



NAJWYŻSZA IZBA KONTROLI

Delegatura w Katowicach

LKA – 4101-25-02/2012

P/12/191

WYSTĄPIENIE POKONTROLNE

I. Dane identyfikacyjne kontroli

Numer i tytuł kontroli	Kontrola nr: P/12/191 - Uzyskiwanie i przetwarzanie przez uprawnione podmioty danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180 c i d ustawy Prawo telekomunikacyjne
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Katowicach
Kontroler	Anna Loppe, główny specjalista kontroli państwowej, upoważnienie do kontroli nr 82793 z 24 września 2012 r. (dowód: akta kontroli str. 1-2)
Jednostka kontrolowana	Prokuratura Okręgowa w Katowicach ¹ , ul. Wita Stwosza 31, 40-042 Katowice
Kierownik jednostki kontrolowanej	Krzysztof Kołaczek, Prokurator Okręgowy w Katowicach, zwany dalej Prokuratorem Okręgowym. (dowód: akta kontroli str. 4)

II. Ocena kontrolowanej działalności

Ocena ogólna

Najwyższa Izba Kontroli ocenia pozytywnie, pomimo stwierdzonych nieprawidłowości², działalność Prokuratury w zakresie uzyskiwania i przetwarzania danych z bilingów, informacji o lokalizacji oraz innych danych³, o których mowa w art. 180 c i d ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne⁴, w okresie od 1 stycznia 2011 r. do 12 grudnia 2012 r.

Uzasadnienie oceny ogólnej

Prokurator Okręgowy w Katowicach określił zasady bezpieczeństwa oraz organizacji pracy przy uzyskiwaniu danych telekomunikacyjnych, o których mowa w art. 180 c i d powołanej wyżej ustawy, a także procedury korzystania z tego systemu oraz zapewnił przekazywanie prokuratorom danych telekomunikacyjnych udostępnionych za pomocą systemu teleinformatycznego zgodnie z treścią wydanych przez nich postanowień.

Jednak wydawanie zarządzeń o doręczeniu postanowień i ich doręczanie odbywało się z naruszeniem terminu określonego w art. 218 § 2 ustawy z dnia 6 czerwca 1997 r. Kodeks postępowania karnego⁵. Ponadto stwierdzono nieprzestrzeganie przepisów wewnętrznych w zakresie przechowywania kodów PIN do Systemu Retencji i Udostępniania Danych „RUDA” P4 Sp. z o.o.⁶.

Powyższa ocena została wydana w oparciu o badanie strony organizacyjno-formalnej uzyskiwania przez Prokuraturę danych telekomunikacyjnych.

¹ Zwana dalej „Prokuraturą”.

² Najwyższa Izba Kontroli stosuje, w ocenie ogólnej i przy ocenach częściowych, 3-stopniową skalę ocen: pozytywna, pozytywna mimo stwierdzonych nieprawidłowości, negatywna.

³ Zwanych dalej „danymi telekomunikacyjnymi”.

⁴ Dz. U. Nr 171 poz.1800 ze zm., zwanej dalej „ustawą Prawo telekomunikacyjne”.

⁵ Dz. U. Nr 89 poz. 555 ze zm., zwanego dalej „k.p.k.”.

⁶ Zwanego dalej „Systemem RUDA”.

III. Opis ustalonego stanu faktycznego

1. Zabezpieczenie danych telekomunikacyjnych

1.1. Procedury wewnętrzne dotyczące zabezpieczenia w aktach postępowania przygotowawczego danych telekomunikacyjnych

Opis stanu
faktycznego

W Prokuraturze nie określono procedur wewnętrznych dotyczących zabezpieczenia w aktach prowadzonych postępowań przygotowawczych danych telekomunikacyjnych przed ich udostępnieniem osobom nieupoważnionym lub zabranieniem przez osobę nieuprawnioną. Prokurator Okręgowy wyjaśnił, że dane telekomunikacyjne, zawarte w aktach spraw, zabezpieczano na podstawie art. 181 § 2 k.p.k. oraz wydanego na jego podstawie Rozporządzenia Ministra Sprawiedliwości z dnia 20 lutego 2012 r. w sprawie sposobu postępowania z protokołami przesłuchań i innymi dokumentami lub przedmiotami, na które rozciąga się obowiązek zachowania w tajemnicy informacji niejawnych albo zachowania tajemnicy związanej z wykonywaniem zawodu lub funkcji⁷.

(dowód: akta kontroli str. 3, 5-6, 9-10)

Przeprowadzone w Wydziale V Śledczym Prokuratury⁸ oględziny sposobu zabezpieczenia w aktach postępowań danych telekomunikacyjnych, przed ich udostępnieniem osobom nieupoważnionym, wykazały, że przechowywano je w sposób zapewniający ich bezpieczeństwo. Spośród 29 postępowań prowadzonych przez Wydział w okresie objętym kontrolą, w trakcie których żądano wydania danych telekomunikacyjnych, oględzinom poddano zabezpieczenie ww. danych dla czterech postępowań przygotowawczych (13,8%).

(dowód: akta kontroli str. 177-181, 551-553)

1.2. Procedury bezpieczeństwa danych telekomunikacyjnych opracowane w Prokuraturze

Opis stanu
faktycznego

W Prokuraturze obowiązywały procedury bezpieczeństwa danych telekomunikacyjnych określone w:

- 1) „Instrukcji korzystania z sieci komputerowej oraz bezpieczeństwa danych systemu informatycznego”, wprowadzonej zarządzeniem Nr 30/06 Prokuratora Okręgowego z 10 marca 2006 r.⁹,
- 2) „Zasadach organizacji pracy stanowisk dostępowych do Systemu Retencji i Udostępniania Danych „RUDA” P4 Sp. z o.o. w Prokuraturze Okręgowej w Katowicach¹⁰”, wprowadzonych zarządzeniem Nr 84/12 Prokuratora Okręgowego z 21 maja 2012 r., zmienionych zarządzeniem nr 86/12 Prokuratora Okręgowego z dnia 25 maja 2012 r.

Ustalono w Instrukcji korzystania z sieci komputerowej i zasadach organizacji Systemu Ruda procedury zapewniały bezpieczeństwo, poufność i integralność danych telekomunikacyjnych.

(dowód: akta kontroli str. 5, 15-38, 50-70)

1.3. Zabezpieczenia przewidziane w procedurach, o których mowa w pkt 1.2. niniejszego wystąpienia pokontrolnego

Opis stanu
faktycznego

Ustalono w Instrukcji korzystania z sieci komputerowej postanowienia określające m.in.:

- sposób administrowania siecią oraz obowiązki i uprawnienia Administratora Bezpieczeństwa Informacji oraz administratorów sieci,
- obszar systemu, w tym pomieszczenia systemu i dostęp osób do tych pomieszczeń,

⁷ Dz. U. z 2012 r., poz. 219.

