



SEJM
RZECZYPOSPOLITEJ POLSKIEJ
VIII kadencja

Druk nr 183-A

D O D A T K O W E S P R A W O Z D A N I E
KOMISJI ADMINISTRACJI I SPRAW WEWNĘTRZNYCH

**o poselskim projekcie ustawy o zmianie
ustawy o Policji oraz niektórych innych
ustaw (druk nr 154).**

Sejm na 8. posiedzeniu w dniu 14 stycznia 2016 r. - zgodnie z art. 47 ust.1 regulaminu Sejmu – skierował ponownie projekt ustawy zawarty w druku nr 183 do Komisji Administracji i Spraw Wewnętrznych w celu rozpatrzenia wniosku i poprawek zgłoszonych w drugim czytaniu.

Komisja Administracji i Spraw Wewnętrznych - po rozpatrzeniu wniosku i poprawek na posiedzeniu w dniu 14 stycznia 2016 r.

wnosi:

W y s o k i S e j m raczy następujące poprawki:

1) w art. 1 w pkt 1 po lit. f dodać nową zmianę w brzmieniu:

„...) po ust. 12 dodaje się ust. 12a w brzmieniu:

„12a. Usługodawca świadczący usługi drogą elektroniczną będący mikro lub małym przedsiębiorcą w rozumieniu przepisów ustawy o swobodzie działalności gospodarczej zapewnia warunki techniczne i organizacyjne umożliwiające prowadzenie przez Policję kontroli operacyjnej stosownie do posiadanej infrastruktury.”;

– KP Nowoczesna

– przyjąć

Uwaga: poprawki nr 1, 7, 16, 25, 27, 34 i 42 należy rozpatrywać łącznie.

2) w art. 1 w pkt 1 lit. g nadać brzmienie:

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

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

1) zawierają informacje:

a) o których mowa w art. 178 Kodeksu postępowania karnego,

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

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

2) zawierają 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 te materiały sądowi, który wydał postanowienie w przedmiocie zastosowania kontroli operacyjnej, wraz z wnioskiem o ich wykorzystanie w postępowaniu karnym.

15g. Sąd, niezwłocznie po złożeniu wniosku przez Komendanta Głównego Policji Komendanta CBŚP albo komendanta wojewódzkiego Policji, wydaje postanowienie o dopuszczalności wykorzystania w postępowaniu karnym materiałów mogących zawierać informację stanowiącą tajemnicę związaną z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu, a także zarządza niezwłoczne zniszczenie materiałów, których wykorzystanie w postępowaniu karnym jest niedopuszczalne.

15h. Na postanowienie sądu w przedmiocie dopuszczalności wykorzystania w postępowaniu karnym materiałów mogących zawierać informacje stanowiące tajemnicę związaną z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, Komendantowi Głównemu Policji Komendantowi CBŚP lub komendantowi wojewódzkiemu przysługuje zażalenie. Do zażalenia stosuje się odpowiednio przepisy Kodeksu postępowania karnego.

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

–KP Nowoczesna

– odrzucić

Uwaga: poprawki nr 2, 8, 17, 26, 28, 37 i 43 należy rozpatrywać łącznie.

3) w art. 1 pkt 2 nadać brzmienie:

„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, gdy inne środki okazały się bezskuteczne albo mogą być nieprzydatne, Policja może uzyskać dane:

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

- 2) określone w art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. poz. 1529, z późn. zm.), zwane dalej „danymi pocztowymi”
– oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.
2. Przedsiębiorca telekomunikacyjny, operator pocztowy lub usługodawca świadczący usługi drogą elektroniczną udostępnia nieodpłatnie dane, o których mowa w ust. 1:
 - 1) policjantowi wskazanemu w pisemnym wniosku Komendanta Głównego Policji, Komendanta CBŚP, komendanta wojewódzkiego Policji albo osoby przez nich upoważnionej;
 - 2) na ustne żądanie policjanta posiadającego pisemne upoważnienie osób, o których mowa w pkt 1;
 - 3) za pośrednictwem sieci telekomunikacyjnej policjantowi posiadającemu pisemne upoważnienie osób, o których mowa w pkt 1;
3. W przypadku, o którym mowa w ust. 2 pkt 3, udostępnianie danych, o których mowa w ust. 1, odbywa się bez udziału pracowników przedsiębiorcy telekomunikacyjnego, operatora pocztowego lub usługodawcy świadczącego usługi drogą elektroniczną, lub przy niezbędnym ich udziale, jeżeli możliwość taka jest przewidziana w porozumieniu zawartym pomiędzy Komendantem Głównym Policji a tym podmiotem.
4. Udostępnienie Policji danych, o których mowa w ust. 1, może nastąpić za pośrednictwem sieci telekomunikacyjnej jeżeli:
 - 1) wykorzystywane sieci telekomunikacyjne zapewniają:
 - a) możliwość ustalenia osoby uzyskującej dane, ich rodzaju oraz czasu, w którym zostały uzyskane,
 - b) zabezpieczenie techniczne i organizacyjne uniemożliwiające osobie nieuprawnionej dostęp do danych;
 - 2) jest to uzasadnione specyfiką lub zakresem zadań wykonywanych przez jednostki organizacyjne Policji albo prowadzonych przez nie czynności.
5. Komendant Główny Policji, Komendant CBŚP i komendant wojewódzki Policji prowadzą rejestry wystąpień o uzyskanie danych telekomunikacyjnych, pocztowych i internetowych zawierające informacje identyfikujące jednostkę organizacyjną Policji i funkcjonariusza Policji uzyskującego te dane, ich rodzaj, cel uzyskania oraz czas, w którym zostały uzyskane. Rejestry prowadzi się w formie elektronicznej, z zachowaniem przepisów o ochronie informacji niejawnych.
6. Dane, o których mowa w ust. 1, które mają znaczenie dla postępowania karnego Komendant Główny Policji, Komendant CBŚP albo komendant wojewódzki Policji przekazują prokuratorowi właściwemu miejscowo lub rzeczowo. Prokurator podejmuje decyzję o zakresie i sposobie wykorzystania przekazanych danych.
7. Dane, o których mowa w ust. 1, które nie mają znaczenia dla postępowania karnego, podlegają niezwłocznemu komisijnemu i protokolarnemu zniszczeniu.
8. 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.”;”;

– KP PO

– odrzucić

Uwaga: poprawki nr 3, 4, 6, 9, 10, 12–14, 18–23, 29–31, 35, 36, 38–40, 44–46, 48–54 należy rozpatrywać łącznie.

4) w art. 1 pkt 3 nadać brzmienie:

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

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

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

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

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

3a. W przypadku stwierdzenia przez sąd okręgowy braku podstaw do pozyskania danych telekomunikacyjnych lub pocztowych, zgromadzone dane podlegają niezwłocznemu komisijnemu i protokolarnemu zniszczeniu.

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

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

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

- 1) z wykazu, o którym mowa w art. 179 ust. 9 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;
- 2) o których mowa w art. 161 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne,
- 3) w przypadku użytkownika, który nie jest osobą fizyczną numer zakończenia sieci oraz siedzibę lub miejsce wykonywania działalności gospodarczej, firmę lub nazwę i formę organizacyjną tego użytkownika,
- 4) w przypadku stacjonarnej publicznej sieci telekomunikacyjnej – także nazwę miejscowości oraz ulicy, przy której znajduje się zakończenie sieci, udostępnione użytkownikowi

- oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.
2. Do udostępniania i przetwarzania danych, o których mowa w ust. 1, art. 20c ust. 2–8 stosuje się.”;”;

– KP PO

– odrzucić

5) w art. 1 pkt 3 art. 20ca nadać brzmienie:

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

2. Organ Policji, o którym mowa w ust. 1, przekazuje, z zachowaniem przepisów o ochronie informacji niejawnych, sądowi okręgowemu, o którym mowa w ust. 1, informacje o każdorazowym wystąpieniu o dane, o których mowa w art. 20c ust. 1, na warunkach określonych w art. 20c ust. 2, 3 i 4, a ponadto sporządza i przekazuje, w okresach półrocznych, sprawozdanie obejmujące:

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

2) kwalifikacje prawne czynów, w związku z zaistnieniem których wystąpiono o dane telekomunikacyjne, pocztowe lub internetowe albo informacje o pozyskaniu danych w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych.

