KPB-P/12/191
Nr ewid. 107/2013/P/12/191/KPB
Wersja jawna

Informacja o wynikach kontroli

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

MISJĄ

Najwyższej Izby Kontroli jest dbałość o gospodarność i skuteczność w służbie publicznej dla Rzeczypospolitej Polskiej

WIZJĄ

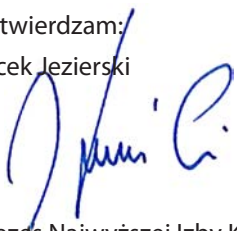
Najwyższej Izby Kontroli jest cieszący się powszechnym autorytetem najwyższy organ kontroli państwowej, którego raporty będą oczekiwanym i poszukiwanym źródłem informacji dla organów władzy i społeczeństwa

Radca Prezesa NIK
p. o. Dyrektor Departamentu Porządku
i Bezpieczeństwa Wewnętrznego:
Marek Bieńkowski

Akceptuję:
Marian Cichosz

Wiceprezes Najwyższej Izby Kontroli

Zatwierdzam:
Jacek Jezierski



Prezes Najwyższej Izby Kontroli
dnia 12 czerwca 2013

Najwyższa Izba Kontroli
ul. Filtrowa 57
02-056 Warszawa
T/F +48 22 444 50 00

www.nik.gov.pl

Spis treści

WPROWADZENIE 5

1. ZAŁOŻENIA KONTROLI 6

2. PODSUMOWANIE WYNIKÓW KONTROLI 8
   2.1. Ogólna ocena kontrolowanej działalności 8
   2.2. Przestrzeganie praw i wolności obywatelskich w związku z pozyskiwaniem danych telekomunikacyjnych 13
   2.3. Uwagi końcowe i wnioski 17

2. WAŻNIEJSZE WYNIKI KONTROLI 18
   3.1. Charakterystyka obszaru objętego kontrolą 18
   3.2. Istotne ustalenia kontroli 23
      3.2.1. Agencja Bezpieczeństwa Wewnętrznego 23
      3.2.2. Centralne Biuro Antykorupcyjne 25
      3.2.3. Policja 30
      3.2.4. Służba Kontrwywiadu Wojskowego 35
      3.2.5. Straż Graniczna 38
      3.2.6. Żandarmeria Wojskowa 42
      3.2.7. Ministerstwo Finansów 46
      3.2.8. Urząd Komunikacji Elektronicznej 48
      3.2.9. Sądy 52
      3.2.10. Prokuratury 54
      3.2.11. Przedsiębiorcy telekomunikacyjni 56
      3.2.12. Retencja danych a prawa i wolności obywatelskie 59
   3.3. Dobre praktyki 72

4. INFORMACJE DODATKOWE O PRZEPROWADZONEJ KONTROLI 74
   4.1. Przygotowanie kontroli 74
   4.2. Postępowanie kontrolne i działania podjęte po zakończeniu kontroli 74

5. ZAŁĄCZNIKI 76

Wykaz stosowanych skrótów i pojęć

ABW	Agencja Bezpieczeństwa Wewnętrznego
CBA	Centralne Biuro Antykorupcyjne
GIODO	Generalny Inspektor Ochrony Danych Osobowych
KGP	Komenda Główna Policji
KWP	Komenda Wojewódzka Policji
KG SG	Komenda Główna Straży Granicznej
SKW	Służba Kontrwywiadu Wojskowego
UKE	Urząd Komunikacji Elektronicznej
ŻW	Żandarmeria Wojskowa
Prawo telekomunikacyjne	Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. Nr 171 poz. 1800 ze zm.)
ustawa o NIK	Ustawa z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2012 r., poz. 82 ze zm.)
ustawa o Policji	Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2011 r. Nr 287, poz. 1687 ze zm.)
ustawa o Straży Granicznej	Ustawa z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2011 r. Nr 116, poz. 675 ze zm.)
ustawa o ABW	Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2010 r. Nr 29, poz. 154 ze zm.)
ustawa o CBA	Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. z 2012 r., poz. 621)
ustawa o Żandarmerii Wojskowej	Ustawa z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. Nr 123, poz. 1353 ze zm.)
ustawa o SKW i SWW	Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. Nr 104, poz. 709 ze zm.)
ustawa o ochronie danych osobowych	Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.)
ustawa o ochronie informacji niejawnych	Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228)
dane telekomunikacyjne (dane retencyjne)	dane, o których mowa w art. 180c i d Prawa telekomunikacyjnego

WPROWADZENIE

Kontrola została przeprowadzona z inicjatywy własnej Najwyższej Izby Kontroli w związku z przygotowywaną nowelizacją Prawa Telekomunikacyjnego w zakresie retencji oraz uzyskiwania danych telekomunikacyjnych przez uprawnione podmioty. Przyczyną podjęcia przedmiotowej kontroli były również liczne doniesienia mediów i organizacji społecznych wskazujące na społeczne zapotrzebowanie dokonania wiarygodnej analizy i oceny, przez zewnętrzną i niezależną instytucję, obowiązujących przepisów i procedur stosowanych przez podmioty uprawnione do żądania danych telekomunikacyjnych. Analiza przedkontrolna przeprowadzona przez NIK wskazywała, że w związku z pozyskiwaniem i przetwarzaniem danych telekomunikacyjnych może dochodzić do naruszenia praw i wolności obywatelskich. Z drugiej strony pojawiały się argumenty, iż bez wykorzystania tego środka, wykrycie sprawców wielu przestępstw nie byłoby możliwe. Kontrola miała dostarczyć niezbędnych materiałów do przeprowadzenia analizy ww. zakresie oraz ewentualnego sformułowania wniosków w przedmiocie zmian obowiązujących przepisów bądź utrwalonej praktyki.

1 ZAŁOŻENIA KONTROLI

Kontrola planowa nr P/12/191 – Uzyskiwanie i przetwarzanie przez uprawnione podmioty danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180c i d ustawy Prawo telekomunikacyjne[1] została przeprowadzona z inicjatywy Najwyższej Izby Kontroli. W porozumieniu z Prezesem NIK, kontrolę równoległą u operatorów telekomunikacyjnych przeprowadził Generalny Inspektor Ochrony Danych Osobowych.

Cel główny kontroli

Celem głównym kontroli była ocena procesu uzyskiwania i przetwarzania przez uprawnione podmioty danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180c i d ustawy Prawo telekomunikacyjne.

Cele szczegółowe

Celem kontroli była ocena:

1. Przyjętych uregulowań wewnętrznych oraz ustanowionej struktury organizacyjnej, w obszarze uzyskiwania, przetwarzania, wykorzystania i niszczenia danych telekomunikacyjnych.
2. Wykorzystywania, przez uprawnione służby i organy państwa, przyznanych im uprawnień, a w szczególności przestrzeganie obowiązujących zasad, przepisów ustawowych oraz procedur wewnętrznych w zakresie żądania, uzyskiwania, przetwarzania, wykorzystania i niszczenia danych telekomunikacyjnych.
3. Realizacji przez Prezesa Urzędu Komunikacji Elektronicznej zadań w zakresie regulacji i kontroli rynku usług telekomunikacyjnych, oraz skuteczności w tworzeniu warunków realizacji zasady subsydiarności[2] w dziedzinie uzyskiwania przez uprawnione podmioty danych telekomunikacyjnych.
4. Zabezpieczenia danych telekomunikacyjnych oraz terminowości realizacji obowiązków ustawowych przez jednostki organizacyjne sądów i prokuratur.
5. Działań operatorów i przedsiębiorców telekomunikacyjnych w zakresie zgodności pozyskiwania, przechowywania i przekazywania danych z obowiązującymi przepisami, w tym w szczególności przepisami o ochronie danych osobowych[3].

Kontrola miała również za zadanie zidentyfikowanie w przepisach dotyczących żądania, uzyskiwania, przetwarzania, wykorzystania i niszczenia danych telekomunikacyjnych obszarów wymagających zmian legislacyjnych, w tym wskazanie przepisów, które ze względu na sposób zapisu, brak definicji, trudności interpretacyjne, nie są możliwe do precyzyjnego i jednolitego zastosowania, a także wskazanie dobrych praktyk, których wdrożenie może przyczynić się do ograniczenia występujących w tym obszarze nieprawidłowości.

---

1 Dane niezbędne do: 1) ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego: a) inicjującego połączenie, b) do którego kierowane jest połączenie; 2) określenia: a) daty i godziny połączenia oraz czasu jego trwania, b) rodzaju połączenia, c) lokalizacji telekomunikacyjnego urządzenia końcowego oraz dane, o których mowa w art. 159 ust. 1 pkt 1 i 3-5, w art. 161 oraz w art. 179 ust. 9 (Dz. U. Nr 171, poz. 1800 ze zm.).

2 Zasada subsydiarności oznacza, iż określone środki mogą mieć zastosowanie jedynie wówczas, gdy użycie innych środków do osiągnięcia zamierzonego celu nie jest możliwe lub jest nadmiernie utrudnione. Zasada subsydiarności ma chronić obywateli przed nadmierną ingerencją państwa w sferę ich praw i wolności.

3 Cel realizowany przez GIODO w ramach kontroli równoległej.

Podstawa prawna, kryteria kontroli

Kontrolę przeprowadzono na podstawie art. 2 ust. 1 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[4], zgodnie z kryteriami określonymi w art. 5 ust. 1 ustawy, tj. legalności, gospodarności, celowości i rzetelności.

Zakres przedmiotowy kontroli

Kontrolą objęto proces uzyskiwania 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. Zakres kontroli prowadzonej przez NIK musiał ulec jednakże znacznemu ograniczeniu, ze względu na przepisy dotyczące niezależności sądów i niezawisłości sędziowskiej oraz przepisy ustaw szczegółowych, wyłączające spod kontroli NIK, sprawy związane z prowadzeniem czynności operacyjno-rozpoznawczych[5]. NIK nie mogła również objąć kontrolą działalności operatorów telekomunikacyjnych, ze względu na fakt, iż są podmiotami prywatnymi. W niniejszej Informacji wykorzystano jednakże wyniki kontroli równoległej przeprowadzonej przez GIODO u pięciu niżej wymienionych operatorów telekomunikacyjnych, w zakresie zgodności przetwarzania danych z przepisami ustawy o ochronie danych osobowych[6].

Zakres podmiotowy kontroli

Kontrolą objęto Agencję Bezpieczeństwa Wewnętrznego, Centralne Biuro Antykorupcyjne, wybrane jednostki Policji (Komendę Główną Policji, 3 Komendy Wojewódzkie), Komendę Główną Straży Granicznej, Służbę Kontrwywiadu Wojskowego, Żandarmerię Wojskową, Ministerstwo Finansów (Służba Celna oraz Departament Wywiadu Skarbowego), 3 wybrane Sądy Okręgowe oraz 4 Prokuratury Okręgowe, a także Urząd Komunikacji Elektronicznej.
Kontrolą GIODO objęci zostali: Polska Telefonia Cyfrowa S.A., Netia S.A., Polkomtel Sp. z o. o., P4 Sp. z o.o., Polska Telefonia Komórkowa – Centertel Sp. z o.o.

Wykaz jednostek objętych kontrolą przedstawiono w załączniku nr 5.1. na str. 76 Informacji.

Okres objęty kontrolą

Kontrolą objęto okres od 1 stycznia 2011 do 30 czerwca 2012 r. Uwzględniono w niej ponadto działania i zdarzenia zaistniałe przed i po ww. okresie, mające bezpośredni związek z zagadnieniami będącymi przedmiotem kontroli.

4 Dz. U. Nr 227, poz. 1482 ze zm.

5 Kwestia ta została szczegółowo omówiona w pkt 3.1. na str. 20 i n.

6 Raport GIODO zostanie opublikowany równocześnie z Informacją NIK.

2 PODSUMOWANIE WYNIKÓW KONTROLI

2.1 Ogólna ocena kontrolowanej działalności

Najwyższa Izba Kontroli ocenia pozytywnie, pomimo stwierdzonych nieprawidłowości[7], działalność kontrolowanych organów, służb i formacji w zakresie uzyskiwania i przetwarzania przez nie danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180c i d ustawy Prawo telekomunikacyjne[8].

W ocenie NIK, system pozyskiwania i przetwarzania ww. danych[9] zapewniał realizację ustawowych zadań przez kontrolowane podmioty. Wprowadzone zasady i procedury umożliwiały szybkie i sprawne pozyskiwanie danych w związku z prowadzonymi postępowaniami. Możliwość sięgania po dane telekomunikacyjne mieli jedynie upoważnieni pracownicy i funkcjonariusze, a krąg osób posiadających takie upoważnienie był w kontrolowanych instytucjach ściśle określony.

Stwierdzone nieprawidłowości wiązały się m.in. z: przypadkami nieprzestrzegania obowiązujących przepisów, zasad i procedur oraz naruszenia tajemnicy telekomunikacyjnej; pozyskiwaniem danych za pośrednictwem sieci telekomunikacyjnej i systemów teleinformatycznych niespełniających wymagań technicznych i organizacyjnych; żądaniem udostępnienia danych telekomunikacyjnych za okres przekraczający 24 m-ce[10], nieusuwaniem zbędnych danych telekomunikacyjnych; brakiem właściwego nadzoru nad realizowanymi działaniami, w tym w szczególności nad przestrzeganiem przez przedsiębiorców telekomunikacyjnych obowiązków określonych w Prawie telekomunikacyjnym.

W ocenie NIK, obowiązujące przepisy w zakresie pozyskiwania przez uprawnione podmioty danych telekomunikacyjnych nie chronią w stopniu wystarczającym praw i wolności obywatelskich przed nadmierną ingerencją ze strony państwa. Niejednolitość i ogólnikowość przepisów uprawniających do pozyskiwania danych telekomunikacyjnych[11], może nasuwać wątpliwości, co do współmierności stosowanych ograniczeń praw i wolności obywatelskich w sferze wolności komunikacji z zasadami określonymi w Konstytucji RP.

Należy ponadto zauważyć, iż obowiązujący system zbierania informacji o zakresie wykorzystania przez organy państwa danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180c i d ustawy Prawo telekomunikacyjne, nie pozwala na określenie rzeczywistej liczby dokonywanych sprawdzeń. Brak jest również mechanizmów kontroli o charakterze zewnętrznym, które pozwoliłyby na weryfikację zakresu wykorzystywania danych telekomunikacyjnych przez uprawnione podmioty, a w szczególności zasadności ich pozyskiwania i przetwarzania.

---

7 Standardy kontroli NIK przewidują trzystopniową skalę ocen kontrolowanej działalności: ocena pozytywna, ocena pozytywna mimo stwierdzonych nieprawidłowości i ocena negatywna.

8 Ocena ta została wydana w oparciu o badanie strony organizacyjno-formalnej uzyskiwania przez uprawnione podmioty danych telekomunikacyjnych. Ze względu na ograniczenia ustawowe kompetencji kontrolnych NIK, przedmiotem kontroli nie mogła być ocena zasadności pozyskiwania przez uprawnione podmioty danych telekomunikacyjnych.

9 Kwestie te zostały szczegółowo omówione w rozdziale 3 Informacji.

10 Po nowelizacji ustawy Prawo Telekomunikacyjne z dnia 16 listopada 2012 r. (Dz. U. z 2012 r., poz. 1445) termin ten od 21 stycznia 2013 r. uległ skróceniu do 12 m-cy.

11 Kwestie te omówiono szerzej w podrozdziale 3.1. na str. 18-23 oraz 5.4 na str. 82-88.

Agencja Bezpieczeństwa Wewnętrznego

NIK oceniła pozytywnie działalność Szefa Agencji Bezpieczeństwa Wewnętrznego w zakresie objętym kontrolą.

Pozyskiwanie i wykorzystywanie danych telekomunikacyjnych w ABW odbywało się zgodnie z przepisami oraz regulacjami wewnętrznymi. Wewnętrzne procedury były kompletne, spójne i gwarantowały bezpieczeństwo pozyskanych danych telekomunikacyjnych, minimalizując ryzyko nadużyć. Działania Szefa ABW w powyższym zakresie wsparte były prawidłowo działającym systemem kontroli wewnętrznej.

Uchybienia dotyczyły: braku skutecznej reakcji ABW na fakt otrzymywania od operatorów danych telekomunikacyjnych w szerszym zakresie, niż wynikało to ze stosownego zapytania.

[szerzej o wynikach kontroli ABW na str. 23 Informacji]

Centralne Biuro Antykorupcyjne

NIK oceniła pozytywnie, pomimo stwierdzonych nieprawidłowości, działalność Szefa Centralnego Biura Antykorupcyjnego w objętym kontrolą zakresie.

Szef Centralnego Biura Antykorupcyjnego prawidłowo unormował zasady uzyskiwania i przetwarzania w CBA danych, o których mowa w art. 180c i d Prawa telekomunikacyjnego. Pozyskane dane zostały zabezpieczone przed nieuprawnionym dostępem lub zniszczeniem. Zapewniono także poufność przekazywania danych pomiędzy uprawnionymi komórkami organizacyjnymi CBA.

W trakcie kontroli stwierdzono jednakże przypadki naruszenia obowiązujących przepisów wewnętrznych, przy udzielaniu upoważnień do występowania o udostępnienie danych telekomunikacyjnych. Ujawniono również nieprawidłowości w zakresie pozyskiwania danych za pośrednictwem sieci telekomunikacyjnej i systemów teleinformatycznych. Ponadto ustalono, iż Szef CBA nie dysponował pełnym zakresem informacji, które umożliwiłyby sprawowanie rzetelnego nadzoru nad pozyskiwaniem danych telekomunikacyjnych w przypadku zapytań kierowanych za pomocą systemów teleinformatycznych.

[szerzej o wynikach kontroli CBA na str. 25 Informacji]

Policja

NIK oceniła pozytywnie, pomimo stwierdzonych nieprawidłowości, działalność Komendanta Głównego Policji w zakresie objętym kontrolą.

Komendant Główny Policji prawidłowo uregulował w KGP sposób udzielania pisemnych upoważnień do uzyskiwania danych telekomunikacyjnych oraz zapewnił nadzór nad ich pozyskiwaniem i przetwarzaniem. Pozyskane dane zostały prawidłowo zabezpieczone przed nieuprawnionym dostępem. Zapewniono także poufność przekazywania danych pomiędzy uprawnionymi komórkami organizacyjnymi KGP.

W trakcie kontroli ujawniono nieprawidłowości w zakresie pozyskiwania danych za pośrednictwem sieci telekomunikacyjnej i systemów teleinformatycznych oraz usuwania zbędnych danych telekomunikacyjnych. NIK zwróciła również uwagę na brak odpowiednich procedur wewnętrznych, które zapobiegłyby wystąpieniu nieprawidłowości lub pozwoliłyby na bieżąco je eliminować.

NIK pozytywnie oceniła działalność Komendantów Wojewódzkich Policji w Katowicach, Rzeszowie i Wrocławiu. Wydając oceny pozytywne, NIK wzięła pod uwagę, iż ww. Komendanci funkcjonują w ramach zhierarchizowanej struktury organizacyjnej, co skutkowało ograniczonym ich wpływem na prawidłowość realizacji zadań związanych z dostępem do danych telekomunikacyjnych.

[szerzej o wynikach kontroli Policji na str. 30 Informacji]

Służba Kontrwywiadu Wojskowego

Najwyższa Izba Kontroli oceniła pozytywnie działalność Szefa SKW w zbadanym zakresie.

Szef SKW, w ramach posiadanych kompetencji, uregulował i doprecyzował aktami wewnętrznymi zasady uzyskiwania i przetwarzania w SKW danych od operatorów telekomunikacyjnych. Pozyskane dane zostały prawidłowo zabezpieczone przed nieuprawnionym dostępem oraz przed ich utratą lub zniszczeniem. Zapewniono także poufność przekazywania danych pomiędzy uprawnionymi jednostkami organizacyjnymi SKW.

[szerzej o wynikach kontroli SKW na str. 35 Informacji]

Straż Graniczna

Najwyższa Izba Kontroli oceniła pozytywnie działalność Komendanta Głównego Straży Granicznej w zakresie objętym kontrolą.

Komendant Główny Straży Granicznej prawidłowo zorganizował system uzyskiwania i przetwarzania danych telekomunikacyjnych. Ustanowiono zabezpieczenia techniczne i organizacyjne uniemożliwiające wykorzystanie danych telekomunikacyjnych niezgodnie z celem ich uzyskania, wprowadzono mechanizmy w celu eliminacji ryzyka wystąpienia zdarzeń niepożądanych, określono procedury niszczenia danych telekomunikacyjnych niemających znaczenia dla postępowania karnego. Prawidłowo zorganizowano współpracę z przedsiębiorcami telekomunikacyjnymi.

Uchybienia dotyczyły braku rejestru osób upoważnionych do uzyskiwania danych za pomocą sieci telekomunikacyjnej, nieokreślenia zadań w zakresie pozyskiwania danych telekomunikacyjnych w regulaminach wewnętrznych niektórych komórek organizacyjnych i zakresach obowiązków funkcjonariuszy. Stwierdzono również pojedyncze przypadki naruszenia obowiązujących przepisów i procedur.

[szerzej o wynikach kontroli Straży Granicznej na str. 38 Informacji]

Żandarmeria Wojskowa

Najwyższa Izba Kontroli oceniła pozytywnie działalność Komendanta Głównego Żandarmerii Wojskowej w kontrolowanym zakresie.

Przyjęte w Komendzie Głównej Żandarmerii Wojskowej rozwiązania organizacyjno-prawne oraz techniczne zapewniały bezpieczeństwo pozyskiwania i przetwarzania danych telekomunikacyjnych. Przyjęty tryb postępowania eliminował ryzyko wystąpienia zdarzeń niepożądanych w zakresie nieuprawnionego dostępu do danych telekomunikacyjnych.

[szerzej o wynikach kontroli ŻW na str. 42 Informacji]

Ministerstwo Finansów

Najwyższa Izba Kontroli oceniła pozytywnie działalność Ministra Finansów w zbadanym zakresie.

W Ministerstwie Finansów prawidłowo unormowano zasady uzyskiwania i przetwarzania danych, o których mowa w art. 180c i d Prawa telekomunikacyjnego. Działania dotyczące uzyskiwania i przetwarzania danych były realizowane przez Departament Wywiadu Skarbowego zgodnie z wytycznymi zawartymi w ustawie o kontroli skarbowej. Pozyskane dane zostały zabezpieczone przed nieuprawnionym dostępem lub zniszczeniem. Zapewniono także poufność przekazywania danych pomiędzy uprawnionymi komórkami organizacyjnymi.

[szerzej o wynikach kontroli MF na str. 46 Informacji]

Urząd Komunikacji Elektronicznej

Najwyższa Izba Kontroli negatywnie oceniła działalność Prezesa UKE w zakresie nadzoru nad realizacją obowiązków informacyjnych określonych w art. 180g ust. 1 ustawy Prawo telekomunikacyjne oraz realizację obowiązku sprawozdawczego określonego w art. 180g ust. 2 ww. ustawy, a także nadzór i kontrolę Prezesa UKE nad przestrzeganiem przez przedsiębiorców telekomunikacyjnych obowiązków określonych w art. 180a, 180 c i 180d ustawy.

Prezes UKE nie sprawował, pomimo posiadania stosownych kompetencji ustawowych, skutecznego nadzoru nad wywiązywaniem się przez przedsiębiorców telekomunikacyjnych z nałożonych na nich obowiązków.

Opracowywane przez Prezesa UKE informacje w zakresie wykorzystania przez uprawnione podmioty danych retencyjnych nie odpowiadały stanowi rzeczywistemu. Prezentowane informacje były niepełne, a przedstawiane przez poszczególne podmioty dane nieporównywalne. Ze względu na popełnione błędy metodologiczne oraz zaniedbania, jakiekolwiek wnioskowanie statystyczne na ich podstawie w przedmiocie zakresu retencji danych w Polsce, jest w ocenie NIK nieuprawnione.

[szerzej o wynikach kontroli UKE na str. 48 Informacji]

Sądy

Najwyższa Izba Kontroli oceniła pozytywnie administracyjno-organizacyjną działalność Sądu Okręgowego w Bydgoszczy oraz w Szczecinie w zakresie uzyskiwania i przetwarzania danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180 c i d Prawa Telekomunikacyjnego. Przedmiotem oceny NIK nie była jednakże, stosownie do ograniczeń ustawowych, działalność orzecznicza – w związku z tym, w zakresie objętym kontrolą, zebrano jedynie informacje o charakterze statystycznym, opierając się na dokumentach udostępnionych przez sądy oraz operatorów telekomunikacyjnych[12].

W wyniku analizy ww. informacji stwierdzono m.in. liczne przypadki: kierowania wniosków o udostępnienie danych telekomunikacyjnych w sprawach cywilnych, bez uzyskania uprzednio zgody abonenta; wskazywania niewłaściwych przepisów, jako podstawy udostępnienia danych telekomunikacyjnych; żądania treści sms-ów oraz powoływania się na przepisy postępowania karnego w sprawach cywilnych; występowania o dane telekomunikacyjne za okres przekraczający

[12] Kwestia ta została szczegółowo omówiona w pkt 3.1. na str. 18.

24 miesiące[13]; odmowy udostępnienia przez operatorów danych telekomunikacyjnych, ze względu na brak podstawy prawnej do takiego wystąpienia i uchylenia tajemnicy telekomunikacyjnej lub na niewykonalność postanowienia Sądu z innych przyczyn formalno-prawnych; nie realizowania obowiązku informacyjnego, w stosunku do osób, których dane telekomunikacyjne pozyskiwano. W ocenie NIK, biorąc pod uwagę systematyczny (powtarzający się) charakter wyżej opisanych nieprawidłowości, istnieje wysokie ryzyko ich występowania również w innych sądach. O stwierdzonych nieprawidłowościach NIK, w trybie art. 62a ustawy o NIK, zawiadomiła Ministra Sprawiedliwości[14], który poinformował, że rozważy podjęcie, w ramach posiadanych kompetencji, stosownych działań. NIK zwróciła ponadto uwagę na fakt, iż brak dostępu do danych telekomunikacyjnych za pomocą systemów teleinformatycznych, wydłużał o kilka tygodni czas niezbędny na uzyskanie danych telekomunikacyjnych na potrzeby toczącego się postępowania.

W Sądzie Okręgowym w Warszawie kontrola nie została zakończona – po stwierdzeniu przez kontrolera NIK niezgodności prezentowanych danych ze stanem faktycznym, Prezes Sądu uniemożliwiła dalsze prowadzenie czynności kontrolnych, powołując się na zasadę niezawisłości sędziowskiej[15].

[szerzej o wynikach kontroli Sądów na str. 52 Informacji]

Prokuratury

Najwyższa Izba Kontroli oceniła pozytywnie, pomimo stwierdzonych nieprawidłowości, działalność Prokuratury Okręgowej w Warszawie i Katowicach oraz pozytywnie działalność Prokuratury Okręgowej w Rzeszowie i Wrocławiu, w zakresie uzyskiwania i przetwarzania danych, o których mowa w art. 180c i d ustawy Prawo telekomunikacyjne.

Kontrolowani Prokuratorzy Okręgowi określili zasady bezpieczeństwa oraz organizacji pracy przy uzyskiwaniu danych telekomunikacyjnych oraz zapewnili przekazywanie prokuratorom danych telekomunikacyjnych udostępnionych za pomocą systemu teleinformatycznego, zgodnie z treścią wydanych przez nich postanowień.

W trakcie kontroli stwierdzono jednakże, iż prokuratorzy nie wydawali zarządzeń o doręczeniu postanowień[16] informujących obywateli o pozyskaniu ich danych telekomunikacyjnych w związku z toczącym się postępowaniem lub wydawali je ze znacznym opóźnieniem, w stosunku do terminu określonego w art. 218 § 2 zd. 2 ustawy z dnia 6 czerwca 1997 r. Kodeks postępowania karnego[17]. Ponadto stwierdzono przypadki żądania udostępnienia danych telekomunikacyjnych za okres przekraczający 24 m-ce, żądania udostępnia treści przekazów telekomunikacyjnych w niewłaściwym trybie, naruszenia obowiązujących przepisów wewnętrznych.

NIK zwróciła ponadto uwagę na fakt, iż brak dostępu do danych telekomunikacyjnych za pomocą systemów teleinformatycznych (za wyjątkiem umowy z jednym przedsiębiorcą telekomunikacyjnym), o kilka tygodni wydłużał czas niezbędny do uzyskania danych telekomunikacyjnych na potrzeby toczącego się postępowania. Biorąc pod uwagę, że najwięksi

13 Obecnie okres ten uległ skróceniu do 12 miesięcy.
14 Pismo nr KPB-4101-04-00/2012 z dnia 19 lutego 2013 r.
15 Kwestia ta została szczegółowo omówiona na str. 20-22 Informacji.
16 Postanowienia są doręczane w formie odpisów.
17 Dz. U. z 1997 r., Nr 89, poz. 555 ze zm.

operatorzy telekomunikacyjni opracowali stosowne systemy umożliwiające dostęp elektroniczny, ich wykorzystanie znacząco skróciłoby dostęp do danych.

[szerzej o wynikach kontroli Prokuratur na str. 54 Informacji]

Operatorzy telekomunikacyjni

GIODO, w toku przeprowadzonych kontroli, nie stwierdził uchybień w procesie przetwarzania danych osobowych w zakresie objętym kontrolą. Zwrócił natomiast uwagę na pewne odmienności w interpretacji przepisów dotyczących udostępniania danych telekomunikacyjnych w sprawach o wykroczenia i sprawach cywilnych.

Ponadto prowadzona przez NIK kontrola w podmiotach uprawnionych do pozyskiwania danych telekomunikacyjnych wykazała, iż udostępnione przez niektórych z przedsiębiorców telekomunikacyjnych systemy generowały dane telekomunikacyjne w zakresie szerszym, niż wynikało to zakresu zapytania. Stanowiło to naruszenie art. 160 ust. 1, w związku z art. 159 ust. 1 pkt 3-5 i ust. 3 ustawy Prawo telekomunikacyjne oraz art. 218 § 1 kpk. Izba, stosownie do art. 63 ust. 3 ustawy o NIK, zawiadomiła Prezesa Urzędu Komunikacji Elektronicznej o naruszeniu obowiązku zachowania tajemnicy telekomunikacyjnej.

[szerzej o wynikach kontroli Operatorów telekomunikacyjnych na str. 56 Informacji]

2.2 Przestrzeganie praw i wolności obywatelskich w związku z pozyskiwaniem danych telekomunikacyjnych

Określenie zakresu dopuszczalnej ingerencji państwa w prawa i wolności obywateli jest jednym z fundamentalnych wyzwań demokracji. Odpowiedź na pytanie o zakres dopuszczalnej ingerencji staje się szczególnie trudna, gdy mamy do czynienia z sytuacją, kiedy ingerencja w prawa i wolności obywatelskie znajduje uzasadnienie w konieczności zapewnienia realizacji innych praw podstawowych, takich jak prawo do życia w bezpiecznym otoczeniu, czy też jest uznawana, jako niezbędny środek do zwalczania np. terroryzmu, handlu ludźmi, bądź zagrożeń dla bezpieczeństwa państwa. Jednym z przykładów uprawnień państwa, w sposób istotny ingerującego w sferę praw i wolności obywateli, a w szczególności prawo do prywatności, są uprawnienia przyznane poszczególnym służbom i formacjom do sięgania po dane telekomunikacyjne obywateli. Dlatego podstawowym celem kontroli przeprowadzonej przez NIK było zbadanie, czy w związku z pozyskiwaniem i przetwarzaniem danych telekomunikacyjnych właściwie chronione są prawa i wolności obywateli.