⁸ Zwanym dalej „Wydziałem V”.

⁹ Zwaną dalej „Instrukcją korzystania z sieci komputerowej”.

¹⁰ Zwane dalej „Zasadami organizacji Systemu RUDA”.

- zasady dopuszczenia pracowników do pracy w systemie i dostępu do zasobów systemu informatycznego oraz eksploatacji systemu,
- ogólne wymagania bezpieczeństwa systemu, zasady bezpieczeństwa w zakresie dostępu do danych osobowych systemu oraz postępowanie w przypadku naruszenia bezpieczeństwa systemu bądź inne nieuprawnione pozyskanie lub zmiany danych osobowych,
- zasady przetwarzania danych w systemie oraz tworzenia i przekazywania kopii danych,
- zakres i sposób prowadzenia dokumentacji bezpieczeństwa systemu.

Zgodnie z przedmiotową instrukcją, sieć komputerową w Prokuraturze oddzielono od sieci teleinformatycznych, tj. od sieci internetowej i innych urządzeń teletransmisyjnych nienależących do sieci lokalnej.

(dowód: akta kontroli str. 16-38)

Administratorem Bezpieczeństwa Informacji w Prokuraturze, zgodnie z Zarządzeniem nr 90/05 Prokuratora Okręgowego z dnia 29 listopada 2005 r. jest Naczelnik Wydziału IV do Spraw Informatyzacji i Analiz Prokuratury¹¹.

(dowód: akta kontroli str. 134-136)

Z kolei ustalone w zarządzeniu Nr 84/12 Prokuratora Okręgowego postanowienia, dotyczące organizacji Systemu RUDA, określały m.in. zasady:

- przyznawania i odbierania osobom uprawnień dostępowych (upoważnień) do systemu RUDA oraz nadzoru nad działalnością stanowisk dostępowych,
- przyjmowania postanowień i udzielania odpowiedzi w prokuratorskim punkcie informacyjnym (punkcie CBD-SIP) oraz prowadzenia w formie elektronicznej wykazu o określonej treści (z możliwością jego wydruku) wpływających postanowień, dokonanych zabezpieczeń oraz udzielonych odpowiedzi,
- bezpieczeństwa teleinformatycznego i odpowiedzialności działania stanowisk dostępowych,
- nadzoru nad prawidłowym działaniem stanowisk dostępowych.

Postanowienia Zarządzenia Nr 84/12 Prokuratora Okręgowego z dnia 21 maja 2012 r. zmieniono i uzupełniono Zarządzeniem Nr 86/12 Prokuratora Okręgowego z dnia 25 maja 2012 r. w zakresie m.in. dotyczącym przyjmowania postanowień i dokonywania zapytań do systemu RUDA oraz sposobu zapisywania uzyskanych danych i ich przekazywania właściwemu prokuratorowi.

(dowód: akta kontroli str. 50-70)

W toku oględzin, przeprowadzonych 31 października 2012 r., w obecności Naczelnika Wydziału IV, stwierdzono, że w Wydziale tym znajdowało się 6 stanowisk dostępowych pozyskiwania danych telekomunikacyjnych w ramach Systemu RUDA. Stanowiska te zabezpieczono w sposób minimalizujący ryzyko związane z naruszeniem bezpieczeństwa danych telekomunikacyjnych. Sposób wejścia do systemu spełniał wymagania zawarte w ustalonych zasadach i minimalizował ryzyko związane z naruszeniem poufności danych telekomunikacyjnych.

Przy stanowiskach dostępowych pracowały osoby upoważnione do dostępu do danych telekomunikacyjnych, o których mowa w art. 180 c i d Prawa telekomunikacyjnego, posiadanych przez operatora sieci Play (P4 Sp. z o.o.).

W pomieszczeniach, gdzie znajdowały się stanowiska dostępowe, monitory komputerów, na których przetwarzano dane telekomunikacyjne, umiejscowiono na biurkach użytkowników, w sposób uniemożliwiający osobie wchodzącej do pomieszczenia podgląd zapisów na ekranach.

Koperty z kodami PIN do Systemu RUDA, zamknięte w jednej kopercie, znajdowały się w pomieszczeniu bezpieczeństwa, w którym pracowali administratorzy systemu informatycznego Prokuratury. Wejście w korytarz, z którego można wejść do pomieszczenia

¹¹ Zwany dalej „Wydziałem IV”.

bezpieczeństwa odgrodzono od pozostałej przestrzeni drzwiami, zamkniętymi na zamek cyfrowy, a wejście do pomieszczenia bezpieczeństwa zabezpieczono dodatkowo systemem kontroli dostępu umiejscowionym przy drzwiach wejściowych. W pomieszczeniu znajdował się sejf zamykany na zamek cyfrowy, przy czym dokumentacja związana z obsługą stanowisk dostępowych oraz koperty z kodami PIN znajdowały się w zamykanej meblowej szafie zasuwanej, która w trakcie oględzin była otwarta. Wśród dokumentacji związanej z obsługą stanowisk dostępowych do Systemu RUDA znajdowały się m.in. oryginały formularzy rejestracyjnych użytkowników systemu. Ponadto, w Wydziale IV znajdował się pokój nr 1227, w którym mieściło się do dnia 30 września 2012 r. (jak wyjaśnił w trakcie oględzin Naczelnik Wydziału) pomieszczenie specjalisty ds. bezpieczeństwa, w którym znajdowała się szafa metalowa, zamykana na klucz oraz sejf. W trakcie oględzin pomieszczenia nie użytkowano.

(dowód: akta kontroli str. 103-105)

Ustalone
nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następujące nieprawidłowości:

Niezgodne z wewnętrznym uregulowaniem przechowywanie w Wydziale IV kopert z kodami PIN do Systemu RUDA, w meblowej szafie w pomieszczeniu bezpieczeństwa, zamiast w sejfie w pomieszczeniu specjalisty ds. bezpieczeństwa.

W toku przeprowadzonych oględzin funkcjonowania procedur zabezpieczenia danych telekomunikacyjnych, pozyskiwanych za pomocą Systemu RUDA, stwierdzono, że koperty z kodami PIN znajdowały się w pomieszczeniu bezpieczeństwa (pokój nr 1216) w szafie meblowej, zamykanej na klucz, co było niezgodne z § 5 ust. 12 zarządzenia nr 84/12 Prokuratora Okręgowego w Katowicach w sprawie określenia zasad organizacji pracy stanowisk dostępowych do Systemu „RUDA”. W trakcie oględzin ww. szafa była otwarta. W pomieszczeniu bezpieczeństwa znajdował się sejf zamykany na zamek cyfrowy.

