przejrzystość dokumentacji i rejestrów.”;

2) art. 10b otrzymuje brzmienie:

„Art. 10b. 1. W celu rozpoznawania, zapobiegania, zwalczania, wykrywania albo uzyskania i utrwalenia dowodów przestępstw określonych w art. 1 ust. 2 pkt 4 oraz ust. 2a Straż Graniczna może mieć, gdy inne środki okazały się bezskuteczne albo mogą być nieprzydatne, udostępniane dane:

1) o których mowa w art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243, 827 i 1198), zwane dalej „danymi telekomunikacyjnymi”,
2) identyfikujące podmiot korzystający z usług pocztowych w rozumieniu art. 2 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. poz. 1529) oraz dotyczące faktu, okoliczności świadczenia tych usług lub korzystania z nich, zwane dalej „danymi pocztowymi”

– oraz może je przetwarzać.

2. Podmiot prowadzący działalność telekomunikacyjną lub operator świadczący usługi pocztowe 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,
4) organowi Straży Granicznej wskazanemu w postanowieniu sądu wyrażającym zgodę na pozyskanie danych telekomunikacyjnych lub pocztowych, w przypadkach, o których mowa w art. 10ba ust. 1 lub 3.

3. W przypadku, o którym mowa w ust. 2 pkt 3, udostępnianie danych, o których mowa w ust. 1, odbywa się bez udziału pracowników podmiotu prowadzącego działalność telekomunikacyjną lub operatora świadczącego usługi pocztowe, 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. Materiały uzyskane w wyniku czynności związanych z udostępnieniem danych, o których mowa w ust. 1, które zawierają informacje mające znaczenie dla postępowania karnego, Komendant Główny Straży Granicznej lub komendant oddziału Straży Granicznej przekazują prokuratorowi właściwemu miejscowo lub rzeczowo.

6. Materiały uzyskane w wyniku czynności związanych z udostępnieniem danych, o których mowa w ust. 1, które nie zawierają informacji mających znaczenie dla postępowania karnego, podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu.

7. Dane, o których mowa w ust. 1, przetwarza się przez okres, w którym są one niezbędne do realizacji ustawowych zadań, przy czym, nie rzadziej niż co 3 lata, dokonuje się weryfikacji potrzeby dalszego ich przetwarzania.

8. W przypadku gdy w wyniku weryfikacji ustalono, że dalsze przetwarzanie danych, o których mowa w ust. 1, nie jest niezbędne dla realizacji ustawowych zadań, dane te oraz materiały, o których mowa w ust. 6, niezwłocznie, nie później jednak niż w terminie 14 dni od dnia zakończenia weryfikacji, niszczy komisja powołana przez Komendanta Głównego Straży Granicznej lub komendanta oddziału Straży Granicznej. Z czynności komisji sporządza się protokół.”;

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

„Art.10ba. 1. Jeżeli z materiałów, o których mowa w art. 10b ust. 5 wynika, że zawierają one dane dotyczące bezpośrednio osoby wykonującej zawód lub funkcję, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, Komendant Główny

Straży Granicznej lub komendant oddziału Straży Granicznej przekazują prokuratorowi te materiały.

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

3. Sąd okręgowy wydaje postanowienie o stwierdzeniu dopuszczalności wykorzystania w postępowaniu karnym materiałów zawierających dane, o których mowa ust. 1, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu, albo zarządza ich komisyjne i protokolarne zniszczenie, w terminie 14 dni od dnia złożenia wniosku przez prokuratora.

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

Art. 10bb. 1. Jeżeli z materiałów sprawy wynika, że konieczne jest pozyskanie danych telekomunikacyjnych lub pocztowych dotyczących bezpośrednio osoby wykonującej zawód lub funkcję, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, organ Straży Granicznej występuje do właściwego miejscowo sądu okręgowego z pisemnym wnioskiem o wyrażenie, w drodze postanowienia, zgody na pozyskanie tych danych i ich wykorzystanie w postępowaniu karnym.

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

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

4. Sąd okręgowy wydaje postanowienie w przedmiocie zgody na pozyskanie danych i ich wykorzystanie w postępowaniu karnym gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu.

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

6. W przypadku nieuwzględnienia zażalenia organ Straży Granicznej, który wystąpił o przekazanie danych osób, o których mowa w ust. 1, jest zobowiązany do:

1) wydania zarządzenia o ich niezwłocznym, komisyjnym i protokolarnym zniszczeniu – w przypadku gdy dane te zostały przekazane;
2) poinformowania podmiotu prowadzącego działalność telekomunikacyjną lub operatora świadczącego usługi pocztowe o braku zgody na ich przekazanie – w przypadku gdy dane te nie zostały przekazane.

7. W przypadku gdy zgromadzone zgodnie z ust. 1 lub 3 dane telekomunikacyjne lub pocztowe nie zawierają informacji mających znaczenie dla prowadzonego postępowania karnego, organ Straży Granicznej, który wnioskował o ich udostępnienie, zarządza ich niezwłoczne, komisyjne i protokolarne zniszczenie.

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

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

2. Organ Straży Granicznej, który wystąpił z wnioskiem, przekazuje sądowi okręgowemu, o którym mowa w ust. 1, raz na 6 miesięcy, sprawozdanie obejmujące:

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

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

telekomunikacyjnych lub pocztowych oraz materiałami uzyskanymi w wyniku podjętych czynności.

4. W przypadku stwierdzenia przez sąd okręgowy braku podstaw do pozyskania danych telekomunikacyjnych lub pocztowych, zgromadzone dane podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu. Przepis ust. 10b ust. 8 stosuje się odpowiednio.

5. O zarządzeniu zniszczenia danych organ Straży Granicznej jest obowiązany do niezwłocznego poinformowania sądu okręgowego, o którym mowa w ust. 1.

Art. 10bd. 1. W celu zapobiegania lub wykrywania przestępstw Straż Graniczna może mieć udostępniane dane abonamentowe:

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

– oraz może je przetwarzać.

2. Do udostępniania danych, o których mowa w ust. 1, art. 10b ust. 2–8 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, jeżeli wartość przedmiotu czynu lub uszczuplenie należności publicznoprawnej przekracza w dacie popełnienia czynu zabronionego pięćdziesięciokrotną wysokość minimalnego wynagrodzenia za pracę określonego na podstawie odrębnych przepisów lub przestępstw, o których mowa w art. 2 ust. 1 pkt 14b, wywiad skarbowy, może mieć, gdy inne środki okazały się bezskuteczne albo mogą być nieprzydatne, udostępniane dane:

1) o których mowa w art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243, 827 i 1198), zwane dalej „danymi telekomunikacyjnymi”,

2) identyfikujące podmiot korzystający z usług pocztowych w rozumieniu art. 2 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. poz. 1529) oraz dotyczące faktu, okoliczności świadczenia tych usług lub korzystania z nich, zwane dalej „danymi pocztowymi”

– oraz może je przetwarzać.”,

b) w ust. 2 dodaje się pkt 4 w brzmieniu:

„4) Generalnemu Inspektorowi Kontroli Skarbowej w przypadku postanowienia Sądu Okręgowego w Warszawie wyrażającego zgodę na pozyskanie danych w przypadkach, o których mowa w art. 36bc ust. 1 lub 3.”,

c) uchyla się ust. 4 i 5;

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

„Art. 36ba. 1. Materiały uzyskane w wyniku czynności związanych z udostępnieniem danych, o których mowa w art. 36b ust. 1, które zawierają dowody pozwalające na wszczęcie albo mające znaczenie dla postępowania w sprawie o przestępstwo skarbowe, o którym mowa w art. 36b ust. 1, Generalny Inspektor Kontroli Skarbowej przekazuje Prokuratorowi Generalnemu.

2. Materiały uzyskane w wyniku czynności związanych z udostępnieniem danych, o których mowa w art. 36b ust. 1, które nie zawierają informacji mających znaczenie dla postępowania w sprawie o przestępstwo skarbowe, o którym mowa w art. 36b ust. 1, podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu. Art. 36d ust. 4 pkt 2 stosuje się odpowiednio.

3. Dane, o których mowa w art. 36b ust. 1, przetwarza się przez okres, w którym są one niezbędne do realizacji ustawowych zadań, przy czym, nie rzadziej niż co 3 lata, dokonuje się weryfikacji potrzeby dalszego ich przetwarzania.

4. W przypadku gdy w wyniku weryfikacji ustalono, że dalsze przetwarzanie danych, o których mowa w art. 36b ust. 1, nie jest niezbędne dla realizacji ustawowych zadań, dane te oraz materiały uzyskane w wyniku czynności związanych z udostępnieniem danych telekomunikacyjnych lub pocztowych, podlegają niezwłocznemu, nie później jednak niż w terminie 14 dni od dnia zakończenia

weryfikacji, komisyjnemu i protokolarnemu zniszczeniu. Art. 36d ust. 4 pkt 2 stosuje się odpowiednio.

Art. 36bb. 1. Jeżeli z materiałów uzyskanych na podstawie art. 36b ust. 1 wynika, że zawierają one dane dotyczące bezpośrednio osoby wykonującej zawód lub funkcję, o których mowa w art. 180 § 2 Kodeksu postępowania karnego oraz zawierają dowody pozwalające na wszczęcie albo mające znaczenie dla postępowania w sprawie o przestępstwo lub przestępstwo skarbowe wymienione w art. 36b ust. 1, Generalny Inspektor Kontroli Skarbowej przekazuje Prokuratorowi Generalnemu te materiały.

2. W przypadku, o którym mowa w ust. 1, Prokurator Generalny niezwłocznie po otrzymaniu materiałów kieruje je do Sądu Okręgowego w Warszawie, wraz z wnioskiem o wyrażenie zgody na ich wykorzystanie w postępowaniu w sprawie o przestępstwo lub przestępstwo skarbowe.

3. Sąd Okręgowy w Warszawie wydaje postanowienie o stwierdzeniu dopuszczalności wykorzystania w postępowaniu materiałów zawierających dane, o których mowa ust. 1, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu, albo zarządza ich komisyjne i protokolarne zniszczenie, w terminie 14 dni od dnia złożenia wniosku przez Prokuratora Generalnego.

4. O wykonaniu zarządzenia dotyczącego zniszczenia materiałów zawierających dane, o których mowa w ust. 1, Generalny Inspektor Kontroli Skarbowej jest obowiązany do niezwłocznego poinformowania Sądu Okręgowego w Warszawie.

Art. 36bc. 1. Jeżeli w toku czynności wywiadu skarbowego ustalono, że konieczne jest pozyskanie danych telekomunikacyjnych lub pocztowych dotyczących bezpośrednio osoby wykonującej zawód lub funkcję, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, Generalny Inspektor Kontroli Skarbowej występuje do Sądu Okręgowego w Warszawie z pisemnym wnioskiem o wyrażenie, w drodze postanowienia, zgody na pozyskanie tych danych i ich wykorzystanie w postępowaniu w sprawie o przestępstwo lub przestępstwo skarbowe.

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

3. W przypadkach niecierpiących zwłoki, jeżeli mogłoby to spowodować zagrożenie życia lub zdrowia, możliwość utraty informacji, zatarcie lub zniszczenie dowodów przestępstwa, Generalny Inspektor Kontroli Skarbowej może wystąpić do

podmiotu prowadzącego działalność telekomunikacyjną lub operatora świadczącego usługi pocztowe o przekazanie danych, o których mowa w ust. 1, zwracając się jednocześnie do Sądu Okręgowego w Warszawie z pisemnym wnioskiem o wyrażenie zgody w drodze postanowienia w tej sprawie.

4. Sąd Okręgowy w Warszawie wydaje postanowienie w przedmiocie zgody na pozyskanie danych i ich wykorzystanie w postępowaniu karnym gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu.

5. Na postanowienie sądu o odmowie uwzględnienia wniosku przysługuje zażalenie Generalnemu Inspektorowi Kontroli Skarbowej, który złożył wniosek o wydanie tego postanowienia. Do zażalenia stosuje się odpowiednio przepisy Kodeksu postępowania karnego.

6. W przypadku nieuwzględnienia zażalenia Generalny Inspektor Kontroli Skarbowej, który wystąpił o przekazanie danych osób, o których mowa w ust. 1, jest zobowiązany do:

1) wydania zarządzenia o ich niezwłocznym, komisyjnym i protokolarnym zniszczeniu – w przypadku gdy dane te zostały przekazane;
2) poinformowania podmiotu prowadzącego działalność telekomunikacyjną lub operatora świadczącego usługi pocztowe o braku zgody na ich przekazanie – w przypadku gdy dane te nie zostały przekazane.

7. W przypadku gdy zgromadzone zgodnie z ust. 1 lub 3 dane telekomunikacyjne lub pocztowe nie zawierają informacji mających znaczenie dla prowadzonego postępowania, Generalny Inspektor Kontroli Skarbowej, zarządza ich niezwłoczne, komisyjne i protokolarne zniszczenie.

8. O wydaniu i wykonaniu zarządzenia dotyczącego zniszczenia danych telekomunikacyjnych lub pocztowych, o którym mowa w ust. 6 pkt 1 i ust. 7, Generalny Inspektor Kontroli Skarbowej jest obowiązany do niezwłocznego poinformowania Sądu Okręgowego w Warszawie.

Art. 36bd. 1. Kontrolę nad uzyskiwaniem przez wywiad skarbowy danych telekomunikacyjnych lub pocztowych sprawuje Sąd Okręgowy w Warszawie.

2. Generalny Inspektor Kontroli Skarbowej przekazuje sądowi, o którym mowa w ust. 1, raz na 6 miesięcy, sprawozdanie obejmujące:

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

3. W ramach kontroli, o której mowa w ust. 1, Sąd Okręgowy w Warszawie może zapoznać się z materiałami uzasadniającymi udostępnienie wywiadowi skarbowemu danych telekomunikacyjnych lub pocztowych oraz materiałami uzyskanymi w wyniku podjętych czynności.

4. W przypadku stwierdzenia przez Sąd Okręgowy w Warszawie braku podstaw do pozyskania danych telekomunikacyjnych lub pocztowych, zgromadzone dane podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu. Art. 36d ust. 4 pkt 2 stosuje się odpowiednio.

5. O zarządzeniu zniszczenia danych Generalny Inspektor Kontroli Skarbowej jest obowiązany do niezwłocznego poinformowania Sądu Okręgowego w Warszawie.

Art. 36be. 1. W celu zapobiegania lub wykrywania przestępstw wywiad skarbowy może mieć udostępniane dane abonamentowe:

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

– oraz może je przetwarzać.

2. Do udostępniania danych, o których mowa w ust. 1, art. 36b ust. 2 i art. 36ba ust. 1–4 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) podsłuchu rozmów prowadzonych przy użyciu środków technicznych;

2) podsłuchu i podglądzie pomieszczeń i osób poza miejscami publicznymi;

3) kontroli treści korespondencji;

4) nadzorze elektronicznym osób, miejsc i przedmiotów oraz środków transportu;

5) kontroli zawartości przesyłek.”,

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

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

4b. Czynności, o których mowa w ust. 4, mogą być realizowane przy użyciu środków technicznych niezbędnych do realizacji celów kontroli operacyjnej.”,

d) ust. 7 otrzymuje brzmienie:

„7. W szczególnie 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, jednokrotnie wydać postanowienie o przedłużeniu kontroli operacyjnej, na czas oznaczony jednak nie dłuższy niż 12 miesięcy.”,

e) 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.”,

f) po ust. 14 dodaje się ust. 14a–14c w brzmieniu:

„14a. Dokumentację materiałów zgromadzonych podczas stosowania kontroli operacyjnej, stanowią:

1) nośniki, na których utrwalone zostały treści rozmów telefonicznych lub innych przekazów informacji albo treści korespondencji lub zawartość przesyłek;
2) kopie wykonane z nośników, o których mowa w pkt 1;
3) dokumenty sporządzone na podstawie informacji utrwalonych na nośnikach lub ich kopiach, o których mowa w pkt 1 i 2.