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

4. Sąd okręgowy w trybie zarządzenia może wskazać, które z pobranych przez Policję danych były pobrane niezasadnie. Organ Policji jest zobowiązany do niezwłocznego, komisyjnego i protokołarnego zniszczenia materiałów, których wykorzystanie w postępowaniu karnym jest niedopuszczalne. Organ Policji niezwłocznie informuje sąd, o zniszczeniu tych materiałów.

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

– KP Nowoczesna

– odrzucić

Uwaga: poprawki nr 5, 11, 15, 24, 32, 41, 47, 55 należy rozpatrywać łącznie.

6) w art. 1 pkt 5 nadać brzmienie:

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

„1. W celu poszukiwania osób zaginionych Policja może uzyskiwać dane telekomunikacyjne i pocztowe oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą; przepisy art. 20c ust. 2–8 stosuje się.”;”;

– KP PO

– odrzucić

7) w art. 2 w pkt 1 po lit. f dodać nową zmianę w brzmieniu:

„...”) po ust. 13 dodaje się ust. 13a w brzmieniu:

„13a. Usługodawca świadczący usługi drogą elektroniczną będący mikro lub małym przedsiębiorcą w rozumieniu przepisów ustawy o swobodzie działalności gospodarczej zapewnia warunki techniczne i organizacyjne umożliwiające prowadzenie przez Straż Graniczną kontroli operacyjnej stosownie do posiadanej infrastruktury.”;

– KP Nowoczesna

– przyjąć

8) w art. 2 w pkt 1 lit. g nadać brzmienie:

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

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

1) zawierają informacje:

a) o których mowa w art. 178 Kodeksu postępowania karnego,

b) o których mowa 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 nakazuje ich niezwłoczne, komisyjne i protokolarne zniszczenie;

2) zawierają 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 przekazuje te materiały sądowi, który wydał postanowienie w przedmiocie zastosowania kontroli operacyjnej, wraz z wnioskiem o ich wykorzystanie w postępowaniu karnym.

16g. Sąd, niezwłocznie po złożeniu wniosku przez Komendanta Głównego Straży Granicznej lub komendanta oddziału Straży Granicznej, wydaje postanowienie o dopuszczalności wykorzystania w postępowaniu karnym materiałów mogących zawierać informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu, a także zarządza niezwłoczne zniszczenie materiałów, których wykorzystanie w postępowaniu karnym jest niedopuszczalne.

16h. Na postanowienie sądu w przedmiocie dopuszczalności wykorzystania w postępowaniu karnym materiałów mogących zawierać informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, Komendantowi Głównemu Straży Granicznej lub komendantowi oddziału Straży Granicznej przysługuje zażalenie. Do zażalenia stosuje się odpowiednio przepisy Kodeksu postępowania karnego.

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

–KP Nowoczesna

– odrzucić

9) w art. 2 pkt 2 nadać brzmienie:

„2) art. 10b otrzymuje brzmienie:

„Art. 10b. 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, gdy inne środki okazały się bezskuteczne albo mogą być nieprzydatne, Straż Graniczna może uzyskać dane:

- 1) określone w art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243, 827 i 1198), zwane dalej „danymi telekomunikacyjnymi”,
 - 2) określone w art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. poz. 1529, z późn. zm.), zwane dalej „danymi pocztowymi”
– oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.
2. Przedsiębiorca telekomunikacyjny, operator pocztowy lub usługodawca świadczący usługi drogą elektroniczną udostępnia nieodpłatnie dane, o których mowa w ust. 1:
- 1) funkcjonariuszowi wskazanemu w pisemnym wniosku Komendanta Głównego Straży Granicznej lub komendanta oddziału Straży Granicznej albo osoby przez nich upoważnionej,
 - 2) na ustne żądanie funkcjonariusza posiadającego pisemne upoważnienie osób, o których mowa w pkt 1,
 - 3) za pośrednictwem sieci telekomunikacyjnej funkcjonariuszowi posiadającemu pisemne upoważnienie osób, o których mowa w pkt 1,
3. W przypadku, o którym mowa w ust. 2 pkt 3, udostępnianie danych, o których mowa w ust. 1, odbywa się bez udziału pracowników przedsiębiorcy telekomunikacyjnego, operatora pocztowego lub usługodawcy świadczącego usługi drogą elektroniczną lub przy niezbędnym ich udziale, jeżeli możliwość taka jest przewidziana w porozumieniu zawartym pomiędzy Komendantem Głównym Straży Granicznej a tym podmiotem.
4. Udostępnienie Straży Granicznej danych, o których mowa w ust. 1, może nastąpić za pośrednictwem sieci telekomunikacyjnej jeżeli:
- 1) wykorzystywane sieci telekomunikacyjne zapewniają:
 - a) możliwość ustalenia osoby uzyskującej dane, ich rodzaju oraz czasu, w którym zostały uzyskane,
 - b) zabezpieczenie techniczne i organizacyjne uniemożliwiające osobie nieuprawnionej dostęp do danych;
 - 2) jest to uzasadnione specyfiką lub zakresem zadań wykonywanych przez jednostki organizacyjne Straży Granicznej albo prowadzonych przez nie czynności.
5. Komendant Główny Straży Granicznej i komendant oddziału Straży Granicznej prowadzą rejestry wystąpień o uzyskanie danych telekomunikacyjnych, pocztowych i internetowych zawierające informacje identyfikujące jednostkę organizacyjną Straży Granicznej i funkcjonariusza uzyskującego te dane, ich rodzaj, cel uzyskania oraz czas,

w którym zostały uzyskane. Rejestry prowadzi się w formie elektronicznej, z zachowaniem przepisów o ochronie informacji niejawnych.

6. Dane, o których mowa w ust. 1, które mają znaczenie dla postępowania karnego, Komendant Główny Straży Granicznej lub komendant oddziału Straży Granicznej przekazują prokuratorowi właściwemu miejscowo lub rzeczowo. Prokurator podejmuje decyzję o zakresie i sposobie wykorzystania przekazanych danych.
7. Dane, o których mowa w ust. 1, które nie mają znaczenia dla postępowania karnego, podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu.
8. Dane, o których mowa w ust. 1, przetwarzają 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.”;”;

– KP PO

– odrzucić

10) w art. 2 pkt 3 nadać brzmienie:

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

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

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

1) liczbę przypadków pozyskania w okresie sprawozdawczym danych telekomunikacyjnych i pocztowych oraz rodzaj tych danych;

2) kwalifikacje prawne czynów w związku z zaistnieniem których wystąpiono o dane telekomunikacyjne i pocztowe.

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

3a. W przypadku stwierdzenia przez sąd okręgowy braku podstaw do pozyskania danych telekomunikacyjnych lub pocztowych, zgromadzone dane podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu.