Zgodnie z § 5 ust. 11 ww. zarządzenia uprawniony użytkownik stanowiska dostępowego, przy pierwszym logowaniu do systemu RUDA, miał obowiązek zmienić kod PIN. Natomiast zgodnie z § 5 ust. 12 zarządzenia, każdorazowa zmiana kodu PIN zobowiązuje uprawnionego użytkownika stanowiska dostępowego do złożenia aktualnej kopii kodu PIN w zamkniętej kopercie w sejfie w pomieszczeniu specjalisty ds. bezpieczeństwa.

(dowód: akta kontroli str. 50, 52-53, 103-105)

Za bezpieczeństwo teleinformatyczne działania stanowisk dostępowych do systemu RUDA (§ 10 zarządzenia nr 84/12 Prokuratora Okręgowego) odpowiadają Administratorzy Systemu Informatycznego Prokuratury. Z kolei nadzór nad prawidłowością działania stanowisk dostępowych, obejmujący w szczególności prawidłowość stosowania procedur i instrukcji oraz nadzór organizacyjny nad stanowiskami dostępowymi do systemu RUDA (§ 4 ust. 1 pkt 2 i § 16 zarządzenia) sprawuje Naczelnik Wydziału IV, będący ponadto Administratorem Bezpieczeństwa Informacji.

(dowód: akta kontroli str. 52-59, 134-136)

Zgodnie z podziałem czynności urzędników Wydziału IV, wprowadzonym zarządzeniem nr 10/12 Prokuratora Okręgowego z 1 października 2012 r., Administratorami Systemu Informatycznego byli Pan S.K., wykonujący m.in. czynności specjalisty ds. bezpieczeństwa oraz Pan M.Z., m.in. koordynujący pracę urzędników – Administratorów Systemu Informatycznego i Informatyków.

(dowód: akta kontroli str. 57, 130-131)

Administratorzy Systemu Informatycznego, Panowie S.K. i M.Z., w złożonych wyjaśnieniach (tej samej treści) podali, że przyczyną przechowywania kopert z kodami PIN do Systemu Ruda niezgodnie z § 5 ust. 12 zarządzenia nr 84/12 Prokuratora Okręgowego były zmiany organizacyjne i lokalowo-osobowe, które zaszły w Prokuraturze. Pomieszczenia specjalisty ds. bezpieczeństwa zmieniły swoje przeznaczenie i stały się pomieszczeniami mieszczącymi: gabinet Naczelnika Wydziału IV oraz sekretariat Wydziału IV. W konsekwencji sejf, który znajdował się w pomieszczeniu specjalisty ds. bezpieczeństwa zabrano z tego pomieszczenia. Zamknięte koperty z kodami PIN przeniesiono do pomieszczenia stanowiącego część serwerowni, znajdującej się w strefie bezpieczeństwa, przez co dostęp do tego pomieszczenia mają tylko osoby upoważnione.

Wyjaśniali, że koperty umieszczono w szafie, w związku z tym że umieszczenie ich w sejfie musi poprzedzić zmiana organizacji ułożenia taśm zabezpieczających kopie zapasowe systemu informatycznego Prokuratury Okręgowej. Ponadto Administratorzy wyjaśniali, że w dniu 31 października 2012 r., w czasie wykonywania czynności związanych z opisywaniem taśm zabezpieczających kopie danych systemu informatycznego, koperty z kodami PIN umieszczono w sejfie.

(dowód: akta kontroli str. 395-400)

Naczelnik Wydziału IV, jako przyczynę nieprawidłowości, wskazał zmiany organizacyjne oraz lokalowo-osobowe w Wydziale IV. Stwierdził, że pomieszczenia specjalisty ds. bezpieczeństwa stały się pomieszczeniami, w których będą mieścić się: gabinet Naczelnika Wydziału IV oraz sekretariat Wydziału IV. Ponadto, od dnia 1 października 2012 r. obowiązki specjalisty ds. bezpieczeństwa wykonuje Administrator Systemu Informatycznego Prokuratury Okręgowej Pan S.K., który faktycznie wykonuje swoje obowiązki w pomieszczeniu bezpieczeństwa. Naczelnik Wydziału IV podał, że z uwagi na zapowiedzianą kontrolę zamknięte koperty z kodami PIN w dniu 31 października 2012 r. przeniesiono do pomieszczenia bezpieczeństwa. Stwierdził także, że koperty te docelowo miały zostać umieszczone w sejfie dużym, a omyłkowo umieszczono je w szafie.

(dowód: akta kontroli str. 137-140)

Uwagi dotyczące
badanej działalności

Za wyjątkiem danych telekomunikacyjnych, pozyskiwanych od operatora sieci Play (P4 Sp. z o.o.), w Prokuraturze nie określono zasad pozyskiwania danych telekomunikacyjnych, o których mowa w art. 180 c i d ustawy Prawo telekomunikacyjne, od innych operatorów sieci.

Prokurator Okręgowy wyjaśnił, że w Prokuraturze do pozyskiwania danych telekomunikacyjnych od innych operatorów sieci stosowane są wprost przepisy art. 218 k.p.k. oraz wydanego na jego podstawie Rozporządzenia Ministra Sprawiedliwości z dnia 20 lutego 2012 roku. W związku z tym dane te pozyskiwano każdorazowo na podstawie postanowienia prokuratora prowadzącego lub nadzorującego konkretne postępowanie przygotowawcze, opartego na wskazanym wyżej przepisie kodeksu postępowania karnego, skierowanego do operatora sieci. Stwierdził, że w związku z tym nie wprowadzono w Prokuraturze odrębnych zasad pozyskiwania przedmiotowych danych telekomunikacyjnych.

(dowód: akta kontroli str. 8-10)

1.4. Prowadzone w Prokuraturze ewidencje umożliwiające odnotowanie, kto, kiedy, w jakim celu oraz jakie dane telekomunikacyjne uzyskiwał

Opis stanu
faktycznego

W Prokuraturze od dnia 22 maja 2012 r. prowadzono ewidencję umożliwiającą odnotowanie jedynie w odniesieniu do operatora sieci Play (P4 Sp. z o.o.), kto, kiedy, w jakiej sprawie i z jakiego wydziału lub prokuratury (postanowienia o żądaniu wydania danych telekomunikacyjnych przesyłane są również z 16 prokuratur rejonowych) występował do operatora o uzyskanie takich danych. Prowadzona ewidencja umożliwiała odnotowanie, który z pracowników Prokuratury Okręgowej przekazywał postanowienia do operatora.

(dowód: akta kontroli str. 3, 5-6)

Porozumienie z operatorem sieci Play (P4 Sp. z o.o.), w sprawie udostępniania danych telekomunikacyjnych za pomocą sieci telekomunikacyjnej, zawarł 24 listopada 2011 r. Prokurator Generalny, który zobowiązał pismem z dnia 19 stycznia 2012 r. Prokuratora Okręgowego do wdrożenia ustaleń w nim zawartych.