W ocenie NIK, obowiązujące przepisy w zakresie pozyskiwania przez uprawnione podmioty danych telekomunikacyjnych nie chronią w stopniu wystarczającym praw i wolności obywatelskich przed nadmierną ingerencją ze strony państwa. Biorąc pod uwagę istniejące uwarunkowania prawno-organizacyjne, projektowane zmiany przepisów na poziomie Unii Europejskiej (UE), a także wyniki przeprowadzonej kontroli, należy rozważyć podjęcie działań w czterech zasadniczych obszarach:

- **zakresu i celu pozyskiwania danych;**
- **kontroli nad procesem pozyskiwania danych;**
- **niszczenia pozyskanych danych w sytuacji, gdy nie są już one dalej niezbędne dla osiągnięcia celów prowadzonego postępowania;**
- **stworzenia mechanizmów sprawozdawczych, które zapewnią rzetelną informację o zakresie pozyskiwania danych telekomunikacyjnych.**

Zakres i cel pozyskiwania danych

Zakres i cel pozyskiwanych przez uprawnione podmioty danych są głównymi czynnikami wpływającymi na ocenę stopnia, ingerencji w prawa obywatelskie. Zgodnie z przepisami Prawa telekomunikacyjnego, operatorzy telekomunikacyjni obowiązani są do przechowywania i udostępniania uprawnionym podmiotom danych niezbędnych do ustalenia: tożsamości osób dokonujących połączenia; identyfikacji urządzeń, za pomocą których dokonano połączenia; miejsc, w których znajdowały się urządzenia; daty i godziny połączenia oraz czasu jego trwania; rodzaju połączenia[18]; a także innych, znajdujących się w posiadaniu operatora danych użytkownika[19]. Zakres pozyskiwanych danych, w ocenie NIK, umożliwiał właściwą realizację zadań przez podmioty uprawnione do pozyskiwania danych telekomunikacyjnych.

W ocenie NIK, doprecyzowania wymaga jednakże cel gromadzenia danych retencyjnych. Obecnie obowiązujące przepisy odwołują się jedynie do zakresu zadań poszczególnych służb bądź ogólnego stwierdzenia, iż dane te są pozyskiwanie w celu zapobiegania lub wykrywania przestępstw. Należy przy tym zauważyć, iż przepisy te umożliwiają wykorzystywanie danych retencyjnych nie tylko do wykrywania przestępstw, ale także w działaniach prewencyjnych czy analitycznych. Precyzyjne określenie katalogu spraw, w których uprawnione służby mogą pozyskiwać dane telekomunikacyjne, ma kluczowe znaczenie dla oceny, czy obowiązujące przepisy nie naruszają zasady proporcjonalności, a tym samym są dopuszczalne w świetle obowiązujących przepisów chroniących prawa i wolności obywatelskie.

Udostępnienie danych telekomunikacyjnych powinno uwzględniać również zasadę subsydiarności[20]. Zgodnie z obowiązującymi przepisami, uprawnione podmioty mogą zwrócić się o udostępnienie danych telekomunikacyjnych w każdym wypadku, a nie jedynie wówczas, „gdy inne środki podejmowane w celu realizacji ustawowego celu okazały się bezskuteczne". Konieczne jest więc wprowadzenie przepisów, które wykorzystanie danych telekomunikacyjnych będą uzależniać od niemożności zastosowania innych, mniej ingerujących w prawa obywatelskie środków.

Obecnie obowiązujące przepisy nie wskazują kategorii osób, w stosunku do których nie można pozyskiwać danych telekomunikacyjnych ze względu na respektowanie ich tajemnicy zawodowej. Ustawodawca nie wyłączył żadnej kategorii użytkowników z kręgu podmiotów, których dane mogą być pozyskiwane, choć dane te mogą być objęte tajemnicą notarialną, adwokacką, radcy prawnego, lekarską lub dziennikarską, której zniesienie jest możliwe wyłącznie, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a dana okoliczność nie może być ustalona na podstawie innego dowodu[21]. W ocenie NIK, należałoby rozważyć wprowadzenie rozwiązań, które będą stwarzać dodatkowe gwarancje w przypadku osób wykonujących tzw. „zawody zaufania publicznego", np. poprzez uzależnienie pozyskania danych retencyjnych od zgody sądu lub innego niezależnego organu[22].

Kontrola nad procesem pozyskiwania danych

W obecnym stanie prawnym nie istnieje żaden podmiot, który mógłby sprawować rzeczywistą kontrolę nad wykorzystaniem przez służby uprawnień do sięgania po dane telekomunikacyjne

18 Art. 180c Prawa telekomunikacyjnego.

19 Określonych w art. 180d Prawa telekomunikacyjnego.

20 Określoną w art. 31 ust.3 Konstytucji RP.

21 Art. 180 § 2 k.p.k. włącza dziennikarza do katalogu osób, które mogą być przesłuchiwane, co do faktów objętych tajemnicą tylko wtedy, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu. Z obowiązku zachowania tajemnicy dziennikarskiej może zwolnić wyłącznie sąd.

22 Szerzej na ten temat w pkt 3.2.12. na str. 59.

obywateli. Sytuacja ta jest wyjątkowa w zestawieniu ze standardami przyjętymi w większości państw Unii Europejskiej[23]. W ocenie NIK, konieczne jest stworzenie instrumentów nadzoru i kontroli nad wykorzystaniem tego środka. Sytuacja, w której jedynym podmiotem oceniającym zasadność pozyskiwania danych telekomunikacyjnych jest jednostka uprawniona do ich pozyskania, jest nie do zaakceptowania w ramach demokratycznego państwa prawnego. Kontrola ta mogłaby być realizowana w formie kontroli uprzedniej i/lub kontroli następczej.

Kontrola uprzednia, czyli realizowana przed skierowaniem zapytania w sprawie udostępnienia danych telekomunikacyjnych, pozwoliłaby nie tylko na istotne zwiększenie nadzoru nad wykorzystaniem tego środka, ale prawdopodobnie przyczyniłaby się również do ograniczenia skali jego wykorzystania. Możliwość zastosowania tej formy kontroli uzależniona jest jednakże od łącznego spełnienia dwóch przesłanek:

a) wskazania (ustanowienia) podmiotu, który „weryfikowałby" wnioski o udostępnienie danych telekomunikacyjnych, a następnie wydawał zgodę na wykorzystanie tego środka,
b) precyzyjnego określenia sytuacji, w których środek ten może być wykorzystany, jako niezbędnego warunku oceny zasadności wniosku.

W ocenie NIK, zadaniem podmiotu powołanego do realizacji kontroli uprzedniej powinna być przede wszystkim ocena zasadności (m.in. w kontekście zasad subsydiarności i proporcjonalności) wniosku o udostępnienie danych telekomunikacyjnych oraz sprawdzenie jego poprawności pod względem formalnym.

Kontrola następcza, czyli realizowana po skierowaniu zapytania w sprawie udostępnienia danych telekomunikacyjnych, miałaby na celu weryfikację poprawności wykorzystania tego środka. W zależności, czy kontrola następcza funkcjonowałaby łącznie z kontrolą uprzednią, czy też samodzielnie, różny musiałby być jej zakres. W pierwszym wypadku mogłaby zostać ograniczona do kontroli wykorzystania tego środka dowodowego pod kątem przestrzegania obowiązujących procedur, w tym prawidłowości przetwarzania pozyskanych danych, ochrony danych przed ich utratą lub udostępnieniem nieuprawnionym osobom, a także ich niezwłocznym niszczeniem, gdy przestały być niezbędne dla realizacji celu, dla którego zostały uzyskane. W drugim przypadku, zakres kontroli musiałby być znacznie szerszy i obejmować również kontrolę zasadności wykorzystania tego środka dowodowego.

Ważnym instrumentem kontroli powinno być rozwiązanie, zgodnie z którym informacja o fakcie pozyskania danych telekomunikacyjnych jest przekazywana osobie, której dane zostały udostępnione. W obecnie obowiązującym stanie prawnym pozyskiwanie danych, o których mowa w art. 180c i d ustawy jest wyłączone zarówno spod kontroli samego zainteresowanego (nie jest on powiadamiany o gromadzeniu dotyczących go danych), jak i spod jakiejkolwiek innej kontroli. Wyjątkiem są tu przepisy postępowania karnego, które przewidują obowiązek informowania przez sądy i prokuratury obywateli o pozyskaniu ich danych telekomunikacyjnych. Realizacja tego obowiązku może być odroczona na czas oznaczony, niezbędny ze względu na dobro sprawy, lecz nie później niż do czasu prawomocnego zakończenia postępowania. W ocenie NIK, należy wprowadzić rozwiązania, zgodnie z którym każdy ma prawo uzyskać informację o pozyskaniu jego danych telekomunikacyjnych (z zastrzeżeniem

[23] W 24 państwach UE taką kontrolę sprawuje sąd lub prokuratura albo niezależny organ administracyjny. Na konieczność wprowadzenia kontroli zewnętrznej zwróciła uwagę Rzecznik Praw Obywatelskich we wniosku do Trybunału Konstytucyjnego, w którym zakwestionowała m.in. zgodność przepisów ustaw kompetencyjnych z art. 8 Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności sporządzonej w Rzymie 4 listopada 1950 r. oraz art. 49 w związku z art. 31 ust. 3 Konstytucji.

możliwości odroczenia przekazania tej informacji ze względu na dobro toczącego się postępowania) bez względu na to, w związku z jakim postępowaniem dane te uzyskano. Jakiekolwiek wyjątki od tej zasady powinny być wskazane wprost w ustawie. Należy przy tym jednakże zauważyć, iż wprowadzenie tego instrumentu będzie mogło w pełni osiągnąć swój cel, gdy zostanie utworzony (wskazany) podmiot wyposażony w kompetencje do kontroli prawidłowości działania służb w tym zakresie[24].

Niszczenie danych

Istotnym elementem oceny obecnie obowiązujących rozwiązań jest kryterium niezbędności. Powinno być ono weryfikowane nie tylko w sytuacji wystąpienia o udostępnienie danych, ale również pod kątem dalszego przechowywania pozyskanych danych. Z art. 51 ust. 2 Konstytucji RP wynika zakaz gromadzenia, w demokratycznym państwie prawnym, danych innych, niż niezbędne. Dane, które stały się zbędne dla toczącego się postępowania, powinny być więc obligatoryjnie niszczone.

Zgodnie z art. 30 ust. 6 ustawy o Żandarmerii Wojskowej, art. 20c ust. 7 ustawy o Policji oraz art. 10b ust. 6 ustawy o Straży Granicznej pozyskane dane telekomunikacyjne, jeśli nie zawierają informacji mających znaczenie dla postępowania karnego, podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu. Stosownie do postanowień art. 36b ust. 5 ustawy o kontroli skarbowej, minister właściwy do spraw finansów publicznych nakazuje niezwłoczne, komisyjne i protokolarne zniszczenie danych uzyskanych od podmiotu prowadzącego działalność telekomunikacyjną w przypadku, gdy uzna wystąpienie z wnioskiem o te dane za nieuzasadnione. Natomiast przepisy ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (SWW), a także ustawy o Centralnym Biurze Antykorupcyjnym w ogóle nie przewidują obowiązku usunięcia zgromadzonych przez nie danych telekomunikacyjnych, gdy przestały być one niezbędne dla prowadzonego postępowania.

W ocenie NIK, konieczne jest pilne wprowadzenie przepisów w zakresie obowiązku niszczenia zbędnych danych telekomunikacyjnych będących w posiadaniu służb. Przepisy powinny nie tylko określić sam obowiązek niszczenia danych, ale również precyzować tryb i sposób jego realizacji.

Sprawozdawczość

Wiarygodne dane dotyczące zakresu wykorzystania środka w postaci zatrzymywania danych mają zasadnicze znaczenie dla wykazania konieczności (zasadności) jego stosowania. Dlatego konieczne jest opracowanie wskaźników pomiarowych oraz procedur sprawozdawczych, które umożliwiają przejrzyste i rzeczowe monitorowanie zatrzymywania danych, bez nakładania jednocześnie nadmiernych obciążeń na organy ścigania.

Jak wykazała kontrola NIK, funkcjonujący obecnie system gromadzenia informacji o pozyskiwaniu danych retencyjnych, nie zapewnia rzetelnej informacji o liczbie tego rodzaju przypadków. Brak jest precyzyjnie określonych wskaźników pomiarowych, a ustanowione procedury nie zapobiegają wystąpieniu rażących błędów. Również zakres gromadzonych danych sprawozdawczych nie pozwala na ocenę, dla jakich celów, jak często i z jakim skutkiem retencja danych jest stosowana. W ocenie NIK, dla prawidłowej oceny funkcjonowania systemu retencji danych niezbędne jest gromadzenie danych w zakresie: liczby przypadków, w których uprawnione organy uzyskiwały

[24] Należy wspomnieć, że znana jest możliwość tzw. sprawdzania pośredniego przez podmiot zaufania publicznego, który po fakcie zawiadamia zainteresowanego, że jego dane gromadzono.

od przedsiębiorców telekomunikacyjnych dane retencyjne (z wyodrębnieniem sytuacji, gdy były to wyłącznie dane osobowe użytkownika); liczby osób, których dane telekomunikacyjne były pozyskiwane i wykorzystywane przez uprawnione organy; łącznej liczby odmów udostępnienia danych (ze wskazaniem zasadniczych przyczyn); informacji na temat rodzaju spraw, w których środek ten wykorzystywano oraz jego skuteczności.

[więcej w rozdziale 3.2.12. na str. 59 Informacji]

2.3 Uwagi końcowe i wnioski

W związku ze stwierdzonymi przez Najwyższą Izba Kontroli nieprawidłowościami, a także wynikami analizy systemowej w zakresie funkcjonowania obecnie przyjętych rozwiązań prawnych, NIK wnosi do Prezesa Rady Ministrów o podjęcie działań w celu:

- **doprecyzowania zakresu danych, które powinny podlegać retencji;**
- **weryfikacji katalogu spraw, na potrzeby których dane telekomunikacyjne mogą być przez uprawnione służby pozyskiwane;**
- **przeanalizowania możliwości wprowadzenia dodatkowych rozwiązań o charakterze gwarancyjnym, ograniczających możliwość pozyskiwania danych retencyjnych w stosunku do osób wykonujących tzw. „zawody zaufania publicznego";**
- **ustanowienia kontroli zewnętrznej nad procesem pozyskiwania danych, obejmującej weryfikację zasadności ich pozyskiwania;**
- **wprowadzenia skutecznych instrumentów gwarantujących niezwłoczne niszczenie pozyskanych danych w sytuacji, gdy nie są już one dalej niezbędne dla osiągnięcia celów prowadzonego postępowania;**
- **ustanowienia mechanizmów sprawozdawczych, które zapewnią rzetelną informację o zakresie pozyskiwania danych telekomunikacyjnych;**
- **wprowadzenia przepisów gwarantujących osobom, których dane bilingowe były pobierane, prawa do informacji o zakresie i czasie zbierania tych danych, po zakończeniu w danej sprawie czynności – wyjątki w tym zakresie powinny określić przepisy ustawy;**
- **opracowania wytycznych dotyczących technicznych i organizacyjnych środków bezpieczeństwa w zakresie uzyskiwania dostępu do danych, w tym procedur ich przekazywania;**
- **wzmocnienia, do czasu wprowadzenia zmian systemowych, nadzoru nad wykorzystaniem przez organy państwa uprawnień w zakresie pozyskiwania danych obywateli.**

3 WAŻNIEJSZE WYNIKI KONTROLI

3.1 Charakterystyka obszaru objętego kontrolą

Stan prawny w zakresie kontrolowanej działalności

W dniu 3 maja 2006 r.[25] weszła w życie dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniającej dyrektywę 2002/58/WE[26], zwana w dalszej części dyrektywą 2006/24/WE lub dyrektywą w sprawie zatrzymywania danych telekomunikacyjnych. Polska skorzystała z możliwości przewidzianej w art. 15 ust. 3 tej dyrektywy i odroczyła jej stosowanie w odniesieniu do zatrzymywania wskazanych danych do dnia 15 marca 2009 r. (maksymalny okres odroczenia przewidziany w dyrektywie).

Zgodnie z art. 1 ust. 1 dyrektywy 2006/24/WE, jej celem było zbliżenie przepisów państw członkowskich w zakresie obowiązków dostawców ogólnie dostępnych usług łączności elektronicznej lub publicznych sieci łączności w zakresie zatrzymywania pewnych danych przez nie generowanych lub przetwarzanych, aby zapewnić ich dostępność w celu dochodzenia, wykrywania i ścigania poważnych przestępstw, określonych w ustawodawstwie każdego państwa członkowskiego.

Zgodnie z art. 180a Prawa telekomunikacyjnego, na operatorze publicznej sieci telekomunikacyjnej oraz dostawcy publicznie dostępnych usług telekomunikacyjnych ciąży obowiązek zatrzymywania i przechowywania przez określony czas, danych o ruchu w sieciach telekomunikacyjnych oraz udostępniania tych danych uprawnionym podmiotom. W tabeli poniżej przedstawiono zakres kompetencji poszczególnych podmiotów uprawnionych do sięgania po dane telekomunikacyjne.

Lp.	Jednostka	Podstawa prawna	Cel sięgania po dane	Typy przestępstw (ograniczenia)
1.	Agencja Bezpieczeństwa Wewnętrznego	art. 28 ustawy o ABW	realizacja wszelkich zadań ustawowych[27]	godzące w bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny[28]
2.	Centralne Biuro Antykorupcyjne	art. 18 ustawy o CBA	realizacja wszelkich zadań ustawowych[29]	korupcyjne, przeciwko instytucjom państwowym i samorządowym, godzące w interesy ekonomiczne państwa
3.	Policja	art. 20c ustawy o Policji	zapobieganie i wykrywanie przestępstw	wszystkie przestępstwa

25 Art. 16 dyrektywy stanowi, że wchodzi ona w życie dwudziestego dnia po jej opublikowaniu w Dzienniku Urzędowym UE; datą publikacji był dzień 13 kwietnia 2006 r.

26 Dz. Urz. UE L 105 z 13.04.2006, str. 54-63

27 Określonych w art. 5 ust. 1 ustawy o ABW, w tym: rozpoznawania, zapobiegania i zwalczanie zagrożeń oraz przestępstw; realizowania zadań związanych z ochroną informacji niejawnych; uzyskiwania, analizowania, przetwarzania informacji mogących mieć istotne znaczenie dla ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego; podejmowanie innych działań określonych w odrębnych ustawach i umowach międzynarodowych.

28 Np.: terroryzm; szpiegostwo; bezprawne ujawnienie lub wykorzystanie informacji niejawnych; przestępstwa godzące w podstawy ekonomiczne państwa; korupcji; nielegalne wytwarzanie, posiadanie i obrót bronią, amunicją i materiałami wybuchowymi, bronią masowej zagłady oraz środkami odurzającymi i psychotropowymi.

29 Określonych w art. 2 ustawy o CBA, w tym rozpoznawanie, zapobieganie i wykrywanie przestępstw; prowadzenie działalności analitycznej; ujawnianie i przeciwdziałanie przypadkom nieprzestrzegania przepisów o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne; ujawnianie przypadków nieprzestrzegania określonych przepisami prawa procedur podejmowania i realizacji decyzji; kontrola prawidłowości i prawdziwości oświadczeń majątkowych.

Lp.	Jednostka	Podstawa prawna	Cel sięgania po dane	Typy przestępstw (ograniczenia)
4.	Służba Kontrwywiadu Wojskowego	art. 32 ustawy o SKW i SWW	realizacja wszelkich zadań ustawowych[30]	przestępstwa popełniane przez żołnierzy pełniących czynną służbę wojskową
5.	Straż Graniczna	art. 10b ustawy o SG	zapobieganie i wykrywanie przestępstw	wszystkie przestępstwa, których zwalczanie pozostaje we właściwości SG[31]
6.	Żandarmeria Wojskowa	art. 30 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych	zapobieganie i wykrywanie przestępstw	wszystkie przestępstwa popełnione przez żołnierzy, pracowników cywilnych wojska (w określonych przypadkach), osoby przebywające na terenach wojskowych[32]
7.	Ministerstwo Finansów – Służba Celna	art. 75d ustawy o Służbie Celnej	zapobieganie i wykrywanie przestępstw	przestępstwa skarbowe[33]
8.	Ministerstwo Finansów – Kontrola Skarbowa	art. 36b ustawy o kontroli skarbowej	zapobieganie i wykrywanie przestępstw, naruszeń przepisów celnych	przestępstwa skarbowe, przestępstwa określone w art. 228-231 kk[34]
9.	Sądy	art. 218 § 1 k.p.k.	jeżeli mają znaczenie dla toczącego się postępowania	wszystkie przestępstwa
10.	Prokuratury	art. 218 § 1 k.p.k.	jeżeli mają znaczenie dla toczącego się postępowania	wszystkie przestępstwa

Z powyższej tabeli wynika, że dane telekomunikacyjne są udostępniane funkcjonariuszom Centralnego Biura Antykorupcyjnego, Służby Kontrwywiadu Wojskowego i Agencji Bezpieczeństwa Wewnętrznego w celu realizacji ich wszystkich zadań ustawowych, również nie pozostających w bezpośrednim związku ze ściganiem przestępstw. W przypadku Policji, Straży Granicznej, Żandarmerii Wojskowej oraz Sądów i Prokuratur uprawnienia do sięgania po dane telekomunikacyjne zostały ograniczone do przypadków ścigania przestępstw, bez uwzględnienia charakteru (wagi) czynu zabronionego. W przypadku pozyskiwania danych przez organy kontroli skarbowej ustawodawca ograniczył je zasadniczo do przypadków ścigania przestępstw skarbowych.

Prezes UKE, wykonujący zadania z zakresu regulacji i kontroli rynku usług telekomunikacyjnych, jest uprawniony do kontroli przestrzegania przepisów, decyzji i postanowień z zakresu telekomunikacji oraz do nakładania kar pieniężnych.

30 Określonych w art. 5 ustawy o SKW i SWW, w tym: rozpoznawanie, zapobieganie oraz wykrywanie przestępstw; ochrona informacji niejawnych; pozyskiwanie, gromadzenie, analizowanie, przetwarzanie informacji mogących mieć znaczenie dla obronności państwa; ochrona bezpieczeństwa jednostek wojskowych, badań naukowych i prac rozwojowych.

31 Np. związanych z przekroczeniem granicy, przestępstw skarbowych, przestępstw przeciwko bezpieczeństwu powszechnemu lub bezpieczeństwu w komunikacji lotniczej, przestępstw popełnianych przez funkcjonariuszy Straży Granicznej.

32 Zobacz art. 4 ust. 1 pkt 4 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych.

33 Wskazane w rozdziale 9 ustawy z dnia 10 września 1999 r. Kodeks Karny Skarbowy (Dz. U. z 2007 r., Nr 111, poz. 765 ze zm.).

34 W przypadku tych ostatnich, o ile zostały popełnione przez osoby zatrudnione lub pełniące służbę w jednostkach organizacyjnych podległych ministrowi właściwemu do spraw finansów publicznych.

Z danych udostępnionych przez Komisję Europejską wynika, iż ponad połowa dokonywanych w całej Unii Europejskiej zapytań dotyczy Polski[35].

[Uwarunkowania prawne zostały szczegółowo przedstawione w załączniku 5.4 na str. 82 Informacji]

Uwarunkowania organizacyjne przeprowadzonej kontroli

Jednym z kluczowych uwarunkowań prowadzonej kontroli był charakter jednostek kontrolowanych, a szczególności przysługujące im uprawnienia chroniące je przed ingerencją innych podmiotów w prowadzoną przez nie działalność.

Kontrola sądów i prokuratur

Zgodnie z art. 29 pkt 2 lit. b ustawy o NIK, upoważnieni przedstawiciele Najwyższej Izby Kontroli mają zagwarantowane prawo dostępu do wszelkich dokumentów związanych z działalnością jednostek kontrolowanych. Jednakże prawo to podlega pewnym ograniczeniom, znajdującym uzasadnienie w przepisach konstytucyjnych lub ustawowych. Kontrola sądów musiała być przeprowadzona z poszanowaniem wyrażonej w Konstytucji RP zasady niezależności sądów i niezawisłości sędziów (art. 45 ust. 1 i 178 ust. 1), a zakres prowadzonych czynności nie mógł prowadzić do naruszenia tych zasad. Drugie ograniczenie uprawnień kontrolnych NIK wynikało z przyznanego prokuratorom atrybutu niezależności, wyrażonego w art. 8 ust. 1 ustawy z dnia 20 czerwca 1985 r. o prokuraturze[36].

W związku z powyższym kontrola sądów i prokuratur miała charakter formalny, w której ocenie podlegała strona formalno-organizacyjna pozyskiwania danych telekomunikacyjnych. Zebrano również dane statystyczne w zakresie realizacji obowiązków ustawowych wobec abonentów telefonów lub nadawców, których wykaz połączeń lub innych przekazów został wydany przez podmioty prowadzące działalność telekomunikacyjną[37].

Kontrola w Sądzie Okręgowym (SO) w Bydgoszczy przebiegała przy pełnej współpracy ze strony Prezesa Sądu. Na szczególne podkreślenie zasługuje fakt, iż wnioski pokontrolne zostały wdrożone nie tylko w kontrolowanej jednostce, ale Prezes Sądu podjął również działania, w celu wyeliminowania ewentualnych nieprawidłowości w sądach rejonowych działających na terenie okręgu. Z kolei przeprowadzenie kontroli w Sądzie Okręgowym w Szczecinie napotkało na początkowe trudności, związane z kwestionowaniem uprawnień NIK do jej przeprowadzenia. Po wymianie korespondencji w tej kwestii, kontrola została przeprowadzona, a wniosek pokontrolny jest realizowany. Natomiast kontrola w Sądzie Okręgowym w Warszawie przebiegała początkowo bez zakłóceń, jednakże po stwierdzeniu przez kontrolera NIK niezgodności przedstawianych danych ze stanem faktycznym, Prezes Sądu uniemożliwiła przeprowadzenie dalszych czynności wskazując, iż jej zdaniem kontrola ta narusza niezawisłość sędziowską[38]. Z tego względu kontrola w SO w Warszawie nie mogła zostać zakończona. Kontrola prokuratur przebiegła bez zakłóceń, przy pełnej współpracy osób nimi kierujących.

35 Sprawozdanie Komisji dla Rady i Parlamentu Europejskiego z oceny dyrektywy w sprawie zatrzymywania danych (dyrektywa 2006/24/WE) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:PL:PDF\

36 Dz. U. z 2011 r., Nr 270, poz. 1599 ze zm.

37 Ograniczając się przy tym do postępowań już zakończonych.

38 Pani Prezes powołała się przy tym na uchwałę Krajowej Rady Sądownictwa z dnia 18 października 2012 r.

Należy zauważyć, iż Sądy powszechne podlegają kontroli NIK na podstawie przepisów art. 203 ust. 1 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. oraz art. 2 ust. 1 ustawy o NIK. Wykonywanie przez NIK, jako naczelny organ kontroli państwowej, podlegający Sejmowi (art. 1 ust. 1 i 2 ustawy o NIK) wszechstronnej (art. 5 ust. 1 ustawy o NIK) kontroli w sferze państwowej, obejmującej działalność organów administracji rządowej, NBP oraz państwowych osób prawnych, dotyczy także działalności innych państwowych jednostek organizacyjnych, tj. jednostek działających w formach określonych w ustawie z dnia 27 sierpnia 2009 r. o finansach publicznych[39]. Zgodnie z art. 9 pkt 1 ustawy o finansach publicznych sektor finansów publicznych tworzą organy władzy publicznej, w tym organy administracji rządowej, organy kontroli państwowej i ochrony prawa oraz sądy i trybunały. Przepis art. 3 ustawy o NIK, określający podstawowy zakres przedmiotowy kontroli realizowanych przez NIK, nie stanowi katalogu zamkniętego. Użycie przez ustawodawcę sformułowania „w szczególności" nie pozostawia wątpliwości, że NIK może badać całokształt działalności danego podmiotu, nie tylko jego działalność finansową, gospodarczą czy organizacyjno-administracyjną. Prawodawca decydując o ograniczeniu zakresu kontroli NIK uczynił to w art. 4 ustawy, wymieniając tam kilkanaście instytucji państwowych (wśród nich Kancelarię Sejmu, Kancelarię Senatu, Sąd Najwyższy i Naczelny Sąd Administracyjny) i enumeratywnie wskazał dopuszczalny zakres kontroli w tych jednostkach, tj. badanie wykonania budżetu, gospodarki finansowej i majątkowej. W tym katalogu podmiotów kontrolowanych przez NIK w ograniczonym zakresie, spośród organów sprawujących wymiar sprawiedliwości, ujęto jedynie Sąd Najwyższy i Naczelny Sąd Administracyjny. Świadczy to, że racjonalny ustawodawca, pomijając w tym przepisie sądy powszechne, postanowił o poddaniu ich wszechstronnej kontroli NIK. W innym przypadku pozbawiłoby to parlament możliwości zdobycia wiedzy w zakresie funkcjonowania jednej z najistotniejszych dla demokratycznego państwa prawnego instytucji, a tym samym racjonalnego podejmowania działań legislacyjnych w tym zakresie.

Art. 178 ust. 1 Konstytucji stanowi, że sędziowie w sprawowaniu swojego urzędu są niezawiśli i podlegają tylko Konstytucji oraz ustawom. W przypadku kontroli sądów wyłączeniu podlega więc kontrola działalności orzeczniczej, co stanowi wyraz poszanowania powyżej zasady. Ratio legis sformułowania zasady niezawisłości sędziów było zagwarantowanie bezstronności wymiaru sprawiedliwości poprzez zapewnienie sędziom możliwości swobodnego, w granicach nakreślonych przez Konstytucję i ustawy, orzekania. Kontrola w zakresie „pozyskiwania, przetwarzania, ochrony i zabezpieczenia danych telekomunikacyjnych, opracowania i przestrzeganie procedur wewnętrznych, stosowanych systemów zabezpieczenia i ochrony danych, prawidłowość i terminowość realizacji ustawowych obowiązków w tym zakresie", nie naruszała tej zasady. Przedmiotem kontroli było bowiem wyłącznie badanie procedur postępowania z danymi telekomunikacyjnymi (danymi osobowymi) oraz zebranie danych statystycznych, odnośnie postępowań już zakończonych, co nie może być uznane za wkroczenie w obszar chroniony niezawisłością sędziowską. Stanowisko to znajduje również potwierdzenie w opinii Kolegium NIK[40]. W związku z powyższym nie można zgodzić się ze stanowiskiem Prezes Sądu Okręgowego

39 Dz. U. Nr 157, poz. 1240 ze zm.

40 W Uchwale Kolegium Najwyższej Izby Kontroli z dnia 30 sierpnia 2005 r. w sprawie wyrażenia opinii dotyczącej stanowiska Ministra Sprawiedliwości oraz Krajowej Rady Sądownictwa w przedmiocie uprawnień Najwyższej Izby Kontroli do kontroli oświadczeń majątkowych składanych przez sędziów, wyrażone zostało następujące stanowisko: „Kolegium odmowę taką uznaje za utrudnianie realizacji ustawowych kompetencji kontrolnych naczelnego organu kontroli państwowej jakim jest Najwyższa Izba Kontroli. Kolegium nie podziela stanowisk Krajowej Rady Sądownictwa oraz Ministra Sprawiedliwości, w których kwestionowane są uprawnienia kontrolerów NIK do dostępu do oświadczeń majątkowych składanych przez sędziów sądów powszechnych".

w Warszawie, iż przez fakt podjęcia przez NIK przedmiotowej kontroli naruszona została niezawisłość sędziowska[41]. Należy zauważyć, iż działania Prezes Sądu Okręgowego w Warszawie nie tylko uniemożliwiły realizację zadań konstytucyjnego organu kontroli, ale wskazują również na wysokie prawdopodobieństwo wystąpienia nieprawidłowości[42].