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

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

Art. 10bb. 1. W celu zapobiegania lub wykrywania przestępstw Straż Graniczna może uzyskiwać dane:

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

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

- 3) w przypadku użytkownika, który nie jest osobą fizyczną: numer zakończenia sieci oraz siedzibę lub miejsce wykonywania działalności gospodarczej, firmę lub nazwę i formę organizacyjną tego użytkownika,
 - 4) w przypadku stacjonarnej publicznej sieci telekomunikacyjnej – także nazwę miejscowości oraz ulicy, przy której znajduje się zakończenie sieci, udostępnione użytkownikowi
– oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.
2. Do udostępniania i przetwarzania danych, o których mowa w ust. 1, art. 10b ust. 2–8 stosuje się.”.”;

– KP PO

– odrzucić

11) w art. 2 w pkt 3 art. 10ba nadać brzmienie:

- „Art. 10ba. 1. Kontrolę nad uzyskiwaniem przez Komendanta Głównego Straży Granicznej lub komendanta oddziału Straży Granicznej danych telekomunikacyjnych, pocztowych lub internetowych sprawuje sąd okręgowy właściwy dla siedziby organu Straży Granicznej, któremu udostępniono te dane.
2. Organ Straży Granicznej, o którym mowa w ust. 1, przekazuje, z zachowaniem przepisów o ochronie informacji niejawnych, sądowi okręgowemu, o którym mowa w ust. 1, informacje o każdorazowym wystąpieniu o dane, o których mowa w art. 10b ust. 1, na warunkach określonych w art. 10b ust. 2, 3 i 4, a ponadto sporządza i przekazuje, w okresach półrocznych, sprawozdanie obejmujące:
- 1) liczbę przypadków pozyskania w okresie sprawozdawczym danych telekomunikacyjnych lub pocztowych oraz rodzaj tych danych;
 - 2) kwalifikacje prawne czynów, w związku z zaistnieniem których wystąpiono o dane telekomunikacyjne, pocztowe lub internetowe albo informacje o pozyskaniu danych w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych.
3. W ramach kontroli, o której mowa w ust. 1, sąd okręgowy może zapoznać się z materiałami uzasadniającymi udostępnienie Straży Granicznej danych telekomunikacyjnych lub pocztowych.
4. Sąd okręgowy w trybie zarządzenia może wskazać, które z pobranych przez Straż Graniczną danych były pobrane niezasadnie. Organ Straży Granicznej jest zobowiązany do niezwłocznego, komisyjnego i protokolarnego zniszczenia materiałów, których wykorzystanie w postępowaniu karnym jest niedopuszczalne. Organ Straży Granicznej niezwłocznie informuje sąd, o zniszczeniu tych materiałów.
5. Kontroli, o której mowa w ust. 1, nie podlega uzyskiwanie danych na podstawie art. 10bb ust. 1.”;

– KP Nowoczesna

– odrzucić

12) w art. 3 w pkt 1 lit. a nadać brzmienie:

„a) ust. 1 otrzymuje brzmienie:

- „1. W celu rozpoznawania, zapobiegania, zwalczania, wykrywania albo uzyskania i utrwalenia dowodów przestępstw skarbowych lub przestępstw, o których mowa w art. 2 ust. 1 pkt 14b i art. 36c ust. 1 pkt 3, gdy inne środki okazały się

bezszykowne albo mogą być nieprzydatne, wywiad skarbowy może uzyskać dane:

- 1) określone w art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243, 827 i 1198), zwane dalej „danymi telekomunikacyjnymi”,
 - 2) określone w art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. poz. 1529, z późn. zm.), zwane dalej „danymi pocztowymi”
- oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.”;”;

– KP PO

– odrzucić

13) w art. 3 w pkt 1 lit. g nadać brzmienie:

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

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

– KP PO

– odrzucić

14) w art. 3 pkt 2 nadać brzmienie:

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

- „Art. 36ba. 1. Kontrolę nad uzyskiwaniem przez wywiad skarbowy danych telekomunikacyjnych i pocztowych sprawuje Sąd Okręgowy w Warszawie, zwany dalej „Sądem”.
2. Generalny Inspektor Kontroli Skarbowej przekazuje Sądowi, w okresach półrocznych, sprawozdanie obejmujące:
- 1) liczbę przypadków pozyskania w okresie sprawozdawczym danych telekomunikacyjnych i pocztowych oraz rodzaj tych danych;
 - 2) kwalifikacje prawne czynów, w związku z zaistnieniem których wystąpiono o dane telekomunikacyjne i pocztowe.
3. W ramach kontroli, o której mowa w ust. 1, Sąd może zapoznać się z materiałami uzasadniającymi udostępnienie wywiadowi skarbowemu danych telekomunikacyjnych i pocztowych oraz materiałami uzyskanymi w wyniku podjętych czynności.
- 3a. W przypadku stwierdzenia przez Sąd braku podstaw do pozyskania danych telekomunikacyjnych lub pocztowych, zgromadzone dane podlegają niezwłocznemu komisijnemu i protokolarnemu zniszczeniu.
4. Sąd informuje Generalnego Inspektora Kontroli Skarbowej o wyniku kontroli w terminie 30 dni od jej zakończenia.
5. Kontroli, o której mowa w ust. 1, nie podlega uzyskiwanie danych na podstawie art. 36bb ust. 1.

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

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

- 2) o których mowa w art. 161 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne,
 - 3) w przypadku użytkownika, który nie jest osobą fizyczną numer zakończenia sieci oraz siedzibę lub miejsce wykonywania działalności gospodarczej, firmę lub nazwę i formę organizacyjną tego użytkownika,
 - 4) w przypadku stacjonarnej publicznej sieci telekomunikacyjnej – także nazwę miejscowości oraz ulicy, przy której znajduje się zakończenie sieci, udostępnione użytkownikowi
– oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.
2. Do udostępniania i przetwarzania danych, o których mowa w ust. 1, art. 36b ust. 2, 3, 6 i 7 oraz art. 36d ust. 1 stosuje się.”;”;

– KP PO

– odrzucić

15) w art. 3 w pkt 2 art. 36ba nadać brzmienie:

- „Art. 36ba. 1. Kontrolę nad uzyskiwaniem przez wywiad skarbowy danych telekomunikacyjnych, pocztowych i internetowych sprawuje sąd okręgowy w Warszawie zwany dalej „Sądem”.
2. Generalny Inspektor Kontroli Skarbowej przekazuje Sądowi, informacje o każdorazowym wystąpieniu o informacje, o których mowa w art. 36b ust. 1, na warunkach określonych w art. 36b ust. 2, 3, 6 i 7, a ponadto sporządza i przekazuje, w okresach półrocznych, sprawozdanie obejmujące:
 - 1) liczbę przypadków pozyskania w okresie sprawozdawczym danych telekomunikacyjnych lub pocztowych oraz rodzaj tych danych;
 - 2) kwalifikacje prawne czynów, w związku z zaistnieniem których wystąpiono o dane telekomunikacyjne, pocztowe lub internetowe albo informacje o pozyskaniu danych w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych.
 3. W ramach kontroli, o której mowa w ust. 1, sąd okręgowy może zapoznać się z materiałami uzasadniającymi udostępnienie wywiadowi skarbowemu danych telekomunikacyjnych lub pocztowych.
 4. Sąd okręgowy w trybie zarządzenia może wskazać, które z pobranych przez wywiad skarbowy danych były pobrane niezasadnie. Organ skarbowy jest zobowiązany do niezwłocznego, komisyjnego i protokolarnego zniszczenia materiałów, których wykorzystanie w postępowaniu karnym jest niedopuszczalne. Organ skarbowy niezwłocznie informuje sąd, o zniszczeniu tych materiałów.
 5. Kontroli, o której mowa w ust. 1, nie podlega uzyskiwanie danych na podstawie art. 36bb ust. 1.”;

– KP Nowoczesna

– odrzucić

16) w art. 3 w pkt 3 po lit. e dodać nową zmianę w brzmieniu:

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

„10a. Usługodawca świadczący usługi drogą elektroniczną będący mikro lub małym przedsiębiorcą w rozumieniu przepisów ustawy o swobodzie działalności gospodarczej zapewnia warunki techniczne i organizacyjne umożliwiające prowadzenie przez wywiad skarbowy kontroli operacyjnej stosownie do posiadanej infrastruktury.”;”;

– **KP Nowoczesna**

– **przyjąć**

17) w art. 3 w pkt 4 lit. b nadać brzmienie:

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

„1f. W przypadku, gdy materiały, o których mowa w ust. 1:

1) zawierają informacje:

a) o których mowa w art. 178 Kodeksu postępowania karnego,

b) o których mowa 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) zawierają informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, Generalny Inspektor Kontroli Skarbowej przekazuje te materiały sądowi, który wydał postanowienie w przedmiocie zastosowania kontroli operacyjnej, wraz z wnioskiem o ich wykorzystanie w postępowaniu karnym.