(dowód: akta kontroli str. 39-48)

Stwierdzono, że Prokurator Okręgowy w Katowicach zarządzeniem Nr 84/12 z dnia 21 maja 2012 r. określił zasady organizacji pracy w Prokuraturze stanowisk dostępowych do Systemu Retencji i Udostępniania Danych „RUDA” P4 Sp. z o.o. Przyjmowanie postanowień i udzielanie odpowiedzi odbywało się, zgodnie z ww. zarządzeniem w Wydziale IV, w punkcie CBD-SIP. W punkcie tym prowadzono w formie elektronicznej, z możliwością wydruku, wykaz wpływających postanowień, dokonanych zabezpieczeń

oraz udzielonych odpowiedzi. Wykaz prowadzono wspólnie dla Prokuratury Okręgowej oraz podległych prokuratur rejonowych, z możliwością podziału na poszczególne prokuratury rejonowe oraz wydziały Prokuratury.

(dowód: akta kontroli str. 50-52, 54-55)

Do dokonywania wglądu, zabezpieczania i uzyskiwania danych w Systemie Ruda upoważniono sześciu pracowników Prokuratury (punktu CBD-SIP), w tym dwóch nadzorujących grupę oraz czterech zwykłych użytkowników. Pracowników upoważnionych przeszkolił operator sieci Play (P4 Sp. z o.o.), w zakresie posługiwania się systemem, w dniu 2 kwietnia 2012 r.

(dowód: akta kontroli str. 66, 74-81)

Zasady organizacji Systemu RUDA, określone zarządzeniem Nr 84/12 Prokuratora Okręgowego, weszły w życie 28 maja 2012 r., a pierwsze postanowienie o żądaniu wydania danych telekomunikacyjnych wpłynęło do punktu CBD-SIP z Prokuratury Rejonowej w Jaworznie 28 maja 2012 r., a z Prokuratury Okręgowej 2 lipca 2012 r. W związku z powyższym nie była możliwa weryfikacja rzetelności ewidencjonowania postanowień wydanych w Prokuraturze Okręgowej, zawierających żądanie udostępnienia danych telekomunikacyjnych za okres od 1 stycznia 2011 r. do 30 czerwca 2012 r.

(dowód: akta kontroli str. 60, 529-550)

Uwagi dotyczące
badanej działalności

W Prokuraturze, w odniesieniu do pozostałych, oprócz operatora sieci Play (P4 Sp. z o.o.), operatorów publicznych sieci telekomunikacyjnych oraz dostawców publicznie dostępnych usług telekomunikacyjnych, nie było ewidencji lub urządzeń umożliwiających odnotowanie kto, kiedy, w jakim celu oraz jakie dane telekomunikacyjne uzyskiwał. Stan ten, co wykazały ustalenia kontroli NIK, utrudniał ustalenie rzetelnych danych o liczbie wydanych w okresie od 1 stycznia 2011 r. do 30 czerwca 2012 r. przez prokuratorów postanowień o żądaniu wydania danych telekomunikacyjnych. W powyższym zakresie stwierdzono m.in., że:

- W dniu 25 października 2012 r. Wydział V wykazał wydanie w tym okresie 238 postanowień, natomiast w dniu 9 listopada 2012 r., po dokonaniu weryfikacji 232 postanowień,
- W dniu 8 października 2012 r. Wydział VI wykazał wydanie w ww. okresie 48 postanowień, natomiast w dniu 10 października 2012 r., po dokonaniu weryfikacji 49 postanowień.

1.5. Dane ilościowe o pozyskanych przez Prokuraturę danych telekomunikacyjnych

Opis stanu
faktycznego

W okresie od 1 stycznia 2011 r. do 30 czerwca 2012 r. w Prokuraturze Okręgowej wydano 281¹² postanowień o żądaniu wydania danych telekomunikacyjnych, w tym 232 postanowienia wydali prokuratorzy Wydziału V, a 49 prokuratorzy Wydziału VI do Spraw Przestępczości Gospodarczej¹³. W postanowieniach żądano różnych kategorii danych wymienionych w art. 161 i 180 c i d ustawy Prawo telekomunikacyjne.

(dowód: akta kontroli str. 228-382, 405-426, 431-433, 448, 450-451, 455-459, 469-470, 599-605, 628-783, 809-816).

Żądano wydania danych dotyczących:

- zakończenia sieci, telekomunikacyjnego urządzenia końcowego oraz użytkownika końcowego inicjującego połączenie (tj. danych określonych w art. 180 c ust. 1 pkt 1 lit. a ww. ustawy) w 248 postanowieniach, przy czym:
 - spośród 148 postanowień wydanych w 2011 r., dane uzyskano w 74 przypadkach, a w 18 ich nie pozyskano. W pozostałych 56 przypadkach, w czasie kontroli NIK, Prokuratura nie miała danych na temat sposobu realizacji postanowień, co wyjaśniano przekazaniem akt spraw wraz z aktem oskarżenia do sądu;

¹² W oparciu o dane zestawienia „Zakres i ilość danych, o których mowa w art. 180 c i d ustawy Prawo telekomunikacyjne, żądanych i pozyskanych od operatorów publicznych sieci telekomunikacyjnych”, przekazane przy piśmie Nr I A 016/108/12 z dnia 9 listopada 2012 r. oraz późniejsze pisma i wyjaśnienia Naczelników Wydziału V i VI dotyczące liczby wydanych postanowień.

¹³ Zwanego dalej „Wydziałem VI”.