14b. Dokumentacja materiałów zgromadzonych podczas stosowania kontroli operacyjnej podlega protokolarnemu i komisyjnemu zniszczeniu w przypadku, o którym mowa w:

1) art. 36d ust. 1 pkt 2 – niezwłocznie po przekazaniu materiałów, które dokumentuje, prokuratorowi;
2) art. 36d ust. 3 – wraz z tymi materiałami.

14c. W przypadku, o którym mowa w art. 36d ust. 1f, dokumentacja materiałów zgromadzonych podczas stosowania kontroli operacyjnej, o której mowa w ust. 14a:

1) pkt 1 – podlega komisyjnemu, protokolarnemu zniszczeniu wraz z materiałami, które dokumentuje, albo niezwłocznie po przekazaniu tych materiałów prokuratorowi;
2) pkt 2 i 3 – nie jest sporządzana.”,

g) ust. 17 otrzymuje brzmienie:

„17. Minister właściwy do spraw finansów publicznych w porozumieniu z Ministrem Sprawiedliwości oraz ministrem właściwym do spraw łączności, określi, w drodze rozporządzenia:

1) sposób dokumentowania kontroli operacyjnej,
2) sposób przechowywania i przekazywania dokumentacji kontroli operacyjnej,
3) szczegółowy sposób dokumentowania materiałów uzyskanych podczas stosowania kontroli operacyjnej oraz sposób przechowywania, przekazywania oraz przetwarzania i niszczenia tych materiałów i dokumentacji,
4) sposób prowadzenia rejestrów, o których mowa w ust. 13a,

5) wzory dokumentów wchodzących w zakres dokumentacji kontroli operacyjnej oraz rejestrów, o których mowa w ust. 13a

– uwzględniając potrzebę zapewnienia niejawnego charakteru podejmowanych czynności i uzyskanych materiałów oraz przejrzystość dokumentacji i rejestrów.”,

h) dodaje się ust. 18 w brzmieniu:

„18. W sprawach dotyczących kontroli operacyjnej lub udostępnienia danych telekomunikacyjnych i pocztowych albo wykorzystania materiałów z tych czynności w postępowaniu karnym w odniesieniu do posłów, senatorów i Prezydenta Rzeczypospolitej Polskiej postanowienie wydaje Pierwszy Prezes Sądu Najwyższego.”;

4) w art. 36d:

a) w ust. 1 uchyla się pkt 1,

b) ust. 1a otrzymuje brzmienie:

„1a. Wykorzystanie dowodu uzyskanego podczas stosowania kontroli operacyjnej jest dopuszczalne wyłącznie w postępowaniu karnym w sprawie o przestępstwo lub przestępstwo skarbowe, w stosunku do którego jest dopuszczalne stosowanie takiej kontroli przez jakikolwiek uprawniony podmiot, prowadzonym w stosunku do osoby, wobec której zarządzono kontrolę operacyjną.”,

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

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

1) zawierają informacje,

a) w art. 178 Kodeksu postępowania karnego,

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

– Generalny Inspektor Kontroli Skarbowej nakazuje ich niezwłoczne, komisyjne i protokolarne zniszczenie;

2) mogą zawierać informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, Generalny Inspektor Kontroli Skarbowej przekazuje Prokuratorowi Generalnemu te materiały.

1g. W przypadku, o którym mowa w ust. 1f pkt 2, Prokurator Generalny niezwłocznie po otrzymaniu materiałów, kieruje je do Sądu, wraz z wnioskiem o:

1) wyrażenie zgody na ich wykorzystanie w postępowaniu w sprawie o przestępstwo lub przestępstwo skarbowe, albo
2) wydanie zarządzenia o ich niezwłocznym, komisyjnym i protokolarnym zniszczeniu.

1h. Sąd wydaje postanowienie o stwierdzeniu 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, albo zarządza ich zniszczenie, w terminie 14 dni od dnia złożenia wniosku przez Prokuratora Generalnego.

1i. Na postanowienie sądu o stwierdzeniu dopuszczalności wykorzystania w postępowaniu karnym materiałów mogących zawierać informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, Prokuratorowi Generalnemu przysługuje zażalenie. Do zażalenia stosuje się odpowiednio przepisy Kodeksu postępowania karnego.”,

d) 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 podlegają niezwłocznemu, komisyjnemu i protokolarnemu zniszczeniu.”,

e) w ust. 4 pkt 1 i 2 otrzymują brzmienie:

„1) kierownik komórki organizacyjnej urzędu obsługującego ministra właściwego do spraw finansów publicznych właściwej w sprawach wywiadu skarbowego – w odniesieniu do materiałów uzyskanych w wyniku czynności podjętych na podstawie art. 36aa ust. 1;

2) Generalny Inspektor Kontroli Skarbowej – w odniesieniu do materiałów uzyskanych w wyniku czynności podjętych na podstawie art. 36b ust. 1, art. 36c ust. 1 i 2 i art. 36ca ust. 1.”,

f) 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 oraz art. 36ca ust. 1, Generalny Inspektor Kontroli Skarbowej jest obowiązany do niezwłocznego poinformowania 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 i pocztowych, 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”.

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

2) tytuł działu IVa otrzymuje brzmienie:

„Przetwarzanie danych osobowych i telekomunikacyjnych”;

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

---

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.

i pocztowych, 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 i pocztowych 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 popełnionych przez osoby, o których mowa w art. 3 ust. 2 pkt 1, 3, 5 i 6 albo w celu ratowania życia lub zdrowia ludzkiego bądź do wsparcia działań poszukiwawczych i ratowniczych Żandarmeria Wojskowa, może mieć, gdy inne środki okazały się bezskuteczne albo mogą być nieprzydatne, udostępniane dane:

1) o których mowa w art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243, 827 i 1198), zwane dalej „danymi telekomunikacyjnymi”;
2) identyfikujące podmiot korzystający z usług pocztowych w rozumieniu art. 2 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. poz. 1529) oraz dotyczące faktu, okoliczności świadczenia tych usług lub korzystania z nich, zwane dalej „danymi pocztowymi”

– oraz może je przetwarzać.

2. Podmiot prowadzący działalność telekomunikacyjną lub operator świadczący usługi pocztowe 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;
4) organowi Żandarmerii Wojskowej wskazanemu w postanowieniu wojskowego sądu wyrażającym zgodę na pozyskanie danych telekomunikacyjnych lub pocztowych w przypadkach, o których mowa w art. 30c ust. 1 lub 3.

3. W przypadku, o którym mowa w ust. 2 pkt 3, udostępnianie danych, o których mowa w ust. 1, odbywa się bez udziału pracowników podmiotu prowadzącego działalność telekomunikacyjną lub pocztową, lub przy 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. Materiały uzyskane w wyniku czynności związanych z udostępnieniem danych o których mowa w ust. 1, które zawierają informacje mające znaczenie dla postępowania karnego Komendant Główny Żandarmerii Wojskowej lub komendant oddziału Żandarmerii Wojskowej przekazują prokuratorowi wojskowemu właściwemu miejscowo lub rzeczowo.

6. Materiały uzyskane w wyniku czynności związanych z udostępnieniem danych o których mowa w ust. 1, które nie zawierają informacji mających znaczenie dla postępowania karnego, podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu.

7. Dane, o których mowa w ust. 1, przetwarza się przez okres, w którym są one niezbędne do realizacji ustawowych zadań, przy czym, nie rzadziej niż co 3 lata, dokonuje się weryfikacji potrzeby dalszego ich przetwarzania.

8. W przypadku gdy w wyniku weryfikacji ustalono, że dalsze przetwarzanie danych, o których mowa w ust. 1, nie jest niezbędne dla realizacji ustawowych zadań,

dane te oraz materiały, o których mowa w ust. 6, niezwłocznie, nie później jednak niż w terminie 14 dni od dnia zakończenia weryfikacji, niszczy komisja powołana przez Komendanta Głównego Żandarmerii Wojskowej lub komendanta oddziału Żandarmerii Wojskowej. Z czynności komisji sporządza się protokół.”;

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

„Art. 30b. 1. Jeżeli z materiałów, o których mowa w art. 30b ust. 5 wynika, że zawierają one dane dotyczące bezpośrednio osoby wykonującej zawód lub funkcję, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, Komendant Główny Żandarmerii Wojskowej lub komendant oddziału Żandarmerii Wojskowej przekazują prokuratorowi wojskowemu te materiały.

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

3. Wojskowy sąd okręgowy wydaje postanowienie o stwierdzeniu dopuszczalności wykorzystania w postępowaniu karnym materiałów zawierających dane, o których mowa ust. 1, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu, albo zarządza ich komisyjne i protokolarne zniszczenie, w terminie 14 dni od dnia złożenia wniosku przez prokuratora wojskowego.

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

Art. 30c. 1. Jeżeli z materiałów sprawy wynika, że konieczne jest pozyskanie danych telekomunikacyjnych lub pocztowych dotyczących bezpośrednio osoby wykonującej zawód lub funkcję, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, organ Żandarmerii Wojskowej występuje do właściwego miejscowo wojskowego sądu okręgowego z pisemnym wnioskiem o wyrażenie, w drodze postanowienia, zgody na pozyskanie tych danych i ich wykorzystanie w postępowaniu karnym.

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

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

4. Sąd okręgowy wydaje postanowienie w przedmiocie zgody na pozyskanie danych i ich wykorzystanie w postępowaniu karnym gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu.

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

6. W przypadku nieuwzględnienia zażalenia organ Żandarmerii Wojskowej, który wystąpił o przekazanie danych osób, o których mowa w ust. 1, jest zobowiązany do:

1) wydania zarządzenia o ich niezwłocznym, komisyjnym i protokolarnym zniszczeniu – w przypadku gdy dane te zostały przekazane;
2) poinformowania podmiotu prowadzącego działalność telekomunikacyjną lub operatora świadczącego usługi pocztowe o braku zgody na ich przekazanie – w przypadku gdy dane te nie zostały przekazane.

7. W przypadku gdy zgromadzone zgodnie z ust. 1 lub 3 dane telekomunikacyjne lub pocztowe nie zawierają informacji mających znaczenia dla prowadzonego postępowania, organ Żandarmerii Wojskowej który wnioskował o ich udostępnienie, zarządza ich niezwłoczne, komisyjne i protokolarne zniszczenie.

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

Art. 30d. 1. Kontrolę nad uzyskiwaniem przez Żandarmerię Wojskową danych telekomunikacyjnych lub pocztowych 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 sądowi okręgowemu, o którym mowa w ust. 1, raz na 6 miesięcy, sprawozdanie obejmujące:

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

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

4. W przypadku stwierdzenia przez wojskowy sąd okręgowy braku podstaw do pozyskania danych telekomunikacyjnych lub pocztowych, zgromadzone dane podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu. Przepis art. 30 ust. 8 stosuje się odpowiednio.

5. O zarządzeniu zniszczenia danych organ Żandarmerii Wojskowej jest obowiązany do niezwłocznego poinformowania wojskowego sądu okręgowego, o którym mowa w ust. 1.

Art. 30e. 1. W celu zapobiegania lub wykrywania przestępstw Żandarmeria Wojskowa może mieć udostępniane dane abonamentowe:

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

– oraz może je przetwarzać.

2. Do udostępniania danych, o których mowa w ust. 1, art. 30e ust. 2–8 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. 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. 265, art. 269, art. 280–282, art. 285 § 1, art. 286 § 1, 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. 56 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 ustawie karnej polskiej

– 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) podsłuchu rozmów prowadzonych przy użyciu środków technicznych;
2) podsłuchu i podglądzie pomieszczeń i osób poza miejscami publicznymi;
3) kontroli treści korespondencji;
4) nadzorze elektronicznym osób, miejsc i przedmiotów oraz środków transportu;
5) 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 pkt 4, polegające na uzyskiwaniu danych w trybie art. 30.

7b. Czynności, o których mowa w ust. 7, mogą być realizowane przy użyciu środków technicznych niezbędnych do realizacji celów kontroli operacyjnej.”,

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, jednokrotnie wydać postanowienie o przedłużeniu kontroli operacyjnej na czas oznaczony, jednak nie dłuższy niż 12 miesięcy. „,

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

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

1) zawierają informacje, o których mowa:
   a) w art. 178 Kodeksu postępowania karnego,
   b) w art. 178a i w art. 180 § 3 Kodeksu postępowania karnego, z wyłączeniem informacji o przestępstwach, o których mowa w art. 240 § 1 Kodeksu karnego

   – Komendant Główny Żandarmerii Wojskowej lub komendant oddziału Żandarmerii Wojskowej nakazują ich niezwłoczne, komisyjne i protokolarne zniszczenie;

2) mogą zawierać informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, Komendant Główny Żandarmerii Wojskowej lub komendant oddziału Żandarmerii Wojskowej przekazują prokuratorowi wojskowemu te materiały.

16g. W przypadku, o którym mowa w ust. 16f pkt 2, 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) wyrażenie zgody na ich wykorzystanie w postępowaniu karnym, albo
2) wydanie zarządzenia o ich niezwłocznym, komisyjnym i protokolarnym zniszczeniu.

16h. Sąd wydaje postanowienie o stwierdzeniu dopuszczalności wykorzystania w postępowaniu karnym materiałów mogących zawierać informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu, albo zarządza ich zniszczenie, w terminie 14 dni od dnia złożenia wniosku przez prokuratora wojskowego.

16i. Na postanowienie sądu o stwierdzeniu dopuszczalności wykorzystania w postępowaniu karnym materiałów mogących zawierać informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa

w art. 180 § 2 Kodeksu postępowania karnego, prokuratorowi wojskowemu przysługuje zażalenie. Do zażalenia stosuje się odpowiednio przepisy Kodeksu postępowania karnego.

16j. O wykonaniu zarządzenia dotyczącego zniszczenia informacji stanowiących tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, organ Żandarmerii Wojskowej jest obowiązany do niezwłocznego poinformowania prokuratora, o którym mowa w ust. 16g.

16k. W sprawach dotyczących kontroli operacyjnej lub udostępnienia danych telekomunikacyjnych i pocztowych albo wykorzystania materiałów z tych czynności w postępowaniu karnym w odniesieniu do posłów, senatorów i Prezydenta Rzeczypospolitej Polskiej postanowienie wydaje Pierwszy Prezes Sądu Najwyższego.”,

f) 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.”,

g) po ust. 19 dodaje się ust. 19a–19c w brzmieniu:

„19a. Dokumentację materiałów zgromadzonych podczas stosowania kontroli operacyjnej, stanowią:

1) nośniki, na których utrwalone zostały treści rozmów telefonicznych lub innych przekazów informacji albo treści korespondencji lub zawartość przesyłek;
2) kopie wykonane z nośników, o których mowa w pkt 1;
3) dokumenty sporządzone na podstawie informacji utrwalonych na nośnikach i kopiach, o których mowa w pkt 1 i 2.

19b. Dokumentacja materiałów zgromadzonych podczas stosowania kontroli operacyjnej podlega protokolarnemu i komisyjnemu zniszczeniu w przypadku, o którym mowa w:

1) ust. 16 – niezwłocznie po przekazaniu materiałów, które dokumentuje, prokuratorowi wojskowemu;
2) ust. 18 – wraz z tymi materiałami.