1g. Sąd, niezwłocznie po złożeniu wniosku przez Generalnego Inspektora Kontroli Skarbowej wydaje postanowienie o dopuszczalności wykorzystania w postępowaniu karnym materiałów mogących zawierać informację stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu, a także zarządza niezwłoczne zniszczenie materiałów, których wykorzystanie w postępowaniu karnym jest niedopuszczalne.

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

– **KP Nowoczesna**

– **odrzuć**

18) art. 4 nadać brzmienie:

„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.) 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.”;”;

– KP PO

– odrzucić

19) w art. 5 pkt 1 nadać brzmienie:

„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.”;”;

– KP PO

– odrzucić

20) w art. 5 pkt 2 nadać brzmienie:

„2) tytuł działu IVa otrzymuje brzmienie:

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

– KP PO

– odrzucić

21) w art. 5 pkt 3 nadać brzmienie:

„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 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.”;”;

– KP PO

– odrzucić

22) w art. 6 pkt 1 nadać brzmienie:

„1) art. 30 otrzymuje brzmienie:

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

- 1) określone w art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243, 827 i 1198), zwane dalej „danymi telekomunikacyjnymi”;
- 2) określone w art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. poz. 1529, z późn. zm.), zwane dalej „danymi pocztowymi”;
– oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.
2. Przedsiębiorca telekomunikacyjny, operator pocztowy lub usługodawca świadczący usługi drogą elektroniczną udostępnia nieodpłatnie dane, o których mowa w ust. 1:
 - 1) żołnierzowi Żandarmerii Wojskowej wskazanemu w pisemnym wniosku Komendanta Głównego Żandarmerii Wojskowej lub komendanta oddziału Żandarmerii Wojskowej albo osoby przez nich upoważnionej;
 - 2) na ustne żądanie żołnierza Żandarmerii Wojskowej posiadającego pisemne upoważnienie osób, o których mowa w pkt 1;
 - 3) za pośrednictwem sieci telekomunikacyjnej żołnierzowi Żandarmerii Wojskowej posiadającemu pisemne upoważnienie osób, o których mowa w pkt 1;
3. W przypadku, o którym mowa w ust. 2 pkt 3, udostępnianie danych, o których mowa w ust. 1, odbywa się bez udziału pracowników przedsiębiorcy telekomunikacyjnego, operatora pocztowego lub usługodawcy świadczącego usługi drogą elektroniczną, lub przy ich niezbędnym współdziałaniu, jeżeli możliwość taką przewiduje porozumienie zawarte pomiędzy Komendantem Głównym Żandarmerii Wojskowej a tym podmiotem.
4. Udostępnienie Żandarmerii Wojskowej danych, o których mowa w ust. 1, może nastąpić za pośrednictwem sieci telekomunikacyjnej, jeżeli:
 - 1) wykorzystywane sieci i system teleinformatyczny zapewniają:
 - a) możliwość ustalenia osoby uzyskującej dane, ich rodzaju oraz czasu, w którym zostały uzyskane,
 - b) zabezpieczenie techniczne i organizacyjne uniemożliwiają osobie nieuprawnionej dostępu do danych;
 - 2) jest to uzasadnione specyfiką lub zakresem zadań wykonywanych przez jednostki organizacyjne Żandarmerii Wojskowej albo prowadzonych przez nie czynności.
5. Komendant Główny Żandarmerii Wojskowej i komendant oddziału Żandarmerii Wojskowej prowadzą rejestr wystąpień o uzyskanie danych telekomunikacyjnych i pocztowych zawierający informacje identyfikujące jednostkę organizacyjną Żandarmerii Wojskowej i żołnierza Żandarmerii Wojskowej uzyskującego te dane, ich rodzaj, cel uzyskania oraz czas, w którym zostały uzyskane. Rejestr prowadzi się w formie elektronicznej, z zachowaniem przepisów o ochronie informacji niejawnych.
6. Dane, o których mowa w ust. 1, które mają znaczenie dla postępowania karnego Komendant Główny Żandarmerii Wojskowej lub komendant oddziału Żandarmerii Wojskowej przekazują prokuratorowi właściwemu

miejscowo lub rzeczowo. Prokurator podejmuje decyzję o zakresie i sposobie wykorzystania przekazanych danych.

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

– KP PO

– odrzucić

23) w art. 6 pkt 2 nadać brzmienie:

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

- „Art. 30b. 1. Kontrolę nad uzyskiwaniem przez Żandarmerię Wojskową danych telekomunikacyjnych i 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, z zachowaniem przepisów o ochronie informacji niejawnych, sądowi okręgowemu, o którym mowa w ust. 1, w okresach półrocznych, sprawozdanie obejmujące:
 - 1) liczbę przypadków pozyskania danych telekomunikacyjnych i pocztowych oraz rodzaj tych danych;
 - 2) kwalifikacje prawne czynów, w związku z zaistnieniem których wystąpiono o dane telekomunikacyjne i pocztowe albo informacje o pozyskaniu danych w celu ratowania życia lub zdrowia ludzkiego bądź do wsparcia działań poszukiwawczych i ratowniczych.
 3. W ramach kontroli, o której mowa w ust. 1, wojskowy sąd okręgowy może zapoznać się z materiałami uzasadniającymi udostępnienie Żandarmerii Wojskowej danych telekomunikacyjnych i pocztowych oraz materiałami uzyskanymi w wyniku podjętych czynności.
 - 3a. W przypadku stwierdzenia przez wojskowy sąd okręgowy braku podstaw do pozyskania danych telekomunikacyjnych lub pocztowych, zgromadzone dane podlegają niezwłocznemu komisijnemu i protokolarnemu zniszczeniu.
 4. Wojskowy sąd okręgowy informuje organ Żandarmerii Wojskowej o wyniku kontroli w terminie 30 dni od jej zakończenia.
 5. Kontroli, o której mowa w ust. 1, nie podlega uzyskiwanie danych na podstawie art. 30c ust. 1.
- Art. 30c. 1. W celu zapobiegania lub wykrywania przestępstw, w tym przestępstw skarbowych, popełnionych przez osoby, o których mowa w art. 3 ust. 2 pkt 1, 3, 4, 5 i 6, albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych, Żandarmeria Wojskowa może uzyskiwać dane:
- 1) z wykazu, o którym mowa w art. 179 ust. 9 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;
 - 2) o których mowa w art. 161 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne,

- 3) w przypadku użytkownika, który nie jest osobą fizyczną numer zakończenia sieci oraz siedzibę lub miejsce wykonywania działalności gospodarczej, firmę lub nazwę i formę organizacyjną tego użytkownika,
 - 4) w przypadku stacjonarnej publicznej sieci telekomunikacyjnej – także nazwę miejscowości oraz ulicy, przy której znajduje się zakończenie sieci, udostępnione użytkownikowi
–oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.
2. Do udostępniania i przetwarzania danych, o których mowa w ust. 1, art. 30 ust. 2–8 stosuje się.”;”;

– KP PO

– odrzucić

24) w art. 6 w pkt 2 w art. 30b ust. 1–4 nadać brzmienie:

- „1. Kontrolę nad uzyskiwaniem przez Komendanta Głównego Żandarmerii Wojskowej lub komendanta oddziału Żandarmerii Wojskowej danych telekomunikacyjnych, pocztowych lub internetowych sprawuje sąd okręgowy właściwy dla siedziby organu Żandarmerii Wojskowej, któremu udostępniono te dane.
2. Organ Żandarmerii Wojskowej, o którym mowa w ust. 1, przekazuje, z zachowaniem przepisów o ochronie informacji niejawnych, sądowi okręgowemu, o którym mowa w ust. 1, informacje o każdorazowym wystąpieniu o dane, o których mowa w art. 20c ust. 1, na warunkach określonych w art. 30 ust. 2, 3 i 4, a ponadto sporządza i przekazuje, w okresach półrocznych, sprawozdanie obejmujące:
 - 1) liczbę przypadków pozyskania w okresie sprawozdawczym danych telekomunikacyjnych lub pocztowych oraz rodzaj tych danych;
 - 2) kwalifikacje prawne czynów, w związku z zaistnieniem których wystąpiono o dane telekomunikacyjne, pocztowe lub internetowe albo informacje o pozyskaniu danych w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych.
3. W ramach kontroli, o której mowa w ust. 1, sąd okręgowy może zapoznać się z materiałami uzasadniającymi udostępnienie Żandarmerii Wojskowej danych telekomunikacyjnych lub pocztowych.
4. Sąd okręgowy w trybie zarządzenia może wskazać, które z pobranych przez Żandarmerii Wojskowej danych były pobrane niezasadnie. Organ Żandarmerii Wojskowej jest zobowiązany do niezwłocznego, komisyjnego i protokolarnego zniszczenia materiałów, których wykorzystanie w postępowaniu karnym jest niedopuszczalne. Organ Żandarmerii Wojskowej niezwłocznie informuje sąd, o zniszczeniu tych materiałów.”;

– KP Nowoczesna

– odrzucić

25) w art. 6 w pkt 3 po lit. e dodać nową zmianę w brzmieniu:

„...”) po ust. 13 dodaje się ust. 13a w brzmieniu:

- „13a. Usługodawca świadczący usługi drogą elektroniczną będący mikro lub małym przedsiębiorcą w rozumieniu przepisów ustawy o swobodzie działalności gospodarczej zapewnia warunki techniczne i organizacyjne umożliwiające prowadzenie przez Żandarmerię Wojskową kontroli operacyjnej stosownie do posiadanej infrastruktury.”;

– KP Nowoczesna

– przyjąć

26) w art. 6 w pkt 3 lit. g nadać brzmienie:

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

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

1) zawierają informacje:

a) o których mowa w art. 178 Kodeksu postępowania karnego,

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

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

2) zawierają 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 przekazuje te materiały sądowi, który wydał postanowienie w przedmiocie zastosowania kontroli operacyjnej, wraz z wnioskiem o ich wykorzystanie w postępowaniu karnym.

16g. Sąd, niezwłocznie po złożeniu wniosku przez Komendanta Główny Żandarmerii Wojskowej lub komendanta oddziału Żandarmerii Wojskowej, wydaje postanowienie o dopuszczalności wykorzystania w postępowaniu karnym materiałów mogących zawierać informację stanowiącą tajemnicę związaną z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu, a także zarządza niezwłoczne zniszczenie materiałów, których wykorzystanie w postępowaniu karnym jest niedopuszczalne.

16h. Na postanowienie sądu w przedmiocie dopuszczalności wykorzystania w postępowaniu karnym materiałów mogących zawierać informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, Komendantowi Głównemu Żandarmerii Wojskowej, lub komendantowi oddziału Żandarmerii Wojskowej przysługuje zażalenie. Do zażalenia stosuje się odpowiednio przepisy Kodeksu postępowania karnego.

16i. Organ Żandarmerii Wojskowej jest obowiązany do wykonania zarządzenia sądu, o którym mowa w ust. 16g, oraz niezwłocznego, komisyjnego i protokolarnego zniszczenia materiałów, których wykorzystanie w postępowaniu karnym jest niedopuszczalne. Organ Żandarmerii Wojskowej niezwłocznie informuje sąd, o którym mowa w ust. 16f, o zniszczeniu tych materiałów.””;

–**KP Nowoczesna**

– **odrzuć**

27) w art. 7 w pkt 2 po lit. f dodać nową zmianę w brzmieniu:

„...) po ust. 12 dodaje się ust. 12a w brzmieniu:

„12a. Usługodawca świadczący usługi drogą elektroniczną będący mikro lub małym przedsiębiorcą w rozumieniu przepisów ustawy o swobodzie działalności gospodarczej zapewnia warunki techniczne i organizacyjne

umożliwiający prowadzenie przez ABW kontroli operacyjnej stosownie do posiadanej infrastruktury.””;

– KP Nowoczesna

– przyjąć

28) w art. 7 w pkt 2 lit. g nadać brzmienie:

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

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

1) zawierają informacje:

a) o których mowa w art. 178 Kodeksu postępowania karnego,

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

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

2) zawierają informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, Szef ABW przekazuje te materiały sądowi, który wydał postanowienie w przedmiocie zastosowania kontroli operacyjnej, wraz z wnioskiem o ich wykorzystanie w postępowaniu karnym.

15i. Sąd, niezwłocznie po złożeniu wniosku przez Szefa ABW, wydaje postanowienie o dopuszczalności wykorzystania w postępowaniu karnym materiałów mogących zawierać informację stanowiącą tajemnicę związaną z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu, a także zarządza niezwłoczne zniszczenie materiałów, których wykorzystanie w postępowaniu karnym jest niedopuszczalne.

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

15k. Szef ABW jest obowiązany do wykonania zarządzenia sądu, o którym mowa w ust. 16g, oraz niezwłoczne, komisyjne i protokolarne zniszczenie materiałów, których wykorzystanie w postępowaniu karnym jest niedopuszczalne. Szef ABW niezwłocznie informuje sąd, o którym mowa w ust. 16f, o zniszczeniu tych materiałów.””;

–KP Nowoczesna

– odrzucić

29) w art. 7 w pkt 3 lit. a nadać brzmienie:

„a) ust. 1 otrzymuje brzmienie:

„1. Jeżeli jest to niezbędne do realizacji zadań, o których mowa w art. 5 ust. 1, gdy inne środki okazały się bezskuteczne albo mogą być nieprzydatne, ABW może uzyskiwać dane:

- 1) określone w art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243, 827 i 1198), zwane dalej „danymi telekomunikacyjnymi”;
- 2) określone w art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. poz. 1529, z późn. zm.), zwane dalej „danymi pocztowymi”;

– KP PO

– odrzucić

30) w art. 7 w pkt 3 lit. d nadać brzmienie:

„d) dodaje się ust. 5–8 w brzmieniu:

- „5. Szef ABW prowadzi rejestr wystąpień o uzyskanie danych telekomunikacyjnych i pocztowych zawierający informacje identyfikujące jednostkę organizacyjną ABW i funkcjonariusza ABW uzyskującego te dane, ich rodzaj, cel uzyskania oraz czas, w którym zostały uzyskane. Rejestr prowadzi się w formie elektronicznej, z zachowaniem przepisów o ochronie informacji niejawnych.
6. Dane, o których mowa w ust. 1, które mają znaczenie dla postępowania karnego Szef ABW przekazuje Prokuratorowi Generalnemu. Prokurator Generalny podejmuje decyzję o zakresie i sposobie wykorzystania przekazanych danych.
7. Dane, o których mowa w ust. 1, które nie mają znaczenia dla postępowania karnego albo nie są istotne dla bezpieczeństwa państwa, podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu.
8. Dane, o których mowa w ust. 1, przetwarzają 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.”;

– KP PO

– odrzucić

31) w art. 7 pkt 4 nadać brzmienie:

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

- „Art. 28a. 1. Kontrolę nad uzyskiwaniem przez ABW danych telekomunikacyjnych i pocztowych sprawuje Sąd Okręgowy w Warszawie.
2. Szef ABW przekazuje, z zachowaniem przepisów o ochronie informacji niejawnych, sądowi, o którym mowa w ust. 1, w okresach półrocznych, sprawozdanie obejmujące:
 - 1) liczbę przypadków pozyskania w okresie sprawozdawczym danych telekomunikacyjnych i pocztowych oraz rodzaj tych danych;
 - 2) kwalifikacje prawne czynów w związku z zaistnieniem których wystąpiono o dane telekomunikacyjne i pocztowe.
3. W ramach kontroli, o której mowa w ust. 1, Sąd może zapoznać się z materiałami uzasadniającymi udostępnienie ABW danych telekomunikacyjnych i pocztowych oraz materiałami uzyskanymi w wyniku podjętych czynności.
- 3a. W przypadku stwierdzenia przez Sąd Okręgowy w Warszawie braku podstaw do pozyskania danych telekomunikacyjnych lub pocztowych, zgromadzone dane podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu.