Kontrola jednostek wykonujących czynności operacyjno-rozpoznawcze

Istotnym ograniczeniem dla prowadzonej przez NIK kontroli był brak dostępu do informacji gromadzonych w ramach prowadzonych czynności operacyjno-rozpoznawczych.

Zakres kompetencji kontrolnych NIK, jak już wyżej wspomniano, został określony w art. 203 ust. 1 Konstytucji RP oraz odpowiednio art. 2 ust. 1 i art. 5 ust. 1 ustawy o NIK. Zgodnie z art. 29 ust. 2 ustawy o NIK, kontroler ma dostęp do dokumentów i materiałów potrzebnych do ustalenia stanu faktycznego w zakresie kontrolowanej działalności zawierających informacje ustawowo chronione, chyba że dostęp ten zostanie ograniczony lub wyłączony na podstawie innych ustaw. W polskim systemie prawnym istnieje wiele tajemnic ustawowych i do większości z nich mają dostęp kontrolerzy NIK, gdyż ustawy wprowadzające obszary chronione nie określiły ograniczeń, co do udostępniania informacji Izbie. Istnieją jednak ustawy, które z uwagi na specyficzny charakter chronionych informacji zawierają rozwiązania reglamentujące dostępność do nich.

Zgodnie z art. 43 ust. 3 ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (zwana dalej ustawą o SKW i SWW) udzielenie informacji określonej osobie lub instytucji nie może dotyczyć m.in. informacji o:

- osobie, jeżeli zostały uzyskane w wyniku prowadzonych przez SKW, SWW albo inne organy, służby lub instytucje państwowe czynności operacyjno-rozpoznawczych;
- szczegółowych formach i zasadach przeprowadzania czynności operacyjno-rozpoznawczych oraz o stosowanych w związku z ich prowadzeniem środkach i metodach.

Ujawnienie informacji, o których mowa wyżej, może nastąpić jedynie w przypadku żądania prokuratora lub sądu, zgłoszonego w celu ścigania karnego za przestępstwo, którego skutkiem jest śmierć człowieka, uszczerbek na zdrowiu lub szkoda w mieniu, albo gdy żądanie prokuratora lub sądu wiąże się z uzasadnionym podejrzeniem popełnienia przestępstwa ściganego z oskarżenia publicznego w związku z wykonywaniem czynności operacyjno-rozpoznawczych.

Podobne obostrzenia zostały sformułowane w art. 39 ust. 3 ustawy o Agencji Bezpieczeństwa Wewnętrznego, w art. 28 ust. 2 ustawy o Centralnym Biurze Antykorupcyjnym, art. 20b i art. 22 ust. 1 ustawy o Policji, art. 9 ust. 1-3 i art. 9 d ustawy o Straży Granicznej, art. 8 ustawy o Służbie Celnej oraz art. 36j ustawy o kontroli skarbowej.

Ustalenia telekomunikacyjne dokonywane są w związku z prowadzonymi czynnościami operacyjno-rozpoznawczymi i dokumentowane są w aktach poszczególnych spraw. W związku z powyższym kontrolerzy NIK nie mieli możliwości pełnego zapoznania się w trakcie postępowania kontrolnego z dokumentami, a tym samym zweryfikowania zasadności zastosowania tego środka.

41 W latach ubiegłych Izba przeprowadziła szereg kontroli w jednostkach organizacyjnych wymiaru sprawiedliwości. Kontrolowano m.in. działalność sądów rejestrowych w zakresie prowadzenia Krajowego Rejestru Sądowego, prawidłowość składania oświadczeń majątkowych przez sędziów oraz realizację obowiązków wynikających z ustawy o bezpieczeństwie imprez masowych. Ustalenia z powyższych kontroli zostały w pełni przyjęte przez Ministra Sprawiedliwości oraz Prezesów kontrolowanych sądów.

42 O fakcie tym NIK powiadomiła Ministra Sprawiedliwości.

Działania kontrolne musiały być, więc realizowane w oparciu o dane zanonimizowane, informacje o charakterze statystycznym oraz dokumenty niejawne, niepodlegające wyłączeniu na podstawie przepisów ustawowych.

Kontrola operatorów telekomunikacyjnych

NIK nie posiada uprawnień kontrolnych w stosunku do funkcjonujących na rynku operatorów telekomunikacyjnych. W ramach przygotowania do kontroli pozyskano jednakże, w trybie art. 29 ust. 1 pkt 2 lit. f dane niezbędne do przeprowadzenia kontroli w służbach i formacjach uprawnionych do pozyskiwania danych telekomunikacyjnych.

Ponadto, na podstawie porozumienia z dnia 12 grudnia 2011 r. zawartego pomiędzy GIODO i Prezesem NIK, podjęto decyzję o przeprowadzeniu przez GIODO kontroli u wybranych operatorów telekomunikacyjnych w zakresie przestrzegania przepisów o ochronie danych osobowych. Kontrola ta była realizowana w pełnej współpracy z NIK, a ustalenia dokonane przez GIODO miały istotne znaczenie dla realizacji wyników kontroli prowadzonej przez NIK.

[Uwarunkowania prawne i organizacyjne przedstawiono w załączniku nr 5.4 na str. 82 Informacji]

3.2 Istotne ustalenia kontroli

W części tej przedstawiono istotne ustalenia kontroli jednostkowych. Teksty wystąpień pokontrolnych dostępne są na stronie www.nik.gov.pl/kontrole/wyniki-kontroli-nik
W niniejszej wersji informacji usunięto ponadto fragmenty, które ze względu na swój niejawnych charakter nie mogły zostać upublicznione. Pełny tekst (niejawny) informacji przekazano najważniejszym osobom w państwie.

3.2.1. Agencja Bezpieczeństwa Wewnętrznego

Pozyskiwanie danych telekomunikacyjnych

Art. 28 ustawy o ABW i AW przewiduje możliwość pozyskiwania danych telekomunikacyjnych w oparciu o pisemny wniosek, ustne żądanie lub za pośrednictwem sieci telekomunikacyjnej. W ABW problematykę w zakresie realizacji uprawnień dotyczących uzyskiwania od podmiotów prowadzących działalność telekomunikacyjną danych, o których mowa w art. 180 c i d ustawy Prawo telekomunikacyjne była uregulowana w dokumentach wewnętrznych. Dokumenty te zawierały szczegółowe wytyczne, procedury oraz normy postępowania zatwierdzone przez Szefa ABW. W ocenie NIK przepisy wewnętrzne i zawarte w nich procedury były kompletne, precyzyjne, spójne oraz gwarantowały optymalny poziom wykorzystania oraz bezpieczeństwa pozyskanych danych.

Większość (86,3%) zapytań kierowana była za pośrednictwem sieci telekomunikacyjnej (z wykorzystaniem elektronicznego systemu zapytań). Kontrola wykazała, iż ustalenia danych telekomunikacyjnych dokonywane były przez jednostki i komórki organizacyjne ABW mające uprawnienia do prowadzenia czynności operacyjno-rozpoznawczych i śledczych oraz wykonujące zadania analityczno-koordynacyjne. W toku kontroli ustalono, iż kwestie te były regulowane indywidulanie dla każdej komórki organizacyjnej na mocy zarządzeń Szefa ABW w sprawie regulaminów organizacyjnych. Przepisy określające wewnętrzną organizację i porządek funkcjonowania jednostek organizacyjnych ABW gwarantowały uzyskanie danych telekomunikacyjnych wówczas, gdy było to uzasadnione specyfiką lub zakresem zadań wykonywanych przez jednostki organizacyjne ABW, albo prowadzonych przez nie czynności.

Osoby upoważnione do sięgania po dane telekomunikacyjne

Zlecania dotyczące ustaleń składają wybrane komórki niektórych departamentów ABW, m.in. Bezpieczeństwa Teleinformatycznego, Postępowań Karnych czy Bezpieczeństwa Wewnętrznego i Audytu. Realizacji zapytań bezpośrednio u operatorów dokonywał Departament Wsparcia Operacyjno-Technicznego ABW oraz komórki odpowiedzialne za koordynację, analitykę i nadzór w Delegaturze Stołecznej, Departamencie Zwalczania Terroryzmu, Departamencie Bezpieczeństwa Wewnętrznego i Audytu oraz Centrum Analiz. Elektroniczny system zapytań działający w ramach sieci wewnętrznej ABW umożliwiał ustalenie funkcjonariusza uzyskującego dane telekomunikacyjne, ich rodzaj oraz czas, w którym zostały pozyskane. Dostęp do sieci odbywał się zgodnie z Procedurami Bezpiecznej Eksploatacji Sytemu.

W próbie kontrolnej obejmującej 528 zapytań, zbadanej m.in. pod kątem czy osoby kierujące zapytanie posiadały stosowne uprawnienia oraz czy informacja została uzyskana na żądanie właściwej komórki organizacyjnej nie stwierdzono nieprawidłowości.

Stworzony system spełniał, w ocenie NIK, wymogi w zakresie weryfikowalności osób upoważnionych do ich przetwarzania.

Sprawność i szybkość pozyskiwania danych teleinformatycznych

W okresie objętym kontrolą nie stwierdzono przypadku odmowy udzielenia przez operatorów danych telekomunikacyjnych. Nie stwierdzono również przypadków opóźnień w udzieleniu odpowiedzi przez operatorów na zapytanie kierowane drogą elektroniczną. W 14 przypadkach zapytań kierowanych w formie pisemnej stwierdzono zwłokę w udzieleniu odpowiedzi przekraczającą dwa miesiące.

Ewidencjonowanie pozyskanych danych telekomunikacyjnych

Dane liczbowe dotyczące zakresu i ilości zapytań złożonych przez ABW w okresie od 1 stycznia 2011 r. do 30 czerwca 2012 r. przedstawiały się następująco:

Rok	Ilość zapytań dotyczących:				Zapytania ogólne	RAZEM
	lokalizacji	wykazu połączeń	ustaleń końcowych użytkowników	ustaleń nr. użytkowanych przez osobę		
1.	2.	3.	4.	5.	6.	7.
2011	7.000	65.000	30.681	20.319	3.250	126.250
2012 (do 30 IV)	3.684	25.302	14.972	8.039	1.429	53.426

W toku kontroli porównano liczbę zapytań kierowanych do operatorów telekomunikacyjnych, z liczbą wykazanych w ewidencji ABW zleceń ustaleń bilingowo-abonenckich. Stwierdzono rozbieżność miedzy tymi liczbami ze względu m.in. na następujące okoliczności:

- zawarcia w zleceniu więcej niż jednego kryterium (np. kilka numerów telefonicznych do tej samej sprawy);
- konieczność ponawiania zapytań do operatów w przypadku abonenta, który skorzystał z usługi przeniesienia numeru;
- konieczność dzielenia zleceń za okresy przekraczające 3 m-ce – jest to maksymalny okres, za który można formułować pojedyncze zlecenia u części operatorów.

NIK zwraca uwagę na fakt, iż wobec braku jednolitej metodologii liczenia danych w poszczególnych służbach, dane te nie mogą być wprost porównywane pomiędzy poszczególnymi służbami, a przytoczone powyżej wielkości należy traktować jako dane szacunkowe.

Ustalono, że niezależnie od faktycznego zainteresowania danego odbiorcy informacji, zakres przekazywanych przez operatorów danych był szerszy niż określony we wniosku. Stanowiło to naruszenie art. 160 ust. 1, w związku z art. 159 ust. 1 pkt 3-5 i ust. 3 ustawy Prawo telekomunikacyjne oraz art. 218 § 1 kpk. Izba, stosownie do art. 63 ust. 3 ustawy o NIK, zawiadomiła Prezesa Urzędu Komunikacji Elektronicznej o naruszeniu obowiązku zachowania tajemnicy telekomunikacyjnej przez operatorów.

Postępowanie ze zbędnymi danymi telekomunikacyjnymi

Przepisy ustawy o ABW, zezwalając na pozyskiwanie danych telekomunikacyjnych, nie przewidują zniszczenia tych spośród pozyskanych danych, które nie zawierają informacji mających znaczenie dla prowadzonego postępowania. W ABW brak jest odrębnych procedur dotyczących oceny zgromadzonych danych telekomunikacyjnych z punktu widzenia realizacji celów, dla których zostały one pozyskane. Dane tego typu są gromadzone i przechowywane i niszczone na zasadach ogólnych. NIK nie wniosła zastrzeżeń do obowiązujących w tym zakresie aktów wewnętrznych[43].

Nadzór i kontrola nad uzyskiwaniem, przetwarzaniem i niszczeniem danych telekomunikacyjnych

Kontrola wykazała, że Departament Bezpieczeństwa Wewnętrznego i Audytu objął kontrolą zagadnienia związane z prawidłowością merytoryczną i formalną prowadzonych procedur operacyjnych przez poszczególne jednostki organizacyjne ABW, w tym przetwarzanie i wykorzystanie danych, o których mowa w art. 180 c i d ustawy Prawo telekomunikacyjne. Wyniki tych kontroli nie wykazały nieprawidłowości. Ponadto ww. Departament sprawdzał i weryfikował sygnały o ewentualnych nieprawidłowościach w zakresie uzyskiwania, przetwarzania i niszczenia danych telekomunikacyjnych. Najwyższa Izba Kontroli oceniła pozytywnie system kontroli wewnętrznej ABW w zakresie zarządzania ryzykiem związanym z bezpieczeństwem pozyskiwanych danych telekomunikacyjnych.

3.2.2. Centralne Biuro Antykorupcyjne

Pozyskiwanie danych telekomunikacyjnych

Ustawa o CBA przewiduje możliwość pozyskiwania danych telekomunikacyjnych w oparciu o pisemny wniosek, ustne żądanie lub za pośrednictwem sieci telekomunikacyjnej. Ze względu na znaczne zróżnicowanie w przypadku CBA tych trybów, wymagają one oddzielnego omówienia.

Pozyskiwanie danych telekomunikacyjnych w oparciu o pisemny wniosek lub ustne żądanie

Ustalenia telekomunikacyjne dokonywane w trybie art. 18 ust. 2 ustawy o CBA, tj. na pisemny wniosek Szefa CBA lub osoby przez niego upoważnionej, jak również na ustne żądanie funkcjonariusza, realizowane były na podstawie ewidencjonowanych w dziennikach korespondencyjnych

[43] M.in. Zarządzenie Nr Pf-77 Szefa ABW z dnia 20 grudnia 2011 r. w sprawie archiwizacji i udostępniania akt w Agencji Bezpieczeństwa Wewnętrznego oraz Decyzja Nr 64 Szefa ABW z dnia 2 czerwca 2004 r. w sprawie niszczenia w jednostkach organizacyjnych ABW elektronicznego nośnika danych zawierających informację niejawne.

zleceń pisemnych. Występowanie przez upoważnionego funkcjonariusza o ustalenie danych telekomunikacyjnych odbywało się za wiedza i zgodą kierownika jednostki lub komórki organizacyjnej. Przyjęta procedura zapewniała właściwy nadzór przełożonych oraz pozawalała na weryfikację zasadności wystąpień o dane telekomunikacyjne. W przypadku uzyskania informacji w trybie zapytania ustnego, sporządzana była stosowna notatka lub adnotacja na wniosku. Zapytania w trybie ustnym realizowane były osobiście przez funkcjonariusza, za okazaniem imiennego upoważnienia i legitymacji. Wyniki sprawdzeń przekazywane były za pokwitowaniem osobie upoważnionej w piśmie zlecającym ustalenia, drogą pisemną lub elektroniczną pocztą szyfrowaną, w zależności od zawartych we wniosku wskazań.

Pozyskiwanie danych za pośrednictwem sieci telekomunikacyjnej

1. Zgodnie z art. 18 ust. 4 pkt 1 lit. a ustawy o CBA udostępnienie CBA danych telekomunikacyjnych może nastąpić za pośrednictwem sieci telekomunikacyjnej, jeżeli sieć ta zapewnia możliwość ustalenia funkcjonariusza CBA uzyskującego te dane, ich rodzaju oraz czasu, w którym zostały uzyskane.

Proces uzyskiwania i przesyłania danych telekomunikacyjnych CBA realizuje za pośrednictwem sieci, o których mowa w art. 18 ust. 2 pkt 3 i 4 ustawy o CBA, należących do największych przedsiębiorców telekomunikacyjnych. Proces przekazywania danych za pośrednictwem sieci został uzgodniony w drodze porozumień zawartych przez Szefa CBA z trzema przedsiębiorcami. Dostęp drogą elektroniczną do danych telekomunikacyjnych przechowywanych przez dwóch pozostałych przedsiębiorców telekomunikacyjnych odbywał się bez zawartych formalnie porozumień. Zasady i warunki współpracy w tym zakresie zostały uzgodnione przez strony w ramach roboczych kontaktów. Uzgodnienia te nie zostały w żaden sposób udokumentowane.

W ocenie NIK, niejednoznaczny zapis art. 18 ust. 3 ustawy o CBA mógł budzić wątpliwości, co do sytuacji, w których istnieje konieczność zawarcia porozumień z przedsiębiorcami telekomunikacyjnymi, w zakresie udostępniania CBA danych za pośrednictwem sieci telekomunikacyjnej. NIK zwróciła jednakże uwagę na fakt, iż niezawarcie stosownych porozumień z operatorami lub brak odpowiednich postanowień w zawartych porozumieniach skutkował tym, że Szef CBA nie mógł skutecznie wyegzekwować od przedsiębiorców telekomunikacyjnych niezbędnych informacji w zakresie zrealizowanych ustaleń związanych z uzyskiwaniem danych telekomunikacyjnych za pośrednictwem sieci. Miało to istotne znaczenie zwłaszcza przy uwzględnieniu faktu, iż CBA nie prowadziło odrębnych ewidencji umożliwiających stwierdzenie, kto, kiedy, w jakim celu oraz jakie dane lub informacje uzyskiwał. W ocenie NIK, brak możliwości uzyskania przez Szefa CBA kompleksowej informacji dotyczących zrealizowanych przez funkcjonariuszy ustaleń telekomunikacyjnych świadczył o braku możliwości sprawowania rzetelnego nadzoru i kontroli w tym zakresie. Wprowadzenie odrębnych rejestrów (ewidencji) zapytań o dane telekomunikacyjne zwiększyłoby nadzór nad działaniami w tym zakresie.

2. Stwierdzono ponadto, iż 3 z 5 systemów, za pomocą których pozyskiwano dane telekomunikacyjne, nie zapewniało w pełnym zakresie możliwości ustalenia wszystkich danych, o których mowa w art. 18 ust. 4 pkt 1 ustawy o CBA, w tym rodzaju uzyskiwanych danych telekomunikacyjnych. W systemie udostępnionym przez Polkomtel S.A. w polu „rodzaj danych" odpowiednio stosowano zapisy w brzmieniu: standardowe lub niestandardowe. W systemie udostępnionym przez P4 Sp. z o.o. w polu „rodzaj danych" wskazywano odpowiednio zapisy

„art. 180c Prawa telekomunikacyjnego" lub „art. 180d Prawa telekomunikacyjnego". Analiza porozumień zawartych przez Szefa CBA z przedsiębiorcami telekomunikacyjnymi wykazała również, że strony nie zawarły w nich stosownych postanowień, co do ciążącego na przedsiębiorcach telekomunikacyjnych obowiązku zapewnienia parametrów sieci umożliwiających ustalenie funkcjonariusza CBA uzyskującego dane telekomunikacyjne, ich rodzaju oraz czasu, w którym zostały uzyskane.

W ocenie NIK, pomimo że ustawodawca nie wskazał podmiotu odpowiedzialnego za realizację wymogów ustawowych, o których mowa w art. 18 ust. 4 pkt 1 lit. a i b ustawy o CBA, to zgodnie z treścią art. 18 ust. 4 ustawy o CBA, w przypadku gdy sieć nie spełniała tych wymogów, nie można było udostępniać danych telekomunikacyjnych za jej pośrednictwem.

Zabezpieczenia organizacyjne i techniczne w zakresie pozyskiwania i przetwarzania danych telekomunikacyjnych

Dostęp drogą elektroniczną do danych przesyłanych zgodnie z art. 18 ust. 2 pkt 3 ustawy o CBA, realizowany był za pomocą usługi poczty elektronicznej, z dodatkowym zabezpieczeniem w postaci szyfrowania i podpisywania wiadomości pocztowych z wykorzystaniem certyfikatów elektronicznych.

Szef CBA szczegółowo uregulował aktami wewnętrznymi zasady ochrony stanowisk dostępowych. Wprowadzono m.in. regulacje w zakresie ochrony kart dostępowych, haseł, kluczy; szczegółowe zasady dostępu do danych i ich przetwarzania; wydawania certyfikatów. Określono także zasady przetwarzania danych telekomunikacyjnych tak, aby zapewnić zgodność procedur postępowania z ustawą o ochronie danych osobowych.

W ocenie NIK, zastosowane środki ochrony dostępu do sieci telekomunikacyjnych służących pozyskiwaniu danych, były wystarczające dla zapewnienia ochrony uzyskanych danych telekomunikacyjnych przed dostępem osób nieuprawnionych.

Osoby upoważnione do sięgania po dane telekomunikacyjne

Szef CBA określił jednostki organizacyjne uprawnione do pozyskiwania i przetwarzania danych telekomunikacyjnych. Jednostką organizacyjną odpowiedzialną za uzyskiwanie danych telekomunikacyjnych oraz teleinformatycznych na potrzeby jednostek organizacyjnych, których siedziby usytuowane są w Warszawie oraz w szczególnie uzasadnionych przypadkach, na potrzeby Delegatur CBA, jest Biuro Techniki Operacyjnej (BTO). Z uwagi na specyfikę działań podejmowanych przez Biuro Kontroli i Spraw Wewnętrznych, a w szczególności konieczność zapewnienia właściwej ochrony tych działań, ustalenia telekomunikacyjne na potrzeby prowadzonych przez funkcjonariuszy tej jednostki spraw, zasadniczo realizowane były bezpośrednio przez to Biuro. W delegaturach CBA jednostkami organizacyjnymi odpowiedzialnymi za uzyskiwanie danych telekomunikacyjnych oraz teleinformatycznych, zgodnie z regulaminami organizacyjnymi poszczególnych delegatur, były zespoły/sekcje wsparcia lub wydziały operacyjno-śledcze.

Zadania związane z realizacją ustaleń telekomunikacyjnych wykonywali funkcjonariusze lub pracownicy wyznaczeni przez kierowników ww. jednostek. Przyjęto również zasadę, że w zakresach obowiązków funkcjonariuszy, którym wydawano upoważnienie Szefa CBA, określano zadania dotyczące dokonywania ustaleń telekomunikacyjnych, stosownie do zakresu merytorycznej działalności komórki organizacyjnej CBA, określonego w regulaminie organizacyjnym.

W ocenie NIK, Szef CBA wprowadził właściwe procedury zarządcze w zakresie pozyskiwania i przetwarzania danych telekomunikacyjnych, a także ochrony ich przed nieuprawnionym ujawnieniem lub utratą. Przyjęte w części jednostek organizacyjnych CBA (w tym centrali CBA) rozwiązanie, zgodnie z którym dane pozyskiwane były za pośrednictwem jednostek „wsparcia", w sposób istotny redukowało ryzyko wystąpienia nieprawidłowości, dlatego zdaniem NIK, rozwiązanie to powinno być przyjęte we wszystkich jednostkach organizacyjnych CBA.

Nie stwierdzono przypadków dokonywania ustaleń telekomunikacyjnych przez funkcjonariuszy, którzy nie posiadaliby stosowanego upoważnienia Szefa CBA.

W trakcie kontroli stwierdzono jednakże przypadki naruszenia obowiązujących regulacji wewnętrznych, poprzez udzielanie upoważnień funkcjonariuszom innych jednostek organizacyjnych, niż wskazane w regulacjach wewnętrznych. Nieprawidłowości te stwierdzono w ośmiu jednostkach organizacyjnych CBA. NIK nie podzieliła argumentacji Szefa CBA dotyczącej pomocniczego charakteru regulaminów organizacyjnych. W ocenie NIK, regulaminy organizacyjne, nadane zarządzeniami Szefa CBA, były wewnętrznymi aktami normatywnymi stanowiącymi podstawę funkcjonowania Biura, regulującymi całokształt stosunków wewnętrznych. Nieprzestrzeganie regulaminów organizacyjnych, polegające na wydawaniu upoważnień Szefa CBA uprawniających do dokonywania ustaleń telekomunikacyjnych funkcjonariuszom z jednostek organizacyjnych, które nie realizują zadań z tym związanych, stanowiło naruszenie organizacji wewnętrznej i ustanowionych przez Szefa CBA zasad funkcjonowania. NIK podzieliła natomiast stanowisko Szefa CBA, iż wydanie ww. funkcjonariuszom upoważnień, nie stanowiło naruszenia art. 18 ustawy o CBA.

Sprawność i szybkość pozyskiwania danych teleinformatycznych

W okresie od 1 stycznia 2011 r. do 18 września 2012 r. odnotowano jedynie dwa przypadki odmowy udostepnienia danych telekomunikacyjnych. Było to spowodowane faktem, iż zakres żądanych danych wykraczał poza 24 miesięczny okres ich retencji. Z analizy materiałów przedłożonych w trakcie kontroli wynika, że udostępnianie danych za pomocą sieci odbywało się w większości przypadków w dniu, w którym skierowano zapytanie lub w dniu następnym. Maksymalny czas oczekiwania na przekazanie danych wynosił 2 dni.

Ewidencjonowanie pozyskanych danych telekomunikacyjnych

W trakcie kontroli nie można było dokonać wiarygodnych ustaleń dotyczących zakresu i ilości danych pozyskanych przez kontrolowaną jednostkę w okresie objętym kontrolą. Prowadzone przez CBA statystyki w zakresie pozyskiwania danych telekomunikacyjnych obejmowały liczbę kierowanych zapytań, a nie ilość uzyskanych danych telekomunikacyjnych. Należy zwrócić uwagę, że obowiązujące przepisy prawne nie nakładają na CBA obowiązku gromadzenia informacji statystycznej na temat ustaleń telekomunikacyjnych. Opracowywane przez CBA statystyki i przyjęta formuła gromadzenia tych danych wynikała jedynie z uregulowań o charakterze wewnętrznym.

Na podstawie przedłożonych przez Szefa CBA zestawień ilościowych zrealizowanych przez CBA zapytań o dane telekomunikacyjne stwierdzono, że okresie od 1 stycznia 2011 r. do 30 czerwca 2012 r., upoważnieni funkcjonariusze CBA występowali na podstawie art. 18 ust. 2 ustawy o CBA do przedsiębiorców telekomunikacyjnych 143 306 razy. Struktura skierowanych zapytań przedstawia się następująco:

Rok	Zapytania o				Razem
	wykazy połączeń	dane abonenta	dane lokalizacyjne	pozostałe sprawdzenia (w tym IP, IMSI)	
1.	2.	3.	4.	6.	7.
2011	6 133	62 054	2 028	553	70 808
01.01. – 30.06.2012	2 981	68 343	751	423	72 498

Z powyższego zestawienia wynika, że w okresie od 1 stycznia 2011 r. do 30 czerwca 2012 r. zapytania o wykazy połączeń stanowiły 6% ogólnej liczby zapytań, zapytania dotyczące lokalizacji telefonu komórkowego – 2%, pozostałe sprawdzenia (w tym dot. danych IP, numerów IMSI) – 1%, natomiast zapytania dotyczące ustalenia danych identyfikujących abonentów stanowiły 91% ogólnej liczby zapytań.

NIK zwraca uwagę na fakt, iż wobec braku jednolitej metodologii liczenia danych w poszczególnych służbach, dane te nie mogą być wprost porównywane pomiędzy poszczególnymi służbami, a przytoczone powyżej wielkości należy traktować jako dane szacunkowe.

Postępowanie ze zbędnymi danymi telekomunikacyjnymi

Przepisy ustawy o CBA, zezwalając na pozyskiwanie danych telekomunikacyjnych, nie przewidują zniszczenia tych spośród pozyskanych danych, które nie zawierają informacji mających znaczenie dla prowadzonego postępowania. Zgodnie z przyjętą w CBA pragmatyką dane telekomunikacyjne, jako dane osobowe, podlegały ochronie na podstawie przepisów o ochronie danych osobowych i odpowiednich przepisów ustawy o CBA. Zgodnie z treścią art. 22a ust. 8 ustawy o CBA, nie rzadziej, niż co 5 lat, w zależności od potrzeby dalszego przetwarzania tych danych, dokonuje się ich weryfikacji i usuwa dane zbędne. W kontrolowanym okresie przeprowadzono weryfikację danych osobowych na podstawie decyzji nr 88/11 Szefa CBA z dnia 21 lutego 2011 r. w sprawie określenia trybu weryfikacji i usuwania danych osobowych przetwarzanych w CBA. NIK pozytywnie oceniła działania Szefa CBA w zakresie postępowania z danymi zbędnymi dla prowadzonych postępowań.

Nadzór i kontrola nad uzyskiwaniem, przetwarzaniem i niszczeniem danych telekomunikacyjnych

W okresie objętym kontrolą w CBA nie przeprowadzano badań audytowych w zakresie uzyskiwania, przetwarzania, wykorzystywania i niszczenia danych telekomunikacyjnych. Nie były też prowadzone kontrole przez wewnętrzną komórkę kontrolą, ani kontrole przez podmioty zewnętrzne. Nie dokonywano analiz, ani ocen działań w CBA w powyższym zakresie. Nadzór na realizacją zadań był prowadzony przez bezpośrednich przełożonych, zgodnie z procedurami określonymi przez Szefa CBA. CBA, jako jedyna spośród kontrolowanych jednostek powołała pełnomocnika do spraw kontroli przetwarzania przez CBA danych osobowych (art. 22b ust. 1 ustawy o CBA). Pełnomocnik, w ramach nadzoru, prowadzi kontrolę prawidłowości przetwarzania przez CBA danych osobowych, a w szczególności ich przechowywania, weryfikacji i usuwania.
Na podstawie Rejestru Skarg i Wniosków CBA stwierdzono, że w kontrolowanym okresie nie wniesiono do Szefa CBA skarg, których przedmiotem było nienależyte wykonywanie przez kontrolowaną jednostkę uprawnień, o których mowa w art. 18 ustawy o CBA.