19c. W przypadku, o którym mowa w ust. 16f, dokumentacja materiałów zgromadzonych podczas stosowania kontroli operacyjnej, o której mowa w ust. 19a:

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

2) pkt 2 i 3 – nie jest sporządzana.”,

h) ust. 20 otrzymuje brzmienie:

„20. Minister Obrony Narodowej, w porozumieniu z Ministrem Sprawiedliwości oraz ministrem właściwym do spraw gospodarki, określi, w drodze rozporządzenia:

1) sposób dokumentowania kontroli operacyjnej,

2) sposób przechowywania i przekazywania wniosków i zarządzeń,

3) sposób przechowywania, przekazywania oraz przetwarzania i niszczenia materiałów uzyskanych podczas stosowania tej kontroli,

4) wzory dokumentów wchodzących w zakres dokumentacji kontroli operacyjnej oraz rejestrów, o których mowa w ust. 17a

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

**Art. 7.** W ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2010 r. Nr 29, poz. 154, z późn. zm.[4)]) wprowadza się następujące zmiany:

1) w art. 5 ust. 1 otrzymuje brzmienie:

„1. Do zadań ABW należy:

1) rozpoznawanie, zapobieganie i zwalczanie naruszających bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny zagrożeń:

a) godzących w niepodległość, suwerenność, międzynarodową pozycję, nienaruszalność terytorium państwa, w tym szpiegostwa lub innych zagrożeń wywiadowczych ze strony obcych służb, obejmujących również zagrożenia

---

4) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2010 r. Nr 182, poz. 1228 i Nr 238, poz. 1578, z 2011 r. Nr 53, poz. 273, Nr 84, poz. 455, Nr 117, poz. 677 i Nr 230, poz. 1371, z 2012 r. poz. 627 i 908, z 2013 r. poz. 628, 675, 1247 i 1351 oraz z 2014 r. poz. 502, 544, 616, 1055 i 1822.

rozpoznawane metodami radiokontrwywiadu i kontrwywiadu elektronicznego,

b) o charakterze terrorystycznym,

c) wynikających z propagowania totalitarnego ustroju państwa, nawoływania do obalenia przemocą demokratycznego ustroju państwa, a także stosowania przemocy lub groźby bezprawnej, publicznego znieważania lub nawoływania do nienawiści z powodu różnic narodowościowych, etnicznych, rasowych, wyznaniowych albo ze względu na bezwyznaniowość,

d) godzących w bezpieczeństwo ekonomiczne państwa, ze szczególnym uwzględnieniem funkcjonowania spółek, o których mowa w ustawie z dnia 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego do spraw Skarbu Państwa oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych (Dz. U. Nr 65, poz. 404),

e) godzących w bezpieczeństwo informacji niejawnych oraz informacji przetwarzanych w systemach teleinformatycznych o szczególnym znaczeniu dla bezpieczeństwa państwa, niezbędnych do zachowania ciągłości funkcjonowania administracji publicznej lub elementów infrastruktury krytycznej w rozumieniu przepisów o zarządzaniu kryzysowym,

f) związanych z obrotem z zagranicą bez zezwolenia towarami, technologiami i usługami, o których mowa w ustawie z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz. U. z 2013 r. poz. 194);

2) rozpoznawanie, zapobieganie i wykrywanie przestępstw:

a) określonych w art. 117–118a, art. 120, art. 121, art. 127–130, art. 132, art. 134, art. 135 § 1 oraz art. 136 § 1 i 2 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. Nr 88, poz. 553, z późn. zm.), zwanej dalej „Kodeksem karnym”, a także określonych w art. 119, art. 126a, art. 231 § 1, art. 252 § 1, art. 255 § 2, art. 256 oraz art. 257 Kodeksu karnego, jeżeli ich popełnienie zagraża bezpieczeństwu państwa lub jego porządkowi konstytucyjnemu,

b) określonych w art. 165a, art. 255a oraz art. 258 § 2 i 4 Kodeksu karnego, określonych w art. 163 § 1 i 3, art. 164 § 1, art. 165 § 1 i 3, art. 166, art. 167, art. 171, art. 173 § 1 i 3, art. 174 § 1, art. 182 § 1, art. 189, art. 223, art. 224 § 3, art. 224a oraz art. 252 § 2 Kodeksu karnego, jeżeli są przestępstwami o charakterze terrorystycznym, a także określonych w art. 168 i art. 175 Kodeksu karnego jeżeli stanowią przygotowanie do popełnienia przestępstwa o charakterze terrorystycznym,

c) określonych w art. 286 § l i 2, art. 287 § l, art. 296 § 3, art. 297 § l i 2, art. 299 § l, 2, 5 i 6, art. 300 § 1–3 oraz art. 305 § l i 2 Kodeksu karnego, powodujących szkodę majątkową lub skierowanych przeciwko mieniu Skarbu Państwa lub innych państwowych osób prawnych, jeżeli wartość przedmiotu przestępstwa przekracza 16–krotność kwoty, o której mowa w art. 115 § 6 Kodeksu karnego,

d) określonych w art. 54 § 1, art. 55 § 1, art. 56 § 1, art. 63 § 1–5, art. 65 § 1, art. 67 § 1, art. 69a § 1, art. 70 § 1, 2 i 4, art. 73a § 1, art. 76 § 1, art. 86 § 1 i 2, art. 87 § 1 i 2, art. 90 § 1, art. 91 § 1 oraz art. 92 § 1 ustawy z dnia 10 września 1999 r. – Kodeks karny skarbowy (Dz. U. z 2013 r. poz. 186, z późn. zm.), jeżeli ich skutkiem jest narażenie na uszczuplenie albo uszczuplenie należności publicznoprawnych przekraczające 10–krotność wielkiej wartości, o której mowa w art. 53 § 16 Kodeksu karnego skarbowego, lub gdy wartość przedmiotu przestępstwa skarbowego przekracza 10–krotność wielkiej wartości,

e) określonych w art. 265 oraz art. 266 § 2 Kodeksu karnego,

f) określonych w art. 269–269b Kodeksu karnego, godzących w bezpieczeństwo informacji, jeżeli informacje te są przetwarzane w systemach teleinformatycznych o szczególnym znaczeniu dla bezpieczeństwa państwa, niezbędnych do zachowania ciągłości funkcjonowania administracji publicznej lub elementów infrastruktury krytycznej w rozumieniu przepisów o zarządzaniu kryzysowym,

g) określonych w art. 33 ust. 1, 2a i 3 ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa

– oraz ustalanie i ściganie ich sprawców;

3) prowadzenie działań w zakresie profilaktyki kontrwywiadowczej;

4) realizowanie, w zakresie swojej właściwości, zadań związanych z ochroną informacji niejawnych oraz wykonywanie funkcji krajowej władzy bezpieczeństwa w zakresie ochrony informacji niejawnych w stosunkach międzynarodowych;

5) uzyskiwanie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć istotne znaczenie dla bezpieczeństwa wewnętrznego państwa lub jego porządku konstytucyjnego;

6) sporządzanie i wydawanie dokumentów, o których mowa w art. 35 ust. 2–4, a także prowadzenie ich rejestru;

7) prowadzenie centralnej ewidencji zainteresowań operacyjnych służb specjalnych;

8) podejmowanie innych działań określonych w odrębnych ustawach i umowach międzynarodowych.”;

2) w art. 27:

a) ust. 6 otrzymuje brzmienie:

„6. Kontrola operacyjna prowadzona jest niejawnie i polega na:

1) podsłuchu rozmów prowadzonych przy użyciu środków technicznych;

2) podsłuchu i podglądzie pomieszczeń i osób poza miejscami publicznymi;

3) kontroli treści korespondencji;

4) nadzorze elektronicznym osób, miejsc i przedmiotów oraz środków transportu;

5) kontroli zawartości przesyłek.”,

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

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

6b. Czynności, o których mowa w ust. 6, mogą być realizowane przy użyciu środków technicznych niezbędnych do realizacji celów kontroli operacyjnej.”,

c) 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 postanowienia o przedłużeniu kontroli operacyjnej na następujące po sobie okresy, z których żaden nie może trwać dłużej niż 12 miesięcy.”,

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

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

1) zawierają informacje, o których mowa:
   a) w art. 178 Kodeksu postępowania karnego,
   b) w art. 178a i w art. 180 § 3 Kodeksu postępowania karnego, z wyłączeniem informacji o przestępstwach, o których mowa w art. 240 § 1 Kodeksu karnego

   – Szef ABW nakazuje ich niezwłoczne, komisyjne i protokolarne zniszczenie;
2) mogą zawierać informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, Szef ABW przekazuje Prokuratorowi Generalnemu te materiały.

15i. W przypadku, o którym mowa w ust. 15h pkt 2, 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) wyrażenie zgody na ich wykorzystanie w postępowaniu karnym, albo
2) wydanie zarządzenia o ich niezwłocznym, komisyjnym i protokolarnym zniszczeniu.

15j. Sąd wydaje postanowienie o stwierdzeniu dopuszczalności wykorzystania w postępowaniu karnym materiałów mogących zawierać informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie

innego dowodu, albo zarządza ich zniszczenie, w terminie 14 dni od dnia złożenia wniosku przez Prokuratora Generalnego.

15k. Na postanowienie sądu o stwierdzeniu dopuszczalności wykorzystania w postępowaniu karnym materiałów mogących zawierać informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, Prokuratorowi Generalnemu przysługuje zażalenie. Do zażalenia stosuje się odpowiednio przepisy Kodeksu postępowania karnego.

15l. O wykonaniu zarządzenia dotyczącego zniszczenia informacji stanowiących tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, Szef ABW jest obowiązany do niezwłocznego poinformowania Prokuratora Generalnego.

15m. W sprawach dotyczących kontroli operacyjnej lub udostępnienia danych telekomunikacyjnych i pocztowych albo wykorzystania materiałów z tych czynności w postępowaniu karnym w odniesieniu do posłów, senatorów i Prezydenta Rzeczypospolitej Polskiej postanowienie wydaje Pierwszy Prezes Sądu Najwyższego.”,

e) po ust. 16a dodaje się ust. 16b–16f w brzmieniu:

„16b. Sąd, Prokurator Generalny oraz Szef ABW prowadzą odrębne 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. Dokumentację materiałów zgromadzonych podczas stosowania kontroli operacyjnej, stanowią:

1) nośniki, na których utrwalone zostały treści rozmów telefonicznych lub innych przekazów informacji albo treści korespondencji lub zawartość przesyłek;

2) kopie wykonane z nośników, o których mowa w pkt 1;

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

16e. Dokumentacja materiałów zgromadzonych podczas stosowania kontroli operacyjnej podlega protokolarnemu i komisyjnemu zniszczeniu w przypadku, o którym mowa w:

1) ust. 15 – niezwłocznie po przekazaniu materiałów, które dokumentuje, prokuratorowi;
2) ust. 16 – wraz z tymi materiałami.

16f. W przypadku, o którym mowa w ust. 15h, dokumentacja materiałów zgromadzonych podczas stosowania kontroli operacyjnej, o której mowa w ust. 16d:

1) pkt 1 – podlega komisyjnemu, protokolarnemu zniszczeniu wraz z materiałami, które dokumentuje, albo niezwłocznie po przekazaniu tych materiałów prokuratorowi;
2) pkt 2 i 3 – nie jest sporządzana.”,

f) ust. 18 otrzymuje brzmienie:

„18. Prezes Rady Ministrów, określi, w drodze rozporządzenia:

1) sposób dokumentowania kontroli operacyjnej,
2) sposób przechowywania i przekazywania dokumentacji kontroli operacyjnej,
3) szczegółowy sposób dokumentowania materiałów uzyskanych podczas stosowania kontroli operacyjnej oraz sposób przechowywania, przekazywania oraz przetwarzania i niszczenia tych materiałów i dokumentacji,
4) sposób prowadzenia rejestrów, o których mowa w ust. 16b – 16c,
5) wzory dokumentów wchodzących w zakres dokumentacji kontroli operacyjnej oraz rejestrów, o których mowa w ust. 16b – 16c

– uwzględniając potrzebę zapewnienia niejawnego charakteru podejmowanych czynności i uzyskanych materiałów oraz przejrzystość dokumentacji i rejestrów.”;

3) w art. 28:

a) ust. 1 otrzymuje brzmienie:

„1. W celu rozpoznawania zagrożeń lub zapobiegania, zwalczania, wykrywania albo utrwalania dowodów przestępstw ABW może, gdy inne środki okazały się bezskuteczne albo mogą być nieprzydatne, 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) identyfikujące podmiot korzystający z usług pocztowych w rozumieniu art. 2 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. poz. 1529) oraz dotyczące faktu, okoliczności świadczenia tych usług lub korzystania z nich, zwane dalej „danymi pocztowymi”

– niezbędne do realizacji zadań, o których mowa w art. 5 ust. 1 pkt 1, 2 lub 5.”,

b) w ust. 2 dodaje się pkt 4 w brzmieniu:

„4) Szefowi ABW w przypadku postanowienia Sądu Okręgowego w Warszawie wyrażającego zgodę na pozyskanie danych w przypadku, o którym mowa w art. 28b ust. 1 lub 3.”,

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 podmiotu wykonującego działalność telekomunikacyjną lub operatora świadczącego usługi pocztowe, lub przy ich niezbędnym współudziale, jeżeli możliwość taką przewiduje porozumienie zawarte pomiędzy Szefem ABW a tym podmiotem.”,

d) dodaje się ust. 5–8 w brzmieniu:

„5. Materiały uzyskane w wyniku czynności związanych z udostępnieniem danych, o których mowa w ust. 1, które zawierają informacje mające znaczenie dla postępowania karnego Szef ABW przekazuje Prokuratorowi Generalnemu.

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

7. Dane, o których mowa w ust. 1, przetwarza się przez okres, w którym są one niezbędne do realizacji ustawowych zadań, przy czym, nie rzadziej niż co 3 lata, dokonuje się weryfikacji potrzeby dalszego ich przetwarzania.

8. W przypadku gdy w wyniku weryfikacji ustalono, że dalsze przetwarzanie danych, o których mowa w ust. 1, nie jest niezbędne dla realizacji ustawowych zadań, dane te oraz materiały, o których mowa w ust. 6, niezwłocznie nie później

jednak niż w terminie 14 dni od dnia zakończenia weryfikacji niszczy komisja powołana przez Szefa ABW. Z czynności komisji sporządza się protokół.”;

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

„Art. 28a. 1. Jeżeli z materiałów sprawy, o których mowa w art. 28 ust. 5 wynika, że zawierają one dane dotyczące bezpośrednio osoby wykonującej zawód lub funkcję, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, Szef ABW przekazuje Prokuratorowi Generalnemu te materiały.

2. W przypadku, o którym mowa w ust. 1, Prokurator Generalny niezwłocznie po otrzymaniu materiałów kieruje je do Sądu Okręgowego w Warszawie, wraz z wnioskiem o wyrażenie zgody na ich wykorzystanie w postępowaniu karnym.

3. Sąd Okręgowy w Warszawie wydaje postanowienie o stwierdzeniu dopuszczalności wykorzystania w postępowaniu karnym materiałów zawierających dane, o których mowa ust. 1, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu, albo zarządza ich komisyjne i protokolarne zniszczenie, w terminie 14 dni od dnia złożenia wniosku przez Prokuratora Generalnego.

4. O wykonaniu zarządzenia dotyczącego zniszczenia materiałów zawierających dane, o których mowa w ust. 1, Szef ABW jest obowiązany do niezwłocznego poinformowania Sądu Okręgowego w Warszawie.

Art. 28b. 1. Jeżeli z materiałów sprawy wynika, że konieczne jest pozyskanie danych telekomunikacyjnych lub pocztowych dotyczących bezpośrednio osoby wykonującej zawód lub funkcję, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, Szef ABW występuje do Sądu Okręgowego w Warszawie z pisemnym wnioskiem o wyrażenie, w drodze postanowienia, zgody na pozyskanie tych danych i ich wykorzystanie w postępowaniu karnym.

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

3. W przypadkach niecierpiących zwłoki, jeżeli mogłoby to spowodować zagrożenie życia lub zdrowia, możliwość utraty informacji, zatarcie lub zniszczenie dowodów przestępstwa, Szef ABW może wystąpić do podmiotu prowadzącego działalność telekomunikacyjną lub operatora świadczącego usługi pocztowe o przekazanie danych, o których mowa w ust. 1, zwracając się jednocześnie do Sądu

Okręgowego w Warszawie z pisemnym wnioskiem o wyrażenie zgody drodze postanowienia w tej sprawie.

4. Sąd okręgowy wydaje postanowienie w przedmiocie zgody na pozyskanie danych i ich wykorzystanie w postępowaniu karnym gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu.