4. Sąd, o którym mowa w ust. 1, informuje Szefa ABW o wyniku kontroli w terminie 30 dni od jej zakończenia.
 5. Kontroli, o której mowa w ust. 1, nie podlega uzyskiwanie danych na podstawie art. 28d ust. 1.
- Art. 28d. 1. W celu realizacji zadań, o których mowa w art. 5 ust. 1, ABW może uzyskiwać dane:
- 1) z wykazu, o którym mowa w art. 179 ust. 9 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne
 - 2) o których mowa w art. 161 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne,
 - 3) w przypadku użytkownika, który nie jest osobą fizyczną numer zakończenia sieci oraz siedzibę lub miejsce wykonywania działalności gospodarczej, firmę lub nazwę i formę organizacyjną tego użytkownika,
 - 4) w przypadku stacjonarnej publicznej sieci telekomunikacyjnej – także nazwę miejscowości oraz ulicy, przy której znajduje się zakończenie sieci, udostępnione użytkownikowi
- oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.
2. Do udostępniania i przetwarzania danych, o których mowa w ust. 1, art. 28 ust. 2–8 stosuje się.”;”;

– KP PO

– odrzucić

32) w art. 7 w pkt 4 art. 28a nadać brzmienie:

- „Art. 28a. 1. Kontrolę nad uzyskiwaniem przez ABW danych telekomunikacyjnych, pocztowych lub internetowych sprawuje sąd okręgowy w Warszawie.
2. Szef ABW przekazuje Sądowi, informacje o każdorazowym wystąpieniu o informacje, o których mowa w art. 28 ust. 1, na warunkach określonych w art. 28 ust. 2, 3 i 4, a ponadto sporządza i przekazuje, w okresach półrocznych, sprawozdanie obejmujące:
 - 1) liczbę przypadków pozyskania w okresie sprawozdawczym danych telekomunikacyjnych lub pocztowych oraz rodzaj tych danych;
 - 2) kwalifikacje prawne czynów, w związku z zaistnieniem których wystąpiono o dane telekomunikacyjne, pocztowe lub internetowe albo informacje o pozyskaniu danych w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych.
 3. W ramach kontroli, o której mowa w ust. 1, sąd okręgowy w Warszawie może zapoznać się z materiałami uzasadniającymi udostępnienie ABW danych telekomunikacyjnych lub pocztowych.
 4. Sąd okręgowy w Warszawie w trybie zarządzenia może wskazać, które z pobranych przez ABW danych były pobrane niezasadnie. Organ ABW jest zobowiązany do niezwłocznego, komisyjnego i protokolarnego zniszczenia materiałów, których wykorzystanie w postępowaniu karnym jest niedopuszczalne. Szef ABW niezwłocznie informuje sąd, o zniszczeniu tych materiałów.
 5. Kontroli, o której mowa w ust. 1, nie podlega uzyskiwanie danych na podstawie art. 28b ust. 1.”;

– KP Nowoczesna

– odrzucić

33) art. 8 nadać brzmienie:

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

1) ust. 6 otrzymuje brzmienie:

„6. Usługodawca ma obowiązek przetwarzać dane określone w art. 180c ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243, 827 i 1198) zwane dalej „danymi telekomunikacyjnymi” jeżeli świadczenie usług wymaga dostępu telekomunikacyjnego określonego w art. 2 pkt 6 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne.”;

2) dodaje się ust. 7 w brzmieniu:

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

– **KP Nowoczesna**

– **odrzuć**

34) w art. 10 w pkt 2 po lit. f dodać nową zmianę w brzmieniu:

„...) po ust. 11 dodaje się ust. 11a w brzmieniu:

„11a. Usługodawca świadczący usługi drogą elektroniczną będący mikro lub małym przedsiębiorcą w rozumieniu przepisów ustawy o swobodzie działalności gospodarczej zapewnia warunki techniczne i organizacyjne umożliwiające prowadzenie przez SKW kontroli operacyjnej stosownie do posiadanej infrastruktury.”;

– **KP Nowoczesna**

– **przyjąć**

35) w art. 10 w pkt 3 lit. a nadać brzmienie:

„a) ust. 1 otrzymuje brzmienie:

„1. Jeżeli jest to niezbędne do realizacji zadań, o których mowa w art. 5, gdy inne środki okazały się bezskuteczne albo mogą być nieprzydatne, SKW może uzyskać dane:

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

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

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

– **KP PO**

– **odrzuć**

36) art. 8 nadać brzmienie:

„Art. 8. W ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422 oraz z 2015 r. poz. 1844) w art. 18 ust. 6 otrzymuje brzmienie:

„6. Na potrzeby prowadzonych postępowań organom państwa usługodawca udziela informacji dotyczących:

- 1) danych identyfikujących urządzenie,
- 2) danych dotyczących rozpoczęcia, zakończenia oraz czasu połączenia.”;”;

– KP PO

– odrzucić

37) w art. 10 w pkt 2 lit. g nadać brzmienie:

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

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

1) zawierają informacje:

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

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

2) zawierają informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, Szef SKW przekazuje te materiały sądowi, który wydał postanowienie w przedmiocie zastosowania kontroli operacyjnej, wraz z wnioskiem o ich wykorzystanie w postępowaniu karnym.

14g. Sąd, niezwłocznie po złożeniu wniosku przez Szefa SKW, wydaje postanowienie o dopuszczalności wykorzystania w postępowaniu karnym materiałów mogących zawierać informację stanowiącą tajemnicę związaną z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu, a także zarządza niezwłoczne zniszczenie materiałów, których wykorzystanie w postępowaniu karnym jest niedopuszczalne.

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

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

–KP Nowoczesna

– odrzucić

38) w art. 10 w pkt 3 lit. d nadać brzmienie:

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

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

– KP PO

– odrzucić

39) w art. 10 w pkt 3 lit. e nadać brzmienie:

„e) dodaje się ust. 7–10 w brzmieniu:

- „7. Szef SKW prowadzi rejestr wystąpień o uzyskanie danych telekomunikacyjnych i pocztowych zawierający informacje identyfikujące jednostkę organizacyjną SKW i funkcjonariusza SKW uzyskującego te dane, ich rodzaj, cel uzyskania oraz czas, w którym zostały uzyskane. Rejestr prowadzi się w formie elektronicznej, z zachowaniem przepisów o ochronie informacji niejawnych.
8. Dane, o których mowa w ust. 1, które mają znaczenie dla postępowania karnego Szef SKW przekazuje Prokuratorowi Generalnemu. Prokurator Generalny podejmuje decyzję o zakresie i sposobie wykorzystania przekazanych danych.
9. Dane, o których mowa w ust. 1, które nie mają znaczenia dla postępowania karnego albo nie są istotne dla obronności Państwa, podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu.
10. Dane, o których mowa w ust. 1, przetwarzają 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.”;

– KP PO

– odrzucić

40) w art. 10 pkt 4 nadać brzmienie:

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

- „Art. 32a. 1. Kontrolę nad uzyskiwaniem przez SKW danych telekomunikacyjnych i pocztowych sprawuje Wojskowy Sąd Okręgowy w Warszawie.
2. Szef SKW przekazuje, z zachowaniem przepisów o ochronie informacji niejawnych, sądowi, o którym mowa w ust. 1, w okresach półrocznych, sprawozdanie obejmujące:
 - 1) liczbę przypadków pozyskania w okresie sprawozdawczym danych telekomunikacyjnych i pocztowych oraz rodzaj tych danych;
 - 2) kwalifikacje prawne czynów, w związku z zaistnieniem których wystąpiono o dane telekomunikacyjne i pocztowe.
 3. W ramach kontroli, o której mowa w ust. 1, Sąd może zapoznać się z materiałami uzasadniającymi udostępnienie SKW danych telekomunikacyjnych i pocztowych oraz materiałami uzyskanymi w wyniku podjętych czynności.
 - 3a. W przypadku stwierdzenia przez Wojskowy Sąd Okręgowy w Warszawie braku podstaw do pozyskania danych telekomunikacyjnych lub pocztowych, zgromadzone dane podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu.
 4. Sąd o którym mowa w ust. 1, informuje Szefa SKW o wyniku kontroli w terminie 30 dni od jej zakończenia.
 5. Kontroli, o której mowa w ust. 1, nie podlega uzyskiwanie danych na podstawie art. 32b ust. 1.
- Art. 32b. 1. W celu realizacji zadań, o których mowa w art. 5, SKW może uzyskiwać dane:
- 1) z wykazu, o którym mowa w art. 179 ust. 9 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;