4.2.3. Policja

Pozyskiwanie danych telekomunikacyjnych

Zgodnie z ustawą o Policji, podmioty prowadzące działalność telekomunikacyjną, udostępniają nieodpłatnie dane telekomunikacyjne policjantowi wskazanemu w pisemnym wniosku Komendanta Głównego Policji lub komendanta wojewódzkiego Policji albo osobie przez nich upoważnionej. Udostępnienie danych może nastąpić na ustne lub pisemne żądanie ww. osób lub za pośrednictwem sieci telekomunikacyjnej. Zgodnie z treścią art. 20c ust. 2a ustawy o Policji udostępnianie danych telekomunikacyjnych może odbywać się bez udziału pracowników podmiotu prowadzącego działalność telekomunikacyjną lub przy niezbędnym ich udziale, jeżeli możliwość taka jest przewidziana w porozumieniu zawartym pomiędzy Komendantem Głównym Policji, a tym podmiotem. W toku kontroli ustalono, że zasadniczo Policja pozyskuje dane za pośrednictwem sieci telekomunikacyjnej, jednakże nie są one pozyskiwane bezpośrednio z urządzeń operatora, tj. bez udziału jego pracowników.

Spośród 14 największych przedsiębiorców telekomunikacyjnych, u których dostęp Policji do danych retencyjnych odbywa się za pośrednictwem sieci, Komendant Główny Policji zawarł porozumienia z trzema przedsiębiorcami. Pozostałe uzgodnienia z operatorami w zakresie procesu przekazywania i przetwarzania danych telekomunikacyjnych udokumentowane zostały w formie notatek służbowych oraz pism. W przypadku porozumień dotyczących trzech operatorów uzyskano wyjaśnienia, że nie zachowała się dokumentacja w zakresie dokonanych uzgodnień.

W wyniku kontroli stwierdzono przypadek nieuprawnionego żądania udostępnienia danych telekomunikacyjnych przez funkcjonariusza Wydziału d/s Zorganizowanej Przestępczości Kryminalnej Zarządu w Warszawie Centralnego Biura Śledczego (CBŚ) KGP, który nie posiadając stosownego upoważnienia Komendanta Głównego Policji, wystąpił telefonicznie do TP S.A. o dane telekomunikacyjne. Zgromadzone dane nie pozwalały na ustalenie, w jakim postępowaniu zostało skierowane zapytanie. Na podstawie art. 51 ust 4. ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli, poinformowano Komendanta Głównego Policji o ustaleniach wskazujących na nieprawidłowości w działalności CBŚ KGP w opisanym wyżej zakresie. Na polecenie Komendanta Głównego Policji wdrożono stosowne czynności wyjaśniające w sprawie nieuprawnionego wystąpienia o dane telekomunikacyjne.

W ocenie NIK, pomimo braku formalnych wymogów, co do zawierania porozumień z przedsiębiorcami telekomunikacyjnymi w zakresie udostępniania Policji danych retencyjnych, ustalenie procedur postępowania pozwoliłoby ograniczyć ryzyko wystąpienia nieprawidłowości w tym zakresie. W szczególności, w zawieranych z operatorami telekomunikacyjnymi porozumieniach, należałoby uregulować procedurę telefonicznego pozyskiwania danych, tak aby wyeliminować możliwość pozyskania tych danych przez osoby nieuprawnione.

Zgodnie z treścią art. 20c ust. 5 pkt 1 lit. a ustawy o Policji udostępnienie Policji danych telekomunikacyjnych może nastąpić za pośrednictwem sieci telekomunikacyjnej, jeżeli wykorzystywane sieci telekomunikacyjne zapewniają możliwość ustalenia osoby uzyskującej dane, ich rodzaju oraz czasu, w którym zostały uzyskane.

W trakcie kontroli stwierdzono, że w Biurze Spraw Wewnętrznych KGP (BSW KGP) dane telekomunikacyjne za pomocą indywidualnej karty wydanej funkcjonariuszowi, uzyskiwane były jeszcze przez dwóch innych funkcjonariuszy tego Biura. Przypadki takie występowały również w komendach wojewódzkich. Wprawdzie wszyscy policjanci posługujący się tą kartą posiadali stosowne upoważnienie Komendanta Głównego Policji lub komendantów wojewódzkich,

uprawniające do dokonywania ustaleń telekomunikacyjnych, jednakże opisana sytuacja spowodowała, że zaewidencjonowane w systemie zapisy dotyczące rejestracji i sprawdzeń nie pozwalały na jednoznaczną i udokumentowaną identyfikację funkcjonariusza uzyskującego dane, czym naruszono przepisy art. 20c ust. 5 pkt 1 lit. a ustawy o Policji.

Zabezpieczenia organizacyjne i techniczne w zakresie pozyskiwania i przetwarzania danych telekomunikacyjnych

Zgodnie z treścią art. 20c ust. 5 pkt 1 lit. b udostępnienie Policji danych telekomunikacyjnych może nastąpić za pośrednictwem sieci telekomunikacyjnej, jeżeli zastosowane w nich zabezpieczenie techniczne i organizacyjne uniemożliwiają osobie nieuprawnionej dostęp do tych danych. Zapewnienie poufności pozyskiwania danych telekomunikacyjnych oraz przekazywanie ich komórkom organizacyjnym KGP wnioskującym o te dane, polegało m.in. na zastosowaniu odpowiednich metod przesyłania (zaszyfrowana transmisja). Sieci wewnętrzne i Internet działały oddzielnie (były odseparowane). Stanowiska komputerowe posiadały oprogramowanie dostępowe i mogły na nich pracować tylko osoby uprawnione posiadające własne konta dostępowe oraz indywidualne karty.
Komputery przeznaczone do pozyskiwania danych telekomunikacyjnych znajdowały się w pomieszczeniach objętych strefami bezpieczeństwa (BK KGP i BWK KGP) lub w zabezpieczonych pomieszczeniach (BSW, CBŚ).
W ocenie NIK, zastosowane środki ochrony dostępu do sieci telekomunikacyjnych służących pozyskiwaniu danych, były wystarczające dla zapewnienia ochrony uzyskanych danych telekomunikacyjnych przed dostępem osób nieuprawnionych.

Osoby upoważnione do sięgania po dane telekomunikacyjne

W Regulaminie Komendy Głównej Policji nie przypisano wprost żadnej z komórek organizacyjnych zadań w zakresie realizacji uprawnień wynikających z art. 20c ustawy o Policji. Kontrola wykazała, że dane telekomunikacyjne w Komendzie Głównej Policji (KGP) były pozyskiwane przez funkcjonariuszy CBŚ KGP, BSW KGP, Biura Wywiadu Kryminalnego KGP (BWK KGP) oraz Biura Kryminalnego KGP (BK KGP). Jedynie Dyrektorzy BK i BSW KGP opracowali w tym zakresie stosowne procedury, jednakże miały one wyłącznie charakter zaleceń.
Dane telekomunikacyjne były pozyskiwane na zlecenia komórek organizacyjnych (Wydziałów) wchodzących w skład ww. Biur, które miały w zakresie swojej właściwości określone zadania związane z zapobieganiem lub wykrywaniem przestępstw, a także Biura Międzynarodowej Współpracy Policji KGP (BMWP KGP).
Osobami uprawnionymi, na podstawie art. 20c ust. 2 ustawy o Policji, do występowania z żądaniem udostępnienia danych telekomunikacyjnych byli policjanci wskazani w pisemnym wniosku Komendanta Głównego Policji lub komendanta wojewódzkiego Policji albo osoby przez nich upoważnione. W celu realizacji ww. uprawnień Komendant Główny Policji wydał decyzję nr 177 z dnia 28 czerwca 2010 r. w sprawie trybu zwracania się do Komendanta Głównego Policji o udzielenie upoważnienia do występowania o udostępnienie danych telekomunikacyjnych (niepublikowana). W treści powołanej wyżej decyzji określono m.in. zasady wydawania upoważnień oraz przesłanki cofnięcia upoważnienia. Zgodnie z przyjętymi w decyzji zasadami, imienne upoważnienia udzielane były policjantom, jeżeli było to uzasadnione zakresem czynności

służbowych (zapobieganie lub wykrywanie przestępstw) i wiązało się z koniecznością dostępu do danych telekomunikacyjnych.
Komendant Główny Policji nie miał prawnego obowiązku wprowadzania szczegółowych regulacji, czy wewnętrznych aktów prawnych w obszarach nieuregulowanych przez ustawę o Policji. Jednakże w ocenie NIK, jedną z głównych przyczyn stwierdzonych w toku kontroli nieprawidłowości był brak odpowiednich procedur wewnętrznych, które zapobiegłyby wystąpieniu nieprawidłowości lub pozwoliłyby na bieżąco je eliminować. Wprowadzenie przepisów (procedur) wewnętrznych w zakresie realizacji przez funkcjonariuszy uprawnień dotyczących żądania i przetwarzania danych telekomunikacyjnych, pozwoliłoby również ujednolicić praktykę postępowania w tym zakresie oraz zwiększyć nadzór nad prowadzonymi działaniami.

Sprawność i szybkość pozyskiwania informacji

W badanej próbie zapytań telekomunikacyjnych nie stwierdzono przypadków przekazywania danych telekomunikacyjnych z opóźnieniem, które utrudniałoby wykonywanie zadań jednostki. W okresie objętym kontrolą NIK wystąpiło natomiast 11 przypadków odmowy lub nie wykonania w pełnym zakresie ustaleń telekomunikacyjnych dla Policji. W odniesieniu do każdej ww. odmowy KGP zwrócił się pisemnie (na podstawie art. 20c ustawy o Policji) do Urzędu Komunikacji Elektronicznej o podjęcie działań mających na celu zaprzestanie przez niektórych operatorów telefonii dalszych tego rodzaju praktyk.

Ewidencjonowanie pozyskanych danych telekomunikacyjnych

Obowiązujące przepisy nie nakładają na Policję obowiązku gromadzenia informacji statystycznej na temat ustaleń telekomunikacyjnych. Wprowadzone w Policji zasady w zakresie ewidencjonowania pozyskiwania danych telekomunikacyjnych obejmowały liczbę kierowanych zapytań, a nie ilość uzyskanych danych telekomunikacyjnych. W związku z tym, nie można było dokonać ustaleń dotyczących zakresu i ilości pozyskanych w okresie objętym kontrolą danych.
Dane liczbowe dotyczące zakresu i liczby zapytań złożonych przez Policję w 2011 r. przedstawiały się następująco[44]:

Rok	Zapytania o:					Razem
	wykazy połączeń	dane abonenta	dane lokalizacyjne	użytkowników zakończenia sieci (abonent IP)	inne (biling z BTS itp.)	
1.	2.	3.	4.	5.	6.	7.
2011	632 606	610 156	102 067	59 902	43 880	1 448 611

[44] Policja odmówiła udostępnienia danych za pierwsze półrocze 2012 r.

Procentowe zestawienie liczby zapytań telekomunikacyjnych KGP odpowiednio w 2011 r. i w I półroczu 2012 r. przedstawia się następująco:

Rodzaj zapytania	2011 r.	2012 r. (I-IV)
lokalizacja telefonów komórkowych	2,3%	4,2%
wykaz połączeń (bilingi, IMEI, MSISDN itp.)	28,1%	35,9%
abonenci (MSISDN, IMEI, SIM, IMSI, REGON, NIP, PESEL, Adres)	68,8%	57,4%
inne (biling z BTS itp.)	0,8%	2,5%
użytkownik zakończenia sieci (abonent IP)	0,4%	0,2%

NIK zwraca uwagę na fakt, iż wobec braku jednolitej metodologii liczenia danych w poszczególnych służbach, dane te nie mogą być wprost porównywane pomiędzy poszczególnymi służbami, a przytoczone powyżej wielkości należy traktować jako dane szacunkowe.

W KGP nie było określonych zasad, ani nie wypracowano jednolitej praktyki prowadzenia rejestrów i urządzeń służących do ewidencjonowania zapytań kierowanych do przedsiębiorców telekomunikacyjnych oraz informacji o efektach realizacji tych zleceń. W efekcie nie było możliwości ustalenia, w jakim zakresie Policja wykorzystuje możliwości w zakresie sięgania po dane obywateli. Np. w BWK KGP zapytania do operatorów telekomunikacyjnych o dane telekomunikacyjne rejestrowane były w dzienniku korespondencyjnym. Na podstawie zapisów w tym dzienniku nie było możliwości jednoznacznego ustalenia ile było takich zapytań. Rejestr prowadzony przez BSW KGP nie pozwalał na określenie osoby kierującej zapytanie, liczby oraz rodzaju zapytań. Natomiast na podstawie rejestru prowadzonego przez CBŚ KGP, nie można było jednoznaczne określić osoby kierującej zapytanie.

W ocenie NIK, ujednolicenie zasad prowadzenia rejestrów, zwiększyłoby kontrolę i ułatwiło nadzór nad prawidłowością realizacji zadań w zakresie pozyskiwania danych telekomunikacyjnych. Rejestry te, w ocenie NIK, w szczególności powinny zawierać informacje dotyczące: daty zapytania i uzyskania odpowiedzi, nazwy operatora do którego skierowano zapytanie, osoby realizującej zapytanie, zakresu zapytania (liczba i rodzaj ustaleń, okres za który pozyskiwane są dane), komórki zlecającej zapytanie, nr sprawy (zlecenia) w ramach którego dokonywane jest sprawdzenie.

Postępowanie z danymi telekomunikacyjnymi zbędnymi

Materiały udostępnione przez podmioty prowadzące działalność telekomunikacyjną, które nie zawierają informacji mających znaczenie dla postępowania karnego, na podstawie art. 20 c ust. 7 ustawy o Policji, podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu.

W komórkach Biur analizujących dane telekomunikacyjne (merytorycznych) były one traktowane, jako jedna z metod pracy operacyjnej. Utrwalone w formie pisemnej dane telekomunikacyjne, zawierające informacje zbędne, podlegały zniszczeniu wg zasad obowiązujących dla materiałów uzyskanych w wyniku czynności operacyjno–rozpoznawczych. W tym celu powoływane były komisje (czynność ta nie była dokumentowana) przez kierownika komórki prowadzącej sprawę. Obowiązkiem komisji było sporządzenie protokołu zawierającego m.in. wykaz zniszczonych dokumentów, dane członków komisji oraz podpis kierownika komórki. W CBŚ KGP stwierdzono jednakże trzy przypadki, gdy zniszczenie danych nie zostało udokumentowane protokołem, lecz w formie odręcznej adnotacji podpisanej przez funkcjonariusza i jego bezpośredniego przełożonego. W ocenie NIK, obowiązująca w poszczególnych komórkach merytorycznych

Biur praktyka zapewniała, co do zasady, niszczenie danych zbędnych, w sposób zgodny z ww. wymogami ustawowymi.
Jednakże w komórkach organizacyjnych KGP pośredniczących w pozyskaniu danych telekomunikacyjnych, nie realizowano obowiązku, o którym mowa cytowanym wyżej art. 20 c ust. 7 ustawy o Policji. Dane telekomunikacyjne, które wpływały na stanowiska dostępowe, a następnie były przekazane komórce, która te dane analizuje (merytorycznej), były usuwane z urządzeń służących do ich pozyskiwania i przekazywania z pominięciem trybu komisyjnego i protokolarnego niszczenia danych telekomunikacyjnych. W wewnętrznych procedurach do realizacji zadań związanych z ustaleniami telekomunikacyjnymi BK KGP określono, że dane te mają być usunięte po wysłaniu do wnioskodawcy. W BWK KGP funkcjonariusze pozyskujący dane telekomunikacyjne mają obowiązek skasowania wszystkich danych telekomunikacyjnych poprzez funkcję usuń oraz opróżnienie tzw. kosza. Kwestia ta nie była uregulowana w formie pisemnych procedur. W toku kontroli nie przedstawiono dowodów na okoliczność kasowania danych telekomunikacyjnych z komputera na stanowisku, służącym do pozyskiwania tych danych od operatorów. W BSW KGP stosowano rozwiązanie, polegające na automatycznym usuwaniu wiadomości z serwera pocztowego po upływie 30 dni od momentu wysłania wiadomości do adresata. Po upływie tego okresu nie było możliwości odzyskania, czy też podejrzenia wysłanej wiadomości zawierającej ustalenia telekomunikacyjne. W BMWP KGP stwierdzono, że w okresie objętym kontrolą przekazane z innych komórek organizacyjnych KGP dane telekomunikacyjne nie były niszczone.
W ocenie NIK, jeżeli dane telekomunikacyjne, wobec braku podstaw prawnych do ich przetwarzania, zostały usunięte z akt poszczególnych spraw poprzez komisyjne zniszczenie, to nie ma również żadnych podstaw prawnych, by dane te były nadal przechowywane w postaci ich w kopii w systemach informatycznych. Dane te powinny być niezwłocznie usunięte, a fakt ten stosownie udokumentowany.
Dane telekomunikacyjne były kopiowane na zewnętrzne nośniki informacji w celu przeniesienia ich z komputera, z zainstalowanym systemem do prowadzenia zapytań u przedsiębiorcy, na komputer w sieci wewnętrznej. Zgodnie z uzyskanymi wyjaśnieniami, przenoszenie na nośnik odbywało się bez otwierania (analizowania) danych zawartych w pliku, a następnie plik trwale usuwano (kasowano) z pamięci poczty i dysków. Nieuprawnione kopiowanie, miało być wyeliminowane z uwagi na dostęp do systemów tylko uprawnionych funkcjonariuszy, którzy mogli dokonywać tego typu czynności. W przypadku nieprawidłowego działania w zakresie kopiowania – rozliczeniu podlegał policjant otrzymujący dane i je wykorzystujący.
W ocenie NIK, opisany wyżej sposób postępowania nie gwarantował, że dane telekomunikacyjne każdorazowo były trwale usuwane z nośników, po poprawnym ich przeniesieniu na docelowy sprzęt komputerowy. Należy zaznaczyć, że kwestia ta nie została uregulowana, co uniemożliwia sprawowanie rzetelnego nadzoru i kontroli nad procesem kopiowania, przenoszenia i usuwania danych telekomunikacyjnych z użytkowanych przez funkcjonariuszy nośników informacji. Niejednolita praktyka postępowania z pozyskanymi danymi telekomunikacyjnymi wskazuje na potrzebę uregulowania kwestii niszczenia tych danych w wewnętrznych aktach prawnych.

Nadzór i kontrola nad uzyskiwaniem, przetwarzaniem i niszczeniem danych telekomunikacyjnych

Nadzór nad realizacją zadań w zakresie uzyskiwania, przetwarzania i niszczenia danych telekomunikacyjnych realizowany był przez bezpośrednich przełożonych, zgodnie z obowiązującymi w Policji regulacjami wewnętrznymi.

W okresie 2011 r. – I półrocze 2012 r. w KGP nie były prowadzone kontrole przez Biuro Kontroli KGP w zakresie ustaleń telekomunikacyjnych, kontroli w takim zakresie nie prowadziły również podmioty zewnętrzne. W 2011 r. Sekcja Bezpieczeństwa Teleinformatycznego i Ochrony Danych Osobowych BOIN KGP przeprowadziła czynności nadzorcze w zakresie retencji danych w kontekście przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. W wyniku przeprowadzonych czynności sformułowane zostały 3 wnioski w tym wniosek o opracowanie dokumentacji bezpieczeństwa, tj. polityki bezpieczeństwa dla zbioru danych osobowych prowadzonego w formie manualnej oraz wypracowanie metod czyniących zadość dyspozycji art. 20 c ust. 7 ustawy o Policji. Ponadto w II półroczu 2012 funkcjonariusze WTO BK KGP dokonali sprawdzeń realizacji sposobu pozyskiwania danych telekomunikacyjnych przez Policję w KWP: Bydgoszcz, Białystok, Olsztyn, Łódź, Kraków i Rzeszów. Wyniki ww. czynności oraz wnioski udokumentowane były w formie notatek służbowych.
NIK zwróciła uwagę na fakt, iż sprawowanie skutecznego nadzoru nad uzyskiwaniem, przetwarzaniem i niszczeniem danych telekomunikacyjnych utrudniał brak jednolitych regulacji wewnętrznych w tym zakresie.

Wybrane ustalenia z kontroli w Komendach Wojewódzkich Policji

NIK pozytywnie oceniła działania Komendantów Wojewódzkich Policji w Katowicach, Rzeszowie i Wrocławiu w zakresie realizacji zadań związanych z uzyskiwaniem i przetwarzaniem danych telekomunikacyjnych w celu zapobiegania lub wykrywania przestępstw. Wydając powyższe oceny NIK uwzględniła, iż Komendanci ci funkcjonują w zhierarchizowanej strukturze organizacyjnej, a ich kompetencje w zakresie zapewnienia prawidłowego pozyskiwania, przetwarzania i niszczenia danych telekomunikacyjnych były ograniczone zakresem posiadanych uprawnień.
Skontrolowani Komendanci Wojewódzcy Policji prawidłowo – w ramach posiadanych kompetencji – uregulowali i doprecyzowali aktami wewnętrznymi zasady uzyskiwania i przetwarzania danych pozyskiwanych od operatorów telekomunikacyjnych w celu zapobiegania lub wykrywania przestępstw. Dokumentacja realizacji czynności w zakresie pozyskiwania, przetwarzania i przekazywania danych telekomunikacyjnych była prowadzona w sposób uporządkowany, przejrzysty, umożliwiający nadzór i bieżącą kontrolę na każdym etapie pozyskiwania tych danych. Prawidłowo dokonano również zabezpieczenia pozyskanych danych przed nieuprawnionym dostępem do nich. Zapewniono także poufność przekazywania danych pomiędzy uprawnionymi komórkami organizacyjnymi Policji. Przeprowadzona kontrola – na bazie próby losowej – zachowania procedur w zakresie występowania o dane do operatorów telekomunikacyjnych, zakresu czasowego żądania, posiadania upoważnień przez funkcjonariuszy, zakresu żądanych danych oraz formy składania zapytań – nie wykazała nieprawidłowości. Stwierdzone przypadki posługiwania się przez kilku funkcjonariuszy wspólną kartą dostępową, były spowodowane dostarczeniem przez KGP po jednej karcie do poszczególnych komend. Nie stwierdzono także nieprawidłowości w sposobie wykorzystywania przez komórki organizacyjne KWP przyznanych im uprawnień do żądania, uzyskiwania, przetwarzania, wykorzystywania i niszczenia danych telekomunikacyjnych.

3.2.4. Służba Kontrwywiadu Wojskowego

Pozyskiwanie danych telekomunikacyjnych

Służba Kontrwywiadu Wojskowego, na podstawie art. 32 ust. 1 ustawy o SKW i SWW, może żądać udostępnienia danych telekomunikacyjnych. Udostępnienie SKW danych telekomunikacyjnych

może nastąpić za pośrednictwem sieci telekomunikacyjnej, jeżeli wykorzystywanie sieci i system teleinformatyczny zapewniają możliwość ustalenia osoby uzyskującej te dane, ich rodzaju oraz czasu, w którym zostały uzyskane oraz zabezpieczenia techniczne i organizacyjne uniemożliwiają osobie nieuprawnionej dostęp do tych danych (art. 32 ust. 6 ustawy o SKW i SWW).

Udostępnianie danych telekomunikacyjnych odbywało się na podstawie porozumień zawartych pomiędzy Szefem SKW a operatorami na podstawie art. 32 ust. 5 ustawy o SKW i SWW. W przypadku podległych jednostek organizacyjnych realizujących ustalenia telekomunikacyjne, przesyłano do operatorów imienne listy osób upoważnionych do realizacji ustaleń telekomunikacyjnych. Wysyłanie zapytań do operatorów zarówno pisemnych, jak i drogą elektroniczną, odbywało się na wniosek żołnierza lub funkcjonariusza, podlegający weryfikacji i zatwierdzeniu przez kierownika jednostki organizacyjnej. Dodatkowo Biuro Techniki i Obserwacji (BTiO) posiadało rolę nadzorczą dla poszczególnych systemów do wysyłania zapytań drogą elektroniczną, poprzez dostęp do bazy danych upoważnionego użytkownika lub poprzez otrzymywanie w formie elektronicznej wszystkich zapytań w okresach kwartalnych. Badanie losowo dobranej próby zapisów dotyczących żądania udostępnienia danych telekomunikacyjnych nie wykazało nieprawidłowości.

Zabezpieczenia organizacyjne i techniczne w zakresie pozyskiwania i przetwarzania danych telekomunikacyjnych

Szef SKW wprowadził procedury bezpieczeństwa danych telekomunikacyjnych związanych z realizacją wniosków o ustalenia telekomunikacyjne, które precyzyjnie regulowały wszystkie niezbędne kwestie w tym zakresie. W SKW prowadzono również analizy ryzyka, których celem było wyeliminowanie potencjalnych nieprawidłowości.

Zastosowane rozwiązania techniczne i organizacyjne umożliwiały jednoznaczne zidentyfikowanie użytkownika końcowego przetwarzającego dane, a podejmowane przez niego działania były na bieżąco rejestrowane przez system informatyczny. Kompleks pomieszczeń, w którym zlokalizowany był system do przetwarzania danych telekomunikacyjnych, znajdował się w I strefie bezpieczeństwa, do której dostęp mieli jedynie upoważnieni pracownicy Wydziału I BTiO. Dostęp do systemu możliwy był jedynie po uprzednim uwierzytelnieniu, a zastosowane rozwiązania techniczne skutecznie ograniczały ryzyko dostępu osób niepowołanych. Po zalogowaniu się, użytkownik miał możliwość uruchomienia tylko tej części oprogramowania systemu, do której przydzielono mu uprawnienia.

W ocenie NIK, zastosowane środki ochrony dostępu do sieci telekomunikacyjnych służących pozyskiwaniu danych, były wystarczające dla zapewnienia ochrony uzyskanych danych telekomunikacyjnych przed dostępem osób nieuprawnionych.

Osoby upoważnione do sięgania po dane telekomunikacyjne

Szef SKW, na podstawie art. 20 ust. 2 ustawy o SKW i SWW, upoważnił dyrektora BTiO oraz jego zastępców do występowania w jego imieniu o dane ujęte w art. 180c i 180d ustawy Prawo telekomunikacyjne. Ponadto Szef SKW upoważnił imiennie, do korzystania z elektronicznych baz danych operatorów telekomunikacyjnych, osoby z dziewięciu jednostek organizacyjnych SKW realizujących czynności operacyjno-rozpoznawcze, na podstawie regulaminów organizacyjnych i instrukcji o czynnościach operacyjnych (Zarząd Operacyjny, Zarząd Ochrony Interesów Ekonomicznych Sił Zbrojnych, Biuro Pełnomocnika Ochrony i Bezpieczeństwa Wewnętrznego, Biuro Radiokontrwywiadu oraz Inspektoratów SKW w Warszawie, Gdyni, Poznaniu, Lublinie i Krakowie). Jednostki te upoważnione były do korzystania, za pomocą indywidualnych kart dostępu, z baz danych pięciu operatorów telekomunikacyjnych.

Sprawność i szybkość pozyskiwania danych teleinformatycznych

Nie stwierdzono przypadków kwestionowania przez operatorów telekomunikacyjnych uprawnień ustawowych SKW i odmowy udostępniania danych telekomunikacyjnych. W jednostce kontrolowanej nie wystąpiły przypadki przekazywania danych telekomunikacyjnych z opóźnieniem, które utrudniałoby wykonywanie zadań jednostki.

Ewidencjonowanie pozyskanych danych telekomunikacyjnych

Obowiązujące przepisy nie nakładają na SKW obowiązku gromadzenia informacji statystycznej na temat ustaleń telekomunikacyjnych. W jednostce kontrolowanej funkcjonuje ewidencja elektroniczna umożliwiająca odnotowanie, kto, kiedy i w jakim celu oraz jakie dane uzyskiwał. Ponadto prowadzona jest w BTiO ewidencja papierowa zapytań jawnych i niejawnych, w formie wydruku treści zapytań do operatorów telekomunikacyjnych, wysłanych drogą elektroniczną. Ewidencja niejawna zapytań prowadzona jest w formie papierowej wyłącznie poprzez BTiO (przechowywany jest drugi egzemplarz zapytania wysłany do operatorów telekomunikacyjnych). Przeprowadzone badanie w zakresie rzetelności prowadzonych ewidencji nie wykazało nieprawidłowości.

Ze sporządzonego, na podstawie elektronicznej bazy danych, zestawienia wynika, iż w 2011 r. ustalenia wykonane przez BTiO dotyczyły 42.386 danych użytkowników, a w I połowie 2012 r. – 16.978 danych. Z zapytaniem o historię połączeń (lokalizacja) w 2011 r. wystąpiono w 1.570 wnioskach (3,7%), a w I połowie 2012 r. w 784 wnioskach (4,6%). Pozostałe zapytania dotyczyły ustalenia danych abonenta. Realizowane przez pozostałe jednostki organizacyjne SKW działania dotyczyły w 2011 r. – 34.122 numerów użytkowników, a w I połowie 2012 r. – 19.560 użytkowników. Na ogólną liczbę 76.508 ustaleń telekomunikacyjnych w 2011 r. i 36.538 w I połowie 2012 r. zrealizowanych przez wszystkie jednostki organizacyjne SKW, ustalenie abonenta przez SKW dotyczyło odpowiednio 73.009 i 34.605 abonentów oraz 3.499 (4,6%) i 1.933 (5,3%) ustaleń historii połączeń (bilingi).

NIK zwraca uwagę na fakt, iż wobec braku jednolitej metodologii liczenia danych w poszczególnych służbach, dane te nie mogą być wprost porównywane pomiędzy poszczególnymi służbami, a przytoczone powyżej wielkości należy traktować jako dane szacunkowe.

Postępowanie ze zbędnymi danymi telekomunikacyjnymi

Oceną zgromadzonych danych zajmuje się jednostka wnioskująca o ich pozyskanie. Przepisy nie nakazują SKW zniszczenia danych telekomunikacyjnych w określonych sytuacjach (np. gdy stały się one zbędne, z punktu widzenia celu dla którego zostały pozyskane). W wyjaśnieniu Szef SKW podał, że „z uwagi na specyfikę zainteresowań SKW zniszczenie tego typu danych mogłoby spowodować ograniczenie możliwości operacyjnych wobec prowadzonych rozpracowań. Ponadto materiały te nie podlegają komisyjnemu zniszczeniu, gdyż nie zostały pozyskane w wyniku stosowania kontroli operacyjnej, a tym samym nie stosuje się wobec nich zapisu art. 31 ust. 15 ustawy o SKW i SWW. Informacje uzyskiwane od operatorów są włączone do procedur operacyjnych i po ich zakończeniu składane i przechowywane w Biurze Ewidencji Archiwum SKW wraz ze wszystkimi materiałami zgromadzonymi w prowadzonej procedurze".

Nadzór i kontrola nad uzyskiwaniem, przetwarzaniem i niszczeniem danych telekomunikacyjnych

W BTiO przeprowadzony został audyt przez Zarząd Bezpieczeństwa Informacji Niejawnych (ZBIN) z zakresu bezpieczeństwa teleinformatycznego. W wyniku audytu BTiO otrzymało Świadectwo Bezpieczeństwa Teleinformatycznego. W wyniku sformułowanych przez ZBIN SKW zaleceń, dwie osoby spośród sześciu, odbyły szkolenia specjalistyczne administratorów systemu (posiadały nieaktualne zaświadczenie o odbytym szkoleniu). Nadzór na realizacją zadań był prowadzony przez bezpośrednich przełożonych, na zasadach analogicznych, jak przy prowadzeniu czynności operacyjno-rozpoznawczych. W kontrolowanym okresie nie wniesiono skarg, których przedmiotem było nienależyte wykonywanie przez kontrolowaną jednostkę uprawnień w związku z pozyskiwaniem danych telekomunikacyjnych.