5. Na postanowienie sądu o odmowie uwzględnienia wniosku przysługuje zażalenie Szefowi ABW. Do zażalenia stosuje się odpowiednio przepisy Kodeksu postępowania karnego.

6. W przypadku nieuwzględnienia zażalenia Szef ABW, który wystąpił o przekazanie danych osób, o których mowa w ust. 1, jest zobowiązany do:

1) wydania zarządzenia o ich niezwłocznym, komisyjnym i protokolarnym zniszczeniu – w przypadku gdy dane te zostały przekazane;
2) poinformowania podmiotu prowadzącego działalność telekomunikacyjną lub operatora świadczącego usługi pocztowe o braku zgody na ich przekazanie – w przypadku gdy dane te nie zostały przekazane.

7. W przypadku gdy zgromadzone zgodnie z ust. 1 lub 3 dane telekomunikacyjne lub pocztowe nie zawierają informacji mających znaczenia dla prowadzonego postępowania, Szef ABW, który wnioskował o ich udostępnienie, zarządza ich niezwłoczne, komisyjne i protokolarne zniszczenie.

8. O wydaniu i wykonaniu zarządzenia dotyczącego zniszczenia danych telekomunikacyjnych lub pocztowych, o których mowa w ust. 6 pkt 1 i ust. 7, Szef ABW, jest obowiązany do niezwłocznego poinformowania Sądu Okręgowego w Warszawie.

Art. 28c. 1. Kontrolę nad uzyskiwaniem przez ABW danych telekomunikacyjnych lub pocztowych sprawuje Sąd Okręgowy w Warszawie.

2. Szef ABW przekazuje sądowi, o którym mowa w ust. 1, raz na 6 miesięcy, sprawozdanie obejmujące:

1) liczbę przypadków pozyskania danych telekomunikacyjnych lub pocztowych oraz ich rodzaj;
2) podstawę prawną pozyskania danych telekomunikacyjnych lub pocztowych;
3) rodzaje przestępstw, w związku z zaistnieniem których wystąpiono o dane telekomunikacyjne lub pocztowe;

4) liczbę przypadków, ze wskazaniem ich podziału na rodzaje spraw, w których wystąpiono o dane telekomunikacyjne lub pocztowe.

4. W ramach kontroli, o której mowa w ust. 1, sąd może zapoznać się z materiałami uzasadniającymi udostępnienie ABW danych telekomunikacyjnych lub pocztowych oraz materiałami uzyskanymi w wyniku podjętych czynności.

5. W przypadku stwierdzenia przez sąd braku podstaw do pozyskania danych telekomunikacyjnych lub pocztowych, zgromadzone dane podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu. Przepis art. 28 ust. 8 stosuje się odpowiednio.

6. O zarządzeniu zniszczenia danych Szef ABW jest obowiązany do niezwłocznego poinformowania sądu, o którym mowa w ust. 1.

Art. 28d. 1. W celu zapobiegania lub wykrywania przestępstw ABW może mieć udostępniane dane abonamentowe:

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

– oraz może je przetwarzać.

2. Do udostępniania danych, o których mowa w ust. 1, art. 28 ust. 2–8 stosuje się.”.

**Art. 8.** 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. 9.** 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. 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, 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) podsłuchu rozmów prowadzonych przy użyciu środków technicznych;
2) podsłuchu i podglądzie pomieszczeń i osób poza miejscami publicznymi;
3) kontroli treści korespondencji;
4) nadzorze elektronicznym osób, miejsc i przedmiotów oraz środków transportu;
5) kontroli zawartości przesyłek.”,

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

„4a. Kontroli operacyjnej nie stanowią czynności, o których mowa w ust. 4 pkt 4, polegające na uzyskiwaniu danych w trybie art. 32.

4b. Czynności, o których mowa w ust. 4, mogą być realizowane przy użyciu środków technicznych niezbędnych do realizacji celów kontroli operacyjnej.”,

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 postanowienia o przedłużeniu kontroli operacyjnej na następujące po sobie okresy, z których żaden nie może trwać dłużej niż 12 miesięcy.”,

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

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

1) zawierają informacje, o których mowa:

a) w art. 178 Kodeksu postępowania karnego,

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

– Szef SKW nakazuje ich niezwłoczne, komisyjne i protokolarne zniszczenie;

2) mogą zawierać informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, Szef SKW przekazuje Prokuratorowi Generalnemu te materiały.

14g. W przypadku, o którym mowa w ust. 14f pkt 2, 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) wyrażenie zgody na ich wykorzystanie w postępowaniu karnym, albo
2) wydanie zarządzenia o ich niezwłocznym, komisyjnym i protokolarnym zniszczeniu.

14h. Sąd wydaje postanowienie o stwierdzeniu dopuszczalności wykorzystania w postępowaniu karnym materiałów mogących zawierać informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu, albo zarządza ich zniszczenie, w terminie 14 dni od dnia złożenia wniosku przez Prokuratora Generalnego.

14i. Na postanowienie sądu o stwierdzeniu dopuszczalności wykorzystania w postępowaniu karnym materiałów mogących zawierać informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, Prokuratorowi Generalnemu przysługuje zażalenie. Do zażalenia stosuje się odpowiednio przepisy Kodeksu postępowania karnego.

14j. O wykonaniu zarządzenia dotyczącego zniszczenia informacji stanowiących tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, Szef SKW jest obowiązany do niezwłocznego poinformowania Prokuratora Generalnego.

14k. W sprawach dotyczących kontroli operacyjnej lub udostępnienia danych telekomunikacyjnych i pocztowych albo wykorzystania materiałów z tych

czynności w postępowaniu karnym w odniesieniu do posłów, senatorów i Prezydenta Rzeczypospolitej Polskiej postanowienie wydaje Pierwszy Prezes Sądu Najwyższego.”,

f) po ust. 15a dodaje się ust. 15b–15e w brzmieniu:

„15b. Szef SKW prowadzi rejestry wniosków, zarządzeń, zgód i postanowień dotyczących kontroli operacyjnej.

15c. Dokumentację materiałów zgromadzonych podczas stosowania kontroli operacyjnej, stanowią:

1) nośniki, na których utrwalone zostały treści rozmów telefonicznych lub innych przekazów informacji albo treści korespondencji lub zawartość przesyłek;
2) kopie wykonane z nośników, o których mowa w pkt 1;
3) dokumenty sporządzone na podstawie informacji utrwalonych na nośnikach i kopiach, o których mowa w pkt 1 i 2.

15d. Dokumentacja materiałów zgromadzonych podczas stosowania kontroli operacyjnej podlega protokolarnemu i komisyjnemu zniszczeniu w przypadku, o którym mowa w:

1) ust. 14 – niezwłocznie po przekazaniu materiałów, które dokumentuje, prokuratorowi;
2) ust. 15 – wraz z tymi materiałami.

15e. W przypadku, o którym mowa w ust. 14f, dokumentacja materiałów zgromadzonych podczas stosowania kontroli operacyjnej, o której mowa w ust. 15c:

1) pkt 1 – podlega komisyjnemu, protokolarnemu zniszczeniu wraz z materiałami, które dokumentuje, albo niezwłocznie po przekazaniu tych materiałów prokuratorowi;
2) pkt 2 i 3 – nie jest sporządzana.”,

g) ust. 16 otrzymuje brzmienie:

„16. Prezes Rady Ministrów, określi, w drodze rozporządzenia:

1) sposób dokumentowania kontroli operacyjnej,
2) sposób przechowywania i przekazywania dokumentacji kontroli operacyjnej,

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

4) sposób prowadzenia rejestrów, o których mowa w ust. 15b,

5) wzory dokumentów wchodzących w zakres dokumentacji kontroli operacyjnej oraz rejestrów, o których mowa w ust. 15b

– uwzględniając potrzebę zapewnienia niejawnego charakteru podejmowanych czynności i uzyskanych materiałów oraz przejrzystość dokumentacji i rejestrów.”;

2) w art. 32:

a) ust. 1 otrzymuje brzmienie:

„1. W celu rozpoznawania, zapobiegania, zwalczania, wykrywania albo utrwalania dowodów przestępstw SKW może, gdy inne środki okazały się bezskuteczne albo mogą być nieprzydatne, uzyskiwać informacje niezbędne do realizacji zadań, o których mowa w art. 5 ust. 1 pkt 1, 7 i 8 oraz ust. 2, w postaci danych:

1) określonych 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), zwanych dalej „danymi telekomunikacyjnymi”;

2) identyfikujących podmiot korzystający z usług pocztowych w rozumieniu art. 2 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. poz. 1529) oraz dotyczących faktu, okoliczności świadczenia tych usług lub korzystania z nich, zwanych dalej „danymi pocztowymi”.”,

b) w ust. 2 w pkt 3 kropkę zastępuje się średnikiem i dodaje się pkt 4 w brzmieniu:

„4) Szefowi SKW w przypadku postanowienia Wojskowego Sądu Okręgowego w Warszawie wyrażającego zgodę na pozyskanie danych w przypadkach, o których mowa w art. 32a ust. 1 lub 3.”,

c) ust. 5 otrzymuje brzmienie:

„5. W przypadku, o którym mowa w ust. 2 pkt 3, udostępnianie danych telekomunikacyjnych lub pocztowych odbywa się bez udziału pracowników podmiotu wykonującego działalność telekomunikacyjną lub operatora świadczącego usługi pocztowe 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 lub pocztowych może nastąpić za pośrednictwem sieci telekomunikacyjnej, jeżeli:”,

e) dodaje się ust. 7–10 w brzmieniu:

„7. Materiały uzyskane w wyniku czynności związanych z udostępnieniem danych o których mowa w ust. 1, które zawierają informacje mające znaczenie dla postępowania karnego Szef SKW przekazuje Prokuratorowi Generalnemu.

8. Materiały uzyskane w wyniku czynności związanych z udostępnieniem danych, o których mowa w ust. 1, które nie zawierają informacji mających znaczenie dla postępowania karnego albo nie są istotne dla bezpieczeństwa państwa, podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu.

9. Dane, o których mowa w ust. 1, przetwarza się przez okres, w którym są one niezbędne do realizacji ustawowych zadań, przy czym, nie rzadziej niż co 3 lata, dokonuje się weryfikacji potrzeby dalszego ich przetwarzania.

10. W przypadku gdy w wyniku weryfikacji ustalono, że dalsze przetwarzanie danych, o których mowa w ust. 1, nie jest niezbędne dla realizacji ustawowych zadań, dane te oraz materiały, o których mowa w ust. 8, niezwłocznie, nie później jednak niż w terminie 14 dni od dnia zakończenia weryfikacji, niszczy komisja powołana przez Szefa SKW. Z czynności komisji sporządza się protokół.”;

3) po art. 32 dodaje się art. 32a–32d w brzmieniu:

„Art. 32a. 1. Jeżeli z materiałów, o których mowa w art. 32 ust. 7 wynika, że zawierają one dane dotyczące bezpośrednio osoby wykonującej zawód lub funkcję, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, Szef SKW przekazuje Prokuratorowi Generalnemu te materiały.

2. W przypadku, o którym mowa w ust. 1, Prokurator Generalny niezwłocznie po otrzymaniu materiałów kieruje je do Wojskowego Sądu Okręgowego w Warszawie, wraz z wnioskiem o wyrażenie zgody na ich wykorzystanie w postępowaniu karnym.

3. Wojskowy Sąd Okręgowy w Warszawie wydaje postanowienie o stwierdzeniu dopuszczalności wykorzystania w postępowaniu karnym materiałów zawierających dane, o których mowa ust. 1, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu, albo zarządza ich komisyjne i protokolarne zniszczenie, w terminie 14 dni od dnia złożenia wniosku przez Prokuratora Generalnego.

4. O wykonaniu zarządzenia dotyczącego zniszczenia materiałów zawierających dane, o których mowa w ust. 1, Szef SKW jest obowiązany do niezwłocznego poinformowania Wojskowego Sądu Okręgowego w Warszawie.

Art. 32b. 1. Jeżeli z materiałów sprawy wynika, że konieczne jest pozyskanie danych telekomunikacyjnych lub pocztowych dotyczących bezpośrednio osoby wykonującej zawód lub funkcję, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, Szef SKW występuje do Wojskowego Sądu Okręgowego w Warszawie z pisemnym wnioskiem o wyrażenie, w drodze postanowienia, zgody na pozyskanie tych danych i ich wykorzystanie w postępowaniu karnym.

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

3. W przypadkach niecierpiących zwłoki, jeżeli mogłoby to spowodować zagrożenie życia lub zdrowia, możliwość utraty informacji, zatarcie lub zniszczenie dowodów przestępstwa, Szef SKW może wystąpić do podmiotu prowadzącego działalność telekomunikacyjną lub operatora świadczącego usługi pocztowe o przekazanie danych, o których mowa w ust. 1, zwracając się jednocześnie do Wojskowego Sądu Okręgowego w Warszawie z pisemnym wnioskiem o wyrażenie zgody w drodze postanowienia w tej sprawie.

4. Wojskowy Sąd Okręgowy w Warszawie wydaje postanowienie w przedmiocie zgody na pozyskanie danych i ich wykorzystanie w postępowaniu karnym gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu.

5. Na postanowienie sądu o odmowie uwzględnienia wniosku przysługuje zażalenie Szefowi SKW. Do zażalenia stosuje się odpowiednio przepisy Kodeksu postępowania karnego.

6. W przypadku nieuwzględnienia zażalenia Szef SKW, który wystąpił przekazanie danych osób, o których mowa w ust. 1, jest zobowiązany do:

1) wydania zarządzenia o ich niezwłocznym, komisyjnym i protokolarnym zniszczeniu – w przypadku gdy dane te zostały przekazane;
2) poinformowania podmiotu prowadzącego działalność telekomunikacyjną lub operatora świadczącego usługi pocztowe o braku zgody na ich przekazanie – w przypadku gdy dane te nie zostały przekazane.

7. W przypadku gdy zgromadzone zgodnie z ust. 1 lub 3 dane telekomunikacyjne lub pocztowe nie zawierają informacji mających znaczenia dla prowadzonego postępowania, Szef SKW zarządza ich niezwłoczne, komisyjne i protokolarne zniszczenie.

8. O wydaniu i wykonaniu zarządzenia dotyczącego zniszczenia danych telekomunikacyjnych lub pocztowych, o którym mowa w ust. 6 pkt 1 i ust. 7, Szef SKW, jest obowiązany do niezwłocznego poinformowania Wojskowego Sądu Okręgowego w Warszawie.

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

2. Szef SKW przekazuje sądowi, o którym mowa w ust. 1, raz na 6 miesięcy, sprawozdanie obejmujące:

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

4. W ramach kontroli, o której mowa w ust. 1, sąd może zapoznać się z materiałami uzasadniającymi udostępnienie SKW danych telekomunikacyjnych lub pocztowych oraz materiałami uzyskanymi w wyniku podjętych czynności.

5. W przypadku stwierdzenia przez sąd braku podstaw do pozyskania danych telekomunikacyjnych lub pocztowych, zgromadzone dane podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu. Przepis art. 32 ust. 10 stosuje się odpowiednio.

6. O zarządzeniu zniszczenia danych Szef SKW jest obowiązany do niezwłocznego poinformowania sądu, o którym mowa w ust. 1.

Art. 32d. 1. W celu zapobiegania lub wykrywania przestępstw SKW może mieć udostępniane dane abonamentowe:

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

2) 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,

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

– oraz może je przetwarzać.