- w odniesieniu do 100 postanowień wydanych w I półroczu 2012 r. dane pozyskano w 47 przypadkach, a w 53 ich nie uzyskano;
- zakończenia sieci, telekomunikacyjnego urządzenia końcowego oraz użytkownika końcowego, do którego kierowane było połączenie (tj. danych określonych w art. 180 c ust. 1 pkt 1 lit. b ustawy) w 202 postanowieniach, przy czym:
 - spośród 97 postanowień z 2011 r., dane pozyskano w 41 przypadkach, a w 3 ich nie uzyskano. Dla pozostałych 53 przypadków, w czasie kontroli NIK, Prokuratura nie miała danych na ten temat (z uwagi na przekazanie akt spraw wraz z aktem oskarżenia do sądu);
 - w przypadku 105 postanowień wydanych w I półroczu 2012 r., dane pozyskano w 53 przypadkach, a w 52 ich nie uzyskano;
- lokalizacji telekomunikacyjnego urządzenia końcowego (danych określonych w art. 180 c ust. 1 pkt 2 lit. c ustawy) w 183 postanowieniach, przy czym:
 - spośród 88 postanowień z 2011 r. dane pozyskano w 28 przypadkach, a w 8 ich nie uzyskano. Dla pozostałych 52 przypadków Prokuratura, w czasie kontroli NIK, nie miała danych na ten temat (akta sprawy przekazane z aktem oskarżenia do sądu);
 - w przypadku 95 postanowień wydanych w I półroczu 2012 r. dane pozyskano w 56 przypadkach, a w 39 ich nie uzyskano;
- daty i godziny połączenia oraz czasu jego trwania (danych określonych w art. 180 c ust. 1 pkt 2 lit. a ustawy) w 222 postanowieniach, przy czym:
 - spośród 115 postanowień z 2011 r. dane pozyskano w 47 przypadkach, a w 11 ich nie uzyskano. Dla pozostałych 57 przypadków Prokuratura nie miała danych na ten temat (akta sprawy przekazane wraz z aktem oskarżenia do sądu);
 - w przypadku 107 postanowień wydanych w I półroczu 2012 r. dane pozyskano w 64 przypadkach, a w 43 ich nie uzyskano;
- rodzaju połączenia (danych określonych w art. 180 c ust. 1 pkt 2 lit. b ustawy Prawo telekomunikacyjne) w 24 postanowieniach, w tym:
 - spośród 17 postanowień z 2011 r. dane pozyskano w 9 przypadkach, a w 8 ich nie uzyskano
 - w przypadku 7 postanowień wydanych w I półroczu 2012 r. dane pozyskano w 4 przypadkach, a w 3 ich nie uzyskano;
- nieudanych prób uzyskania połączenia w 4 postanowieniach wydanych w I półroczu 2012 r. We wszystkich przypadkach pozyskano żądane dane;
- użytkownika, niezbędnych do wystawienia rachunku na podstawie jednego postanowienia z 2011 r. - nie uzyskano żądanych danych;
- o których mowa w art. 161 ustawy Prawo telekomunikacyjne na mocy 113 postanowień, w tym:
 - spośród 58 postanowień z 2011 r. dane pozyskano w 3 przypadkach, a w 4 ich nie uzyskano. Dla pozostałych 51 przypadków nie było danych (akta sprawy przekazane wraz z aktem oskarżenia do sądu);
 - w przypadku 55 postanowień wydanych w I półroczu 2012 r. dane pozyskano w 13 przypadkach, a w 42 ich nie uzyskano.

Przyczynami nieuzyskiwania przez Prokuraturę żądanych danych telekomunikacyjnych były m.in.: nieposiadanie przez operatora żądanych danych w systemie, działanie telefonu w systemie prepaid, brak przynależności telefonu (numeru) do sieci operatora, brak rejestracji użytkownika numeru u operatora, awaria systemu informatycznego operatora lub nieposiadanie przez niego narzędzia umożliwiającego realizację postanowienia, objęcie

postanowieniem dużej ilości numerów występujących w wykazach, co spowodowało niepodanie przez operatora danych abonentów, wymaganie podania danych starszych niż 24-miesięczny okres ich retencji, brak współpracy podanego nr IMEI z kartą SIM, zwrot postanowienia w celu doprecyzowania żądania. W jednym przypadku operator nie udzielił żadnej odpowiedzi na otrzymane postanowienie.

(dowód: akta kontroli str. 228-382, 405-426, 431-433, 448, 450-451, 455-459, 469-470, 599-605, 628-783, 809-816)

1.6. Upoważnienie osób kierujących zapytania do operatorów telekomunikacyjnych do dokonywania tej czynności

Opis stanu
faktycznego

We wszystkich przypadkach kierowanych zapytań w sprawie danych telekomunikacyjnych w Prokuraturze występowały osoby do tego upoważnione, tj. prokuratorzy Wydziału V i Wydziału VI. Forma zapytań – postanowienie – była zgodna z przepisem art. 218 § 1 k.p.k. Dane we wszystkich przypadkach uzyskiwano na żądanie właściwych komórek organizacyjnych (Wydziałów).

(dowód: akta kontroli str. 228-382, 628-783)

Ocena częściowa

Najwyższa Izba Kontroli ocenia pozytywnie, mimo stwierdzonej nieprawidłowości, działalność w badanym obszarze.

2. Sprawność i szybkość pozyskiwania informacji

2.1. Przypadki kwestionowania legitymacji Prokuratury do uzyskania żądanych danych telekomunikacyjnych

Opis stanu
faktycznego

W okresie objętym kontrolą nie odnotowano w Prokuraturze przypadków kwestionowania uprawnień prokuratora do żądania danych telekomunikacyjnych.

(dowód: akta kontroli str. 554, 557)

2.2. Przypadki przekazywania danych telekomunikacyjnych ze znaczną zwłoką

Opis stanu
faktycznego

W ww. okresie nie odnotowano przypadków odmowy przekazania przez operatora lub przekazania ze znaczną zwłoką żądanych danych telekomunikacyjnych.

W jednym przypadku (na 281 wydanych postanowień) Prokuratura nie otrzymała odpowiedzi na postanowienie skierowane do operatora. Prokuratura nie podejmowała dalszych działań w celu uzyskania odpowiedzi od tego operatora. Natomiast w 9 przypadkach przedsiębiorca telekomunikacyjny nie przekazał żądanych informacji, gdyż nie dysponował danymi abonenta, posiadającego numer telefonu działającego w systemie prepaid¹⁴.

(dowód: akta kontroli str. 416, 447-450, 554-557)

2.3. Uwarunkowania organizacyjno – prawne oraz techniczne przyjęte w Prokuraturze wpływające na sprawność i szybkość uzyskiwania danych telekomunikacyjnych

Opis stanu
faktycznego

Na poprawę sprawności i szybkości uzyskiwania danych telekomunikacyjnych i ich wykorzystania w realizacji zadań służbowych, wykonywanych w celu wykrywania przestępstw, wpłynęło wdrożenie w Prokuraturze Systemu RUDA.

¹⁴ Liczbę przypadków ustalono na podstawie zestawienia „Zakres i ilość danych, o których mowa w art. 180 c i d ustawy Prawo telekomunikacyjne, żądanych i pozyskanych od operatorów publicznych sieci telekomunikacyjnych”, przekazanego przy piśmie Nr I A 016/108/12 z 9 listopada 2012 r. oraz „Zestawienia dotyczącego czasokresów/dni, za jakie Prokuratura Okręgowa w Katowicach żądała wydania danych, o których mowa w art. 180 c i d ustawy Prawo telekomunikacyjne” przekazanego przy piśmie Nr I A 016/108/12 z 27 listopada 2012 r.

Jak wyjaśnił Prokurator Okręgowy, wdrożenie systemu z reguły przyspieszyło otrzymywanie żądanych danych o kilka tygodni.

(dowód: akta kontroli str. 555, 557-558)

Uwagi dotyczące
badanej działalności

Uwarunkowania organizacyjno–techniczne, poprawiające sprawność i szybkość uzyskiwania danych telekomunikacyjnych, dotyczyły wyłącznie danych pozyskiwanych przez Prokuraturę Okręgową od operatora sieci Play (P4 Sp. z o.o.). W przypadku innych operatorów sieci dane telekomunikacyjne pozyskiwała Prokuratura drogą tradycyjną, tj. w formie postanowień i odpowiedzi operatorów przesyłanych drogą pocztową.