- 2) o których mowa w art. 161 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne,
 - 3) w przypadku użytkownika, który nie jest osobą fizyczną numer zakończenia sieci oraz siedzibę lub miejsce wykonywania działalności gospodarczej, firmę lub nazwę i formę organizacyjną tego użytkownika,
 - 4) w przypadku stacjonarnej publicznej sieci telekomunikacyjnej – także nazwę miejscowości oraz ulicy, przy której znajduje się zakończenie sieci, udostępnione użytkownikowi
– oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.
2. Do udostępniania i przetwarzania danych, o których mowa w ust. 1, art. 32 ust. 2–10 stosuje się.”;”;

– KP PO

– odrzucić

41) w art. 10 w pkt 4 art. 32a nadać brzmienie:

- „Art. 32a. 1. Kontrolę nad uzyskiwaniem przez SKW danych telekomunikacyjnych, pocztowych lub internetowych sprawuje Wojskowy Sąd Okręgowy w Warszawie.
2. Szef SKW przekazuje, z zachowaniem przepisów o ochronie informacji niejawnych sądowi, o którym mowa w ust. 1, informacje o każdorazowym wystąpieniu o dane, o których mowa w art. 32 ust. 1, na warunkach określonych w art. 32 ust. 2, 3 i 4, a ponadto sporządza i przekazuje, w okresach półrocznych, sprawozdanie obejmujące:
 - 1) liczbę przypadków pozyskania w okresie sprawozdawczym danych telekomunikacyjnych lub pocztowych oraz rodzaj tych danych;
 - 2) kwalifikacje prawne czynów, w związku z zaistnieniem których wystąpiono o dane telekomunikacyjne, pocztowe lub internetowe albo informacje o pozyskaniu danych w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych.
 3. W ramach kontroli, o której mowa w ust. 1, Wojskowy Sąd Okręgowy w Warszawie może zapoznać się z materiałami uzasadniającymi udostępnienie SKW danych telekomunikacyjnych lub pocztowych.
 4. Wojskowy Sąd Okręgowy w Warszawie w trybie zarządzenia może wskazać, które z pobranych przez SKW danych były pobrane niezasadnie. Organ SKW jest zobowiązany do niezwłocznego, komisyjnego i protokolarnego zniszczenia materiałów, których wykorzystanie w postępowaniu karnym jest niedopuszczalne. Szef SKW niezwłocznie informuje sąd, o zniszczeniu tych materiałów.
 5. Kontroli, o której mowa w ust. 1, nie podlega uzyskiwanie danych na podstawie art. 28b ust. 1.”;

– KP Nowoczesna

– odrzucić

42) w art. 11 w pkt 2 po lit. e dodać nową zmianę w brzmieniu:

„...”) po ust. 12 dodaje się ust. 12a w brzmieniu:

- „12a. Usługodawca świadczący usługi drogą elektroniczną będący mikro lub małym przedsiębiorcą w rozumieniu przepisów ustawy o swobodzie działalności gospodarczej zapewnia warunki techniczne i organizacyjne

umożliwiający prowadzenie przez CBA kontroli operacyjnej stosownie do posiadanej infrastruktury.””;

– **KP Nowoczesna**

– **przyjąć**

43) w art. 11 w pkt 2 lit. f nadać brzmienie:

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

„15f. W przypadku, gdy materiały, o których mowa w ust. 154:

1) zawierają informacje:

a) o których mowa w art. 178 Kodeksu postępowania karnego,

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

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

2) zawierają informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, Szef CBA przekazuje te materiały sądowi, który wydał postanowienie w przedmiocie zastosowania kontroli operacyjnej, wraz z wnioskiem o ich wykorzystanie w postępowaniu karnym.

15g. Sąd, niezwłocznie po złożeniu wniosku przez Szefa CBA, wydaje postanowienie o dopuszczalności wykorzystania w postępowaniu karnym materiałów mogących zawierać informację stanowiącą tajemnicę związaną z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu, a także zarządza niezwłoczne zniszczenie materiałów, których wykorzystanie w postępowaniu karnym jest niedopuszczalne.

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

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

– **KP Nowoczesna**

– **odrzuć**

44) w art. 11 w pkt 3 lit. a nadać brzmienie:

„a) ust. 1 otrzymuje brzmienie:

„1. Jeżeli jest to niezbędne do realizacji zadań, o których mowa w art. 2, gdy inne środki okazały się bezskuteczne albo mogą być nieprzydatne, CBA może uzyskać dane:

- 1) określone w art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243, 827 i 1198), zwane dalej „danymi telekomunikacyjnymi”,
 - 2) określone w art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. poz. 1529, z późn. zm.), zwane dalej „danymi pocztowymi”,
- oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.”;”;

– KP PO

– odrzucić

45) w art. 11 w pkt 3 lit. d nadać brzmienie:

„d) dodaje się ust. 5–8 w brzmieniu:

- „5. Szef CBA prowadzi rejestr wystąpień o uzyskanie danych telekomunikacyjnych i pocztowych zawierający informacje identyfikujące jednostkę organizacyjną CBA i funkcjonariusza CBA uzyskującego te dane, ich rodzaj, cel uzyskania oraz czas, w którym zostały uzyskane. Rejestr prowadzi się w formie elektronicznej, z zachowaniem przepisów o ochronie informacji niejawnych.
6. Dane, o których mowa w ust. 1, które mają znaczenie dla postępowania karnego Szef CBA przekazuje Prokuratorowi Generalnemu. Prokurator Generalny podejmuje decyzję o zakresie i sposobie wykorzystania przekazanych danych.
7. Dane, o których mowa w ust. 1, które nie mają znaczenia dla postępowania karnego, podlegają niezwłocznemu komisijnemu i protokolarnemu zniszczeniu.
8. 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.”;”;

– KP PO

– odrzucić

46) w art. 11 pkt 4 nadać brzmienie:

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

- „Art. 18a. 1. Kontrolę nad uzyskiwaniem przez CBA danych telekomunikacyjnych i pocztowych sprawuje Sąd Okręgowy w Warszawie.
2. Szef CBA przekazuje, z zachowaniem przepisów o ochronie informacji niejawnych, sądowi, o którym mowa w ust. 1, w okresach półrocznych, sprawozdanie obejmujące:
 - 1) liczbę przypadków pozyskania w okresie sprawozdawczym danych telekomunikacyjnych i pocztowych oraz rodzaj tych danych;
 - 2) kwalifikacje prawne czynów w związku z zaistnieniem których wystąpiono o dane telekomunikacyjne i pocztowe.
3. W ramach kontroli, o której mowa w ust. 1, Sąd może zapoznać się z materiałami uzasadniającymi udostępnienie CBA danych telekomunikacyjnych i pocztowych oraz materiałami uzyskanymi w wyniku podjętych czynności.
- 3a. W przypadku stwierdzenia przez Sąd Okręgowy w Warszawie braku podstaw do pozyskania danych telekomunikacyjnych lub pocztowych, zgromadzone dane podlegają niezwłocznemu komisijnemu i protokolarnemu zniszczeniu.
4. Sąd, o którym mowa w ust. 1, informuje Szefa CBA o wyniku kontroli w terminie 30 dni od jej zakończenia.