2. Do udostępniania danych, o których mowa w ust. 1, art. 32 ust. 2–10 stosuje się.”.

**Art. 10.** 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. 17:

a) ust. 5 otrzymuje brzmienie:

„5. Kontrola operacyjna prowadzona jest niejawnie i polega na:

1) podsłuchu rozmów prowadzonych przy użyciu środków technicznych;

2) podsłuchu i podglądzie pomieszczeń i osób poza miejscami publicznymi;

3) kontroli treści korespondencji;

4) nadzorze elektronicznym osób, miejsc i przedmiotów oraz środków transportu;

5) kontroli zawartości przesyłek.”,

b) po ust. 5 dodaje się ust. 5a i 5b w brzmieniu:

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

5b. Czynności, o których mowa w ust. 5, mogą być realizowane przy użyciu środków technicznych niezbędnych do realizacji celów kontroli operacyjnej.”,

c) 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 postanowienia o przedłużeniu kontroli

operacyjnej na następujące po sobie okresy, z których żaden nie może trwać dłużej niż 12 miesięcy.”,

d) po ust. 15e dodaje się ust. 15f–15k w brzmieniu:

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

1) zawierają informacje, o których mowa:

a) w art. 178 Kodeksu postępowania karnego,

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

– Szef CBA nakazuje ich niezwłoczne, komisyjne i protokolarne zniszczenie;

2) mogą zawierać informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, Szef CBA przekazuje Prokuratorowi Generalnemu te materiały.

15g. W przypadku, o którym mowa w ust. 15f pkt 2, 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) wyrażenie zgody na ich wykorzystanie w postępowaniu karnym, albo

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

15h. Sąd wydaje postanowienie o stwierdzeniu dopuszczalności wykorzystania w postępowaniu karnym materiałów mogących zawierać informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu, albo zarządza ich zniszczenie, w terminie 14 dni od dnia złożenia wniosku przez Prokuratora Generalnego.

15i. Na postanowienie sądu o stwierdzeniu dopuszczalności wykorzystania w postępowaniu karnym materiałów mogących zawierać informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, Prokuratorowi Generalnemu

przysługuje zażalenie. Do zażalenia stosuje się odpowiednio przepisy Kodeksu postępowania karnego.

15j. O wykonaniu zarządzenia dotyczącego zniszczenia informacji stanowiących tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, Szef CBA jest obowiązany do niezwłocznego poinformowania Prokuratora Generalnego.

15k. W sprawach dotyczących kontroli operacyjnej lub udostępnienia danych telekomunikacyjnych i pocztowych albo wykorzystania materiałów z tych czynności w postępowaniu karnym w odniesieniu do posłów, senatorów i Prezydenta Rzeczypospolitej Polskiej postanowienie wydaje Pierwszy Prezes Sądu Najwyższego.”,

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

„16b. Sąd, Prokurator Generalny i Szef CBA prowadzą rejestry, odpowiednio: postanowień, zarządzeń i wniosków dotyczących kontroli.

16c. Dokumentację materiałów zgromadzonych podczas stosowania kontroli operacyjnej, stanowią:

1) nośniki, na których utrwalone zostały treści rozmów telefonicznych lub innych przekazów informacji albo treści korespondencji lub zawartość przesyłek;
2) kopie wykonane z nośników, o których mowa w pkt 1;
3) dokumenty sporządzone na podstawie informacji utrwalonych na nośnikach i kopiach, o których mowa w pkt 1 i 2.

16d. Dokumentacja materiałów zgromadzonych podczas stosowania kontroli operacyjnej podlega protokolarnemu i komisyjnemu zniszczeniu w przypadku, o którym mowa w:

1) ust. 15 – niezwłocznie po przekazaniu materiałów, które dokumentuje, prokuratorowi;
2) ust. 16 – wraz z tymi materiałami.

16e. W przypadku, o którym mowa w ust. 15f, dokumentacja materiałów zgromadzonych podczas stosowania kontroli operacyjnej, o której mowa w ust. 15c:

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

2) pkt 2 i 3 – nie jest sporządzana.”,

f) ust. 18 otrzymuje brzmienie:

„18. Prezes Rady Ministrów, określi, w drodze rozporządzenia:

1) sposób dokumentowania kontroli operacyjnej,

2) sposób przechowywania i przekazywania dokumentacji kontroli operacyjnej,

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

4) sposób prowadzenia rejestrów, o których mowa w ust. 16b,

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

– uwzględniając potrzebę zapewnienia niejawnego charakteru podejmowanych czynności i uzyskanych materiałów oraz przejrzystość dokumentacji i rejestrów.”;

2) w art. 18:

a) ust. 1 otrzymuje brzmienie:

„1. W celu rozpoznawania, zapobiegania, zwalczania, wykrywania albo utrwalania dowodów przestępstw CBA może, gdy inne środki okazały się bezskuteczne albo mogą być nieprzydatne, uzyskiwać informacje niezbędne do realizacji zadań, o których mowa w art. 2 ust. 1 pkt 1, 2 i 4, w postaci danych:

1) określonych 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), zwanych dalej „danymi telekomunikacyjnymi”,

2) identyfikujących podmiot korzystający z usług pocztowych w rozumieniu art. 2 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. poz. 1529) oraz dotyczących faktu, okoliczności świadczenia tych usług lub korzystania z nich, zwanych dalej „danymi pocztowymi”.”,

b) w ust. 2 dodaje się pkt 4 w brzmieniu:

„4) Szefowi CBA w przypadku postanowienia Sądu Okręgowego w Warszawie wyrażającego zgodę na pozyskanie danych w przypadkach, o których mowa w art. 18b ust. 1 lub 3.”,

c) ust. 3 otrzymuje brzmienie:

„3. W przypadku, o którym mowa w ust. 2 pkt 3, udostępnianie danych telekomunikacyjnych lub pocztowych odbywa się bez udziału pracowników podmiotu prowadzącego działalność telekomunikacyjną lub operatora świadczącego usługi pocztowe przy niezbędnym ich współudziale, jeżeli możliwość taką przewiduje porozumienie zawarte pomiędzy Szefem CBA a tym podmiotem.”,

d) dodaje się ust. 5–8 w brzmieniu:

„5. Materiały uzyskane w wyniku czynności związanych z udostępnieniem danych o których mowa w ust. 1, które zawierają informacje mające znaczenie dla postępowania karnego Szef CBA przekazuje Prokuratorowi Generalnemu.

6. Materiały uzyskane w wyniku czynności związanych z udostępnieniem danych, o których mowa w ust. 1, które nie zawierają informacji mających znaczenie dla postępowania karnego albo nie są istotne dla bezpieczeństwa państwa, podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu.

7. Dane, o których mowa w ust. 1, przetwarza się przez okres, w którym są one niezbędne do realizacji ustawowych zadań, przy czym, nie rzadziej niż co 3 lata, dokonuje się weryfikacji potrzeby dalszego ich przetwarzania.

8. W przypadku gdy w wyniku weryfikacji ustalono, że dalsze przetwarzanie danych, o których mowa w ust. 1, nie jest niezbędne dla realizacji ustawowych zadań, dane te oraz materiały, o których mowa w ust. 6, niezwłocznie, nie później jednak niż w terminie 14 dni od dnia zakończenia weryfikacji, niszczy komisja powołana przez Szefa CBA. Z czynności komisji sporządza się protokół.”;

3) po art. 18 dodaje się art. 18a–18d w brzmieniu:

„Art. 18a. 1. Jeżeli z materiałów, o których mowa w art. 18 ust. 5 wynika, że zawierają one dane dotyczące bezpośrednio osoby wykonującej zawód lub funkcję, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, Szef CBA przekazuje Prokuratorowi Generalnemu te materiały.

2. W przypadku, o którym mowa w ust. 1, prokurator wojskowy niezwłocznie po otrzymaniu materiałów kieruje je do Sądu Okręgowego w Warszawie, wraz z wnioskiem o wyrażenie zgody na ich wykorzystanie w postępowaniu karnym.

3. Sąd Okręgowy w Warszawie wydaje postanowienie o stwierdzeniu dopuszczalności wykorzystania w postępowaniu karnym materiałów zawierających dane, o których mowa ust. 1, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu, albo zarządza ich komisyjne i protokolarne zniszczenie, w terminie 14 dni od dnia złożenia wniosku przez Prokuratora Generalnego.

4. O wykonaniu zarządzenia dotyczącego zniszczenia materiałów zawierających dane, o których mowa w ust. 1, Szef CBA jest obowiązany do niezwłocznego poinformowania Sądu Okręgowego w Warszawie.

Art. 18b. 1. Jeżeli z materiałów sprawy wynika, że konieczne jest pozyskanie danych telekomunikacyjnych lub pocztowych dotyczących bezpośrednio osoby wykonującej zawód lub funkcję, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, Szef CBA występuje do Sądu Okręgowego w Warszawie z pisemnym wnioskiem o wyrażenie, w drodze postanowienia, zgody na pozyskanie tych danych i ich wykorzystanie w postępowaniu karnym.

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

3. W przypadkach niecierpiących zwłoki, jeżeli mogłoby to spowodować zagrożenie życia lub zdrowia, możliwość utraty informacji, zatarcie lub zniszczenie dowodów przestępstwa, Szef CBA może wystąpić do podmiotu prowadzącego działalność telekomunikacyjną lub operatora świadczącego usługi pocztowe o przekazanie danych, o których mowa w ust. 1, zwracając się jednocześnie do Sądu Okręgowego w Warszawie z pisemnym wnioskiem o wyrażenie zgody w drodze postanowienia w tej sprawie.

4. Sąd Okręgowy w Warszawie wydaje postanowienie w przedmiocie zgody na pozyskanie danych i ich wykorzystanie w postępowaniu karnym gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu.

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

6. W przypadku nieuwzględnienia zażalenia Szef CBA, który wystąpił o przekazanie danych osób, o których mowa w ust. 1, jest zobowiązany do:

1) wydania zarządzenia o ich niezwłocznym, komisyjnym i protokolarnym zniszczeniu – w przypadku gdy dane te zostały przekazane;
2) poinformowania podmiotu prowadzącego działalność telekomunikacyjną lub pocztową o braku zgody na ich przekazanie – w przypadku gdy dane te nie zostały przekazane.

7. W przypadku gdy zgromadzone zgodnie z ust. 1 lub 3 dane telekomunikacyjne nie zawierają informacji mających znaczenia dla prowadzonego postępowania, Szef CBA zarządza ich niezwłoczne, komisyjne i protokolarne zniszczenie.

8. O wydaniu i wykonaniu zarządzenia dotyczącego zniszczenia danych telekomunikacyjnych lub pocztowych, o których mowa w ust. 6 pkt 1 i ust. 7, Szef CBA jest obowiązany do niezwłocznego poinformowania Sądu Okręgowego w Warszawie.

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

2. Szef CBA przekazuje sądowi, o którym mowa w ust. 1, raz na 6 miesięcy, sprawozdanie obejmujące:

1) liczbę przypadków pozyskania danych telekomunikacyjnych lub pocztowych oraz ich rodzaj;
2) podstawę prawną pozyskania danych telekomunikacyjnych lub pocztowych;
3) rodzaje przestępstw, w związku z zaistnieniem których wystąpiono o dane telekomunikacyjne lub pocztowe;
4) liczbę przypadków zwalczania korupcji w instytucjach państwowych i samorządzie terytorialnym oraz działalności godzącej w interesy ekonomiczne państwa, w których wystąpiono o dane telekomunikacyjne lub pocztowe.

4. W ramach kontroli, o której mowa w ust. 1, sąd może zapoznać się z materiałami uzasadniającymi udostępnienie CBA danych telekomunikacyjnych lub pocztowych oraz materiałami uzyskanymi w wyniku podjętych czynności.

5. W przypadku stwierdzenia przez sąd braku podstaw do pozyskania danych telekomunikacyjnych lub pocztowych, zgromadzone dane podlegają niezwłocznemu

komisyjnemu i protokolarnemu zniszczeniu. Przepis art. 18 ust. 8 stosuje się odpowiednio.

6. O zarządzeniu zniszczenia danych Szef CBA jest obowiązany do niezwłocznego poinformowania sądu, o którym mowa w ust. 1.

Art. 18d. 1. W celu zapobiegania lub wykrywania przestępstw CBA może mieć udostępniane dane abonamentowe:

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

– oraz może je przetwarzać.

2. Do udostępniania danych, o których mowa w ust. 1, art. 18 ust. 2–8 stosuje się.”.

**Art. 11.** W ustawie z dnia 27 sierpnia 2009 r. o Służbie Celnej (Dz. U. z 2013 r. poz. 1404, z późn. zm.[5)]) 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, z wyłączeniem art. 108 § 2 Kodeksu karnego skarbowego, Służba Celna, może mieć, gdy inne środki okazały się bezskuteczne albo mogą być nieprzydatne, udostępniane dane, 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”, oraz może je przetwarzać.”,

   b) w ust. 2 dodaje się pkt 4 w brzmieniu:

      „4) organowi Służby Celnej wskazanemu w postanowieniu sądu wyrażającym zgodę na pozyskanie danych telekomunikacyjnych w przypadkach, o których mowa w art. 75db ust. 1 lub 3.”,

---

5) 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.

c) ust. 5 otrzymuje brzmienie:

„5. Materiały uzyskane w wyniku czynności związanych z udostępnieniem danych telekomunikacyjnych, które zawierają informacje mające znaczenie dla postępowania karnego lub postępowania karnego skarbowego, Szef Służby Celnej albo dyrektor izby celnej przekazuje prokuratorowi właściwemu ze względu na siedzibę organu przekazującego .”,

d) dodaje się ust. 6–8 w brzmieniu:

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

7. Dane telekomunikacyjne przetwarza się przez okres, w którym są one niezbędne do realizacji ustawowych zadań, przy czym, nie rzadziej niż co 3 lata, dokonuje się weryfikacji potrzeby dalszego ich przetwarzania.

8. W przypadku gdy w wyniku weryfikacji ustalono, że dalsze przetwarzanie danych telekomunikacyjnych nie jest niezbędne dla realizacji ustawowych zadań, dane te oraz materiały, o których mowa w ust. 6, niezwłocznie, nie później jednak niż w terminie 14 dni od dnia zakończenia weryfikacji, niszczy komisja powołana przez Szefa Służby Celnej albo dyrektora izby celnej. Z czynności komisji sporządza się protokół.”;

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

„Art. 75da. 1. Jeżeli z materiałów sprawy, o których mowa w art. 75d ust. 5 wynika, że zawierają one dane dotyczące bezpośrednio osoby wykonującej zawód lub funkcję, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, Szef Służby Celnej albo dyrektor izby celnej przekazuje prokuratorowi te materiały.

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

3. Sąd okręgowy wydaje postanowienie o stwierdzeniu dopuszczalności wykorzystania w postępowaniu karnym lub postępowaniu karnym skarbowym materiałów zawierających dane, o których mowa ust. 1, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego

dowodu, albo zarządza ich komisyjne i protokolarne zniszczenie, w terminie 14 dni od dnia złożenia wniosku przez prokuratora.

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

5. W sprawach dotyczących udostępnienia danych telekomunikacyjnych i pocztowych albo wykorzystania materiałów z tych czynności w postępowaniu karnym w odniesieniu do posłów, senatorów i Prezydenta Rzeczypospolitej Polskiej postanowienie wydaje Pierwszy Prezes Sądu Najwyższego.

Art. 75db. 1. Jeżeli w toku czynności ustalono, że konieczne jest pozyskanie danych telekomunikacyjnych dotyczących bezpośrednio osoby wykonującej zawód lub funkcję, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, Szef Służby Celnej albo dyrektor izby celnej występuje do właściwego miejscowo sądu okręgowego z pisemnym wnioskiem o wyrażenie, w drodze postanowienia, zgody na pozyskanie tych danych i ich wykorzystanie w postępowaniu karnym skarbowym.

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

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

4. Sąd okręgowy wydaje postanowienie w przedmiocie zgody na pozyskanie danych i ich wykorzystanie w postępowaniu karnym gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu.

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

6. W przypadku nieuwzględnienia zażalenia organ Służby Celnej, który wystąpił o przekazanie danych osób, o których mowa w ust. 1, jest zobowiązany do:

1) zarządzenia niezwłocznego, komisyjnego i protokolarnego zniszczenia tych danych – w przypadku gdy dane te zostały przekazane;
2) poinformowania podmiotu prowadzącego działalność telekomunikacyjną o braku zgody na ich przekazanie – w przypadku gdy dane te nie zostały przekazane.