3.2.5. Straż Graniczna

Pozyskiwanie danych telekomunikacyjnych

W Komendzie Głównej Straży Granicznej nie zostały ustanowione pisemne procedury wewnętrzne w zakresie realizacji uprawnień dotyczących uzyskiwania od przedsiębiorców telekomunikacyjnych danych, o których mowa w art. 180c i 180d Prawa telekomunikacyjnego. W trakcie kontroli prowadzone były prace nad przygotowaniem algorytmu postępowania przy pobieraniu danych telekomunikacyjnych.

Pozyskiwanie danych telekomunikacyjnych w oparciu o pisemny wniosek lub ustne żądanie

Ustalenia telekomunikacyjne dokonywane w trybie art. 10b ust. 2 pkt 1 ustawy o Straży Granicznej, tj. na pisemny wniosek Komendanta Głównego Straży Granicznej lub osoby przez niego upoważnionej, jak również na ustne żądanie funkcjonariusza (wydane na podstawie art. 10b ust. 2 pkt 2), realizowane były na podstawie ewidencjonowanych w rejestrze upoważnień. Występowanie przez upoważnionego funkcjonariusza o ustalenie danych telekomunikacyjnych odbywało się za wiedzą i zgodą kierownika komórki organizacyjnej. Przyjęta praktyka poddawała wykonywanie ustaleń telekomunikacyjnych nadzorowi przełożonych oraz pozawalała na weryfikację zasadności wystąpień o dane telekomunikacyjne. W okresie objętym kontrolą nie były kierowane zapytania do przedsiębiorców telekomunikacyjnych w trybie ustnego żądania udostępnienia danych, o których mowa w art. 180c i d ustawy Prawo telekomunikacyjne. Badanie losowo dobranej próby zapisów dotyczących żądania udostępnienia danych telekomunikacyjnych nie wykazało nieprawidłowości.

Komendant Główny Straży Granicznej nie miał prawnego obowiązku wprowadzenia pisemnych regulacji w zakresie pozyskiwania danych telekomunikacyjnych, a praktyka stosowana w KGSG była właściwa. Jednakże w ocenie NIK, wprowadzenie pisemnych procedur wewnętrznych w zakresie żądania i przetwarzania danych telekomunikacyjnych we wszystkich komórkach pozwoliłoby na ujednolicenie procedur i zwiększenie nadzoru nad realizowanymi czynnościami. Zwiększeniu nadzoru służyłoby również wprowadzenie rozwiązań, zgodnie z którymi ustalenia dokonywane byłyby przez inne jednostki organizacyjne, niż prowadzące postępowanie (jednostki merytoryczne).

Pozyskiwanie danych za pośrednictwem sieci telekomunikacyjnej

Zgodnie z art. 10b ust. 1 pkt 3 ustawy o Straży Granicznej udostępnienie Straży Granicznej danych telekomunikacyjnych może nastąpić za pośrednictwem sieci telekomunikacyjnej funkcjonariuszowi

posiadającemu pisemne upoważnienie. Zgodnie z art. 10b ust. 4 pkt 1 lit. a ustawy o Straży Granicznej sieci telekomunikacyjne mają zapewniać możliwość ustalenia osoby uzyskującej dane, ich rodzaju oraz czasu, w którym zostały uzyskane.
Proces uzyskiwania i przesyłania danych telekomunikacyjnych KGSG realizuje za pośrednictwem sieci, należących do przedsiębiorców telekomunikacyjnych. Proces przekazywania danych za pośrednictwem sieci został uzgodniony w drodze porozumień zawartych przez Komendanta Głównego Straży Granicznej z przedsiębiorcami. Systemy zapewniały dostęp do danych telekomunikacyjnych przez całą dobę. Wykorzystywane w KGSG sieci telekomunikacyjne, wraz ze stosowanymi rozwiązaniami organizacyjnymi, zapewniały możliwość ustalenia osoby uzyskującej dane, ich rodzaju oraz czasu, w którym zostały uzyskane. Badanie losowo dobranej próby zapisów dotyczących żądania udostępnienia danych telekomunikacyjnych nie wykazało nieprawidłowości.

Zabezpieczenia organizacyjne i techniczne w zakresie pozyskiwania i przetwarzania danych telekomunikacyjnych

W Komendzie Głównej zostały opracowane i wdrożone procedury regulujące dostęp do systemów informatycznych. Procedury te zostały opracowane w odniesieniu do systemów, w których przetwarzane są zbiory danych osobowych oraz w których przetwarzane są informacje niejawne. W odniesieniu do systemów informatycznych przetwarzających informacje niejawne, na podstawie ustawy o ochronie informacji niejawnych, opracowana została dla każdego systemu dokumentacja bezpieczeństwa, tj. Szczególne Wymagania Bezpieczeństwa oraz Procedury Bezpiecznej Eksploatacji. Na podstawie dokumentacji bezpieczeństwa systemy teleinformatyczne obecnie eksploatowane uzyskały akredytację bezpieczeństwa teleinformatycznego.
W odniesieniu do systemów informatycznych przetwarzających zbiory danych osobowych, które nie zostały oznaczone klauzulą tajności, opracowane zostały dokumenty przedstawiające sposób ochrony danych osobowych. W dokumentacji bezpieczeństwa systemów informatycznych, zostały zawarte procedury wymagane przepisami prawa, w tym dotyczące zasad dostępu do tych systemów oraz rozliczalności w zakresie uzależnionym od specyfiki systemu teleinformatycznego, a mających na celu zapewnienie bezpieczeństwa i ochrony samych systemów i przetwarzanych w nich danych.
Dostęp do danych przetwarzanych w systemach teleinformatycznych posiadają wyłącznie osoby posiadające stosowne uprawnienia, logując się na swoje indywidualne konto przy użyciu hasła lub karty mikroprocesorowej.
Komputery przeznaczone do pozyskiwania danych telekomunikacyjnych znajdowały się w odpowiednio zabezpieczonych pomieszczeniach.
W ocenie NIK, zastosowane środki ochrony dostępu do sieci telekomunikacyjnych służących pozyskiwaniu danych, były wystarczające dla zapewnienia ochrony uzyskanych danych telekomunikacyjnych przed dostępem osób nieuprawnionych.

Osoby upoważnione do sięgania po dane telekomunikacyjne

Podmiotami uprawnionymi do uzyskiwania i przetwarzania danych telekomunikacyjnych w Komendzie Głównej Straży Granicznej były komórki organizacyjne, które regulaminami wewnętrznymi zostały powołane do rozpoznawania, zapobiegania i wykrywania przestępstw, tj. Zarząd Operacyjno-Śledczy (ZOŚ) i Zarząd Spraw Wewnętrznych (ZSW).

Stwierdzono, że nie we wszystkich zakresach zadań komórek organizacyjnych ww. zarządów, zamieszczono zadanie uzyskiwania danych telekomunikacyjnych oraz nie wszyscy funkcjonariusze upoważnieni do uzyskiwania danych telekomunikacyjnych mieli ujęte takie zadania w zakresie obowiązków służbowych.
Upoważnienia do wymiany informacji drogą elektroniczną z przedsiębiorcami telekomunikacyjnymi miały formę zatwierdzonych przez Komendanta Głównego list, podpisanych przez dyrektorów wnioskujących, z danymi funkcjonariuszy (m.in. imię i nazwisko, identyfikator). Listy upoważnionych funkcjonariuszy były przekazywane do Biuro Łączności i Informatyki (BŁiI) i przesyłane do właściwych przedsiębiorców telekomunikacyjnych. BŁiI zajmowało się dystrybucją kart dostępu i czytników kart.
W Komendzie Głównej Straży Granicznej nie był prowadzony rejestr upoważnień wydanych funkcjonariuszom do uzyskiwania danych za pośrednictwem sieci telekomunikacyjnej. Brak rejestru spowodował w dwóch przypadkach trudności w wykazaniu upoważnień funkcjonariuszy do występowania o dane telekomunikacyjne. W jednym przypadku nie odnaleziono upoważnienia funkcjonariusza ZSW do występowania o dane telekomunikacyjne, choć dysponował on kartą dostępu. Ponadto kontrola wykazała, że dwóch funkcjonariuszy ZSW występujących o dane telekomunikacyjne nie miało upoważnienia administratora do przetwarzania danych w systemie, do czego zobowiązuje art. 37 ustawy o ochronie danych osobowych.
W ocenie NIK, brak rejestru funkcjonariuszy upoważnionych do uzyskiwania danych telekomunikacyjnych za pośrednictwem sieci telekomunikacyjnych oraz nieokreślenie zadań w zakresie pozyskiwania danych telekomunikacyjnych w regulaminach wewnętrznych niektórych jednostek organizacyjnych i zakresach obowiązków funkcjonariuszy, może mieć wpływ na realizację skutecznego nadzoru i kontroli nad procesem pozyskiwania danych telekomunikacyjnych.

Sprawność i szybkość pozyskiwania danych teleinformatycznych

W kontrolowanym okresie nie wystąpiły przypadki odmowy udostępnienia danych telekomunikacyjnych, jak również nie odnotowano przypadków przekazywania tych danych z opóźnieniem, które utrudniałoby wykonanie zadań jednostce. Przedsiębiorcy telekomunikacyjni nie kwestionowali uprawnień Komendanta Głównego do uzyskiwania danych telekomunikacyjnych.

Ewidencjonowanie pozyskanych danych telekomunikacyjnych

W trakcie kontroli nie można było dokonać wiarygodnych ustaleń dotyczących zakresu i ilości danych pozyskanych przez kontrolowaną jednostkę w okresie objętym kontrolą. Prowadzone przez SG statystyki w zakresie pozyskiwania danych telekomunikacyjnych obejmowały liczbę kierowanych zapytań, a nie ilość uzyskanych danych telekomunikacyjnych. Należy zwrócić uwagę, że obowiązujące przepisy prawne nie nakładają na SG obowiązku gromadzenia informacji statystycznej na temat ustaleń telekomunikacyjnych. Opracowywane przez SG statystyki i przyjęta formuła gromadzenia tych danych wynikała jedynie z uregulowań o charakterze wewnętrznym.
W Komendzie Głównej prowadzona jest ewidencja, w której odnotowano, kto, kiedy, w jakim celu oraz jakie dane lub informacje uzyskiwał. Ewidencję, zwaną rejestrami, prowadziły odrębnie ZOŚ i ZSW, przy czym w ZSW ewidencja prowadzona była także odrębnie w wewnętrznych komórkach organizacyjnych. Ewidencja pozwalała na odtworzenie procesu uzyskiwania danych telekomunikacyjnych od sporządzenia wniosku przez funkcjonariusza wykonującego czynności operacyjno-rozpoznawcze, przez jego zatwierdzenie przez przełożonych, realizację przez osoby

posiadające dostęp do systemów udostępnionych przez operatorów telekomunikacyjnych, do otrzymania wnioskowanych danych. Funkcjonariusz wnioskujący o dane telekomunikacyjne sporządzał wniosek w dwóch egzemplarzach i rejestrował go w kancelarii. Jeden egzemplarz trafiał do komórki realizującej zapytania do operatorów, a drugi włączany był do materiałów sprawy.
Stwierdzono jeden przypadek różnicy między treścią wniosku (wykaz połączeń) a treścią zapisaną w rejestrze wniosków (ustalenie abonenta).
Na wybranej przez NIK próbie dokonano weryfikacji prowadzonych rejestrów, poprzez porównanie ewidencji prowadzonej przez SG z danymi uzyskanymi od operatorów telekomunikacyjnych. Kontrola nie wykazała nieprawidłowości.
Na podstawie przedłożonych przez Komendanta Głównego Straży Granicznej zestawień zrealizowanych przez Straż Graniczną zapytań o dane telekomunikacyjne stwierdzono, że okresie od 1 stycznia 2011 r. do 30 czerwca 2012 r., upoważnieni funkcjonariusze Straży Granicznej występowali na podstawie art. 10b ustawy o Straży Granicznej do przedsiębiorców telekomunikacyjnych 521 903 razy, w tym Komenda Główna 8 707. Struktura skierowanych zapytań przedstawia się następująco:

Rok	Zapytania o:				Razem
	wykazy połączeń	dane abonenta	dane lokalizacyjne	Inne	
1.	2.	3.	4.	5.	7.
Od 01.01.2011 r. do 30.06.2012 r.	220 694	228 654	60 315	12 240	521 903

Z powyższego zestawienia wynika, że w okresie od 1 stycznia 2011 r. do 30 czerwca 2012 r. w Straży Granicznej zapytania o wykazy połączeń stanowiły 42,3% ogólnej liczby zapytań, zapytania dotyczące lokalizacji 11,6%, inne zapytania 2,3%, natomiast zapytania o dane abonenta stanowiły 43,8% ogólnej liczby zapytań.

NIK zwraca uwagę na fakt, iż wobec braku jednolitej metodologii liczenia danych w poszczególnych służbach, dane te nie mogą być wprost porównywane pomiędzy poszczególnymi służbami, a przytoczone powyżej wielkości należy traktować jako dane szacunkowe.

Postępowanie ze zbędnymi danymi telekomunikacyjnymi

Zgodnie z art. 10b ust. 6 ustawy o Straży Granicznej materiały uzyskane w wyniku czynności podjętych na podstawie ust. 1, które nie zawierają informacji mających znaczenie dla postępowania karnego, podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu.

W Komendzie Głównej w okresie od 1 stycznia 2011 r. do 30 czerwca 2012 r. niszczono komisyjnie materiały uzyskane w wyniku czynności podjętych na podstawie art. 10b ust. 1 ustawy o Straży Granicznej, które nie zawierały informacji mających znaczenie dla postępowania karnego. Sporządzono łącznie 20 protokołów. Materiały zniszczono w następujący sposób: dane w formie zapisów na nośnikach elektronicznych – dysk twardy, pamięć typu pendrive – zostały usunięte poprzez przeniesienie pojedynczych plików lub całych folderów zawierających dane do „Kosza", a następnie opróżnienie „Kosza" (procedura taka została skonsultowana i zaakceptowana przez Biuro Ochrony Informacji Niejawnych Komendy Głównej), płyty CD były fizycznie niszczone, natomiast dane w postaci dokumentów w formie papierowej niszczone były poprzez fizyczne ich pocięcie

w niszczarce. W przypadku likwidacji stanowiska komputerowego, na którym przetwarzane były dane telekomunikacyjne przed oddaniem dysku do właściwych komórek organizacyjnych pionu łączności i informatyki celem zniszczenia, dokonywano wstępnego fizycznego uszkadzania dysku, np. poprzez jego przewiercenie.

Nadzór i kontrola nad uzyskiwaniem, przetwarzaniem i niszczeniem danych telekomunikacyjnych

W okresie objętym kontrolą w Komendzie Głównej Straży Granicznej nie przeprowadzano badań audytowych w zakresie uzyskiwania, przetwarzania, wykorzystywania i niszczenia danych telekomunikacyjnych przez Zespół Audytu Wewnętrznego Komendy Głównej ani audytorów zewnętrznych. Nie były też prowadzone kontrole przez wewnętrzną komórkę kontrolą, tj. Inspektorat Nadzoru i Kontroli Komendanta Głównego Straży Granicznej, ani kontrole przez podmioty zewnętrzne. Nie dokonywano analiz, ani ocen działań w Straży Granicznej w powyższym zakresie. Nadzór na realizacją zadań był prowadzony przez bezpośrednich przełożonych, na zasadach analogicznych, jak przy prowadzeniu czynności operacyjno-rozpoznawczych.
Na podstawie Rejestru Skarg i Wniosków KGSG stwierdzono, że w kontrolowanym okresie nie wniesiono do Komendanta Głównego Straży Granicznej skarg, których przedmiotem było nienależyte wykonywanie przez kontrolowaną jednostkę uprawnień, o których mowa w art. 10b ustawy o Straży Granicznej.
NIK zwróciła uwagę na konieczność zapewnienia zewnętrznego, w stosunku do komórek organizacyjnych wnioskujących i realizujących zapytania o dane telekomunikacyjne, nadzoru i kontroli nad realizacją przez poszczególnych funkcjonariuszy uprawnień związanych z uzyskiwaniem i przetwarzaniem danych telekomunikacyjnych.

3.2.6. Żandarmeria Wojskowa

Pozyskiwanie danych telekomunikacyjnych

Zgodnie z art. 30 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, Żandarmeria Wojskowa może żądać udostępnienia danych telekomunikacyjnych. Udostępnienie danych może nastąpić na ustne lub pisemne żądanie upoważnionego funkcjonariusza lub za pośrednictwem sieci telekomunikacyjnej.
W Komendzie Głównej Żandarmerii Wojskowej ustanowione zostały wewnętrzne przepisy (procedury) w zakresie realizacji uprawnień dotyczących uzyskiwania od podmiotów prowadzących działalność telekomunikacyjną danych, o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne. Dane telekomunikacyjne były pozyskiwane na pisemne lub ustne żądanie, a także z wykorzystaniem sieci teleinformatycznych. Dostęp do danych telekomunikacyjnych za pośrednictwem sieci telekomunikacyjnej przy wykorzystaniu odpowiednich systemów teleinformatycznych zapewniło 6 największych operatorów telefonicznych. KGŻW zawarła 3 porozumienia z operatorami telekomunikacyjnymi w sprawie dostępu do systemu elektronicznego danych abonentów. W powyższych porozumieniach zawarto odniesienia do dostępu do środków technicznych i organizacyjnych operatora, w tym określono parametry techniczne stanowiska komputerowego przeznaczonego do wymiany informacji oraz procedurę składania zapytań oraz przekazywania odpowiedzi. Sprawdzenia u pozostałych operatorów realizowane były na pisemny wniosek Komendanta Głównego ŻW.
Zgodnie z art. 30 ust. 4 ustawy o Żandarmerii Wojskowej, udostępnienie danych telekomunikacyjnych może nastąpić za pośrednictwem sieci telekomunikacyjnej, w szczególności jeżeli wykorzystywane

sieci i system teleinformatyczny zapewniają możliwość ustalenia osoby uzyskującej dane, jeżeli zabezpieczenie techniczne i organizacyjne uniemożliwiają osobie nieuprawnionej dostęp do danych oraz jest to uzasadnione specyfiką lub zakresem zadań wykonywanych przez jednostki organizacyjne Żandarmerii Wojskowej albo prowadzonych przez nie czynności.
W latach 2011–2012 jedną kartą dostępu do systemu danego operatora posługiwało się 4 żołnierzy ŻW. Karty kryptograficzne umożliwiające dostęp do systemów (aplikacji) pięciu operatorów telekomunikacyjnych posiadały certyfikat wystawiony na konkretną osobę – żołnierza Wydziału Zabezpieczenia i Ewidencji. Stwierdzono jednakże przypadki, gdy z karty certyfikowanej na danego żołnierza korzystały również inne osoby. W przypadkach korzystania z sieci przez żołnierza nieposiadającego certyfikowanej na siebie karty skutkowało to ujawnianiem w systemie operatora „certyfikowanego" żołnierza, a nie osoby faktycznie korzystającej (pobierającej dane) z sieci. Natomiast dostęp do sieci jednego z operatorów telekomunikacyjnych umożliwiała karta, na podstawie której poprzez system kodowy, operator identyfikował służbę która zwróciła się do niego z zapytaniem – nie było jednakże możliwe ustalenie żołnierza, który pobierał dane. Jednakże identyfikacja osoby pobierającej dane była zapewniona przez system informatyczny KGŻW, a także poprzez wewnętrzne rejestry (od lipca 2012 r. w ewidencji elektronicznej KGŻW). W praktyce około 90% sprawdzeń dokonywało dwóch żołnierzy KGŻW mających w zakresie swoich obowiązków realizację ustaleń u operatorów telekomunikacyjnych. Pozostałe 10% wynikało z zastępstw.

Zabezpieczenia organizacyjne i techniczne w zakresie pozyskiwania i przetwarzania danych telekomunikacyjnych

W KGŻW pomieszczenie, w którym uzyskuje się i przetwarza dane telekomunikacyjne, znajduje się w II strefie ochronnej, do której dostęp mają wyłącznie upoważnieni żołnierze. Zabezpieczenia organizacyjne związane z dostępem do danych telekomunikacyjnych wynikały z zarządzeń wewnętrznych Komendanta Głównego Żandarmerii Wojskowej. Ewidencja osób realizujących konkretne zapytania do operatora telekomunikacyjnego była prowadzona w rejestrach sprawdzeń u operatorów telefonicznych (do 18 lipca 2012 r. w formie papierowej, a następnie w formie elektronicznej).

Pozyskane dane teleinformatyczne przesyłane były pomiędzy jednostkami ŻW za pismem o klauzuli „zastrzeżone" lub przekazywane bezpośrednio osobie zainteresowanej za pokwitowaniem w rejestrze sprawdzeń u operatorów telefonicznych. W przypadku ustalania lokalizacji abonenta informacja była przekazywana bezpośrednio od operatora na uprawniony numer telefonu żołnierza prowadzącego czynności operacyjno-rozpoznawcze.

W ocenie NIK, zastosowane środki ochrony dostępu do sieci telekomunikacyjnych służących pozyskiwaniu danych, były wystarczające dla zapewnienia ochrony uzyskanych danych telekomunikacyjnych przed dostępem osób nieuprawnionych.

Osoby upoważnione do sięgania po dane telekomunikacyjne

W wytycznych przyjęto, iż w zakresie uzyskiwania danych od operatorów telefonicznych lub innych podmiotów wykonujących działalność telekomunikacyjną (zwanych dalej „operatorami") jedyną uprawnioną komórką wewnętrzną w ŻW jest Wydział Zabezpieczenia i Ewidencji w Zarządzie Dochodzeniowo-Śledczym KGŻW (zwany dalej „WZiE").

Zgodnie z wytycznymi na 2011 r., z wnioskiem o sprawdzenie do szefa Wydziału Zabezpieczenia i Ewidencji mogli występować komendanci placówek, wydziałów oraz szefowie Wydziału Operacyjno-Rozpoznawczego i Wydziału Dochodzeniowo-Śledczego. W wytycznych na 2012 r. przyjęto, iż z wnioskami mogli występować komendanci terenowej jednostki organizacyjnej ŻW, szef wydziału kryminalnego lub dochodzeniowo-śledczego terenowego oddziału ŻW, żołnierz Zarządu Dochodzeniowo-Śledczego po akceptacji przez bezpośredniego przełożonego, szef Oddziału Wewnętrznego i Ochrony Informacji Niejawnych KGŻW. W rozkazie KGŻW z 13 lipca 2012 r. w sprawie wprowadzenia wytycznych, nie wyszczególniono podmiotów uprawnionych do występowania z wnioskiem, lecz ogólnie zaznaczono, iż z wnioskiem należy występować do Komendanta Głównego ŻW. Zgodnie ze wzorem załączonym do rozkazu, wniosek powinien być podpisany przez komendanta oddziału ŻW oraz zaopiniowany przez szefa Oddziału Kryminalnego KGŻW i szefa Wydziału Zabezpieczenia i Ewidencji KGŻW.
Udzielanie imiennych upoważnień (w zakresie ustnego żądania danych telekomunikacyjnych oraz za pośrednictwem sieci telekomunikacyjnej) zostało powiązane z zakresem czynności (zakresem obowiązków) w odniesieniu do 3 żołnierzy Wydziału Zabezpieczenia i Ewidencji Zarządu Dochodzeniowo-Śledczego KGŻW. W dwóch przypadkach osoby zastępujące żołnierzy stale wykonujących zadania w zakresie pozyskiwania danych telekomunikacyjnych nie miały tych zadań wpisanych do zakresów obowiązków.
W ocenie NIK przyjęty sposób pozyskiwania danych od operatorów za pośrednictwem wyspecjalizowanej komórki KGŻW stanowi przykład dobrej praktyki zabezpieczenia przed nieuprawnionym lub niecelowym pozyskiwaniem danych telekomunikacyjnych. NIK wskazuje na konieczność zamieszczenia w zakresach obowiązków wszystkich funkcjonariuszy dokonujących sprawdzeń stosownych zapisów.

Sprawność i szybkość pozyskiwania danych teleinformatycznych

W KGŻW nie było przypadków, gdy żądania formułowane przez kontrolowaną jednostkę w zakresie udostępnienia danych telekomunikacyjnych spotykały się z kwestionowaniem jej upoważnienia do uzyskania żądanych danych, ani też sytuacji, gdy dane telekomunikacyjne przekazywane były ze znaczną zwłoką.

Ewidencjonowanie pozyskanych danych telekomunikacyjnych

Prowadzone przez ŻW statystyki w zakresie pozyskiwania danych telekomunikacyjnych obejmowały liczbę kierowanych zapytań, a nie ilość uzyskanych danych telekomunikacyjnych. Należy zwrócić uwagę, że obowiązujące przepisy prawne nie nakładały na ŻW obowiązku gromadzenia informacji statystycznej na temat ustaleń telekomunikacyjnych. Opracowywane przez ŻW statystyki i przyjęta formuła gromadzenia tych danych wynikała z uregulowań o charakterze wewnętrznym.
W latach 2011–2012 r. (do lipca 2012 r.) w KGŻW prowadzono 7 rejestrów papierowych „Sprawdzenia u operatorów telefonicznych" (zwane dalej „rejestrami"). W KGŻW liczba porządkowa rejestru (pozycja rejestru) nie odzwierciedlała liczby zapytań oraz kolejności rejestrowanych spraw w KGŻW. Pozycja zapytania nie odnosiła się do jednego abonenta lub np. do jednego telefonu. Tym samym pod daną pozycją wskazywano na jeden numeru telefonu lub kilku numerów. W dniu 18 lipca 2012 r., ze względu na konieczność prowadzenia szczegółowych statystyk dotyczących pozyskiwanych danych telekomunikacyjnych, zmieniono formę prowadzenia ewidencji sprawdzeń u operatorów telefonicznych z papierowej na elektroniczną. W systemie elektronicznym jedna

pozycja rejestru odpowiadała jednemu zapytaniu operatora, co eliminuje ograniczenia statystyk papierowych. Na wybranej przez NIK próbie dokonano weryfikacji prowadzonych rejestrów, poprzez porównanie ewidencji prowadzonej przez KGŻW z danymi uzyskanymi od operatorów telekomunikacyjnych. Kontrola nie wykazała nieprawidłowości.

Na podstawie danych zawartych w rejestrach stwierdzono, iż w zakresie dotyczącym ustalenia danych abonenta lub numeru telefonu w 2011 r. (ogółem 6351 sprawdzeń) do operatorów występowano 4029 razy (63,4%), w tym o ustalenie abonenta – 3123 razy oraz o ustalenie numeru telefonu – 906 razy, a o pozostałe dane (np. bilingi, lokalizacje) – 2322 razy (36,6%). W 2012 r. (I półrocze – ogółem 2506 sprawdzeń) występowano o dane, które winne być dostępne w ramach usługi „Ogólnokrajowej informacji o numerach telefonicznych", o dane publiczne występowano 1901 razy (75,9%), w tym o ustalenie abonenta – 1541 razy oraz o ustalenie numeru telefonu – 360 razy, a o pozostałe dane – 605 razy (24,1%).

NIK zwraca uwagę na fakt, iż wobec braku jednolitej metodologii liczenia danych w poszczególnych służbach, dane te nie mogą być wprost porównywane pomiędzy poszczególnymi służbami, a przytoczone powyżej wielkości należy traktować jako dane szacunkowe.

Postępowanie ze zbędnymi danymi telekomunikacyjnymi

Zgodnie z art. 30 ust. 6 ustawy o ŻW dane telekomunikacyjne, które nie zawierają informacji mających znaczenie dla postępowania karnego, podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu.

W KGŻW nie było jednolitej pisemnej procedury oceny zgromadzonych danych telekomunikacyjnych, z punktu widzenia ich przydatności do realizacji celów, dla których zostały one pozyskane. Tym niemniej zebrane dane telekomunikacyjne podlegały kontroli w ramach prowadzonych przez Oddział Kryminalny lub Oddział Dochodzeniowo-Śledczy nadzorów w terenowych jednostkach organizacyjnych ŻW. W trakcie kontroli ocenie podlegała całość realizowanych czynności, w tym zasadność wystąpienia o dane telekomunikacyjne oraz sposób ich wykorzystania. W przypadku postępowań przygotowawczych nadzór nad tymi postępowaniami sprawował dodatkowo prokurator. We wskazanych wcześniej wytycznych szefa Zarządu Dochodzeniowo-Śledczego KGŻW oraz wytycznych Komendanta Głównego ŻW wskazano na konieczność analizowania uzyskanych od operatorów danych pod kątem ich znaczenia procesowego lub operacyjnego (dane takie należało niezwłocznie przekazywać prokuratorowi). W okresie objętym kontrolą nie dokonywano niszczenia danych telekomunikacyjnych.

Nadzór i kontrola nad uzyskiwaniem, przetwarzaniem i niszczeniem danych telekomunikacyjnych

Nadzór nad realizacją zadań sprawował szef Wydziału Zabezpieczenia i Ewidencji, kontrolując, realizowane czynności na etapie ich pozyskiwania, przetwarzania i przechowywania. Natomiast sposób wykorzystania tych danych w dalszych czynnościach operacyjno-rozpoznawczych lub dochodzeniowo-śledczych podlegał kontroli przez przełożonych osoby prowadzącej daną sprawę oraz w ramach prowadzonego przez KGŻW nadzoru. W trakcie tych kontroli ocenie podlegała całość realizowanych czynności, w tym sposób wykorzystania danych telekomunikacyjnych. W latach 2011–2012 każdy oddział podlegał sprawdzeniu 1-2 razy w ciągu roku. Wyniki czynności kontrolnych ujmowane były w pisemnym meldunku do Komendanta Głównego ŻW. W latach 2011–2012, poza kontrolą NIK, inne kontrole zewnętrzne i badania audytowe w obszarze

uzyskiwania, przetwarzania, wykorzystania i niszczenia danych telekomunikacyjnych w Żandarmerii Wojskowej nie były prowadzone. Kontrole wewnętrzne ŻW w przedmiotowym obszarze realizowane były w ramach nadzorów – nie stwierdzono uchybień.
W KGŻW nie odnotowano skarg osób, wobec których realizowano ustalenie u podmiotów wykonujących działalność telekomunikacyjną.

3.2.7. Ministerstwo Finansów

Wywiad Skarbowy i Służba Celna

Służba Celna uzyskała uprawnienia umożliwiające uzyskiwanie danych telekomunikacyjnych (art. 75d ustawy o Służbie Celnej) z dniem 14 lipca 2011 r., na podstawie art. 7 pkt 4 ustawy z dnia 26 maja 2011 r. o zmianie ustawy o grach hazardowych i niektórych innych ustaw.

Departament Wywiadu Skarbowego Ministerstwa Finansów, pozyskiwał dane telekomunikacyjne w trybie określonym w art. 36b ustawy z dnia 28 września 1991 r. o kontroli skarbowej. Dane te uzyskiwano z wykorzystaniem Systemu Elektronicznej Wymiany Informacji (SEWI). Administratorem SEWI jest Wydział Techniki Departamentu Wywiadu Skarbowego. Określona w SEWI komunikacja Wydziału Techniki z wydziałami Wywiadu Skarbowego w terenie realizowana jest za pośrednictwem niejawnego systemu MF ALERT, z wykorzystaniem poczty elektronicznej. Zatwierdzona przez Dyrektora Departamentu Wywiadu Skarbowego „Instrukcja użytkownika Systemu Elektronicznej Wymiany Informacji" określa między innymi procedurę składania i akceptacji wniosku o dostęp do danych telekomunikacyjnych, dostęp do systemów teleinformatycznych oraz kontrolę tego dostępu. Zgodnie z Instrukcją, z SEWI korzystać mogą jedynie pracownicy Wywiadu Skarbowego. Pracownik zwraca się z pisemną prośbą do naczelnika Wydziału Wywiadu Skarbowego. Pismo powinno zawierać wszelkie cechy sprawy (numer/kryptonim sprawy), dla której złożone zostanie zlecenie wraz z uzasadnieniem. Po uzyskaniu pisemnej akceptacji przełożonego, pismo kierowane jest do właściwej komórki obsługującej system MF ALERT celem realizacji.