2.4. Legalność żądania danych retencyjnych

Opis stanu
faktycznego

Zgodnie z art. 180 a ust. 1 pkt. 1 ustawy Prawo telekomunikacyjne, operator publicznej sieci telekomunikacyjnej oraz dostawca publicznie dostępnych usług telekomunikacyjnych są obowiązani na własny koszt zatrzymywać i przechowywać dane, o których mowa w art. 180 c, generowane w sieci telekomunikacyjnej lub przez nich przetwarzane, na terytorium Rzeczypospolitej Polskiej, przez okres 24 miesięcy¹⁵, licząc od dnia połączenia, a z dniem upływu tego okresu dane te niszczyć, z wyjątkiem tych, które zabezpieczono, zgodnie z przepisami odrębnymi.

Zbadano 83 postanowienia o żądaniu wydania danych telekomunikacyjnych, sformułowane w okresie objętym kontrolą, stwierdzając że w 63,9% przypadków dotyczyły one danych, których okres przechowywania przez operatorów nie był dłuższy niż 24 miesiące.

(dowód: akta kontroli str. 191-210, 224, 234-237, 244-246, 275-276, 278-279, 281-282, 290, 307-308, 352-353, 364, 374-375, 412-421, 439-440, 464-467, 626-627, 790-795).

Natomiast w 30 przypadkach¹⁶ (36,1% zbadanych), w wydanych w Wydziałach V i VI Prokuratury postanowieniach, żądano od operatorów publicznej sieci telekomunikacyjnej udostępnienia danych telekomunikacyjnych za okres dłuższy, niż byli oni zobowiązani je przechowywać (tj. powyżej 24 miesięcy od dnia połączenia lub nieudanej próby połączenia). Przeprowadzona analiza i uzyskane wyjaśnienia w powyższym zakresie wykazały, że:

- 14 postanowień wydano w sprawie o sygn. V Ds 51/09,
- 3 postanowienia wydano w sprawie o sygn. V Ds. 2/11. Prokurator wyjaśnił, że przesłanką dla ich sformułowania był interes śledztwa oraz dążenie do ustalenia wszystkich istotnych okoliczności sprawy,
- 2 postanowienia wydano w sprawie o sygn. V Ds 12/12. Prokurator stwierdził, że analiza dowodów zgromadzonych w toku śledztwa doprowadziła do ustalenia, iż pomocnym dla realizacji celu postępowania będzie uzyskanie od operatorów telekomunikacyjnych informacji o abonentach numerów wskazanych w postanowieniach, a okres za jaki żądano informacji dotyczył przedmiotu postępowania,

¹⁵ Zgodnie z brzmieniem art. 180a ust. 1 pkt 1 obowiązującym do 20 stycznia 2013 r. Od dnia 21 stycznia 2013 r. okres ten wynosi 12 miesięcy.

¹⁶ Postanowienia w sprawach o: 1) sygn. akt V Ds 51/09 z 31 stycznia 2011 r. do TP S.A., 2) sygn. akt V Ds 51/09 z 9 sierpnia 2011 r. do TP S.A., 3) sygn. akt V Ds. 2/11 z 14 lutego 2011 r. do PTK Centertel Sp. z o.o., 4) sygn. akt V Ds. 2/11 z 25 stycznia 2011 r. do Polkomtel S.A., 5) sygn. akt V Ds. 2/11/S, z 25 stycznia 2011 r., do PTK Centertel, 6) sygn. akt V Ds 51/09, z 31 stycznia 2011 r. do Netii, 7) sygn. akt V Ds 51/09, z 9 marca 2011 r. do T-Mobile, 8) sygn. akt V Ds 51/09 z 9 marca 2011 r. do T - Mobile, 9) sygn. akt V Ds 51/09 z 9 marca 2011 r. do T – Mobile, 10) sygn. akt V Ds 51/09 z 9 marca 2011 r. do Polkomtel SA, 11) sygn. akt V Ds 51/09 z 9 marca 2011 r. do PTK Centertel, 12) sygn. akt V Ds 51/09 z 9 marca 2011 r. do PTK Centertel, 13) sygn. akt V Ds 51/09 z 9 marca 2011 r. do PTK Centertel, 14) sygn. akt V Ds 51/09 z 9 sierpnia 2011 r. do UPC Polska, 15) sygn. akt V Ds 12/12 z 26 marca 2012 r. do T-Mobile, 16) sygn. akt V Ds 12/12 z 26 kwietnia 2012 r. do PTK Centertel, 17) sygn. akt V Ds 64/11 z 2 sierpnia 2011 r. do PTK Centertel, 18) sygn. akt VI Ds 66/08 z 28 lipca 2011 r. do PTK Centertel, 19) sygn. akt VI Ds 66/08 z 7 września 2011 r. do PLAY, 20) sygn. akt VI Ds 53/10 z 13 lutego 2012 r. do Polkomtel SA, 21) sygn. akt VI Ds 53/10 z 13 lutego 2012 r. do T-Mobile, 22) sygn. akt VI Ds 53/10 z 13 lutego 2012 r. do Play, 23) sygn. akt VI Ds 62/11 z 14 maja 2012 r. do PTK Centertel, 24) sygn. akt VI Ds 94/11 z 28 maja 2012 r. do UPC Polska, 25) sygn. akt VI Ds 94/11 z 28 maja 2012 r. do PTK Centertel, 26) sygn. akt V Ds 51/09 z 22 sierpnia 2011 r. do PTK Centertel, 27) sygn. akt V Ds 51/09 z 9 marca 2011 r. do TP SA, 28) sygn. akt V Ds 51/09 z 9 marca 2011r. do TP SA, 29) sygn. akt V Ds 80/10 z 10 października 2011 r. do PTK Centertel, 30) sygn. akt V Ds 80/10 z 10 października 2011 r. do Polskiej Telefonii Cyfrowej Sp. z o.o.