7. W przypadku gdy zgromadzone zgodnie z ust. 1 lub 3 dane telekomunikacyjne nie zawierają informacji mających znaczenia dla prowadzonego postępowania, organ Służby Celnej, który wnioskował o ich udostępnienie, zarządza ich niezwłoczne, komisyjne i protokolarne zniszczenie.

8. O zarządzeniu zniszczenia danych telekomunikacyjnych, o których mowa w ust. 6 pkt 1 i ust. 7, oraz o jego wykonaniu organ Służby Celnej jest obowiązany niezwłocznie poinformować sąd okręgowy.

Art. 75dc. 1. Kontrolę nad uzyskiwaniem przez Służbę Celną danych w zakresie art. 180c oraz art. 180d ustawy – Prawo telekomunikacyjne sprawuje sąd okręgowy właściwy dla siedziby organu Służby Celnej, któremu udostępniono te dane.

2. Organ Służby Celnej, o którym mowa w ust. 1, informuje sąd okręgowy, o którym mowa w ust. 1, o każdym udostepnieniu Służbie Celnej danych telekomunikacyjnych, oraz uzasadnia konieczność pozyskania danych telekomunikacyjnych, wskazując rodzaje przestępstw, w związku z zaistnieniem których wystąpiono o dane telekomunikacyjne.

3. Organ Służby Celnej, o którym mowa w ust. 1, przekazuje sądowi okręgowemu, o którym mowa w ust. 1, raz na 6 miesięcy, sprawozdanie obejmujące:

1) liczbę przypadków pozyskania danych telekomunikacyjnych lub pocztowych oraz ich rodzaj;
2) podstawę prawną pozyskania danych telekomunikacyjnych;
3) rodzaje przestępstw, w związku z zaistnieniem których wystąpiono o dane telekomunikacyjne;
4) liczbę przypadków, w których wystąpiono o dane z podziałem na podstawę prawną przestępstw, w związku zaistnieniem których wystąpiono o dane telekomunikacyjne.

4. W ramach kontroli, o której mowa w ust. 1, sąd okręgowy może zapoznać się z materiałami uzasadniającymi udostępnienie Służbie Celnej danych telekomunikacyjnych oraz materiałami uzyskanymi w wyniku podjętych czynności.

5. W przypadku stwierdzenia przez sąd okręgowy braku podstaw do pozyskania danych telekomunikacyjnych, zgromadzone dane podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu. Przepis art. 75d ust. 8 stosuje się odpowiednio.

6. O zarządzeniu zniszczenia danych organ Służby Celnej jest obowiązany do niezwłocznego poinformowania sądu okręgowego, o którym mowa w ust. 1.

Art. 75dd. 1. W celu zapobiegania lub wykrywania przestępstw Służba Celna może mieć udostępniane dane abonamentowe:

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

– oraz może je przetwarzać.

2. Do udostępniania danych, o których mowa w ust. 1, art. 75d ust. 2–8 stosuje się.”.

**Art. 12.** 1. Do kontroli operacyjnej, która była prowadzona przed dniem wejścia w życie ustawy i nie została zakończona, stosuje się art. 19 ust. 15f–15i ustawy z dnia 6 kwietnia 1990 r. o Policji, art. 9e ust. 16f–16i ustawy z dnia 12 października 1990 r. o Straży Granicznej, art. 36d ust. 1f–1h i 5 ustawy z dnia 28 września 1991 r. o kontroli skarbowej, art. 31 ust. 16f–16i ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 27 ust. 15h–15k ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 31 ust. 14f–14i ustawy z dnia 9 czerwca o 2006 r. Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego i art. 17 ust. 15f–15i ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym, w brzmieniu nadanym niniejszą ustawą.

2. Kontrola operacyjna, 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 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych, w dotychczasowym brzmieniu, która była prowadzona przed dniem wejścia w życie niniejszej ustawy, może być nadal prowadzona nie dłużej niż przez 6 miesięcy od dnia wejścia w życie niniejszej ustawy, chyba że termin jej zakończenia, określony w postanowieniu sądu, upływa wcześniej.

3. W zakresie nieuregulowanym w ust. 1 i 2 do kontroli operacyjnej, która była prowadzona przed dniem wejścia w życie ustawy i nie została zakończona, stosuje się przepisy dotychczasowe.

**Art. 13.** 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 ust. 2, 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. 14.** 1. W terminie 30 dni od dnia wejścia w życie niniejszej ustawy Komendant Główny Policji, Komendant Główny Straży Granicznej, Generalny Inspektor Kontroli Skarbowej, Komendant Główny Żandarmerii Wojskowej, Szef Agencji Bezpieczeństwa Wewnętrznego, Szef Służby Kontrwywiadu Wojskowego oraz Szef Centralnego Biura Antykorupcyjnego nakazują niezwłoczne, komisyjne i protokolarne zniszczenie dokumentacji materiałów zgromadzonych podczas stosowania kontroli operacyjnej przed dniem wejścia w życie niniejszej ustawy.

2. Przepisu ust. 1 nie stosuje się do dokumentacji materiałów, o których mowa w art. 27 ust. 15f ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu.

**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, wszczętych i niezakończonych przed dniem wejścia w życie niniejszej ustawy, oraz do zgromadzonych danych stosuje się przepisy ustaw zmienianych w art. 2–11, w brzmieniu nadanym niniejszą ustawą.

**Art. 16.** Do spraw i postępowań prowadzonych przez Agencję Bezpieczeństwa Wewnętrznego, wszczętych i niezakończonych przed dniem wejścia w życie niniejszej ustawy, stosuje się przepisy dotychczasowe.

**Art. 17.** Dotychczasowe przepisy wykonawcze wydane na podstawie:

1) art. 19 ust. 21 ustawy z dnia 6 kwietnia 1990 r. o Policji zachowują moc do dnia wydania przepisów wykonawczych na podstawie art. 19 ust. 21 tej ustawy w brzmieniu nadanym niniejszą ustawą,
2) art. 9e ust. 20 ustawy z dnia 12 października 1990 r. o Straży Granicznej zachowują moc do dnia wydania przepisów wykonawczych na podstawie art. 9e ust. 20 tej ustawy w brzmieniu nadanym niniejszą ustawą,
3) art. 36c ust. 17 ustawy z dnia 28 września 1991 r. o kontroli skarbowej zachowują moc do dnia wydania przepisów wykonawczych na podstawie art. 36c ust. 17 tej ustawy w brzmieniu nadanym niniejszą ustawą,
4) art. 31 ust. 20 ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych zachowują moc do dnia wydania przepisów wykonawczych na podstawie art. 31 ust. 20 tej ustawy w brzmieniu nadanym niniejszą ustawą,
5) art. 27 ust. 18 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu zachowują moc do dnia wydania przepisów wykonawczych na podstawie art. 27 ust. 18 tej ustawy w brzmieniu nadanym niniejszą ustawą,
6) art. 31 ust. 16 ustawy z dnia 9 czerwca o 2006 r. Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego zachowują moc do dnia wydania przepisów wykonawczych na podstawie art. 31 ust. 16 tej ustawy w brzmieniu nadanym niniejszą ustawą,

7) art. 17 ust. 18 ustawy z dnia 9 czerwca 2006 r. Centralnym Biurze Antykorupcyjnym zachowują moc do dnia wydania przepisów wykonawczych na podstawie art. 17 ust. 18 ustawy tej ustawy w brzmieniu nadanym niniejszą ustawą

– nie dłużej jednak niż przez 12 miesięcy od dnia wejścia w życie niniejszej ustawy.

**Art. 18.** Ustawa wchodzi w życie z dniem 1 stycznia 2016 r.

# U Z A S A D N I E N I E

## 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 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2010 r. Nr 29, poz. 154, z późn. zm.), ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2015 r. poz. 355 i 529), 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 2011 r. Nr 41, poz. 214, 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 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 i 1822) oraz ustawy z dnia 27 sierpnia 2009 r. o Służbie Celnej (Dz. U. z 2013 r. poz. 1404, 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 oraz rozwiązania w innych krajach, w szczególności w krajach członkowskich OECD/UE

Trybunał na wnioski 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 Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego i Centralnym Biurze Antykorupcyjnym.

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 Centralnego Biura Antykorupcyjnego, 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 elementy 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. O ile Trybunał nie kwestionuje ogólnego zakreślenia w ustawie zadań służb ochrony państwa, to już przesłanki niejawnego pozyskiwania informacji o osobach mają być zdefiniowane przez ustawodawcę wyczerpująco. Należy jeszcze raz podkreślić, że na podstawie brzmienia przepisu ustawy jednostka ma wiedzieć, jakie zachowania narażają ją nie tylko na ewentualną odpowiedzialność karną, lecz również umożliwią prowadzenie w stosunku do niej czynności operacyjno-rozpoznawczych, głęboko ingerujących w jej prywatność.

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 (np. „podsłuch rozmów telefonicznych", „podsłuch i podgląd pomieszczeń i osób", „podsłuch techniczny środków łączności przewodowej i radiowej", „nadzór elektroniczny osób, miejsc i przedmiotów oraz środków transportu", „nadzór elektroniczny środków łączności przewodowej lub radiowej"). 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 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. Wreszcie konieczne jest także uregulowanie procedury raportowania z przeprowadzonych w sposób niejawny czynności i środków gwarantujących przekazanie zapisów w stanie nienaruszonym, umożliwiającym ich późniejszą weryfikację. W powyższym zakresie nie jest konstytucyjnie akceptowalne unormowanie istotnych elementów procedury w wewnętrznie obowiązujących aktach normatywnych ustanawianych w ramach struktury organizacyjnej danej służby prowadzącej te czynności.

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 musi 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. Zastosowanie zasady subsydiarności przed wystąpieniem o udostępnienie danych telekomunikacyjnych w przypadku ścigania niektórych przestępstw mogłoby okazać się niemożliwe, a także utrudnić skuteczne ściganie ich sprawców (np. przestępstw popełnionych przy użyciu urządzeń telekomunikacyjnych oraz coraz popularniejszych przestępstw internetowych, gdy nie ma innych czynności, które można wykonać albo wykazać ich nieskuteczność). Podkreślenia wymaga także, że pozyskiwanie danych telekomunikacyjnych nie wiąże się z tak dużą ingerencją w sferę prywatności jednostek i tajemnicę komunikowania się jak kontrola operacyjna, ponieważ nie istnieje prawna możliwość pozyskiwania w tym trybie treści indywidualnych komunikatów przekazywanych za pomocą sieci telekomunikacyjnych.

Z przesłanką subsydiarności wiąże się wprowadzenie proceduralnego wymogu, którym jest kontrola nad niejawnym 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 wskazał, że 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.

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 pozyskanie 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.

Według Trybunału, niejawne pozyskiwanie przez organy władzy publicznej informacji o jednostce wymaga zachowania daleko idących gwarancji proceduralnych.

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 nad procesem 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. 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 dostrzega jednak argumenty za wprowadzeniem kontroli uprzedniej w pewnych wypadkach. W szczególności chodzić może o dostęp do danych telekomunikacyjnych osób wykonujących zawody zaufania publicznego lub jeśli nie ma konieczności pilnego działania służb. 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.

*Rozwiązania w innych krajach, w szczególności w krajach członkowskich OECD/UE*

W Wielkiej Brytanii istnieje wyspecjalizowana kontrola parlamentarna nad służbami specjalnymi (Agencies): Służbą Bezpieczeństwa (Security Service), Tajną Służbą Wywiadowczą (Secret Intelligence Service) oraz Służbą Nasłuchu Radioelektronicznego (Government Communications Headquarters). Kontrola jest sprawowana przez Parlamentarną Komisję ds. Służb Specjalnych (Intelligence and Security Committee). W jej skład wchodzi dziewięciu desygnowanych przez premiera reprezentantów obu izb parlamentu. Kompetencje komisji są jednak ograniczone do bieżącej kontroli wobec służb specjalnych, oceny wydatków przeznaczanych na ich działalność. Komisja jest zobowiązana do składania rocznych raportów ze swej pracy w Izbie Gmin. W pierwszej kolejności komisja składa raport premierowi, który może wyłączyć z niego treści, których ujawnienie mogłoby zagrażać bezpieczeństwu państwa. Kontrola sprawowana przez komisję jest w znacznym stopniu ograniczona, gdyż szefowie poszczególnych służb mogą odmówić udzielenia informacji członkom tego gremium ze względu na bezpieczeństwo państwa. W związku z tym, jej działalność kontrolna nie sięga całości działalności operacyjnej. W kontekście kontroli zewnętrznej nad działalnością operacyjną działa dwóch komisarzy. Są oni powoływani na trzyletnie kadencje przez premiera spośród osób pełniących uprzednio wyższe funkcje sędziowskie i w okresie pełnienia swojej funkcji są całkowicie niezależni od premiera. Każdy z nich składa szefowi gabinetu roczny raport ze swej działalności. Premier decyduje, podobnie jak w przypadku raportu Komisji ds. Służb Specjalnych, które treści nie powinny zostać upublicznione, ponieważ przyniosłoby to szkodę bezpieczeństwu państwa, utrudniło zapobieganie i wykrywanie poważnej przestępczości, godziło w brytyjską gospodarkę lub szkodziło interesom poszczególnych służb. Komisarze różnią się zakresem kontrolowanych czynności operacyjno-rozpoznawczych. Komisarz ds. Kontroli Korespondencji i Stosowania Podsłuchu Telefonicznego (Interception of Communications Commissioner) skupia się na weryfikacji wydawanych przez ministrów zezwoleń na zastosowanie kontroli korespondencji i podsłuchu telefonicznego. Z kolei Komisarz ds. Służb Specjalnych (Intelligence Services Commissioner) odpowiedzialny jest za stałą kontrolę nad wydawanymi przez ministrów zezwoleniami upoważniającymi do ingerencji w nienaruszalność mieszkania. Jest on także

odpowiedzialny za monitorowanie prowadzonej przez funkcjonariuszy służb specjalnych inwigilacji i pracy z osobowymi źródłami informacji. Osobne funkcje kontrolne powierzone zostały Trybunałowi ds. Uprawnień Śledczych (Investigatory Powers Tribunal). Jest to instytucja niezależna od rządu i składa się z wyższych rangą przedstawicieli zawodów prawniczych i sądownictwa. Jej podstawowym zadaniem jest rozpatrywanie skarg obywateli odnoszących się do korzystania przez funkcjonariuszy służb specjalnych z przyznanych im ustawowo uprawnień.

W Danii Krajowa Agencja Informatyczno–Telekomunikacyjna monitoruje spełnienie wymogów, zgodnie z którymi dostawcy sieci i usług łączności elektronicznej muszą dopilnować, aby sprzęt i systemy techniczne pozwoliły Policji na dostęp do informacji o ruchu telekomunikacyjnym.

W przypadku Irlandii wyznaczony sędzia ma prawo do prowadzenia dochodzenia oraz składania sprawozdania w sprawie tego, czy właściwe organy krajowe postępują zgodnie z przepisami prawa.

W Holandii Agencja Komunikacji Radiowej nadzoruje realizację zobowiązań przez dostawców Internetu i usług telefonicznych; organ ds. ochrony danych pełni ogólny nadzór nad przetwarzaniem danych osobowych.

W przypadku Bułgarii Komisja Ochrony Danych Osobowych monitoruje przetwarzanie i przechowywanie danych w celu zapewnienia zgodności z wymogami. Parlamentarna komisja w Zgromadzeniu Narodowym monitoruje procedury udzielania zezwoleń i dostępu do danych telekomunikacyjnych.