Kontrola wykazała, iż wygenerowane zapisy zleceń – pod względem ustalenia rodzaju i numeru zlecenia, numeru pisma, na podstawie którego złożono zlecenie, daty tworzenia zlecenia oraz wskazania nadawcy zapytania – spełniały wymagania określone w wewnętrznych aktach prawnych.

Zabezpieczenia organizacyjne i techniczne w zakresie pozyskiwania i przetwarzania danych telekomunikacyjnych

Systemy teleinformatyczne zostały zabezpieczone w sposób uniemożliwiający nieuprawniony dostęp do przetwarzania danych telekomunikacyjnych. System teleinformatyczny składa się z pięciu stanowisk. Cztery stanowiska służą do przetwarzania danych od operatorów. Jedno stanowisko MF ALERT o klauzuli poufnej służy do przesyłania wniosków oraz uzyskanych danych telekomunikacyjnych pomiędzy jednostkami organizacyjnymi Wywiadu Skarbowego. Wejście do pokoju, w którym znajdują się ww. stanowiska, jest możliwe jedynie dla osób uprawnionych. Użytkownikami systemu przetwarzania danych są upoważnieni przez GIKS pracownicy Wydziału Techniki posiadający imienne karty mikroprocesorowe umożliwiające indywidualne korzystanie z systemów wymiany informacji. Do przenoszenia danych pomiędzy jawnymi systemami przedsiębiorców telekomunikacyjnych, a niejawnym systemem poczty elektronicznej wykorzystywane są przenośne pamięci USB Flash Driver. Nie opracowano pisemnych procedur

przechowywania ww. nośników, zabezpieczenia przed ich wyniesieniem oraz postępowania w przypadku ich uszkodzenia.
Przesyłanie zleceń do Wydziału Techniki i otrzymywanie odpowiedzi jest realizowane za pośrednictwem poczty elektronicznej. Odbiorca informacji zobligowany jest do odpowiedniego zabezpieczenia otrzymanych danych oraz rejestracji dokumentu po jego wydruku.

Osoby upoważnione do sięgania po dane telekomunikacyjne

Zgodnie z Zarządzeniem Nr 40 Ministra Finansów z dnia 26 września 2011 r. zmieniającym zarządzenie w sprawie nadania statutów izbom celnym i urzędom celnym, w skład Izby Celnej w Opolu weszła komórka organizacyjna realizująca zadania z zakresu e-kontroli, która wykonuje te zadania na rzecz całej Służby Celnej.
Z wnioskami do operatorów występował Dyrektor Izby Celnej w Opolu lub pod jego nieobecność osoba pełniąca obowiązki Dyrektora.

Upoważnienie Generalnego Inspektora Kontroli Skarbowej (GIKS) do uzyskiwania od podmiotów prowadzących działalność telekomunikacyjną i operatorów świadczących usługi pocztowe danych, o których mowa w art. 180c i 180d ustawy Prawo telekomunikacyjne posiadało dziewięciu pracowników Departamentu Wywiadu Skarbowego. Zlecenia mogą składać uprawnieni pracownicy posiadający prawo dostępu do Systemu MF ALERT. Rejestr osób upoważnionych przez Generalnego Inspektora Kontroli Skarbowej do występowania do przedsiębiorców telekomunikacyjnych i operatorów pocztowych z wnioskami o udostępnienie danych, prowadzony jest w formie elektronicznej. W rejestrze odnotowana jest data, numer upoważnienia, jego zakres oraz data upływu upoważnienia.

Przeprowadzone badanie wykazało, iż we wszystkich przypadkach o informacje za pośrednictwem sieci telekomunikacyjnej występowały upoważnione osoby.

Sprawność i szybkość pozyskiwania danych teleinformatycznych

Nie wystąpiły przypadki kwestionowania przez operatorów telekomunikacyjnych żądania uzyskania danych telekomunikacyjnych, odmowy udostępnienia lub przekazywania informacji z opóźnieniem, które utrudniałoby wykonywanie zadań jednostki.

Ewidencjonowanie pozyskanych danych telekomunikacyjnych

Ewidencja upoważnień do uzyskiwania i przetwarzania danych telekomunikacyjnych, prowadzona jest przez Administratora Bezpieczeństwa Informacji Izby Celnej w Opolu. W okresie od 1 stycznia 2011 r. do 30 czerwca 2012 r. występowano z wnioskami o dane telekomunikacyjne 26 razy w trybie określonym w art. 75 d. Ponadto urzędy celne uzyskiwały dane telekomunikacyjne od operatorów telekomunikacyjnych na podstawie wystąpień w trybie art. 218 kpk w zw. z art. 113 § 1 kks i art. 122 § 1 pkt 1 kks[45] i otrzymały ogółem w okresie objętym kontrolą 484 odpowiedzi, zawierających 170 danych dotyczących lokalizacji, 184 dane dotyczące wykazów połączeń z danego numeru i 426 danych dotyczących użytkownika.
Departament Wywiadu Skarbowego korzystając z uprawnień wynikających z art. 36 b ustawy o kontroli skarbowej, w okresie od 2010 r. do końca I połowy 2012 r. skierował do przedsiębiorców telekomunikacyjnych, łącznie 10.338 wystąpień. Największa liczba wystąpień miała miejsce

[45] Ustawa z dnia 10 września 1999 r. Kodeks karny skarbowy (Dz. U. 2013 r. Nr 186 j.t.).

w 2010 r. – 4.968. Dane te ustalono na podstawie wyjaśnień, gdyż Departament Wywiadu Skarbowego do kontroli przedłożył jedynie bazę danych telekomunikacyjnych (tzw. ewidencję) wygenerowaną z raportu systemu poczty elektronicznej e-mail MS Outlook za okres od 1 stycznia 2012 r. do 30 czerwca 2012 r. Kontrolerom nie została udostępniona baza danych telekomunikacyjnych z systemu za 2011 r. oraz ewidencja dokumentacji poszczególnych zapytań wystosowanych w formie pisemnej za okres od 2011 r. do końca I półrocza 2012 r., ponieważ dokumentacja dotycząca ustaleń i sprawdzeń u operatorów telekomunikacyjnych za ten okres została zniszczona.

Postępowanie ze zbędnymi danymi telekomunikacyjnymi

Zgodnie z uregulowaniami wewnętrznymi, w przypadku danych, które nie są wykorzystane podczas prowadzonych czynności, odbiorca informacji zobligowany jest do bezzwłocznego ich usunięcia z komputera lub zniszczenia.

Departament Wywiadu Skarbowego opracował zasady postępowania z tymi danymi. Przyjęta forma komisyjnego i protokolarnego niszczenia wyżej wymienionych danych była zgodna z wytycznymi określonymi w ustawie o kontroli skarbowej. Pisma dotyczące wyżej wymienionych danych i zapytania pochodzące od komórek wywiadu skarbowego w formie elektronicznej podlegają zniszczeniu po sporządzeniu odpowiednich zestawień statystycznych.

Nadzór i kontrola nad uzyskiwaniem, przetwarzaniem i niszczeniem danych telekomunikacyjnych

W okresie objętym kontrolą Wydział Nadzoru i Kontroli Departamentu Wywiadu Skarbowego Ministerstwa Finansów przeprowadził 9 kontroli kompleksowych Wydziałów Wywiadu Skarbowego w Urzędach Kontroli Skarbowej, które objęły również zasadność uzyskiwania, wykorzystania i niszczenia danych telekomunikacyjnych. W przypadku stwierdzenia nieprawidłowości nakazywano ich usunięcie. Inne kontrole i badania audytowe nie były prowadzone.

3.2.8. Urząd Komunikacji Elektronicznej

Nadzór nad realizacją przez operatorów telekomunikacyjnych obowiązku określonego w art. 180g ust. 1 Prawa telekomunikacyjnego

Na koniec stycznia 2011 r. do rejestru przedsiębiorców telekomunikacyjnych (dalej: rejestr), o którym mowa w art. 10 ust. 1 Prawa telekomunikacyjnego wpisanych było 7814 przedsiębiorców. W terminie ustawowym, tj. do 31 stycznia następnego roku, informacje o których mowa w art. 180g ust. 1 ww. ustawy, za rok 2010 złożyło 117 przedsiębiorców. Po terminie ustawowym, ale przed terminem przesłania przez Prezesa UKE informacji, o której mowa w art. 180g ust. 2 Ustawy do Komisji Europejskiej, tj. przed 17 marca 2011 r., informację złożyło 166 przedsiębiorców, a po tym terminie – 25 przedsiębiorców. Nie przekazało informacji 7.506 przedsiębiorców. Na koniec stycznia 2012 r. do rejestru wpisanych było 7.549 przedsiębiorców. W terminie ustawowym informacje, o których mowa w art. 180g ust. 1 ustawy, za rok 2011 złożyło 542 przedsiębiorców. Po terminie ustawowym, ale przed terminem przesłania przez Prezesa UKE informacji, o której mowa w art. 180g ust. 2 ustawy do Komisji Europejskiej, tj. przed 30 marca 2012 r., informację złożyło 633 przedsiębiorców, a po tym terminie – 73 przedsiębiorców. Nie przekazało informacji 6.301 przedsiębiorców.

W celu egzekwowania od przedsiębiorców realizacji obowiązków wynikających z art. 180g Ustawy, Prezes UKE podejmował lub inicjował następujące działania:

- w okresie poprzedzającym termin złożenia informacji przez przedsiębiorców na stronie internetowej UKE zamieszczana była informacja przypominająca o obowiązku złożenia informacji, wraz ze wzorem formularza i treścią rozporządzenia wprowadzającego ten wzór;
- pracownicy Departamentu Spraw Obronnych UKE udzielali przedsiębiorcom wyjaśnień odnośnie sposobu i zakresu realizacji obowiązku;
- w roku 2012 wysłane zostało drogą elektroniczną wezwanie do złożenia informacji do przedsiębiorców, których adresy poczty elektronicznej znane były pracownikom UKE, tj. 143;
- w 2011 r. wobec 12 przedsiębiorców prowadzono postępowania wyjaśniające i administracyjne, w wyniku których wydano 5 decyzji o nałożeniu kar za niezłożenie lub spóźnione złożenie informacji;
- w 2012 r. wobec 7 przedsiębiorców prowadzono 1 postępowanie kontrolne i 6 postępowań wyjaśniających, w wyniku których wszczęto 3 postępowania administracyjne w sprawie nałożenia kar.

Postępowania wyjaśniające i kontrolne w związku z niewypełnieniem obowiązku określonego w art. 180g Prawa telekomunikacyjnego wszczynane były przez Prezesa UKE wyłącznie na skutek skarg lub innych pism od instytucji albo osób fizycznych, natomiast nie były przeprowadzane kontrole planowe z inicjatywy własnej Prezesa UKE. W toku tych postępowań Prezes UKE ustalał fakt otrzymania przez przedsiębiorców zapytań, o których mowa w art. 180g, poprzez wezwanie przedsiębiorców do udzielenia informacji o liczbie takich zapytań w trybie art. 6 ust. 1 ww. ustawy lub na podstawie faktu późniejszego złożenia przez przedsiębiorców tej informacji po terminie ustawowym. W uzasadnieniach decyzji o nałożeniu kary za naruszenie obowiązku, o którym mowa w art. 180g ust. 1, Prezes UKE wskazywał m. in. na skutek w postaci nierzetelnej statystyki odnośnie liczby żądań udostępnienia danych, kierowanej do Komisji Europejskiej.

Najwyższa Izba Kontroli oceniła negatywnie niewielką aktywność Prezesa UKE w powyższym zakresie, w szczególności ograniczenie działań nadzorczych wyłącznie do podmiotów wskazanych w otrzymanych skargach. W efekcie nie podjęto przewidzianych przepisami prawa działań w stosunku chociażby do części przedsiębiorców, którzy nie realizowali obowiązku informacyjnego. Art. 209 ust. 1 pkt 28 Prawa telekomunikacyjnego w sposób imperatywny określa, że przedsiębiorca niewywiązujący się z obowiązku informacyjnego podlega karze. Obowiązek powyższy ma na celu nie tylko zapewnienie rzetelności sprawozdań kierowanych do Komisji Europejskiej, co m.in. podkreślał Prezes UKE w nakładanych przez siebie w pojedynczych przypadkach karach, ale również dostarczenie społeczeństwu obiektywnej informacji na temat zakresu ingerencji służb w prawa i wolności obywatelskie. Należy podkreślić, iż Prezes UKE nie dysponując sprawozdaniami, o którym mowa w art. 180g ust. 1 Prawa telekomunikacyjnego, nie może rzetelnie określić ilości udostępnionych danych, gdyż nie jest możliwe ustalenie, czy przyczyną nienadesłania sprawozdania jest niewystąpienie przypadków wskazanych w ww. artykule, czy też niewywiązanie się przedsiębiorcy z nałożonego obowiązku.

Rzetelność informacji przekazywanych przez operatorów

Informacje, o których mowa w art. 180g ust. 1 Prawa telekomunikacyjnego były sporządzane przez przedsiębiorców zgodnie ze wzorem określonym w rozporządzeniu Ministra Infrastruktury z dnia 30 grudnia 2009 r. w sprawie wzoru formularza służącego do przekazywania przez przedsiębiorcę telekomunikacyjnego Prezesowi Urzędu Komunikacji Elektronicznej informacji dotyczących

udostępniania danych[46], z wyjątkiem 7 przedsiębiorców, którzy złożyli te informacje niezgodnie ze wzorem lub w innej formie.
Składane przez przedsiębiorców informacje, poza sprawdzeniem poprawności wypełnienia numeru RPT[47] i nazwy przedsiębiorcy oraz matematycznej zgodności wypełniania poszczególnych pozycji w formularzu, nie były przez Prezes UKE weryfikowane. W efekcie, pomimo że niektóre informacje zawierały ewidentne błędy, nie zostały one wykryte. Przykładowo, jeden z przedsiębiorców wykazał w informacji za lata 2010 i 2011 otrzymanie zapytań w liczbie odpowiednio 1.365 i 11.466 wyłącznie za okres 1 miesiąca wstecz od zatrzymania danych, a w kolumnach 2-24 miesiące wykazał 0 zapytań. Na pytanie kontrolera przedsiębiorca wyjaśnił, że dane określone w art. 180g zostały przez niego przedstawione w sposób błędny na skutek niezrozumienia treści formularza. Prezes UKE nie zwrócił się do przedsiębiorcy o zweryfikowanie prawidłowości zestawienia. Inny z przedsiębiorców, wraz z informacją na formularzu, przedstawił szczegółowy wykaz żądań udostępnienia danych. Informacje z wykazu różniły się od informacji podanych na formularzu w zakresie liczby zapytań i czasu pomiędzy zatrzymaniem danych, a ich udostępnieniem. Pomimo tego UKE, nie podjęło żadnych działań w celu wyjaśnienia rozbieżności.

Najwyższa Izba Kontroli, jako nierzetelny oceniła brak jakiejkolwiek, choćby wyrywkowej, weryfikacji informacji przekazywanych przez przedsiębiorców. Art. 199 i następne Ustawy pozwalały Prezesowi UKE na kontrolę w zakresie rzetelności przedkładanych przez przedsiębiorców informacji, w szczególności dostęp do niezbędnych dokumentów. Należy podkreślić, iż weryfikacja statystyczna ilości zrealizowanych żądań uprawnionych podmiotów nie musiała się wiązać z dostępem do dokumentów objętych tajemnicą postępowań.

Metodologia zliczania danych

W ocenie Ministra Administracji i Cyfryzacji, właściwego do spraw łączności, żądanie od przedsiębiorców telekomunikacyjnych ujawnienia objętych tajemnicą telekomunikacyjną danych określonych w art. 159 ust. 1 pkt 1 Prawa telekomunikacyjnego, w zakresie ograniczonym wyłącznie do danych wymienionych w art. 161 ust. 2 pkt 1-6 ww. ustawy (dane personalne), należy do żądań objętych obowiązkiem sprawozdawczym określonym w art. 180g ust. 1 w zw. z art. 180c ust. 1 ustawy[48]. Dane personalne powinny być, więc wykazywane w formularzu określonym w rozporządzeniu Ministra Infrastruktury z 30 grudnia 2009 r.
W ocenie Prezesa UKE, wykazywanie w sprawozdaniu do Komisji Europejskiej zapytań o dane personalne abonentów, bez powiązania z innymi danymi telekomunikacyjnymi, nie jest wymagane przez Komisję Europejską.
Spośród 5 przedsiębiorców, którzy zrealizowali najwięcej żądań udostępnienia danych, 4 przedsiębiorców nie wykazywało zapytań wyłącznie o personalia abonentów, ponieważ według tych przedsiębiorców zapytania takie nie mieszczą się w ramach określonych przez art. 180g Prawa telekomunikacyjnego. Jeden z przedsiębiorców, w składanych do Prezesa UKE informacjach, uwzględniał również zapytania wyłącznie o dane personalne abonentów.
Niezależnie od przyjętej interpretacji w zakresie wykazywania danych dotyczących abonentów należy zauważyć, iż informacje przekazywane przez UKE obywatelom i Komisji Europejskiej były

46 Dz. U. z 2010 r. Nr 3, poz. 15.
47 RPT – numer w rejestrze przedsiębiorców telekomunikacyjnych.
48 Pismo DKSiW-096-1171/2012-IP z dnia 4 grudnia 2012 r.

nierzetelne, gdyż zostały oparte zarówno na informacjach operatorów telekomunikacyjnych, którzy nie wliczali tego rodzaju danych, jak również takich, którzy te dane w swoich sprawozdaniach wykazywali. W ocenie NIK, obowiązkiem Prezesa UKE było podjęcie działań, które zapewniłyby porównywalność przedstawianych przez operatorów danych.
Ustalono ponadto, iż wszystkie przypadki dotyczące zapytań o personalia abonentów za 2011 r., w liczbie 513.857 w sprawozdaniu jednego z przedsiębiorców zostały wykazane, jako dotyczące pierwszego miesiąca. Ponadto w informacjach za 2010 i 2011 r. uwzględniono informację jednego z przedsiębiorców, że wszystkie przypadki udostępnienia danych, tj. 1365 w 2010 r. i 11.466 r., nastąpiły w ciągu 1 miesiąca od zatrzymania, podczas gdy wykazanie wszystkich zapytań w pierwszej kolumnie było wynikiem błędnego zrozumienia przez przedsiębiorcę treści formularza. W ocenie NIK, błędy te mogły w poważnym stopniu zakłócić rozkład statystyczny zapytań w zakresie okresu, jakiego dotyczy zapytanie. Należy zwrócić uwagę, iż dane prezentowane przez UKE były przekazywane nie tylko Komisji Europejskiej dla celów statystycznych, ale również brane pod uwagę w trakcie prowadzonych prac legislacyjnych nad nowelizacją Prawa telekomunikacyjnego, w zakresie okresu retencji danych i stanowiły podstawę dla uzasadnienia skrócenia tego okresu do 12 miesięcy.

NIK zwróciła ponadto uwagę na fakt, iż w ujawnionych statystykach mogło dochodzić do zawyżenia liczby zapytań, ze względu na konieczności składania żądań udzielenia informacji o tych samych danych telekomunikacyjnych jednocześnie do kilku przedsiębiorców. Było to związane z możliwością przeniesienia numeru do innego operatora. Dane pozwalające na określenie tego rodzaju przypadków nie były zbierane.

* * *

Biorąc pod uwagę powyżej wskazane ustalenia kontroli NIK, należy stwierdzić, iż opracowywane przez Prezesa UKE informacje w zakresie wykorzystania przez służby danych retencyjnych nie odpowiadały stanowi rzeczywistemu. Prezentowane informacje są niepełne, a przedstawiane przez poszczególne podmioty dane nieporównywalne. Ze względu na opisane powyżej błędy metodologiczne oraz zaniedbania, jakiekolwiek wnioskowanie statystyczne w przedmiocie zakresu retencji danych w Polsce, jest w ocenie NIK nieuprawnione.

Sprawowanie przez Prezesa UKE kontroli nad realizacją przez przedsiębiorców obowiązków w zakresie retencji danych telekomunikacyjnych

Nie wszyscy operatorzy i przedsiębiorcy telekomunikacyjni realizowali obowiązek, o którym mowa w art. 180a ust. 1 pkt 1 i 2 Prawa telekomunikacyjnego. W latach 2011-2012 Prezes UKE, w reakcji na skargi i pisma osób fizycznych, przedsiębiorców i instytucji publicznych przeprowadził 17 postępowań kontrolnych obejmujących realizację obowiązków, o których mowa w art. 180a, 180 c i 180d ww. ustawy. W ich wyniku stwierdzono nienależyte zabezpieczenie danych określonych w art. 180a ust. 1 u 6 przedsiębiorców i nieprzechowywanie danych abonentów przez 6 przedsiębiorców. Na 6 przedsiębiorców nałożono kary w łącznej wysokości 35.500 zł. Weryfikacja przez Prezesa UKE usunięcia przez przedsiębiorców nieprawidłowości stwierdzonych w toku kontroli polegała na przyjęciu oświadczeń przedsiębiorców o usunięciu nieprawidłowości.
Kryterium doboru przedsiębiorców do kontroli wypełniania obowiązków określonych w art. 180a, 180c i 180d ustawy był fakt uzyskania przez Prezesa UKE informacji wskazujących na niewłaściwą

realizację ww. obowiązków przez przedsiębiorców. Prezes UKE nie przeprowadzał kontroli w zakresie prawidłowości realizacji przez przedsiębiorców obowiązku niszczenia danych telekomunikacyjnych po okresie retencji, a w szczególności zakresu danych, jakie przedsiębiorcy przechowują po okresie retencji, z uwzględnieniem celowości i legalności ich przechowywania.

W ocenie NIK, podejmowanie przez Prezesa UKE postępowań wyjaśniających i kontrolnych w zakresie realizacji obowiązków określonych w art. 180a, 180 c i 180d Prawa telekomunikacyjnego wyłącznie na podstawie sygnałów zewnętrznych było niewystarczające, dla zapewnienia należytego przechowywania, udostępniania i terminowego niszczenia danych telekomunikacyjnych.

3.2.9. Sądy

Przedmiotem kontroli NIK nie była, stosownie do ograniczeń ustawowych, działalność orzecznicza – w tym zakresie zebrano jedynie informacje o charakterze statystycznym. Należy jednakże zauważyć, iż w szeregu przypadków, w których występowano o przekazanie danych telekomunikacyjnych, operatorzy odmówili ich udostępnienia, wskazując na brak podstawy do formułowania takiego żądania przez sądy lub względy formalno-prawne. Sądy nie pozyskiwały danych z wykorzystaniem systemów teleinformatycznych – udostępnienie danych telekomunikacyjnych następowało w formie pisemnej, po otrzymaniu przez operatora stosownego postanowienia lub zarządzenia w tej sprawie.

Sąd Okręgowy w Bydgoszczy

Wszystkie uzyskane dane telekomunikacyjne zabezpieczone były poprzez włączenie ich do akt spraw, których dotyczyły i były chronione na tych samych zasadach, jak inne dokumenty zgromadzone w postępowaniu sądowym[49].

W badanym okresie Sąd skierował do operatorów telekomunikacyjnych 29 wniosków o udostępnienie danych telekomunikacyjnych, z tego 11 w sprawach karnych i 18 w sprawach cywilnych.

W jednym przypadku, w sprawie prowadzonej przez I Wydział Cywilny, wydanie wniosku było poprzedzone uzyskaniem zgody osoby, której dane miały być udostępnione. Natomiast we wszystkich 17 badanych przypadkach spraw prowadzonych przez X Wydział Cywilny Rodzinny, w których wnioskowano o dane telekomunikacyjne, Sąd Okręgowy (SO) nie uzyskał zgody nadawcy lub odbiorcy, których dane te dotyczą[50]. W 16 przypadkach operatorzy odmówili udostępnienia żądanych danych. Sądy nie podejmowały dalszych działań w celu uzyskania żądanych danych.

Ustalono ponadto, że w 16 przypadkach wnioskowano o wydanie nie tylko bilingów połączeń, ale również o utrwalone treści sms. Należy zwrócić uwagę, że nie jest możliwe udostępnienie treści sms, bez wcześniejszego zarządzenia kontroli i utrwalania rozmów telefonicznych, co jest możliwe w trybie art. 237 k.p.k., w celu ściganie jedynie niektórych, szczególnie poważnych przestępstw[51].

---

49 Kwestię dostępu do akt sądowych regulują przepisy postępowania karnego i cywilnego.

50 Wszystkie wnioski dotyczyły spraw rozwodowych.

51 W art. 237 § 1 k.p.k. określono, że po wszczęciu postępowania sąd na wniosek prokuratora może zarządzić kontrolę i utrwalanie treści rozmów telefonicznych w celu wykrycia i uzyskania dowodów dla toczącego się postępowania lub zapobieżenia popełnieniu nowego przestępstwa. Natomiast w art. 237 § 3 k.p.k. określono, że kontrola i utrwalanie treści rozmów telefonicznych są dopuszczalne tylko wtedy, gdy toczące się postępowanie lub uzasadniona obawa popełnienia nowego przestępstwa dotyczy, zabójstwa, narażenia na niebezpieczeństwo powszechne lub sprowadzenia katastrofy, handlu ludźmi, uprowadzenia osoby, wymuszania okupu, uprowadzenia statku powietrznego lub wodnego, rozboju, kradzieży rozbójniczej lub wymuszenia rozbójniczego, zamachu na niepodległość lub integralność państwa,

Wydział III Karny w okresie objętym kontrolą występował 11 razy o dane telekomunikacyjne w pięciu sprawach sądowych, w tym 4 niezakończonych. Zebrano dane na temat 9 takich przypadków[52]. We wszystkich postanowieniach, jako podstawę prawną żądania danych telekomunikacyjnych wskazano art. 218 § 1 k.p.k. Zgodnie z art. 218 § 2 k.p.k. postanowienie Sądu o wydanie danych telekomunikacyjnych, o którym mowa w § 1, doręcza się adresatom korespondencji oraz abonentowi telefonu lub nadawcy, którego wykaz połączeń lub innych przekazów informacji został wydany. Doręczenie postanowienia może być odroczone na czas oznaczony, niezbędny ze względu na dobro sprawy, lecz nie później niż do czasu prawomocnego zakończenia postępowania. We wszystkich 9 skontrolowanych przypadkach SO nie doręczył ww postanowienia.

Ponadto stwierdzono, iż Sąd w 6 przypadkach[53] występował o dane telekomunikacyjne obejmujące okres przekraczający 24 miesiące od daty wydania postanowienia.

Sąd Okręgowy w Szczecinie

Wszystkie uzyskane dane telekomunikacyjne zabezpieczone były poprzez włączenie ich do akt spraw, których dotyczyły i chronione w taki sam sposób jak pozostałe dokumenty procesowe.

W okresie objętym kontrolą Sąd 28 razy w 19 sprawach (3 karnych oraz 16 cywilnych i rodzinnych) występował o uzyskanie danych telekomunikacyjnych. Spośród 19 spraw operatorzy telekomunikacyjni odmówili udostępnienia żądanych danych telekomunikacyjnych w 14 sprawach (tj. 74% spraw, w których występowano o takie dane), wskazując jako przyczynę brak podstawy prawnej do takiego wystąpienia i uchylenia tajemnicy telekomunikacyjnej lub na niewykonalność postanowienia Sądu z innych formalno-prawnych przyczyn, w tym:

- w 9 sprawach (z 19, tj. 47%) ze względu na brak wskazania podstawy prawnej;
- w 8 sprawach (z 19, tj. 42%) ze względu na okres za jaki żądano udostępnienia danych telekomunikacyjnych, który przekraczał 24 miesięczny okres zatrzymywania i przechowywania tych danych przez przedsiębiorców telekomunikacyjnych określony w art. 180a ustawy Prawo telekomunikacyjne;
- w 2 sprawach cywilnych (z 16, tj. 13%), ze względu na powołanie się na art. 248 k.p.c., jako podstawę prawną żądania danych telekomunikacyjnych;
- w jednej sprawie cywilnej rodzinnej występując o dane telekomunikacyjne, Sąd powołał się na przepisy k.p.k. – jako podstawę prawną wystąpienia o dane telekomunikacyjne wskazano art. 180 § 1 i art. 218 § 1 k.p.k.;
- w jednej sprawie cywilnej rodzinnej żądano treści wiadomości tekstowych wychodzących i przychodzących na wskazany numeru telefonu.

---

zamachu na konstytucyjny ustrój państwa lub jego naczelne organy, albo na jednostkę Sił Zbrojnych Rzeczypospolitej Polskiej, szpiegostwa lub ujawnienia informacji niejawnych o klauzuli tajności „tajne" lub „ściśle tajne", gromadzenia broni, materiałów wybuchowych lub radioaktywnych, fałszowania oraz obrotu fałszywymi pieniędzmi, środkami lub instrumentami płatniczymi albo zbywalnymi dokumentami uprawniającymi do otrzymania sumy pieniężnej, towaru, ładunku albo wygranej rzeczowej albo zawierającymi obowiązek wpłaty kapitału, odsetek, udziału w zyskach lub stwierdzenie uczestnictwa w spółce, wytwarzania, przetwarzania, obrotu i przemytu środków odurzających, prekursorów, środków zastępczych lub substancji psychotropowych, zorganizowanej grupy przestępczej, mienia znacznej wartości, użycia przemocy lub groźby bezprawnej w związku z postępowaniem karnym, łapownictwa i płatnej protekcji, stręczycielstwa, kuplerstwa i sutenerstwa, przestępstw określonych w rozdziale XVI k.k. oraz w art. 5-8 Rzymskiego Statutu Międzynarodowego Trybunału Karnego, sporządzonego w Rzymie dnia 17 lipca 1998 r. (Dz. U. z 2003 r. Nr 78, poz. 708).

52 Akta 2 pozostałych spraw znajdowały się poza siedzibą SO.

53 Tj.: pięć w X Wydziale Cywilnym Rodzinnym i jeden w I Wydziale Cywilnym.

Ponadto stwierdzono, że:

- w 3 sprawach cywilnych zapytania do przedsiębiorców telekomunikacyjnych skierowano bez wcześniejszego wniosku (zgody) abonenta, o której mowa w art. 159 ust. 2 pkt 2 ustawy Prawo telekomunikacyjne, a w 12 sprawach cywilnych rodzinnych nie poinformowano przedsiębiorcy telekomunikacyjnego o takiej zgodzie lub wniosku abonenta;
- we wszystkich 3 sprawach karnych doręczenie postanowień nie było odraczane, a postanowienia te nie były przekazywane abonentom, pomimo istnienia obowiązku określonego w art. 218 § 2 k.p.k.

Sądy nie podejmowały dalszych działań w celu uzyskania żądanych danych.

Sąd Okręgowy w Warszawie

Prezes Sądu Okręgowego w Warszawie uniemożliwiła przeprowadzenie kontroli. Ustalenia dokonane przed momentem, gdy kontrolerom uniemożliwiono przeprowadzenia dalszych czynności, wskazywały na istotne ryzyko zaistnienia przypadków analogicznych, jak opisane powyżej[54].