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

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

- 1) z wykazu, o którym mowa w art. 179 ust. 9 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;
 - 2) o których mowa w art. 161 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne,
 - 3) w przypadku użytkownika, który nie jest osobą fizyczną: numer zakończenia sieci oraz siedzibę lub miejsce wykonywania działalności gospodarczej, firmę lub nazwę i formę organizacyjną tego użytkownika,
 - 4) w przypadku stacjonarnej publicznej sieci telekomunikacyjnej – także nazwę miejscowości oraz ulicy, przy której znajduje się zakończenie sieci, udostępnione użytkownikowi
– oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.
2. Do udostępniania i przetwarzania danych, o których mowa w ust. 1, art. 18 ust. 2–8 stosuje się.”;

– KP PO

– odrzucić

47) w art. 11 w pkt 4 art. 18a nadać brzmienie:

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

2. Szef CBA przekazuje, z zachowaniem przepisów o ochronie informacji niejawnych sądowi okręgowemu, o którym mowa w ust. 1, informacje o każdorazowym wystąpieniu o dane, o których mowa w art. 18 ust. 1, na warunkach określonych w art. 28 ust. 2, 3 i 4, a ponadto sporządza i przekazuje, w okresach półrocznych, sprawozdanie obejmujące:
 - 1) liczbę przypadków pozyskania w okresie sprawozdawczym danych telekomunikacyjnych lub pocztowych oraz rodzaj tych danych;
 - 2) kwalifikacje prawne czynów, w związku z zaistnieniem których wystąpiono o dane telekomunikacyjne, pocztowe lub internetowe albo informacje o pozyskaniu danych w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych.
3. W ramach kontroli, o której mowa w ust. 1, Sąd Okręgowy w Warszawie może zapoznać się z materiałami uzasadniającymi udostępnienie CBA danych telekomunikacyjnych lub pocztowych.
4. Sąd Okręgowy w Warszawie w trybie zarządzenia może wskazać, które z pobranych przez CBA danych były pobrane niezasadnie. Organ CBA jest zobowiązany do niezwłocznego, komisijnego i protokolarnego zniszczenia materiałów, których wykorzystanie w postępowaniu karnym jest niedopuszczalne. Szef CBA niezwłocznie informuje sąd, o zniszczeniu tych materiałów.
5. Kontroli, o której mowa w ust. 1, nie podlega uzyskiwanie danych na podstawie art. 18b ust. 1.”;

– KP Nowoczesna

– odrzucić

48) w art. 12 w pkt 1 lit. a nadać brzmienie:

„a) ust. 1 otrzymuje brzmienie:

„1. W celu zapobiegania lub wykrywania przestępstw skarbowych, o których mowa w rozdziale 9 Kodeksu karnego skarbowego, gdy inne środki okazały się bezskuteczne albo mogą być nieprzydatne, Służba Celna może uzyskiwać dane 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” oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.”;

– KP PO

– odrzucić

49) w art. 12 w pkt 1 lit. b nadać brzmienie:

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

„Przedsiębiorca telekomunikacyjny lub usługodawca świadczący usługi drogą elektroniczną udostępnia nieodpłatnie dane telekomunikacyjne.”;

– KP PO

– odrzucić

50) w art. 12 w pkt 1 lit. c nadać brzmienie:

„c) ust. 3 otrzymuje brzmienie:

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

– KP PO

– odrzucić

51) w art. 12 w pkt 1 lit. d nadać brzmienie:

„d) w ust. 4 wprowadzenie do wyliczenia otrzymuje brzmienie:

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

– KP PO

– odrzucić

52) w art. 12 w pkt 1 lit. e nadać brzmienie:

„e) ust. 5 otrzymuje brzmienie:

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

– KP PO

– odrzucić

53) w art. 12 w pkt 1 lit. f nadać brzmienie:

„f) dodaje się ust. 6–8 w brzmieniu:

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

7. Szef Służby Celnej i dyrektor izby celnej prowadzi rejestr wystąpień o uzyskanie danych telekomunikacyjnych zawierający informacje identyfikujące jednostkę organizacyjną Służby Celnej i funkcjonariusza uzyskującego te dane, ich rodzaj, cel uzyskania oraz czas, w którym zostały uzyskane. Rejestr prowadzi się w formie elektronicznej, z zachowaniem przepisów o ochronie informacji niejawnych.
8. 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.”;”;

– KP PO

– odrzucić

54) w art. 12 pkt 2 nadać brzmienie:

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

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

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

- 1) liczbę przypadków pozyskania w okresie sprawozdawczym danych telekomunikacyjnych oraz rodzaj tych danych;
- 2) kwalifikacje prawne czynów w związku z zaistnieniem których wystąpiono o dane telekomunikacyjne.

3. 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.

3a. W przypadku stwierdzenia przez sąd okręgowy braku podstaw do pozyskania danych telekomunikacyjnych lub pocztowych, zgromadzone dane podlegają niezwłocznemu komisijnemu i protokolarnemu zniszczeniu.

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

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

Art. 75db. 1. W celu zapobiegania lub wykrywania przestępstw skarbowych, o których mowa w rozdziale 9 Kodeksu karnego skarbowego, Służba Celna może uzyskiwać dane:

- 1) z wykazu, o którym mowa w art. 179 ust. 9 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne
- 2) o których mowa w art. 161 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne,
- 3) w przypadku użytkownika, który nie jest osobą fizyczną numer zakończenia sieci oraz siedzibę lub miejsce wykonywania działalności gospodarczej, firmę lub nazwę i formę organizacyjną tego użytkownika,

- 4) w przypadku stacjonarnej publicznej sieci telekomunikacyjnej – także nazwę miejscowości oraz ulicy, przy której znajduje się zakończenie sieci, udostępnione użytkownikowi
– oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczy.
2. Do udostępniania i przetwarzania danych, o których mowa w ust. 1, art. 75d ust. 2–8 stosuje się.”.”;

– KP PO

– odrzucić

55) w art. 12 pkt 2 nadać brzmienie:

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

- „Art. 75da. 1. Kontrolę nad uzyskiwaniem przez Służbę Celną danych telekomunikacyjnych sprawuje sąd okręgowy właściwy dla siedziby organu Służby Celnej, któremu udostępniono te dane.
2. Organ Służby Celnej, o którym mowa w ust. 1, przekazuje, z zachowaniem przepisów o ochronie informacji niejawnych sądowi okręgowemu, o którym mowa w ust. 1, informacje o każdorazowym wystąpieniu o dane, o których mowa w art. 75d, na warunkach określonych w art. 75d ust. 2, 3 i 4, a ponadto sporządza i przekazuje, w okresach półrocznych, sprawozdanie obejmujące:
 - 1) liczbę przypadków pozyskania w okresie sprawozdawczym danych telekomunikacyjnych oraz rodzaj tych danych;
 - 2) kwalifikacje prawne czynów, w związku z zaistnieniem których wystąpiono o dane telekomunikacyjne.
 3. W ramach kontroli, o której mowa w ust. 1, Sąd Okręgowy może zapoznać się z materiałami uzasadniającymi udostępnienie Służbie Celnej danych telekomunikacyjnych.
 4. Sąd okręgowy w trybie zarządzenia może wskazać, które z pobranych przez Służbę Celną danych były pobrane niezasadnie. Organ Służby Celnej jest zobowiązany do niezwłocznego, komisyjnego i protokolarnego zniszczenia materiałów, których wykorzystanie w postępowaniu karnym jest niedopuszczalne. Szef Służby Celnej niezwłocznie informuje sąd, o zniszczeniu tych materiałów.
 5. Kontroli, o której mowa w ust. 1, nie podlega uzyskiwanie danych na podstawie art. 75db ust. 1.”;

– KP Nowoczesna

– odrzucić

Warszawa, dnia 14 stycznia 2016 r.

Sprawozdawca

Przewodniczący Komisji

/-/ Krzysztof Łapiński

/-/ Arkadiusz Czartoryski