- 1 postanowienie wydano w sprawie o sygn. V Ds 64/11. Prokurator wyjaśnił, że przyczyną żądania tych danych był wzgląd na interes śledztwa,
- 2 postanowienia wydano w sprawie o sygn. V Ds 80/10. Prokurator prowadzący wyjaśnił, że żądając wydania danych telekomunikacyjnych za lata 2001-2003 kierował się wyłącznie interesem śledztwa, starając się wykorzystać wszystkie możliwości, by wyjaśnić okoliczności zdarzeń będących przedmiotem postępowania i dotrzeć do ustalenia prawdy materialnej;
- 4 postanowienia wydano w sprawach o sygn. VI Ds 66/08 i sygn. VI Ds 94/11. Prokurator wyjaśniła że przyczyną ich żądania był fakt, iż okres jakiego dotyczyły zdarzenia będące przedmiotem śledztwa wykraczał poza 24 miesięczny czas przechowywania danych telekomunikacyjnych, uzyskanie zaś tych danych było jedynym sposobem ustalenia sprawców przestępstwa;
- 3 postanowienia wydano w sprawie o sygn. VI Ds 53/10. Prokurator wyjaśniła, że przyczyną ich żądania było to, iż okres jakiego dotyczyło zdarzenie przestępne, stanowiące przedmiot śledztwa, był dłuższy niż przewidziany przepisami ustawy Prawo telekomunikacyjne 24-miesięczny termin przechowywania danych telekomunikacyjnych;
- 1 postanowienie wydano w sprawie o sygn. VI Ds 62/11.P Prokurator wyjaśniła, że zażądała od operatora udostępnienia danych osobowych, o których mowa w art. 180 c ustawy Prawo telekomunikacyjne – za okres od stycznia 2008 r. do grudnia 2010 r. – z uwagi na fakt, iż przedmiot śledztwa obejmował ten okres działalności podmiotów i osób fizycznych.
(dowód: akta kontroli str. 207-210, 224, 412-421, 434-442, 461-468, 606-614, 626-627, 790-795, 798-801)

Naczelnik Wydziału V wyjaśnił, że przyczynami żądania ww. danych były: interes śledztwa, dążenie do ustalenia wszystkich istotnych okoliczności sprawy, dążenie do realizacji celów postępowania przygotowawczego określonych w art. 2 § 1 pkt 1 k.p.k. i dążenie do ustalenia prawdy materialnej. Podkreślił, że podając przyczyny żądania ww. danych opierał się na wyjaśnieniach złożonych przez prokuratorów, którzy bezpośrednio zajmowali się postępowaniami. Stwierdził, że jego zdaniem art. 218 k.p.k. nie zawiera żadnej klauzuli limitującej okres za jaki można żądać danych określonych w tym przepisie. Natomiast adresatem normy prawnej zawartej w art. 180 a ust. 1 pkt 1 ustawy Prawo telekomunikacyjne jest operator sieci telekomunikacyjnej i dostawca publicznie dostępnych usług telekomunikacyjnych, a nie prokurator.

(dowód: akta kontroli str. 443-450)

Natomiast Naczelnik Wydziału VI wyjaśnił, że nie analizował ww. postępowań pod kątem sformułowanych w nich żądań wydania danych telekomunikacyjnych. Stwierdził, że z pisemnych informacji przedłożonych mu przez prokuratorów nadzorujących poszczególne postępowania wynika, iż formułując poszczególne postanowienia kierowali się oni przedmiotem konkretnego postępowania.

(dowód: akta kontroli str. 618-621)

Uwagi dotyczące
badanej działalności

W ocenie NIK, występowanie do operatorów telekomunikacyjnych o udostępnienie danych retencyjnych, przekraczających ustawowy okres ich przechowywania, może prowadzić do naruszenia tajemnicy telekomunikacyjnej przez operatorów. NIK zwraca ponadto uwagę na fakt, iż w przypadku udostępnienia wnioskowanych danych mogłoby dojść do nieuprawnionego ich przetwarzania przez prokuratora, gdyż zgodnie z art. 180 a ust. 1 pkt 1 ustawy Prawo telekomunikacyjne, maksymalny czas ich przechowywania, w okresie objętym kontrolą, wynosił 24 miesiące, a po tym okresie dane takie winny zostać usunięte. Należy zauważyć, że obowiązek przekazywania tego typu danych, a także uprawnienie do ich żądania, stanowi wyjątek od zasady tajemnicy telekomunikacyjnej i jak każdy wyjątek od zasad prawnych, w szczególności chroniących konstytucyjne prawa obywatelskie, nie może być interpretowany rozszerzająco.

3. Terminowość realizacji obowiązków ustawowych

Opis stanu
faktycznego

Pod kątem realizacji obowiązku doręczenia postanowienia o żądaniu wydania danych telekomunikacyjnych abonentowi telefonu, którego wykaz połączeń lub innych przekazów informacji wydano¹⁷, zbadano wszystkie postanowienia, wydane w okresie objętym kontrolą, w toku prawomocnie zakończonych postępowań. Badaniem objęto 11 postanowień (wydanych w trakcie 5 postępowań przygotowawczych), stwierdzając że 9 z nich wysłano do abonentów dopiero w trakcie kontroli NIK, po zadaniu przez kontrolera pytań odnośnie braku ich doręczenia. W przypadku dwóch zbadanych postanowień nie było obowiązku doręczenia ich abonentom, ponieważ w związku z nimi nie wydali operatorzy sieci żądanych danych telekomunikacyjnych.

(dowód: akta kontroli str. 169, 383-391, 476, 622-627, 806)

W okresie od 1 stycznia 2011 r. do 30 czerwca 2012 r. Prokuratura nie kierowała do podmiotów prowadzących działalność telekomunikacyjną postanowień o żądaniu zabezpieczenia na nośniku lub w systemie informatycznym danych, o których mowa w art. 180 c i d ustawy Prawo telekomunikacyjne, tj. w trybie art. 218 a k.p.k.

(dowód: akta kontroli str. 387, 391)

Ustalone
nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następujące nieprawidłowości:

Niedoręczenie abonentom telefonów, w terminie nie później niż do czasu prawomocnego zakończenia postępowania, 9 postanowień¹⁸ wydanych w sprawach prawomocnie zakończonych. Stanowiło to naruszenie art. 218 § 2 k.p.k. stanowiącego, że postanowienie takie doręcza się m.in. abonentowi telefonu, którego wykaz połączeń lub innych przekazów informacji wydano. Doręczenie to może być odroczone na czas oznaczony, niezbędny ze względu na dobro sprawy, lecz nie później niż do czasu prawomocnego zakończenia postępowania. Skutkiem powyższego naruszono uprawnienia abonentów telefonów, których dotyczyły ww. postanowienia.

(dowód: akta kontroli str. 169, 191-204, 207-210, 383-388, 473-479, 484-486, 622-627)

Prokurator, który wydał sześć omawianych postanowień (cztery w sprawie o sygn. akt V Ds. 73/10 oraz dwa w sprawie o sygn. akt V Ds. 78/10) wyjaśnił, że przyczyną ich niedoręczenia było sporządzenie ich na drukach, które nie zawierały punktu dotyczącego doręczenia postanowień abonentom telefonów. Ponadto, na podstawie art. 40 ust. 2 pkt. 2 ustawy o NIK odmówił złożenia wyjaśnienia co do innej przyczyny niedoręczenia postanowień (po wskazaniu przez kontrolera, iż niekompletność druków postanowień nie tłumaczy faktu ich niedoręczenia). W wyjaśnieniach nadmienił, że brak doręczenia ww. postanowień został konwalidowany 8 listopada 2012 r. poprzez wysłanie ich do ustalonych na podstawie odpowiedzi operatorów sieci abonentów.