**3. Różnice między dotychczasowym a projektowanym stanem prawnym**

Realizując wyrok Trybunału Konstytucyjnego oraz uwzględniając część minimalnych wymagań, jakie łącznie powinny spełniać przepisy regulujące niejawne pozyskiwanie przez władze publiczne w demokratycznym państwie prawa informacji o jednostkach, w projekcie ustawy:

3.1. Określono przesłanki stosowania kontroli operacyjnej i dostępu do danych telekomunikacyjnych.

Trybunał Konstytucyjny zwrócił uwagę na niedookreślony 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". Obowiązujące przepisy nie precyzują, o jakie dokładnie przestępstwa chodzi ani w jakich dokładnie aktach normatywnych mają być 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 projektowanych:

– 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. 5 ust. 1 ustawy o ABW i AW doprecyzowano katalog przestępstw, do których rozpoznawania, zapobiegania i zwalczania uprawniona jest ABW;
– art. 31 ust. 1 ustawy o ŻW wskazano zamknięty katalog przestępstw, w odniesieniu do których może zostać zarządzona kontrola operacyjna.

W zakresie udostępniania danych telekomunikacyjnych doprecyzowano, że dane telekomunikacyjne mogą być udostępniane w celu rozpoznawania, zapobiegania, zwalczania, wykrywania albo uzyskania i utrwalenia dowodów przestępstw:

– ściganych z oskarżenia publicznego albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych – art. 20c ust. 1 ustawy o Policji;
– określonych w art. 1 ust. 2 pkt 4 oraz ust. 2a ustawy o SG – art. 10b ust. 1 tej ustawy;
– skarbowych, jeżeli wartość przedmiotu czynu lub uszczuplenie należności publicznoprawnej przekracza w dacie popełnienia czynu zabronionego

pięćdziesięciokrotną wysokość minimalnego wynagrodzenia za pracę określonego na podstawie odrębnych przepisów lub przestępstw, o których mowa w art. 2 ust. 1 pkt 14b – art. 36b ust. 1 ustawy o kontroli skarbowej;

– popełnionych przez osoby, o których mowa w art. 3 ust. 2 pkt 1, 3, 5 i 6 ustawy o ŻW albo w celu ratowania życia lub zdrowia ludzkiego bądź do wsparcia działań poszukiwawczych i ratowniczych – art. 30 ust. 1 tej ustawy;
– wskazanych w projektowanym brzmieniu art. 5 ust. 1 pkt 1, 2 lub 5 ustawy o ABW i AW – art. 28 ust. 1 tej ustawy;
– wskazanych w art. 5 ust. 1 pkt 1, 7 i 8 oraz ust. 2 ustawy o SKW i SWW – art. 32 ust. 1 tej ustawy;
– wskazanych w art. 2 ust. 1 pkt 1, 2 i 4 ustawy o CBA – art. 18 ust. 1 tej ustawy;
– skarbowych, o których mowa w rozdziale 9 ustawy o SC, z wyłączeniem art. 108 § 2 Kodeksu karnego skarbowego.

Ponadto z zakresu reglamentowanego dostępu do danych telekomunikacyjnych wyłączono dane abonamentowe.

3.2. Określono rodzaje środków niejawnego pozyskiwania informacji.

W aktualnym stanie prawnym 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 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 jednostkach, 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 sposoby prowadzenia kontroli operacyjnej. Zgodnie z projektem, kontrola operacyjna prowadzona jest niejawnie i polega na: podsłuchu rozmów

prowadzonych przy użyciu środków technicznych, podsłuchu i podglądzie pomieszczeń i osób poza miejscami publicznymi, kontroli korespondencji, nadzorze elektronicznym osób, miejsc i przedmiotów oraz środków transportu oraz kontrolowaniu zawartości przesyłek. Ponadto, w celu przejrzystości regulacji, w projekcie zostały enumeratywnie wskazane czynności, które nie stanowią kontroli operacyjnej.

3.3. Określono rodzaj dokumentacji prowadzonej w związku ze stosowaniem kontroli operacyjnej.

Z obowiązujących aktów wykonawczych przeniesiono do materii ustawowej regulację określającą, co stanowi dokumentację materiałów zgromadzonych podczas stosowania kontroli operacyjnej oraz określającą rejestry dokumentacji związanej z jej prowadzeniem. Dokumentację materiałów stanowią: nośniki, na których utrwalone zostały treści rozmów telefonicznych lub innych przekazów informacji albo treści korespondencji lub zawartość przesyłek; kopie wykonane z nośników oraz dokumenty sporządzone na podstawie informacji utrwalonych na nośnikach i kopiach. Natomiast organy uczestniczące w procesie stosowania kontroli operacyjnej będą obowiązane prowadzić rejestry postanowień, pisemnych zgód, wniosków i zarządzeń dotyczących kontroli operacyjnej.

3.4. Określono maksymalny okres prowadzenia kontroli operacyjnej.

W obecnym stanie prawnym przepisy nie przewidują maksymalnego czasu prowadzenia kontroli operacyjnej. Na przykładzie art. 19 ustawy o Policji, kontrolę operacyjną zarządza się na okres nie dłuższy niż 3 miesiące. Niemniej sąd okręgowy może, na pisemny wniosek Komendanta Głównego Policji, Komendanta Centralnego Biura Śledczego Policji albo komendanta wojewódzkiego Policji, złożony po uzyskaniu pisemnej zgody właściwego prokuratora, na okres nie dłuższy niż kolejne 3 miesiące, wydać postanowienie o jednorazowym jej przedłużeniu, 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, sąd okręgowy, na pisemny wniosek Komendanta Głównego Policji, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, może wydać postanowienie o prowadzeniu kontroli operacyjnej przez czas oznaczony również po upływie ww. okresów

Realizując postulat Trybunału, dotyczący sprecyzowania w ustawie maksymalnego czasu prowadzenia niejawnych czynności, po upływie których dalsze ich prowadzenie jest już

niedopuszczalne, ustawodawca 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 wskazał maksymalny okres stosowania kontroli operacyjnej. W projekcie doprecyzowane zostało, 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, również na podstawie postanowienia sądu, prowadzenie kontroli operacyjnej po upływie ww. okresów, jednak nie dłużej niż 12 miesięcy. Maksymalny, więc okres stosowania przez te służby kontroli operacyjnej będzie łącznie wynosił 18 miesięcy.

Ze względu na specyfikę zadań realizowanych przez służby specjalne, ograniczenia takie nie zostały wprowadzone w odniesieniu do kontroli operacyjnej stosowanej przez te służby. W projektowanych art. 27 ust. 9 ustawy o ABW i AW, art. 31 ust. 7 ustawy o SKW i SWW, art. 17 ust. 9 ustawy o CBA, określono, że 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 służby. Przyjęcie takiego rozwiązania w odniesieniu do służb specjalnych jest niezbędne z perspektywy bieżących zagrożeń, m.in. w kontekście przyjmowanego obecnie modus operandi sprawców takich przestępstw jak przestępstwa o charakterze terrorystycznym, sabotaż, czy szpiegostwo, wykorzystujących tzw. „uśpione ogniwo”. 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.

Regulacje prawne zawarte w art. 180a ust.1 pkt 1 ustawy – Prawo telekomunikacyjne przewidują obowiązek dla operatorów publicznej sieci telekomunikacyjnej oraz dostawców

publicznie dostępnych usług telekomunikacyjnych, do 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. Zgodnie ze stanowiskiem reprezentowanym przez służby ochrony państwa, oceny zasadności przechowywania przez okres 12 miesięcy danych telekomunikacyjnych należy dokonać przez pryzmat przydatności możliwości pozyskiwania tych danych i 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 uzasadniając potrzebę 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 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.

3.5. Określono zasady i procedury dotyczące weryfikacji i niszczenia danych telekomunikacyjnych zbędnych dla prowadzonego postępowania.

W celu wykonania orzeczenia Trybunału stwierdzającego niezgodność przepisów ustawy o ABW i AW, ustawy SKW i SWW oraz ustawy CBA, w zakresie w jakim nie przewidują zniszczenia danych telekomunikacyjnych niemających znaczenia dla prowadzonego postępowania, w projekcie ustawy wprowadzono ujednolicone dla wszystkich służb procedury postępowania z materiałami uzyskanymi w wyniku czynności związanych z pozyskaniem tych danych. 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, materiały uzyskane w wyniku czynności związanych z udostępnianiem danych telekomunikacyjnych, które zawierają informacje mające znaczenie dla postępowania karnego lub mogące stanowić dowód w postępowaniu karnym, przekazywane są właściwemu prokuratorowi. Materiały, które nie zawierają takich informacji lub nie mogą stanowić dowodu w postępowaniu karnym, będą podlegać niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu. Jednocześnie, na wzór obecnie obowiązujących regulacji m.in. w art. 20c ust. 7 ustawy o Policji, art. 10b ust. 6 ustawy o SG, przyjęto, że zniszczeniu będą podlegać wszystkie materiały uzyskane w wyniku czynności związanych z udostępnieniem danych telekomunikacyjnych.

Dane będą mogły być przetwarzane przez okres, w którym są one niezbędne do realizacji ustawowych zadań, przy czym nie rzadziej niż co 3 lata dokonywana będzie weryfikacja potrzeby dalszego ich przetwarzania. W przypadku, gdy w wyniku weryfikacji ustalone zostanie, że dalsze przetwarzanie danych telekomunikacyjnych nie jest niezbędne materiały te nie później niż w terminie 14 dni od dnia zakończenia weryfikacji będą podlegać zniszczeniu.

Jednocześnie, pomimo, że Trybunał nie wykluczył możliwości zróżnicowania ochrony prawnej prywatności jednostek z uwagi na ich status obywatelski, poprzez dopuszczalne wprowadzenie 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 dalsze przechowywanie danych cudzoziemców, które są nieprzydane w prowadzonym postępowaniu karnym.

3.6. Określono organy oraz procedurę kontroli pozyskiwania danych telekomunikacyjnych.

W odróżnieniu od procesu udostępniania danych telekomunikacyjnych, obowiązujące przepisy przewidują wzmocniony nadzór prokuratorski i sądowy w odniesieniu do kontroli operacyjnej prowadzonej 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, obowiązujące zasady i procedury związane z wykorzystaniem materiałów w prowadzonych postępowaniach oraz niszczeniem tych materiałów, a skończywszy na obowiązkach informacyjnych wobec Sejmu i Senatu. Realizując wyrok Trybunału, stwierdzający za niezgodne z Konstytucją RP obecne uregulowania, które nie przewidują niezależnej kontroli udostępniania danych telekomunikacyjnych, o których mowa w art. 180c i 180d ustawy – Prawo telekomunikacyjne w projekcie ustawy zaproponowano, aby podmiotem wyznaczonym do kontroli nad uzyskiwaniem 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 kontroli skarbowej, Agencji Bezpieczeństwa Wewnętrznego i Centralnego Biura Antykorupcyjnego oraz Wojskowy Sąd Okręgowy w Warszawie – w odniesieniu do Służby Kontrwywiadu Wojskowego.

Udostępnianie danych telekomunikacyjnych będzie się odbywało z poszanowaniem zasady subsydiarności.

Jednocześnie na uprawnione formacje został nałożony obowiązek przekazywania, raz na 6 miesięcy, sprawozdań obejmujących: liczbę przypadków pozyskania danych telekomunikacyjnych lub pocztowych oraz ich rodzaj; podstawę prawną pozyskania danych; rodzaje przestępstw, w związku z zaistnieniem których wystąpiono o dane; 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 telekomunikacyjnych oraz materiałami uzyskanymi w wyniku podjętych czynności. W przypadku stwierdzenia przez sąd braku podstaw do pozyskania danych telekomunikacyjnych, zgromadzone dane podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu. O zarządzeniu zniszczenia danych formacja jest obowiązana do niezwłocznego poinformowania prokuratora, który skierował materiały do sądu.

Ponadto projekt ustawy przewiduje zobowiązanie prezesów (wojskowych) sądów okręgowych do corocznego przekazywania Ministrowi Sprawiedliwości informacji na temat przetwarzania danych telekomunikacyjnych (z podziałem na liczbę i rodzaj udostępnianych danych) oraz wyników przeprowadzonych kontroli, w terminie do dnia 31 marca roku następującego po roku nią objętym.

Minister Sprawiedliwości został zobowiązany do corocznego przedstawiania Sejmowi i Senatowi zagregowanej informacji na temat przetwarzania danych telekomunikacyjnych oraz wyników przeprowadzonych kontroli, w terminie do dnia 30 czerwca roku następującego po roku nią objętym.

W aktualnym stanie prawnym obowiązek informowania Sejmu i Senatu w odniesieniu do danych dotyczących kontroli operacyjnej prowadzonej przez uprawnione służby, spoczywa na Prokuratorze Generalnym, na podstawie art. 10ea ustawy o prokuraturze. Ponadto, zgodnie z art. 19 ust. 22 ustawy o Policji, minister właściwy do spraw wewnętrznych ma obowiązek przedstawiania Sejmowi i Senatowi informacji o działalności Policji określonej w art. 19 ust. 1–21 (kontrola operacyjna), w tym informacji i danych, o których mowa w art. 20 ust. 3 tej ustawy (tajemnica bankowa i ubezpieczeniowa). Powyższe informacje przedkładane są corocznie, najpóźniej do dnia 30 czerwca roku następnego po roku nią objętym.

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

*W zakresie kontroli operacyjnej:*

Wykonując wyrok Trybunału odnoszący 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–15i ustawy o Policji, art. 9e ust. 16f–16i ustawy o SG, art. 36d ust. 1f–1h ustawy o kontroli skarbowej, art. 31 ust. 16f–16i ustawy o ŻW, art. 27 ust. 15h–15k ustawy o ABW i AW, art. 31 ust. 14f–14i ustawy o SKW i SWW,

art. 17 ust. 15e–15i ustawy o CBA, zaproponowano, aby w przypadku, w którym 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), właściwy organ przekazując je prokuratorowi wskazywał fragmenty mogące je zawierać. Materiały te następnie kierowane będą do sądu, który zarządził kontrolę operacyjną wraz z wnioskiem o: wyrażenie zgody na ich wykorzystanie w postępowaniu karnym albo wydanie zarządzenia o ich niezwłocznym, komisyjnym i protokolarnym zniszczeniu. Sąd wydając postanowienie 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. Na postanowienie sądu o stwierdzeniu dopuszczalności wykorzystania w postępowaniu karnym tych prokuratorowi będzie przysługiwało zażalenie.

O wykonaniu zarządzenia dotyczącego zniszczenia materiałów, właściwy podmiot niezwłocznie informuje sąd okręgowy.

W sytuacji, kiedy będzie zachodzić przypuszczenie, że materiały uzyskane w wyniku kontroli operacyjnej będą zawierać informacje objęte zakazami dowodowymi, o których mowa w art. 178 k.p.k., tj. dotyczących faktów, o których obrońca lub adwokat dowiedział się udzielając porady prawnej lub prowadząc sprawę, albo faktów, o których dowiedział się duchowny przy spowiedzi, proponuje się, aby właściwy organ wnioskujący o zarządzenie kontroli operacyjnej nakazywał niezwłoczne, komisyjne i protokolarne ich zniszczenie. Analogiczne rozwiązanie będzie miało zastosowanie dla objętych zakazami dowodowymi: tajemnicy mediatora oraz o źródle informacji dziennikarza.