3.2.10. Prokuratury

Prokuratury, w celu uzyskania danych telekomunikacyjnych, zasadniczo korzystały z formy pisemnej. Za pomocą systemów teleinformatycznych uzyskiwano dane od jednego z przedsiębiorców telekomunikacyjnych na podstawie porozumienia zawartego przez Prokuratora Generalnego. Spośród skontrolowanych podmiotów, za pomocą systemów teleinformatycznych od operatorów innych niż ww., dane pozyskiwała jedynie Prokuratura we Wrocławiu (na podstawie porozumień zawartych przez Prokuratora Okręgowego). Wykorzystanie systemów teleinformatycznych znacząco skracało czas niezbędny do uzyskania żądanych danych.

Prokuratura Okręgowa w Warszawie

Prokurator Okręgowy w Warszawie określił zasady bezpieczeństwa oraz organizacji pracy przy uzyskiwaniu danych telekomunikacyjnych, o których mowa w art. 180c i d Prawa telekomunikacyjnego, 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.

W trakcie kontroli stwierdzono jednakże, że wydawanie zarządzeń o doręczeniu postanowień[55] przez prokuratorów, a także ich doręczanie odbywało się z naruszeniem terminu określonego w art. 218 § 2 zd. 2 k.pk. Stwierdzono, że w 43 przypadkach spośród 74 zbadanych (tj. w 58%) nie wydawano zarządzeń o doręczeniu postanowień wydanych na podstawie art. 218 § 1 kpk abonentom, wydawano je po upływie terminu wskazanego w art. 218 § 2 zd. 2 kpk lub doręczano postanowienia po upływie tego terminu, co stanowi naruszenie art. 218 § 2 zd. 2 kpk[56].

---

54 NIK powiadomiła o tym Ministra Sprawiedliwości. Kwestia ta została szczegółowo omówiona na str. 21-22 Informacji.

55 Postanowienia są doręczane w formie odpisów.

56 Art. 218 § 2 k.p.k. stanowi, 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.

Stwierdzono ponadto pojedyncze przypadki żądania udostępnienia danych telekomunikacyjnych za okres przekraczający 24 m-ce oraz żądania udostępnia treści przekazów telekomunikacyjnych w niewłaściwym trybie.

Prokuratura Okręgowa w Katowicach

Prokurator Okręgowy w Katowicach określił zasady bezpieczeństwa oraz organizacji pracy przy uzyskiwaniu danych telekomunikacyjnych, o których mowa w art. 180c i d Prawa telekomunikacyjnego, 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 kpk. 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 operatorzy sieci nie wydali żądanych danych telekomunikacyjnych.

Ponadto ustalono, że w 30 przypadkach (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).

Ponadto stwierdzono nieprzestrzeganie przepisów wewnętrznych w zakresie przechowywania kodów PIN do Systemu Retencji i Udostępniania Danych – nie były one właściwie zabezpieczone.

Prokuratura Okręgowa w Rzeszowie

Obowiązujące w Prokuraturze procedury wewnętrzne dotyczące zabezpieczenia w aktach postępowania przygotowawczego danych telekomunikacyjnych przed ich udostępnieniem osobom nieupoważnionym regulowały wszystkie istotne, z punktu widzenia zapewnienia realizacji celów, dla których przewidziano uzyskiwanie danych telekomunikacyjnych.

Procedury bezpieczeństwa danych telekomunikacyjnych zapisanych w systemie lub na nośniku informatycznym, sposób ich zabezpieczenia oraz reagowania w przypadku wystąpienia zagrożeń gwarantowały bezpieczeństwo, poufność, integralność i rozliczalność danych telekomunikacyjnych.

Przeprowadzone w trakcie kontroli oględziny strefy, w której przechowywane są dane telekomunikacyjne potwierdziły, że ryzyka związane z bezpieczeństwem, poufnością, integralnością i rozliczalnością danych telekomunikacyjnych zostały zminimalizowane.

W kontroli ustalono, że wystąpiły przypadki braku doręczenia abonentom telefonów postanowień, na podstawie których uzyskano wykaz połączeń z ich telefonów, mimo prawomocnego zakończenia prowadzonych postępowań przygotowawczych. Spośród objętych kontrolą 40 postanowień, wydanych na podstawie art. 218 § 1 kpk, żadne nie zostało doręczone abonentom telefonów lub nadawcom, których wykazy połączeń lub innych przekazów informacji zostały przekazane Prokuraturze, do czasu prawomocnego ich zakończenia. W trakcie trwania kontroli, prokuratorzy prowadzący te postępowania wydali niezbędne zarządzenia w zakresie realizacji doręczeń.

Prokuratura Okręgowa we Wrocławiu

Wewnętrzne uregulowania organizacyjne, wprowadzone przez Prokuratora Okręgowego gwarantowały właściwą realizację zadań związanych z wykorzystaniem danych retencyjnych. NIK stwierdziła prawidłową organizację systemu pozyskiwania danych telekomunikacyjnych, należyte zabezpieczenie materiałów przed dostępem osób nieuprawnionych. Dane telekomunikacyjne były pozyskiwane w oparciu o właściwą podstawę prawną i wyłącznie przez osoby uprawnione.
Pozyskiwane materiały były w sposób właściwy zabezpieczane przed dostępem osób nieuprawnionych. Transmisja danych drogą elektroniczną była realizowana wyłącznie przez wyznaczone osoby, przy zastosowaniu indywidualnych kart dostępu i tokenów. Przesyłanie danych przez operatorów odbywało się z wykorzystaniem zaszyfrowanych stron internetowych (htpps) zaś dostarczanie materiałów właściwym prokuratorom poprzez wyizolowaną komputerową sieć wewnętrzną Prokuratury. Pozyskiwane dane telekomunikacyjne, jako element akt głównych postępowań były przechowywane wyłącznie w gabinetach prokuratorów, w metalowych szafach. W działalności Prokuratury Okręgowej we Wrocławiu w zakresie realizacji obowiązków ustawowych związanych z pozyskiwaniem danych telekomunikacyjnych nie stwierdzono nieprawidłowości.

3.2.11. Przedsiębiorcy telekomunikacyjni

Kontrola operatorów telekomunikacyjnych została przeprowadzona przez GIODO. Dane ujęte w niniejszym punkcie Informacji o wynikach kontroli zostały przedstawione na podstawie przygotowanego przez GIODO „Sprawozdanie z kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych przeprowadzonych u operatorów publicznej sieci telekomunikacyjnej, dostawców publicznie dostępnych usług telekomunikacyjnych" z dnia 30 listopada 2012 r. Wszystkie skontrolowane podmioty zostały wpisane do Rejestru przedsiębiorców telekomunikacyjnych prowadzonego przez Prezesa Urzędu Komunikacji Elektronicznej[57].

Realizacja obowiązku zatrzymywania danych

Objęci kontrolami przedsiębiorcy telekomunikacyjni prawidłowo realizowali wskazany w art. 180a ust. 1 pkt 1 Prawa telekomunikacyjnego[58], obowiązek zatrzymania i przechowywania danych, o których mowa w art. 180c Prawa telekomunikacyjnego[59].

Dane retencyjne udostępniane były w formie elektronicznej Agencji Bezpieczeństwa Wewnętrznego, Centralnemu Biuru Antykorupcyjnemu, Policji, Służbie Kontrwywiadu Wojskowego, Straży Granicznej, Generalnemu Inspektorowi Kontroli Skarbowej i Żandarmerii Wojskowej, a także Prokuraturze Generalnej (przez jednego z operatorów). Pozostałym uprawnionym podmiotom,

[57] Wszelkie informacje oraz dokumenty przekazane przez przedsiębiorców w związku z kontrolami objęte są tajemnicą przedsiębiorstwa, o której mowa w art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2003 r. Nr 153, poz. 1503 ze zm.).

[58] Art. 180a ust. 1. Z zastrzeżeniem art. 180c ust. 2 pkt 2, operator publicznej sieci telekomunikacyjnej oraz dostawca publicznie dostępnych usług telekomunikacyjnych są obowiązani na własny koszt: 1) zatrzymywać i przechowywać dane, o których mowa w art. 180c, generowane w sieci telekomunikacyjnej lub przez nich przetwarzane, na terytorium Rzeczypospolitej Polskiej, przez okres 24 miesięcy, licząc od dnia połączenia lub nieudanej próby połączenia, a z dniem upływu tego okresu dane te niszczyć, z wyjątkiem tych, które zostały zabezpieczone, zgodnie z przepisami odrębnymi.

[59] Tj. danych niezbędnych do ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego inicjującego połączenie oraz zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego, do którego kierowane jest połączenie; określenia daty i godziny połączenia oraz czasu jego trwania, określenie rodzaju połączenia, określenie lokalizacji telekomunikacyjnego urządzenia końcowego.

głównie sądom i prokuraturom, dane retencyjne udostępniane są na podstawie wydanych przez nie postanowień w formie pisemnej.

Dane retencyjne były udostępniane za pomocą systemów teleinformatycznych przeważnie za pomocą przeglądarki internetowej w szyfrowanej sesji https. Dostęp do systemu informatycznego posiadali tylko upoważnieni pracownicy uprawnionych podmiotów, na podstawie nadanych uprawnień oraz specjalnie wydanych dla nich certyfikatów. Certyfikaty te umieszczane były na indywidualnych kartach mikroprocesorowych i były używane podczas logowania do systemu. Logowanie wymagało również wprowadzenia kodu PIN. Po zalogowaniu upoważniony użytkownik, w zależności od nadanych uprawnień mógł zadać zapytanie w zakresie danych retencyjnych.

Niektóre skontrolowane podmioty realizowały obowiązek, o którym mowa w 180a ust. 1 pkt 1 Prawa telekomunikacyjnego, samodzielnie. Część powierzyła, w całości lub w części, realizację tego obowiązku, zgodnie z art. 180b ust. 2 Prawa telekomunikacyjnego[60], (np. w zakresie usługi poczty elektronicznej, telefonii stacjonarnej) innym podmiotom, na podstawie zawartych w tym zakresie umów.

Ponadto kontrolowane podmioty spełniały obowiązek zatrzymywania i przechowywania, a także udostępniania danych retencyjnych na rzecz operatorów „wirtualnych", korzystających z ich infrastruktury, na zasadach określonych w umowach zawartych z tymi operatorami.

Zabezpieczenie danych osobowych

Zgodnie z przepisami art. 180e ustawy Prawo telekomunikacyjne, w celu ochrony danych, o której mowa w art. 180a ust. 1 pkt 3, przedsiębiorcy telekomunikacyjni stosowali odpowiednie środki techniczne i organizacyjne, które zapewniały dostęp do tych danych jedynie upoważnionym pracownikom. Dostęp do danych retencyjnych w objętych kontrolą podmiotach posiadali upoważnieni pracownicy, ujęci w ewidencjach osób zatrudnionych przy przetwarzaniu danych osobowych, o których mowa w art. 39 ust. 1 ustawy o ochronie danych osobowych[61].
Przedsiębiorcy telekomunikacyjni prowadzili dokumentację opisującą sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, tj. politykę bezpieczeństwa i instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych. W kontrolowanych podmiotach wyznaczeni zostali administratorzy bezpieczeństwa informacji (art. 36 ust. 3 ustawy[62]). Ponadto, sprawowana była kontrola nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu były przekazywane (art. 38 ustawy[63]).

Dane, o których mowa w art. 180c Prawa telekomunikacyjnego, dla których upłynął okres 24 miesięcy, licząc od dnia połączenia lub nieudanej próby połączenia były usuwane z systemów

[60] Art. 180b ust. 1 – obowiązek, o którym mowa w art. 180a ust. 1, może być wykonywany wspólnie przez dwóch lub więcej operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych. Ust. 2. – operator publicznej sieci telekomunikacyjnej lub dostawca publicznie dostępnych usług telekomunikacyjnych może powierzyć realizację obowiązku, o którym mowa w art. 180a ust. 1, w drodze umowy, innemu przedsiębiorcy telekomunikacyjnemu. Powierzenie to nie zwalnia powierzającego z odpowiedzialności za realizację tego obowiązku.

[61] Art. 39 ust. 1 – administrator danych prowadzi ewidencję osób upoważnionych do ich przetwarzania, która powinna zawierać: 1) imię i nazwisko osoby upoważnionej, 2) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych, 3) identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

[62] Art. 36 ust. 3 – administrator danych wyznacza administratora bezpieczeństwa informacji, nadzorującego przestrzeganie zasad ochrony, o których mowa w ust. 1, chyba że sam wykonuje te czynności.

[63] Art. 38 – administrator danych jest obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

informatycznych automatycznie, poprzez wdrożenie niezbędnych mechanizmów w tych systemach (zdefiniowanie procedur dotyczących usuwania danych) lub ręcznie przez administratora systemu, bądź innego upoważnionego pracownika.

Udostępnianie danych retencyjnych w sprawach innych, niż przestępstwa

Stwierdzono przypadki udostępniania danych sądom w sprawach o wykroczenia, na podstawie postanowień tych sądów. Ponadto operatorzy udostępniali dane telekomunikacyjne sądom cywilnym oraz komornikom. Jako podstawę żądania danych wskazywano art. 248 kpc[64], natomiast w przypadku komorników sądowych art. 2 ust. 5 ustawy z dnia 29 sierpnia 1997 r. o komornikach sądowych i egzekucji[65]. Komornikom sądowym udostępniane były na ich wniosek informacje o numerach rachunków bankowych, z których opłacane były rachunki za usługi telekomunikacyjne. Część objętych kontrolą podmiotów nie udostępniała danych retencyjnych sądom cywilnym oraz komornikom. Stanowisko to było uzasadniane tym, że przepisy Prawa Telekomunikacyjnego (art. 159 ust. 4) jak i Kodeksu Postępowania Cywilnego (art. 248 i in.) nie mogą stanowić podstawy ujawnienia tajemnicy telekomunikacyjnej, np. w zakresie udostępniania przez operatorów bilingów na potrzeby spraw rozwodowych. Jak wskazał jeden z operatorów, w latach 2009–2012 pracownicy, w tym członkowie Zarządu byli karani grzywnami w związku z nieudostępnieniem danych telekomunikacyjnych. Jednocześnie, w wyniku postępowań odwoławczych, uzyskiwano orzeczenia potwierdzające zasadność postępowania operatora w tych sprawach.

W związku z dużą ilością zapytań o informacje niebędące danymi retencyjnymi, np. treści sms, na swoich stronach internetowych przedsiębiorcy telekomunikacyjni zamieszczali wskazówki mające na celu ułatwienie formułowanie zapytań o dane retencyjne.

Ustalenia NIK związane z funkcjonowaniem operatorów telekomunikacyjnych

Kontrola prowadzona w podmiotach uzyskujących dane telekomunikacyjne wykazała, iż systemy teleinformatyczne generują dane telekomunikacyjne w zakresie szerszym, niż to jest określone w treści postanowień, zawierających żądanie udostępnienia danych telekomunikacyjnych oraz zwolnienie z tajemnicy telekomunikacyjnej. Stanowiło to naruszenie art. 160 ust. 1[66], w związku z art. 159 ust. 1 pkt 3-5[67] i ust. 3[68] ustawy Prawo telekomunikacyjne oraz art. 218 § 1 kpk[69].

---

64 Art. 248 § 1 Kpc – każdy obowiązany jest przedstawić na zarządzenie sądu w oznaczonym terminie i miejscu dokument znajdujący się w jego posiadaniu i stanowiący dowód faktu istotnego dla rozstrzygnięcia sprawy, chyba że dokument zawiera informacje niejawne.

65 Dz. U. z 2011 r. Nr 231 poz. 1376 ze zm.

66 Art. 160 ust. 1 – podmiot uczestniczący w wykonywaniu działalności telekomunikacyjnej w sieciach publicznych oraz podmioty z nim współpracujące są obowiązane do zachowania tajemnicy telekomunikacyjnej.

67 Art. 159 ust. 1 pkt 3-5 – tajemnica komunikowania się w sieciach telekomunikacyjnych, zwana dalej „tajemnicą telekomunikacyjną", obejmuje dane transmisyjne, które oznaczają dane przetwarzane dla celów przekazywania komunikatów w sieciach telekomunikacyjnych lub naliczania opłat za usługi telekomunikacyjne, w tym dane lokalizacyjne, które oznaczają wszelkie dane przetwarzane w sieci telekomunikacyjnej wskazujące położenie geograficzne urządzenia końcowego użytkownika publicznie dostępnych usług telekomunikacyjnych; dane o lokalizacji, które oznaczają dane lokalizacyjne wykraczające poza dane niezbędne do transmisji komunikatu lub wystawienia rachunku; dane o próbach uzyskania połączenia między zakończeniami sieci, w tym dane o nieudanych próbach połączeń, oznaczających połączenia między telekomunikacyjnymi urządzeniami końcowymi lub zakończeniami sieci, które zostały zestawione i nie zostały odebrane przez użytkownika końcowego lub nastąpiło przerwanie zestawianych połączeń.

68 Art. 159 ust. 3 – z wyjątkiem przypadków określonych ustawą, ujawnianie lub przetwarzanie treści albo danych objętych tajemnicą telekomunikacyjną narusza obowiązek zachowania tajemnicy telekomunikacyjnej.

69 Art. 218 §1 kpk – urzędy, instytucje i podmioty prowadzące działalność w dziedzinie poczty lub działalność telekomunikacyjną, urzędy celne oraz instytucje i przedsiębiorstwa transportowe obowiązane są wydać sądowi lub

Najwyższa Izba Kontroli, stosownie do art. 63 ust. 3 ustawy o NIK, zawiadomiła Prezesa Urzędu Komunikacji Elektronicznej o naruszeniu obowiązku zachowania tajemnicy telekomunikacyjnej przez niektórych przedsiębiorców telekomunikacyjnych. Kontrolę w tym zakresie prowadzi również GIODO.

3.2.12. Retencja danych a prawa i wolności obywatelskie

Pozyskiwanie danych telekomunikacyjnych stanowi istotną ingerencję w sferę praw i wolności obywatelskich. W Polsce, kraju liczącym 37 mln obywateli, jest ponad 58 mln abonentów, co pozwala założyć, iż praktycznie każdy obywatel dysponuje telefonem. Dzisiejsza technologia, pozwala w stopniu niespotykanym nigdy wcześniej, gromadzić olbrzymią ilość danych o każdym obywatelu – nie tylko, z kim, kiedy i jak często się kontaktował, czy gdzie w danym momencie przebywał, ale również np. o numerze posiadanego przez niego rachunku bankowego czy karty płatniczej. Połączenie tych danych z informacjami dostępnymi w innych źródłach (bazy administracji państwowej, portale społecznościowe itp.) oraz wykorzystanie zaawansowanych narzędzi informatycznych do ich analizy (np. w celu tworzenia profili zachowań) powoduje, że sfera naszej prywatność uległa znaczącemu ograniczeniu. Na kwestię tę zwracają nie tylko organizacje broniące praw i wolności obywatelskich[70], ale również organy państwa powołane do ich ochrony[71].

Obok prawa do prywatności, którego elementem składowym jest wolność i ochrona tajemnicy komunikowania się, jedną z najistotniejszych wartości dla każdego człowieka jest bezpieczeństwo. Jak wskazują przedstawiciele służb i formacji powołanych do jego ochrony, skuteczne zapobieganie popełnieniu przestępstw i ich ściganie nie jest obecnie możliwe, bez zapewnienia służbom państwowym dostępu do informacji, w tym dostępu do danych telekomunikacyjnych. Dane te zawierają bowiem wartościowe ślady oraz dowody wykorzystywane do zapobiegania przestępstwom i ich ścigania oraz dla zagwarantowania wymiaru sprawiedliwości w sprawach karnych. Wskazują oni, że ich wykorzystanie doprowadziło do wyroków skazujących za przestępstwa, w sprawach w których bez zatrzymywania danych nie udałoby się nigdy rozwikłać. Podkreślają również inny pozytywny aspekt wykorzystania tego środka – doprowadził on do oczyszczenia z zarzutów szeregu niewinnych osób, bez konieczności stosowania instrumentów bardziej ingerujących w prywatność, jak podsłuchy czy rewizja w miejscu zamieszkania.

Dyskusja na ten temat toczy się nie tylko w Polsce. W swoim raporcie Komisja Europejska[72] oceniła, iż zatrzymywanie danych jest cennym narzędziem dla systemów wymiaru sprawiedliwości w sprawach

prokuratorowi, na żądanie zawarte w postanowieniu, korespondencję i przesyłki oraz dane, o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.), jeżeli mają znaczenie dla toczącego się postępowania. Tylko sąd lub prokurator mają prawo je otwierać lub zarządzić ich otwarcie.

70 Np. Helsińska Fundacja Praw Człowieka Zobacz (www.hfhr.pl), Fundacja Panoptykon (www.panoptykon.org).

71 Rzecznik Praw Obywatelskich złożyła do Trybunału Konstytucyjnego dwa wnioski o zbadanie przepisów uprawniających policję, służby specjalne i inne podmioty odpowiadające za bezpieczeństwo i porządek publiczny do pozyskiwania danych telekomunikacyjnych (sygn. K 23/11 – sprawa połączona z K 21/12, K 48/12, K 34/11) . RPO w przedmiotowych wnioskach wystąpiła m.in. o stwierdzenie zgodności art. 36b ust. 5 ustawy z dnia 28 września 1991 r. o kontroli skarbowej, art. 28 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 18 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym, art. 32 ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, art. 75d ust. 1 ustawy z dnia 27 sierpnia 2009 r. o Służbie Celnej z Konstytucją (www.trybunal.gov.pl).

72 Sprawozdanie Komisji dla Rady i Parlamentu Europejskiego z 18 kwietnia 2011 r. zatytułowane „Sprawozdanie z oceny dyrektywy w sprawie zatrzymywania danych (dyrektywa 2006/24/WE)", KOM(2011) 225 wersja ostateczna. Sprawozdanie to spotkało się z krytyką Europejskiego Inspektora Ochrony Danych Osobowych – zobacz: Opinia Europejskiego Inspektora Ochrony Danych na temat sprawozdania z oceny Komisji dla Rady i Parlamentu Europejskiego w sprawie dyrektywy

karnych oraz organów ścigania w UE. W swoim sprawozdaniu podkreśliła, iż zatrzymanie danych należy do narzędzi dochodzeniowych niezbędnych do tego, by sprostać współczesnym wyzwaniom w zakresie przestępczości, wobec ich różnorodności, ilości i tempa, w sposób kontrolowany i efektywny pod względem kosztów. Zwróciła jednakże równocześnie uwagę na fakt, iż zatrzymanie danych stanowi ograniczenie prawa do życia prywatnego i ochrony danych osobowych stanowiących prawa podstawowe w UE[73]. Zgodnie z art. 52 ust. 1 Karty Praw Podstawowych ograniczenie to musi „być przewidziane ustawą i szanować istotę tych praw i wolności, z zastrzeżeniem zasady proporcjonalności" i być uzasadnione, jako konieczne i rzeczywiście odpowiadające celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób. W praktyce oznacza to, że wszelkie ograniczenia muszą być:

- sformułowane w sposób jasny i przewidywalny,
- konieczne do osiągnięcia celu leżącego w interesie ogólnym lub ochrony praw i swobód innych,
- proporcjonalne do założonego celu,

  oraz
- zachowywać istotę danego prawa podstawowego.

Europejski Trybunał Praw Człowieka w sprawie Marper vs Wielka Brytania[74] stwierdził, że już samo gromadzenie informacji o danej osobie ma bezpośredni wpływ na ochronę jej życia prywatnego, bez względu na to, czy dane te są następnie wykorzystywane. Z kolei w sprawie Schecke[75] Europejski Trybunał Sprawiedliwości orzekł, że ograniczenia w zakresie ochrony danych osobowych są dopuszczalne jedynie pod warunkiem ich „ścisłej proporcjonalności", w stosunku do realizowanego celu. Tym samym uznał, iż kryterium dopuszczalności retencji danych nie jest jego skuteczność w walce z przestępczością, ale niezbędność i proporcjonalność.

Niemiecki Trybunał Konstytucyjny stwierdził, że zatrzymywanie danych może uniemożliwiać swobodną realizację praw podstawowych[76]. Trybunał wprost uznał, że zatrzymywanie danych w ściśle określonym celu i przy zapewnieniu wystarczająco wysokiego poziomu bezpieczeństwa danych nie oznacza naruszenia niemieckiej konstytucji. Równocześnie jednak wyraźnie zaznaczył, że zatrzymywanie danych telekomunikacyjnych stanowi poważne ograniczenie prawa do prywatności i dlatego powinno być dopuszczalne w szczególnie ograniczonej liczbie przypadków. Ocena zasadności zastosowania takiego środka musi uwzględniać zasadę proporcjonalności. Wniosek o udostępnienie danych może być złożony jedynie wówczas, gdy istnieje podejrzenie poważnego przestępstwa lub gdy zagrożone jest bezpieczeństwo państwa. Ponadto wskazał na dalsze ograniczenia w dostępie do danych telekomunikacyjnych, ze względu na charakter niektórych połączeń, o których dane powinny pozostać poufne (np. związanych z potrzebami socjalnymi lub emocjonalnymi). Pozyskane dane powinny być odpowiednio zabezpieczone przed dostępem osób niepowołanych oraz objęte stosownym nadzorem.

---

w sprawie zatrzymywania danych (dyrektywa 2006/24/WE), opublikowaną w Dzienniku Urzędowym Unii Europejskiej z 23 września 2011 r. (2011/C 279/01).

73 Artykuły 7 i 8 Karty praw podstawowych Unii Europejskiej (Dz. U. C 83 z 30.3.2010, s. 389) gwarantują każdemu prawo do „ochrony danych osobowych, które go dotyczą". Prawo to zapisano także w art. 16 Traktatu o funkcjonowaniu Unii Europejskiej (Dz. U. C 83 z 30.3.2010, s. 1).

74 Zgłoszenie nr 30562/04 i 30566/04, http://www.echr.coe.int/echr/

75 Sprawa C-92/09 Volker i Markus Schecke GbR przeciwko Land Hessen oraz C-93/09 Eifert przeciwko Land Hessen i Bundesanstalt für Lanwirtschaft und Ernährung

76 Bundesverfassungsgericht, 1 BvR 256/08 z dnia 2 marca 2010 r., pkt 1-345.

W związku z powyższym, Komisja Europejska zarekomendowała rozważenie: skrócenia okresu przechowywania danych telekomunikacyjnych; ograniczenia katalogu podmiotów mających dostęp do tych danych; ograniczenia celów, w jakich dane te mogą być wykorzystywane (np. poprzez doprecyzowanie katalogu najcięższych przestępstw); ograniczenia kategorii danych, jakie są przechowywane; wprowadzenie rozwiązań gwarantujących, iż dane telekomunikacyjne będą wykorzystywane wyłącznie w celu ścigania poważnych przestępstw.

Rozważane jest również wprowadzenie rozwiązań alternatywnych. Jedną z propozycji jest koncepcja zachowywania danych na żądanie uprawnionego podmiotu. Polega ona na czasowym zabezpieczeniu niektórych danych dotyczących ruchu telekomunikacyjnego i lokalizacji, wyłącznie w odniesieniu do konkretnych osób podejrzanych o działalność przestępczą, a które to dane mogą być udostępnione organom wymiaru sprawiedliwości na mocy zezwolenia sądu. Głównym argumentem wysuwanym przeciwko wdrożeniu tego rozwiązania jest jednakże to, że nie gwarantuje ono dostępu do danych wytworzonych przed nakazem zachowania oraz nie pozwala prowadzić dochodzenia, jeżeli nie jest znany jego cel.

W ocenie NIK, biorąc pod uwagę obecne uwarunkowania prawno-organizacyjne, projektowane zmiany przepisów na poziomie Unii Europejskiej, a także wyniki przeprowadzonej kontroli, należy rozważyć podjęcie działań w czterech zasadniczych obszarach:

- **zakresu i celu pozyskiwania danych;**
- **kontroli nad procesem pozyskiwania danych;**
- **niszczenia pozyskanych danych w sytuacji, gdy nie są już one dalej niezbędne dla osiągnięcia celów prowadzonego postępowania;**
- **stworzenia mechanizmów sprawozdawczych, które zapewnią rzetelną informację o zakresie pozyskiwania danych telekomunikacyjnych.**

Zakres i cel pozyskiwania danych

Zakres i cel pozyskiwanych przez uprawnione służby danych są głównymi czynnikami wpływającym na ocenę stopnia, w jakim wykorzystanie tego środka, ogranicza prawa obywatelskie. Rozważając zakres pozyskiwania danych telekomunikacyjnych należy wskazać na trzy kwestie:

1) zakres danych, który może zostać pozyskany,
2) katalog spraw, w których możliwe jest pozyskanie danych,
3) prawo do zachowania tajemnicy zawodowej.

Ad 1) Zgodnie z art. 180c Prawa telekomunikacyjnego operatorzy telekomunikacyjnie obowiązani są do przechowywania i udostępniania uprawnionym podmiotom danych niezbędnych do: ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego (inicjującego połączenia oraz do którego kierowane jest połączenie) oraz zgodnie z pkt 2 przywołanego przepisu: określenia daty i godziny połączenia oraz czasu jego trwania, rodzaju połączenia, lokalizacji telekomunikacyjnego urządzenia końcowego. Ponadto uprawnione podmioty mają, zgodnie z art. 180d Prawa telekomunikacyjnego dostęp do danych przetwarzanych przez operatorów telekomunikacyjnych dotyczących: użytkownika[77];

[77] Obejmujący: nazwisko i imiona; imiona rodziców; miejsce i datę urodzenia; adres miejsca zameldowania na pobyt stały; numer ewidencyjny PESEL – w przypadku obywatela Rzeczypospolitej Polskiej; nazwę, serię i numer dokumentów potwierdzających tożsamość, a w przypadku cudzoziemca, który nie jest obywatelem państwa członkowskiego albo Konfederacji Szwajcarskiej – numeru paszportu lub karty pobytu; zawarte w dokumentach potwierdzających możliwość

transmisyjnych[78]; lokalizacyjnych[79]; o próbach uzyskania połączenia między zakończeniami sieci, w tym dane o nieudanych próbach połączeń; elektronicznego wykazu abonentów, użytkowników lub zakończeń sieci, uwzględniającego dane uzyskiwane przy zawarciu umowy.

Odnosząc się do sformułowanego katalogu zapytań należy zauważyć, iż jako dane bilingowe nie powinny być traktowane informacje pozwalające na ustalenie, do kogo należy dany numer telefonu czy jakie są jego dane adresowe. Informacja ta ma charakter zbliżony, np. do informacji o właścicielu pojazdu i w związku z tym trudno uznać, że jej udostępnienie uprawnionym organom państwa, w sposób istotny ingeruje w prawo do prywatności. Tego rodzaju ustalenie można porównywać do sprawdzania dokonanego w książce telefonicznej. Z tego też względu, w ocenie NIK, informacje dotyczące ustalenia danych abonenta nie powinny być wykazywane w sprawozdaniach UKE, jako zapytania o dane bilingowe.