Prokurator, który wydał jedno postanowienie (w sprawie o sygn. akt V Ds. 2/11/S), jako przyczynę jego niedoręczenia wskazał niedopatrzenie, po którego ujawnieniu w dniu 24 października 2012 r. przesłano postanowienie abonentowi. Natomiast prokurator, który

¹⁷ Obowiązek określony w przepisie art. 218 § 2 k.p.k.

¹⁸Postanowienia: 1) z 3 stycznia 2011 r. w sprawie o sygn. akt V Ds. 73/10, do Polkomtel S.A., postępowanie zakończone postanowieniem o umorzeniu śledztwa z dnia 10 maja 2011 r., prawomocne z dniem 20 maja 2011 r. 2) z 3 stycznia 2011 r. w sprawie o sygn. akt V Ds. 73/10, do PTC Sp. z o.o., 3) z 3 stycznia 2011 r. w sprawie o sygn. akt V Ds. 73/10, do P4 Sp. z o.o., 4) z 3 stycznia 2011 r. w sprawie o sygn. akt V Ds. 73/10, do TP S.A., 5) z 12 stycznia 2011 r. w sprawie o sygn. akt V Ds. 78/10, do „Polkomtel” S.A., postępowanie zakończone postanowieniem o umorzeniu śledztwa z 2 grudnia 2011 r., prawomocne z dniem 2 grudnia 2011 r., 6) z 15 marca 2011 r. w sprawie o sygn. akt V Ds. 78/10, do „Polkomtel” S.A., 7) z 25 stycznia 2011 r. w sprawie o sygn. akt V Ds. 2/11/S, do Polkomtel S.A., przesłano abonentowi 24 października 2012 r., postępowanie zakończone postanowieniem o umorzeniu śledztwa z dnia 30 grudnia 2011 r., prawomocne z dniem 30 grudnia 2011 r., 8) z 10 października 2011 r., w sprawie o sygn. akt V Ds. 80/10, do T-Mobile, postępowanie zakończone postanowieniem o umorzeniu śledztwa z 6 sierpnia 2012 r., prawomocne z dniem 22 października 2012 r., wysłano abonentowi 6 grudnia 2012 r., 9) z 10 października 2011 r., w sprawie o sygn. akt V Ds. 80/10, do PTK Centertel, wysłano abonentowi 6 grudnia 2012 r.

wydał dwa postanowienia (w sprawie o sygn. akt V Ds. 80/10) wyjaśnił, że przyczyną ich niedoręczenia był fakt, iż akta sprawy znajdowały się w Sądzie Okręgowym w Katowicach, w związku z zaskarżeniem postanowienia o umorzeniu śledztwa. Podnosił również, że prokurator realizuje jednocześnie szereg innych czynności w sprawach pozostających w jego referacie.

Naczelnik Wydziału V, jako powody niedoręczenia ww. postanowień abonentom, wskazał okoliczności podnoszone przez prokuratorów prowadzących postępowania, stwierdzając, że opierał się na ich wyjaśnieniach. Informował m.in. że przyczyną wysłania odpisów postanowień (w sprawie o sygn. akt V Ds. 80/10) abonentom dopiero 6 grudnia 2012 roku, był fakt, iż akta sprawy znajdowały się w Sądzie, w związku z zaskarżeniem postanowienia o umorzeniu śledztwa. Po ich zwrocie i ponownym zapoznaniu się z nimi, prokurator prowadzący postępowanie zrealizował zarządzenia związane z doręczeniem abonentom odpisów postanowień.

(dowód: akta kontroli str. 216-219, 221-223, 392-394, 401-403, 443-446, 798-806)

Stwierdzono, że akta postępowania w sprawie o sygn. akt V Ds. 80/10 wpłynęły do Prokuratury, po wydaniu przez Sąd Okręgowy w Katowicach postanowienia (sygn. akt XXI Kp 286/12), utrzymującego w mocy zaskarżone postanowienie o umorzeniu śledztwa – w dniu 23 października 2012 r., tj. jeden dzień po uprawomocnieniu się postępowania w tej sprawie.

(dowód: akta kontroli str. 807-808)

Ocena częściowa

Najwyższa Izba Kontroli ocenia negatywnie działalność w badanym obszarze.

Wnioski pokontrolne

IV. Uwagi i wnioski

Przedstawiając powyższe oceny i uwagi wynikające z ustaleń kontroli, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli¹⁹, wnosi o:

1. **Przechowywanie kopert z kodami PIN do Systemu RUDA, zgodnie z wewnętrznymi przepisami obowiązującymi w Prokuraturze.**
2. **Doręczenie abonentom odpisów postanowień o żądaniu wydania danych telekomunikacyjnych.**
3. **Rozważenie potrzeby wprowadzenia w Prokuraturze rejestru postanowień wydawanych w oparciu o art. 218 § 1 k.p.k., w celu ułatwienia prokuratorom prowadzącym postępowania terminowej realizacji obowiązku wynikającego z art. 218 § 2 k.p.k. oraz zapewnienia właściwego nadzoru nad wypełnianiem tego obowiązku.**

V. Pozostałe informacje i pouczenia

Prawo zgłoszenia zastrzeżeń

Wystąpienie pokontrolne zostało sporządzone w dwóch egzemplarzach; jeden dla kierownika jednostki kontrolowanej, drugi do akt kontroli.

Zgodnie z art. 54 ustawy o NIK, kierownikowi jednostki kontrolowanej przysługuje prawo zgłoszenia na piśmie umotywowanych zastrzeżeń do wystąpienia pokontrolnego, w terminie 21 dni od dnia jego przekazania. Zastrzeżenia zgłasza się do Dyrektora Delegatury NIK w Katowicach.

Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków

Zgodnie z art. 62 ustawy o NIK, proszę o poinformowanie Najwyższej Izby Kontroli Delegatury w Katowicach, w terminie 15 dni od otrzymania wystąpienia pokontrolnego, o sposobie wykorzystania uwag i wykonania wniosków pokontrolnych oraz o podjętych działaniach lub przyczynach niepodjęcia tych działań.

¹⁹ Dz. U. z 2012 r., poz.82

W przypadku wniesienia zastrzeżeń do wystąpienia pokontrolnego, termin przedstawienia informacji liczy się od dnia otrzymania uchwały o oddaleniu zastrzeżeń w całości lub zmienionego wystąpienia pokontrolnego.

Katowice, dnia 7 lutego 2013 r.

Kontroler
Anna Loppe
Gł. specjalista kontroli państwowej

Najwyższa Izba Kontroli
Delegatura w Katowicach
z up. Wicedyrektor
Eugeniusz Rejman

.....

.....