*W zakresie udostępniania danych telekomunikacyjnych:*

Osoby, o których mowa w art. 180 § 2 k.p.k, zostały także objęte ochroną prawną w związku z pozyskiwaniem przez służby danych telekomunikacyjnych. W przypadkach, gdy z materiałów zgromadzonych w sprawie będzie wynikać, że pozyskane dane telekomunikacyjne lub pocztowe, mogą zawierać informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 k.p.k., zaproponowano następujące rozwiązania:

Jeżeli z materiałów sprawy, będzie wynikać, że materiały uzyskane w wyniku czynności związanych z udostępnieniem danych telekomunikacyjnych mające znaczenie dla

postępowania karnego lub mogące stanowić dowód w postępowaniu karnym, zawierają dane dotyczące bezpośrednio osoby wykonującej zawód lub funkcję, o których mowa w art. 180 § 2 k.p.k., właściwy organ występujący o ich udostępnienie, przekazując te materiały prokuratorowi, będzie wskazywać fragmenty, które zawierają te dane. Prokurator niezwłocznie po otrzymaniu tych materiałów będzie kierować je do właściwego miejscowo sądu okręgowego, wraz z wnioskiem o wyrażenie zgody na ich wykorzystanie w postępowaniu karnym. Następnie, sąd postanowi o ich dalszym wykorzystaniu, albo zarządzi komisyjne i protokolarne zniszczenie. Analogicznie do kontroli operacyjnej sąd przy wydawaniu postanowienia będzie obowiązany kierować się przesłankami wymienionymi w art. 180 § 2 k.p.k.,

Jeżeli w toku czynności ustalone zostanie, że konieczne jest pozyskanie danych telekomunikacyjnych dotyczących bezpośrednio osoby wykonującej zawód, o którym mowa w art. 180 § 2 k.p.k., uprawniony organ będzie występował do sądu o zgodę na pozyskanie tych danych i wykorzystanie w postępowaniu karnym. W przypadkach niecierpiących zwłoki, jeżeli mogłoby to spowodować zagrożenie życia lub zdrowia, możliwość utraty informacji, zatarcie lub zniszczenie dowodów przestępstwa, uprawniony organ będzie mógł wystąpić do podmiotu prowadzącego działalność telekomunikacyjną o przekazanie danych dotyczących bezpośrednio osoby wykonującej zawód, o którym mowa w art. 180 § 2 k.p.k., zwracając się jednocześnie do właściwego miejscowo sądu okręgowego z wnioskiem o wydanie postanowienia w tej sprawie. Sąd także w tych przypadkach będzie kierował się przesłankami z art. art. 180 § 2 k.p.k.

Na postanowienie sądu wydane w sytuacjach, o których mowa w pkt 2 i 3 będzie przysługiwać zażalenie organowi wnioskującemu. Do zażalenia zastosowanie będą miały odpowiednio przepisy Kodeksu postępowania karnego. W przypadku, gdy sąd nie uwzględni zażalenia, właściwy organ formacji mundurowej, będzie zobowiązany do wydania zarządzenia o ich niezwłocznym, komisyjnym i protokolarnym zniszczeniu – w przypadku gdy dane te zostały przekazane bądź do poinformowania podmiotu prowadzącego działalność telekomunikacyjną o braku zgody na ich przekazanie – w przypadku gdy dane te nie zostały przekazane. W przypadku, gdy zgromadzone dane telekomunikacyjne nie będą zawierać informacji mających znaczenia dla prowadzonego postępowania, właściwy organ formacji mundurowej, który wnioskował o ich udostępnienie, zarządzi ich niezwłoczne, komisyjne i protokolarne zniszczenie. O wydaniu i wykonaniu zarządzenia dotyczącego zniszczenia

danych telekomunikacyjnych, konieczne będzie niezwłoczne poinformowanie właściwego sądu

Powyższe propozycje, zostały wprowadzone odpowiednio w art. 20ca i art. 20cb ustawy o Policji, art. 10ba i 10bb ustawy o SG, art. 36bb i art. 36bc ustawy o kontroli skarbowej, art. 30b i 30c ustawy o ŻW, art. 28a i 28b ustawy o ABW oraz AW, art. 32a i 32b ustawy o SKW oraz SWW, art. 18a i art. 18b ustawy o CBA oraz art. 75da i art. 75db ustawy o SC.

3.8. Udostępnianie danych od operatorów świadczących usługi pocztowe.

Wypracowując kompleksowe rozwiązania dodatkowo, obok danych telekomunikacyjnych, objęty został kontrolą sądową proces udostępniania, od operatorów świadczących usługi pocztowe, na podstawie ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. z 2012 r. poz. 1529), danych identyfikujących podmiot korzystający z usług pocztowych oraz dotyczących faktu, okoliczności świadczenia tych usług lub korzystania z nich, do których uzyskiwania są obecnie uprawnione służby (tj. danych pocztowych). Pomimo, że wyrok TK nie obejmuje swoim zakresem danych uzyskiwanych na podstawie prawa pocztowego, powyższe 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 danych pocztowych zbędnych dla prowadzonego postępowania. Skorelowanie regulacji prawnych w stosunku do obu obszaru danych stanowi rozwiązanie systemowe służące pogłębieniu zaufania obywateli do organów państwowych.

3.9. Kontrola operacyjna oraz udostępnianie danych telekomunikacyjnych i pocztowych w odniesieniu do posłów, senatorów i Prezydenta Rzeczypospolitej Polskiej.

W sprawach dotyczących kontroli operacyjnej lub udostępnienia danych telekomunikacyjnych i pocztowych albo wykorzystania materiałów z tych czynności w postępowaniu karnym w odniesieniu do posłów, senatorów i Prezydenta Rzeczypospolitej Polskiej uznano za konieczne, iż postanowienie to, zamiast sądu okręgowego, będzie wydawał Pierwszy Prezes Sądu Najwyższego.

3.10. Nowelizacja ustawy – Prawo telekomunikacyjne.

W projekcie ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw uchylono 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.

Projekt ustawy przewiduje 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.

3.11. Przepisy przejściowe.

Projekt przewiduje, że do kontroli operacyjnej, która była prowadzona przed dniem wejścia w życie projektowanej ustawy i nie została zakończona stosuje się przepisy w brzmieniu nadanym niniejszą ustawą w odniesieniu do materiałów, w stosunku do których zachodzi przypuszczenie, że zawierają informację o których mowa w art. 178 k.p.k. i art. 180 § 2 k.p.k. W stosunku do kontroli operacyjnej, która była przedłużona po upływie ustawowych okresów jej trwania, będzie ona mogła być nadal prowadzona nie dłużej niż przez 6 miesięcy od dnia wejścia w życie niniejszej ustawy, chyba że termin jej zakończenia, określony w postanowieniu sądu, upływa wcześniej.

Poza powyższymi wyjątkami, kontrola operacyjna rozpoczęta przed dniem wejścia w życie niniejszej ustawy będzie prowadzona na podstawie przepisów dotychczasowych.

Projektowane regulacje zawierają obowiązek dla komendantów i szefów uprawnionych do stosowania kontroli operacyjnej służb nakazania w ciągu 30 dni od daty wejścia w życie niniejszej ustawy niezwłocznego, komisyjnego i protokolarnego zniszczenia dokumentacji

materiałów zgromadzonych podczas stosowania kontroli operacyjnej przed dniem wejścia w życie niniejszej ustawy. Obowiązkowi zniszczenia nie podlegają materiały, które są istotne dla bezpieczeństwa państwa.

**4. Skutki projektowanej ustawy**

Projekt uwzględnia stanowisko Trybunału 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 pocztowych.

Wobec tego podstawowym skutkiem projektu będzie urzeczywistnienie zasad i gwarancji konstytucyjnych. 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.

Proponowana nowelizacja może przyczynić się do wzrostu wydatków budżetowych. Jednak określenie skali tego zjawiska nie jest możliwe, jako że będzie ono zależne od decyzji prezesów sądów okręgowych uprawnionych do przeprowadzania kontroli pozyskiwania przez służby danych telekomunikacyjnych i danych pocztowych.

Ustawa nie będzie miała natomiast skutków dla pozostałych jednostek sektora finansów publicznych, w tym jednostek samorządu terytorialnego.

Projekt oddziaływuje na:

1) sądy okręgowe i wojskowe sądy okręgowe, w zakresie jakim nadaje uprawnienie kontrolne nad uzyskiwaniem przez właściwe służby danych telekomunikacyjnych i pocztowych. W ramach przyznanych uprawnień sądy będą mogły zapoznawać się

z materiałami uzasadniającymi wystąpienia o dane telekomunikacyjne i pocztowe 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 i pocztowych, 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 Telekomunikacji 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.

Koszty wprowadzenia regulacji będą związane z nałożonym na sądy okręgowe zadaniem kontroli pozyskiwania przez uprawnione służby danych telekomunikacyjnych i pocztowych. Jednakże, w chwili obecnej, nie jest możliwe szczegółowe wyliczenie kosztów funkcjonowania takiej kontroli, gdyż prezesi sądów okręgowych mogą podjąć autonomiczne decyzje w zakresie zleconych czynności kontrolnych. Nie przewiduje się zwiększenia kosztów finansowych związanych z wprowadzeniem dodatkowych zadań dla służb.

**5. Założenia podstawowych aktów wykonawczych do ustawy**

Projekt ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (druk 697) przewiduje w art. 1 pkt 1 lit. h, art. 2 pkt 1 lit. h, art. 3 pkt 1 lit. art. 3 pkt 3 lit. h, art. 6 pkt 3 lit. h, art. 7 pkt 1 lit. g, art. 9 pkt 1 lit. g, art. 10 pkt 1 lit. g, delegacje ustawowe do wydania aktów wykonawczych, na podstawie:

1) art. 19 ust. 21 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz.U. z 2015 r. poz. 355, z późn zm.);
2) art. 9e ust. 20 ustawy z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2014 r. poz. 1402, z późn. zm.);
3) art. 36c ust. 17 ustawy z dnia 28 września 1991 r. o kontroli skarbowej (Dz.U. z 2015 r. poz. 553);
4) art. 31 ust. 20 ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. z 2013 r. poz. 568, z późn. zm.);
5) art. 27 ust. 18 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2010 r. Nr 29, poz. 154, z późn. zm.) ;
6) art. 31 ust. 16 ustawy z dnia 9 czerwca o 2006 r. Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. z 2014 r. poz. 253, z późn. zm.);
7) art. 17 ust. 18 ustawy z dnia 9 czerwca 2006 r. Centralnym Biurze Antykorupcyjnym(Dz.U.z 2014 r. poz. 1411, z późn. zm.).

Zgodnie z upoważnieniami, w rozporządzeniach uregulowane zostaną: sposób dokumentowania kontroli operacyjnej, sposób przechowywania i przekazywania dokumentacji kontroli operacyjnej, szczegółowy sposób dokumentowania materiałów uzyskanych podczas stosowania kontroli operacyjnej oraz sposób przechowywania, przekazywania oraz przetwarzania i niszczenia tych materiałów i dokumentacji, sposób prowadzenia rejestrów **oraz** wzory dokumentów wchodzących w zakres dokumentacji kontroli operacyjnej oraz rejestrów. Rozporządzenia mają uwzględniać potrzebę zapewnienia niejawnego charakteru podejmowanych czynności i uzyskanych materiałów oraz przejrzystość dokumentacji i rejestrów.

Konieczność wydania nowych aktów wykonawczych wynika z nadania delegacjom ustawowym nowego brzmienia w związku z przeniesieniem do materii ustawowej wybranych przepisów rozporządzeń, dotyczących dokumentacji materiałów zgromadzonych podczas kontroli operacyjnej oraz prowadzenia przez poszczególne służby rejestrów wniosków i zarządzeń kontroli operacyjnej, która to tematyka powinna być, co do zasady, regulowana ustawą.

Zgodnie z art. 17 projektowanej ustawy obecnie obowiązujące rozporządzenia zachowują moc do dnia wydania nowych aktów, jednak nie dłużej jednak niż przez 12 miesięcy od dnia wejścia w życie niniejszej ustawy.

**6. Konsultacje**

Opinie złożyli:

1) Prokuratoria Generalna Skarbu Państwa – która zgłosiła uwagi dotyczące transparentności danych statystycznych dotyczących czynności operacyjno-rozpoznawczych, materii upoważnienia do wydania aktu wykonawczego i rejestru postanowień, zarządzeń oraz wniosków dotyczących Służby Celnej w zakresie kontroli operacyjnej. W toku prac uwzględniono uwagę o charakterze porządkującym odesłanie;
2) Sąd Najwyższy, który nie zgłosił uwag;
3) Fundacja Panoptykon – która zgłosiła szereg uwag, uzasadniających stwierdzenie, iż ustawa nie wykonuje wyroku Trybunału Konstytucyjnego. Projekt uwzględnia jedną z zasadniczych uwag tj. dotyczącą wprowadzenia zasady subsydiarności w udostępnianiu służbom danych telekomunikacyjnych;
4) Prokurator Generalny – który wskazał na szereg nieścisłości i niekonsekwencji w projekcie ustawy. Do istotnych mankamentów zaliczono brak regulacji dotyczących zażalenia osób zainteresowanych oraz prokuratora na wykorzystanie danych telekomunikacyjnych przez osoby pełniące funkcje, o których mowa w art. 180 § 2 k.p.k. Uwagi dotyczyły także m.in. definicji kontroli operacyjnej, przedłużania kontroli, postępowania w sprawie udostępniania danych telekomunikacyjnych. Uwzględniono uwagi dotyczące zakazów dowodowych oraz przesłanek, jakimi sąd kieruje się wydając zgodę na wykorzystanie danych telekomunikacyjnych oraz uwagę dotyczącą zażalenia prokuratora;
5) Minister Sprawiedliwości – który wskazał na konieczność rozważenia zastąpienia zgody sądu kontrolującego udostępnianie danych telekomunikacyjnych zgodą prokuratora. Wskazano także na konieczność uwzględnienia tajemnicy mediatora w zakresie zakazu dowodowego;
6) Minister Finansów – który wskazał, iż ustawa uniemożliwi kontroli skarbowej skuteczną realizację zadań oraz będzie miała szkodliwy wpływ na ochronę interesów ekonomicznych Skarbu Państwa i przestawił szereg uwag usuwających to zagrożenie;
7) Helsińska Fundacja Praw Człowieka – która wskazała m.in. na nieprecyzyjność przepisów dotyczących katalogu środków kontroli operacyjnej, nadmiernie długi okres, o który można przedłużyć kontrolę operacyjną, brak przesłanek wyrażania zgody na wykorzystanie informacji dotyczących tajemnic zawodowych, niedoskonałość regulacji

dotyczących uzyskiwania danych telekomunikacyjnych (szczególności w zakresie braku poszanowania zasady subsydiarności oraz uprzedniej kontroli sądowej);

8) Komendant Główny Straży Granicznej – który przedstawił 16 uwag szczegółowych dotyczących m.in. okresu przedłużania kontroli operacyjnej, tajemnicy mediatora czy też dotyczących spójności terminologicznej ustawy;
9) Naczelna Rada Adwokacka – która zwróciła uwagę, iż tajemnica adwokacka nie jest dostatecznie chroniona zarówno w zakresie kontroli operacyjnej jak i w zakresie udostępniania danych telekomunikacyjnych;
10) Minister Administracji i Cyfryzacji – który wskazał na konieczność doprecyzowania upoważnienia do określenia wzorów rejestrów;
11) Generalny Inspektor Ochrony Danych Osobowych – który zwrócił uwagę na brak uprzedniej sądowej kontroli nad uzyskiwaniem danych telekomunikacyjnych, brak wskazania adekwatności, niezbędności i celowości uzyskiwania tych danych oraz ryzyko nieuzasadnionego bezterminowego przechowywania danych;
12) Krajowa Rada Sądownictwa – która wskazała na konieczność zapewnienia środków na zwiększone zadania sądów;
13) Szef Agencji Bezpieczeństwa Wewnętrznego – który przedstawił szereg uwag o charakterze porządkującym;
14) Prezes Urzędu Telekomunikacji Elektronicznej – który przedstawił uwagi mające na celu wyjaśnienie wątpliwości terminologicznych oraz legislacyjno-porządkowych;
15) Szef Centralnego Biura Antykorupcyjnego – który wskazał m.in. iż niektóre z przepisów w zakresie ustawy o CBA nie są niezbędne do realizacji wyroku Trybunału Konstytucyjnego; wskazano także, iż decyzja o niszczeniu informacji objętych zakazami dowodowymi powinna należeć do sądu, a nie do szefa służby;
16) Minister Obrony Narodowej – który wskazał na konieczność uzupełnienia niektórych przepisów ustawy w zakresie Żandarmerii Wojskowej.

Ponadto Szef Biura Ochrony Rządu uznał za niemożliwe ustosunkowanie się do przedłożonego projektu ustawy.

**7. Oświadczenie o zgodności z prawem Unii Europejskiej**

Zakres przedmiotowy projektowanej ustawy jest zgodny z prawem Unii Europejskiej.