Należy zauważyć, iż przepisy o retencji nie obejmują świadczenia usług drogą elektroniczną. Obecnie obowiązujące prawo przewiduje zatrzymywanie także danych o komunikacji, która odbywa się w Internecie, jedynie przez „dostawców powszechnie dostępnych usług telekomunikacyjnych". A więc obowiązek zatrzymywania danych dotyczy firm telekomunikacyjnych, które świadczą usługę dostępu do Internetu, natomiast już nie firm dostarczających konkretne usługi oparte na Internecie, (co może dotyczyć przede wszystkim poczty elektronicznej, ale również portali społecznościowych czy wyszukiwarek internetowych). W ocenie NIK, należy ujednolicić obowiązujące w tym zakresie przepisy. W przypadku utrzymania przepisów o retencji danych, należy rozważyć rozszerzenie ich zakresu również na dostawców tego rodzaju usług internetowych – trudno, bowiem znaleźć uzasadnienie aksjologiczne, dlaczego osoby korzystające z usług opartych na Internecie miałyby być chronione przed ingerencją ze strony państwa w stopniu większym, niż osoby korzystające z usług telekomunikacyjnych. Należy jednakże zwrócić uwagę na szereg ograniczeń, jakie dotyczą tej sfery: rynek usług internetowych podlega dynamicznym zmianom; duża część podmiotów świadczących usługi internetowe, z których korzystają obywatele polscy, to podmioty zagraniczne. Biorąc pod uwagę powyższe uwarunkowania oraz charakter proponowanej zmiany, kwestia ta wymaga jednakże pogłębionej analizy oraz szerokich konsultacji społecznych.

Rozważenia wymaga również czas, przez jaki dane telekomunikacyjne muszą być przechowywane przez operatorów. Obowiązujące do 20 stycznia 2013 r. przepisy przewidywały przechowywanie danych za okres 24 m-cy, to jest maksymalny dopuszczalny przez Dyrektywę. W większości krajów UE okres ten był znacznie krótszy (6 lub 12 m-cy). Również zalecenia Komisji Europejskiej, jak się wydaje, będą zmierzały w kierunku skrócenia maksymalnego dopuszczalnego okresu retencji danych. Nowelizacja ustawy Prawo telekomunikacyjne z dnia 16 listopada 2012 r.[80] skróciła ten okres do 12 m-cy. Jako uzasadnienie do dokonania zmian wskazano m.in., iż największe znaczenie

wykonania zobowiązania wobec dostawcy publicznie dostępnych usług telekomunikacyjnych wynikającego z umowy o świadczenie usług telekomunikacyjnych. Oprócz ww. danych, dostawca publicznie dostępnych usług telekomunikacyjnych może, za zgodą użytkownika będącego osobą fizyczną, przetwarzać inne dane tego użytkownika w związku ze świadczoną usługą, w szczególności numer konta bankowego lub karty płatniczej, adres korespondencyjny użytkownika, jeżeli jest on inny niż adres miejsca zameldowania na pobyt stały tego użytkownika, a także adres poczty elektronicznej oraz numery telefonów kontaktowych.

78 Oznaczają dane przetwarzane dla celów przekazywania komunikatów w sieciach telekomunikacyjnych lub naliczania opłat za usługi telekomunikacyjne

79 Oznaczają wszelkie dane przetwarzane w sieci telekomunikacyjnej wskazujące położenie geograficzne urządzenia końcowego użytkownika publicznie dostępnych usług telekomunikacyjnych

80 Dz. U. z 2012, poz. 1445.

dla wykrywania i ścigania przestępstw mają dane pochodzące z ostatniego roku. Należy jednakże zauważyć, iż dane które były podstawą dokonania zmian, jak wykazała kontrola NIK, nie były rzetelne. Błędy popełnione przez operatorów telekomunikacyjnych w składanych sprawozdaniach, przy braku kontroli ze strony Prezesa UKE doprowadziły do istotnego zaburzenia proporcji zapytań, zawyżając istotnie liczbę zapytań dotyczących danych za pierwsze miesiące[81]. Ponadto należy zwrócić uwagę, iż zapytania dotyczące okresu powyżej 12 m-cy zasadniczo dotyczą spraw o dużym stopniu komplikacji, których ujawnienie nierzadko następuje po długim czasie od ich popełnienia lub w wyniku długotrwałych śledztw[82]. W ocenie NIK, należałoby rozważyć wprowadzenie mechanizmów, które zapewnią uprawnionym podmiotom dostęp do informacji w okresie dłuższym niż 12 m-cy. Zdaniem NIK, jednym z możliwych rozwiązań byłoby dopuszczenie możliwości gromadzenia danych telekomunikacyjnych przez okres przekraczający 12 miesięcy na żądanie uprawnionego podmiotu, w ściśle określonych sprawach. Operator miałby wówczas obowiązek gromadzenia danych „bilingowych" za okres przekraczający 12 m-cy, ale tylko w stosunku do osób wyraźnie wskazanych przez uprawniony podmiot.

Należy również zauważyć, iż większość danych wskazanych w art. 180c i d Prawa telekomunikacyjnego operatorzy przechowują na potrzeby ewentualnych postępowań reklamacyjnych. Z uwagi na obowiązki określone w art. 165 ust. 2 i art. 168 ust. 1 ww. ustawy dane telekomunikacyjne w znacznym zakresie nie mogą być przez przedsiębiorców telekomunikacyjnych niszczone po okresie retencji, określonym w art. 180a ust. 1 pkt 1 ustawy, ze względu na trzyletni termin przedawnienia roszczeń wynikających z umowy o świadczenie usług telekomunikacyjnych. Przepisy nie określają maksymalnego terminu, w którym przedsiębiorcy telekomunikacyjni mogą przechowywać dane telekomunikacyjne na potrzeby dochodzenia należności z tytułu wykonanych usług. W ocenie NIK, zapewnienie służbom, w ściśle określonych przypadkach, przy zachowaniu kontroli zewnętrznej, dostępu do przechowywanych przez operatorów telekomunikacyjnych danych, umożliwiłoby dalsze skrócenie okresu retencji danych.

Ad 2) W ocenie NIK, doprecyzowania wymaga cel gromadzenia danych retencyjnych. Obecnie obowiązujące przepisy odwołują się jedynie do zakresu zadań poszczególnych służb bądź ogólnego stwierdzenia, iż dane te są pozyskiwanie w celu zapobiegania lub wykrywania przestępstw. Należy przy tym zauważyć, iż przepisy te umożliwiają wykorzystywanie danych retencyjnych nie tylko do wykrywania przestępstw, ale także w działaniach prewencyjnych czy analitycznych. W szczególności omawiane dane są udostępniane:

a) w celu zapobiegania lub wykrywania przestępstw (art. 20c ust. 1 ustawy o Policji oraz art. 10 b ust. 1 ustawy o Straży Granicznej, art. 30 ustawy o Żandarmerii Wojskowej)[83];
b) w celu zapobiegania lub wykrywania przestępstw skarbowych lub przestępstw, o których mowa w art. 2 ust. 1 pkt 14b ustawy o kontroli skarbowej, oraz naruszeń przepisów, o których mowa w art. 2 ust. 1 pkt 12, tj. także w celu zapobiegania i ujawniania przestępstw, o których mowa w art. 228-231 k.k., popełnianych przez osoby zatrudnione lub pełniące służbę w jednostkach organizacyjnych podległych ministrowi właściwemu do spraw finansów publicznych oraz w celu

81 Przypadek zawyżenia przez jednego z przedsiębiorców liczby zapytań za pierwszy miesiąc o 513.857 przypadków, tj. o prawie 100 % w stosunku do liczby zapytań za pierwszy miesiąc do pozostałych przedsiębiorców oraz o prawie 40 % w stosunku do liczby wszystkich zapytań w roku 2011 został opisany w pkt 3.2.8. Informacji na str. 49.

82 Wg danych KG Policji spośród dochodzeń i śledztw trwających powyżej 6 miesięcy, proporcjonalnie najwięcej prowadzonych postępowań dotyczyło zabójstw, pobić ze skutkiem śmiertelnym oraz przestępstw korupcyjnych, urzędniczych, gospodarczych i podatkowych.

83 Warto przypomnieć, że w wyniku debat i uzgodnień, jakie miały miejsce pod koniec 2005 r. w Parlamencie i Radzie UE, zapis o zapobieganiu przestępstwom, jako zbyt daleko idący, został wykreślony z projektu Dyrektywy 2006/24/WE.

zapobiegania i wykrywania naruszeń krajowych przepisów celnych oraz ścigania naruszeń krajowych lub wspólnotowych przepisów celnych (art. 36b ust. 1 pkt 1 ww. ustawy);

c) w celu zapobiegania lub wykrywania przestępstw skarbowych (art. 75d ustawy o Służbie Celnej);

d) w celu realizacji przez ABW zadań, o których mowa w art. 5 ust. 1, tj. rozpoznawania, zapobiegania i zwalczania zagrożeń godzących w bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny, rozpoznawania, zapobiegania i wykrywania przestępstw określonych w art. 5 ust. 1 pkt 2; realizowania, w granicach swojej właściwości, zadań związanych z ochroną informacji niejawnych oraz wykonywania funkcji krajowej władzy bezpieczeństwa w zakresie ochrony informacji niejawnych w stosunkach międzynarodowych; uzyskiwania, analizowania, przetwarzania i przekazywania właściwym organom informacji mogących mieć istotne znaczenie dla ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego, podejmowania innych działań określonych w odrębnych ustawach i umowach międzynarodowych (art. 28 ust. 1 pkt 1 ustawy o ABW i AW);

e) w celu realizacji przez CBA zadań określonych w art. 2 ustawy o CBA, tj. w celu: 1) rozpoznawania, zapobiegania i wykrywania przestępstw wymienionych w art. 2 ust. 1 pkt 1 oraz ścigania ich sprawców, 2) ujawniania i przeciwdziałania przypadkom nieprzestrzegania przepisów ustawy o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne, 3) dokumentowania podstaw i inicjowania realizacji przepisów ustawy z dnia 21 czerwca 1990 r. o zwrocie korzyści uzyskanych niesłusznie kosztem Skarbu Państwa lub innych państwowych osób prawnych[84], ujawniania przypadków nieprzestrzegania określonymi przepisami prawa procedur podejmowania i realizacji decyzji w przedmiocie: prywatyzacji i komercjalizacji, wsparcia finansowego, udzielenia zamówień publicznych, rozporządzenia mieniem jednostek lub przedsiębiorców oraz przyznawania koncesji, zwolnień, zwolnień podmiotowych i przedmiotowych, ulg, preferencji, kontyngentów, plafonów, poręczeń i gwarancji kredytowych, 5) kontroli prawidłowości i prawdziwości oświadczeń majątkowych lub oświadczeń o prowadzeniu działalności gospodarczej osób pełniących funkcje publiczne, o których mowa w art. 115 § 19 k.k., 6) prowadzenia działalności analitycznej dotyczącej zjawisk występujących w obszarze właściwości CBA oraz przedstawiania w tym zakresie informacji Prezesowi Rady Ministrów, Prezydentowi RP, Sejmowi oraz Senatowi, 7) podejmowania innych działań określonych w odrębnych ustawach i umowach międzynarodowych (art. 18 ust. 1 pkt 1ustawy o Centralnym Biurze Antykorupcyjnym);

f) w celu realizacji przez SKW zadań określonych w art. 5, tj.: 1) rozpoznawania, zapobiegania oraz wykrywania popełnionych przez żołnierzy, funkcjonariuszy SKW i SWW oraz pracowników SZ RP i innych jednostek organizacyjnych MON, przestępstw wymienionych w art. 5 ust. 1 pkt 1, 2) realizowania, w granicach swojej właściwości, zadań określonych w przepisach ustawy z 5 sierpnia 2010 r. o ochronie informacji niejawnych[85], 3) uzyskiwania, gromadzenia, analizowania, przetwarzania i przekazywania właściwym organom informacji mogących mieć znaczenie dla obronności państwa, bezpieczeństwa lub zdolności bojowej Sił Zbrojnych oraz podejmowania działań w celu eliminowania ustalonych zagrożeń, 4) prowadzenia kontrwywiadu radioelektronicznego oraz przedsięwzięć z zakresu ochrony kryptograficznej i kryptoanalizy,

84 Dz. U. Nr 44, poz. 255 ze zm.

85 Dz. U. Nr 182, poz.1228.

5) uczestniczenia w planowaniu i przeprowadzaniu kontroli realizacji umów międzynarodowych dotyczących rozbrojenia, 6) ochrony bezpieczeństwa jednostek wojskowych i innych jednostek organizacyjnych MON, 7) ochrony bezpieczeństwa badań naukowych i prac rozwojowych, 9) podejmowania innych działań przewidzianych dla Służby Kontrwywiadu Wojskowego (art. 32 ust. 1 pkt 1 ustawy o SKW i SWW).

W ocenie NIK, powołane wyżej przepisy transponujące dyrektywę do systemu prawnego RP, pozwalają na dostęp do zatrzymanych danych i korzystanie z nich do celów wykraczających poza cele objęte dyrektywą 2006/24/WE. Należy, bowiem zauważyć, iż Dyrektywa zobowiązuje państwa członkowskie do przyjęcia środków mających zapewnić zatrzymywanie danych telekomunikacyjnych w celu prowadzenia śledztwa w sprawie „poważnych przestępstw" oraz ich wykrywania i ścigania, zgodnie z definicjami przyjętymi przez każde państwo członkowskie w swoim prawie krajowym. W ustawodawstwie RP nie występuje jednakże definicja poważnego przestępstwa. Przenosząc to pojęcie na grunt prawa polskiego, nie można utożsamiać go z przestępstwami zagrożonymi karą minimalną trzech lat pozbawienia wolności, czyli zbrodnią[86]. Istnieje, bowiem szereg przestępstw, jak choćby porwanie czy przestępstwo zgwałcenia, które w powszechnej świadomości społecznej zaliczane są do kategorii „poważnych przestępstw", a dla których dolna granica zagrożenia karą pozbawienia wolności została określona poniżej 3 lat. Należy przy tym zwrócić uwagę, iż w tego typu przestępstwach dane bilingowe często są jednym z kluczowych środków dowodowych, prowadzących do ustalenie sprawcy. Trafniejsze, w ocenie NIK, jest podejście zaproponowane w przygotowywanym obecnie projekcie zmian[87], gdzie wskazano, że dane telekomunikacyjne będą mogły być pozyskiwane i wykorzystywane przez uprawnione podmioty, wyłącznie dla potrzeb postępowań w sprawie rozpoznawania, zapobiegania i wykrywania przestępstw zagrożonych karą pozbawienia wolności, której górna granica wynosi, co najmniej 3 lata oraz postępowań w sprawie rozpoznawania, zapobiegania i wykrywania przestępstw popełnionych przy użyciu środków komunikacji elektronicznej. Projekt przewiduje również, iż dane telekomunikacyjne będą mogły być pozyskiwanie i przetwarzane w celu ochrony życia i zdrowia obywateli, m.in. w przypadkach poszukiwania osób zaginionych i przeciwdziałania próbom samobójczym oraz w przypadkach rozpoznawania, zapobiegania i wykrywania innych przestępstw i wykroczeń za zgodą abonenta, którego przedmiotowe dane telekomunikacyjne dotyczą. Dane telekomunikacyjne będą mogły być także pozyskiwanie i przetwarzane w przypadkach rozpoznawania, zapobiegania i wykrywania innych enumeratywnie wymienionych wykroczeń (jak np. fałszywe alarmy bombowe), jeżeli będzie za tym przemawiał ważny interes społeczny. W ocenie NIK, precyzyjne określenie katalog spraw, w których uprawnione służby mogą pozyskiwać dane telekomunikacyjne, ma kluczowe znaczenie dla oceny, czy obowiązujące przepisy nie naruszają zasady proporcjonalności, a tym samym są dopuszczalne w świetle obowiązujących przepisów chroniących prawa i wolności obywatelskie.

W ocenie NIK, udostępnienie danych telekomunikacyjnych powinno uwzględniać również zasadę subsydiarności[88]. Zgodnie z obowiązującymi obecnie przepisami, obowiązek udostępnienia danych dotyczy podmiotu wykonującego działalność telekomunikacyjną w każdym wypadku, gdy zwrócą się o to odpowiednie służby, a nie tylko wtedy, „gdy inne środki podejmowane w celu

86 Propozycja taka znalazła się w jednym z projektów nowelizacji Prawa telekomunikacyjnego.

87 Projekt zmian z 20 grudnia 2012 r. opracowany przez Biuro Kolegium ds. Służb Specjalnych KPRM.

88 Określoną w art. 31 ust.3 Konstytucji RP.

realizacji ustawowego celu okazały się bezskuteczne". Należy podkreślić, że jak zauważył Trybunał Konstytucyjny[89] „(...) nie wystarczy, aby stosowane środki sprzyjały zamierzonym celom, ułatwiały ich osiągnięcie albo były wygodne dla władzy, która ma je wykorzystać do osiągnięcia tych celów. (...) Nie wystarczy, zatem sama celowość, pożyteczność, taniość czy łatwość posługiwania się przez władzę – w odniesieniu do użytego środka. Bez znaczenia jest też argument porównawczy, że podobne środki w ogóle bywają stosowane w innych państwach. (…) Chodzi, zatem o zastosowanie środków niezbędnych (koniecznych) w tym sensie, że będą one chronić określone wartości w sposób, bądź w stopniu, który nie mógłby być osiągnięty przy zastosowaniu innych środków, a jednocześnie winny to być środki jak najmniej uciążliwe dla podmiotów, których prawo bądź wolność ulegają ograniczeniu (...)". Należy również zauważyć, iż zgodnie z orzecznictwem Europejskiego Trybunału Sprawiedliwości, wszelkie ograniczenia prawa do prywatności muszą być proporcjonalne do chronionego interesu powszechnego[90]. Kryterium dopuszczalności ingerencji w prawa podstawowe jest, bowiem obiektywna niezbędność zastosowanego środka, a nie jedynie jego użyteczność do osiągnięcia określonego celu (ścigania przestępstw). W ocenie NIK, konieczne jest, więc rozważenie wprowadzenia przepisów, które wykorzystanie danych telekomunikacyjnych będą uzależniać, od niemożności zastosowania innych, mniej ingerujących w prawa obywatelskie środków.

Osobną kwestią jest sięganie po dane telekomunikacyjne w sprawach cywilnych. Jak wskazują wyniki kontroli przeprowadzonej przez NIK, praktyka w tym zakresie jest niejednolita. Część operatorów przedstawia na żądanie sądów cywilnych dane bilingowe, pomimo braku zgody strony na ich udostępnienie. W ocenie NIK, ani przepisy Prawa telekomunikacyjnego, ani przepisy Kodeksu postępowania cywilnego nie dają podstawy do żądania przez sąd w sprawie cywilnej udostępnienia danych objętych tajemnicą telekomunikacyjną. Podstawą udostępnienia danych może być art. 159 ust. 2 pkt 2 Prawa telekomunikacyjnego, zgodnie z którym przekazywanie lub inne wykorzystywanie treści lub danych objętych tajemnicą telekomunikacyjną, przez osoby inne niż nadawca i odbiorca komunikatu jest zabronione, chyba że nastąpi za zgodą nadawcy lub odbiorcy, których dane te dotyczą. Podstawą przekazania tych danych nie mogą być natomiast artykuły 248 i 251 kodeksu postępowania cywilnego, które odnoszą się do dowodów z dokumentów, gdyż udostępnienie sądowi informacji w tym zakresie nie polega wyłącznie na dostarczeniu sądowi istniejącego dokumentu, ale wymaga jego sporządzenia na podstawie danych stanowiących tzw. tajemnicę telekomunikacyjną[91].

Ad 3) Obecnie obowiązujące przepisy nie wskazują kategorii osób, w stosunku do których niezbędne jest respektowanie ich tajemnicy zawodowej. Ustawodawca nie wyłączył żadnej kategorii użytkowników z kręgu podmiotów, których dane mogą być pozyskiwane, choć dane te mogą być objęte tajemnicą notarialną, adwokacką, radcy prawnego, lekarską lub dziennikarską, której zniesienie jest możliwe wyłącznie, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a dana okoliczność nie może być ustalona na podstawie innego dowodu[92]. Np. w stosunku

89 Wyrok z dnia 12 grudnia 2005 r., sygn. akt K 32/04, OTK z 2005 r., Nr 1 I/A, poz. 132.

90 Sprawa C-92/09 Volker i Markus Schecke GbR przeciwko Land Hessen oraz C-93/09 Eifert przeciwko Land Hessen i Bundesanstalt für Lanwirtschaft und Ernährung.

91 Por. postanowienie Sadu Apelacyjnego w Białymstoku z 6 kwietnia 2011 r., sygnatura akt I A Cz 279/11.

92 Art. 180 § 2 k.p.k. włącza dziennikarza do katalogu osób, które mogą być przesłuchiwane, co do faktów objętych tajemnicą tylko wtedy, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu. Z obowiązku zachowania tajemnicy dziennikarskiej może zwolnić wyłącznie sąd.

do dziennikarzy, art. 180 § 3 k.p.k. ustanawia bezwzględny zakaz dowodowy dotyczący danych umożliwiających identyfikację autora materiału prasowego, listu do redakcji lub innego materiału o tym charakterze, jak również identyfikację osób udzielających informacji opublikowanych lub przekazanych do opublikowania, jeżeli osoby te zastrzegły nieujawnianie danych. Bezwzględność tego zakazu oznacza, że nawet gdyby dziennikarz chciał ujawnić te informacje, to nie wolno mu tego uczynić, a organ procesowy nie może go zwolnić z takiej tajemnicy (z wyjątkami wskazanymi w art. 240 § 1 k.k.). Dziennikarz nie naraża się na represje prawne, odmawiając składania zeznań na te okoliczności. Dopuszczalne jest jednakże legalne uzyskanie i przeprowadzenie w procesie karnym innego dowodu na okoliczność tożsamości osób, o których mowa w art. 180 § 3 k.p.k. Należy jednakże zwrócić uwagę na orzecznictwo Europejskiego Trybunału Praw Człowieka w tym względzie. Przykładowo, w wyroku z 22 listopada 2012 r.[93] stwierdził on, iż prawo musi zapewniać dziennikarzom odpowiednie gwarancje dotyczące ochrony poufności źródeł informacji. Jeżeli chodzi o zastosowanie względem dziennikarzy środków pozwalających na monitorowanie ich rozmów telefonicznych oraz ich obserwację, Trybunał uznał je za sprzeczne z art. 8 i 10 Konwencji, ponieważ ich stosowanie nie zostało nakazane i nie było nadzorowane przez sąd lub organ o porównywalnej niezawisłości i bezstronności. Skarżący mogli jedynie wnieść do sądu skargę na stosowanie takich środków *post factum*. Taka możliwość nie wystarcza, gdyż – w przypadku ujawnienia tożsamości źródła informacji – raz zniszczone zaufanie do dziennikarza nie może w ten sposób zostać przywrócone. Środki kontroli zastosowane w tej sprawie miały dokładnie na celu ujawnienie tego, od kogo skarżący uzyskali sporne dokumenty. Dotyczyły więc samej istoty pracy dziennikarskiej, ingerencja w którą wymaga szczególnego uzasadnienia i kontroli. W ocenie NIK, należałoby rozważyć wprowadzenie rozwiązań, które będą stwarzać dodatkowe gwarancje w przypadku osób wykonujących zawód „zaufania publicznego", np. poprzez uzależnienie pozyskania danych retencyjnych od zgody sądu. Natomiast w przypadku ujawnienia post factum, iż dane dotyczą osoby, która należy do grupy osób wykonujących zawód „zaufania publicznego" dalsze wykorzystanie w stosunku do niej tego środka oraz możliwość wykorzystania już pozyskanych danych powinny być uzależnione od zgody sądu lub innego niezależnego organu.

Kontrola nad procesem pozyskiwania danych

Jak wykazano powyżej, sięganie po dane retencyjne stanowi istotną ingerencję w prawa i wolności obywatelskie, w szczególności prawo do prywatności. Należy podkreślić, iż NIK nie mogła objąć kontrolą, a tym samym ocenić zasadności wykorzystania środka w postaci retencji danych w prowadzonych postępowaniach, ze względu na zakres posiadanych kompetencji. W obecnym stanie prawnym nie istnieje żaden podmiot, który mógłby sprawować rzeczywistą kontrolę nad wykorzystaniem tego środka przez uprawnione organy, służby i formacje. Sytuacja ta jest wyjątkowa w zestawieniu ze standardami przyjętymi w większości państw Unii Europejskiej. W 24 państwach taką kontrolę sprawuje sąd lub prokuratura[94] albo niezależny organ administracyjny[95]. Na konieczność wprowadzenia kontroli zewnętrznej zwróciła uwagę Rzecznik Praw Obywatelskich we wniosku do Trybunału Konstytucyjnego, w którym zakwestionowała

93 Sprawia nr 39315/06, Telegraaf Media Nederland Landelijke Media B.V. i inni przeciwko Holandii.

94 Sądy: Bułgaria, Czechy, Dania, Finlandia, Grecja, Hiszpania, Litwa, Luksemburg, Niemcy (obecnie przepisy o retencji zostały uznane za niekonstytucyjne), Portugalia, Słowenia. Sąd lub prokurator: Belgia, Cypr. Sędzia śledczy lub prokurator: Estonia, Holandia. Prokurator: Węgry i Włochy.

95 Model kontroli administracyjnej został zastosowany we Francji, Irlandii, na Malcie oraz w Wielkiej Brytanii.

zgodność przepisów ustaw kompetencyjnych z art. 8 Konwencji oraz art. 49 w związku z art. 31 ust. 3 Konstytucji. We wniosku wskazano m.in., iż „standardy zawarte w art. 49 Konstytucji oraz w art. 8 Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności nie są respektowane, gdyż ustawodawca nie zapewnił zewnętrznych form kontroli korzystania przez poszczególne służby z przyznanych im szerokich uprawnień w zakresie dostępu do danych objętych tajemnicą telekomunikacyjną". W ocenie NIK, konieczne jest stworzenie instrumentów nadzoru i kontroli nad wykorzystaniem tego środka. Sytuacja, że jedynym podmiotem oceniającym zasadność pozyskiwania danych telekomunikacyjnych jest jednostka uprawniona do ich pozyskania, jest nie do zaakceptowania w ramach demokratycznego państwa prawnego. Nie wynika to oczywiście z faktu, że należy zakładać, iż działanie służb skierowane jest przeciwko obywatelom, ale z tego, że zewnętrzna kontrola takich działań jest standardem służącym i państwu (w tym samym służbom) i społeczeństwu[96].

Rozpatrując zagadnienie kontroli nad pozyskiwaniem danych telekomunikacyjnych należałoby skupić się na dwóch formach jej realizacji:

1) kontroli uprzedniej,
2) kontroli następczej.

Ad 1) Kontrola uprzednia, czyli realizowana przed skierowaniem zapytania w sprawie udostępnienia danych telekomunikacyjnych, pozwoliłaby nie tylko na istotne zwiększenie nadzoru nad wykorzystaniem tego środka, ale prawdopodobnie przyczyniłaby się również do ograniczenia skali jego wykorzystania. Możliwość zastosowania tej formy kontroli uzależniona jest od spełnienia dwóch przesłanek:

a) wskazania (ustanowienia) podmiotu, który „weryfikowałby" wnioski o udostępnienie danych telekomunikacyjnych, a następnie wydawał zgodę na wykorzystanie tego środka;
b) precyzyjnego określenia sytuacji, w których środek ten może być wykorzystany, jako niezbędnego warunku oceny zasadności wniosku.

Ad a) W demokratycznych państwach prawa, podmiotami którym najczęściej powierza się kontrolę w takich sytuacjach są organy sądowe. Kontrola sądowa daje bowiem gwarancję niezależności i bezstronności oraz zapewnia przestrzeganie właściwej procedury. W warunkach polskich, mogłoby to jednak skutkować tym, iż przy dużej ilości spraw sądy nie byłyby w stanie weryfikować tego rodzaju wniosków na bieżąco. Mogłoby to spowodować znaczne opóźnienia, co niejednokrotnie uniemożliwiałoby de facto wykorzystanie tego środka. Alternatywą dla kontroli sądowej mogłoby być powołanie (wskazanie) niezależnego organu, o charakterze zewnętrznym w stosunku do podmiotów posiadających uprawnienia do sięgania po dane telekomunikacyjne. Takie rozwiązanie, jak się wydaje, jest zgodne zarówno z przepisami Konstytucji RP, jak i Konwencji. Jego usytuowanie i skład powinny zapewniać niezależność od władzy wykonawczej (w szczególności służb). Kwestia ta jest jednakże elementem szerszego problemu, związanego z nadzorem nad służbami wykonującymi czynności operacyjno-rozpoznawcze. NIK zaplanowała przeprowadzenie w 2013 r. kompleksowej kontroli w tym zakresie[97], dlatego też ewentualne wnioski w zakresie zasad funkcjonowania takiego podmiotu zostaną sformułowane dopiero po jej przeprowadzeniu.

[96] Już sama świadomość kontroli zewnętrznej przyczyniłaby się do ograniczenia ryzyka wykorzystania tego środka niezgodnie z przeznaczeniem.

[97] Kontrola P/13/099 – Realizacja przez organy państwa nadzoru nad służbami prowadzącymi czynności operacyjno-rozpoznawcze.

Ad b) Ustanowienie niezależnego organu powołanego do sprawowania kontroli uprzedniej nad pozyskiwaniem danych telekomunikacyjnych przez uprawnione podmioty musi wiązać się z określeniem zasad (przesłanek) determinujących możliwość wykorzystania tego środka. Kwestia ta została szerzej omówiona w pkt dotyczącym zakresu pozyskiwanych danych telekomunikacyjnych (powyżej). Zdaniem NIK, zadaniem podmiotu powołanego do realizacji kontroli uprzedniej powinna być przede wszystkim ocena zasadności (m.in. w kontekście zasad subsydiarności i proporcjonalności) wniosku o udostępnienie danych telekomunikacyjnych oraz sprawdzenie jego poprawności pod względem formalnym.

Ad 2) Kontrola następcza, czyli realizowana po skierowaniu zapytania w sprawie udostępnienia danych telekomunikacyjnych, miałaby na celu weryfikację poprawności wykorzystania tego środka. W zależności, czy kontrola następcza funkcjonowałaby łącznie z kontrolą uprzednią, czy też samodzielnie, różny musiałby być jej zakres. W tym pierwszym wypadku mogłaby zostać ona ograniczona do kontroli wykorzystania tego środka dowodowego pod kątem przestrzegania obowiązujących procedur, w tym prawidłowości przetwarzania pozyskanych danych, ochrony danych przed ich utratą lub udostępnieniem nieuprawnionym osobom, a także ich niezwłocznym niszczeniem, gdy przestały być niezbędne dla realizacji celu dla którego zostały uzyskane. W drugim przypadku, zakres kontroli musiałby być znacznie szerszy i obejmować również kontrolę zasadności wykorzystania tego środka dowodowego.

Proponowane w przygotowywanej nowelizacji ustawy zmiany, polegające na utworzeniu instytucji pełnomocników ds. ochrony danych osobowych i telekomunikacyjnych w strukturach podmiotów uprawnionych do pozyskiwania i wykorzystywania danych telekomunikacyjnych, wydają się być niewystarczające, dla zapewnienia właściwej kontroli nad wykorzystaniem tego środka. Celem ich jest bowiem zagwarantowanie odpowiedniego poziomu nadzoru i kontroli pozyskiwania i wykorzystywania danych telekomunikacyjnych oraz danych osobowych. Kontrola wewnętrzna, jakkolwiek stanowi ważny element ograniczenia ryzyka wystąpienia nieprawidłowości w funkcjonowaniu jednostki, nie stanowi jednakże instrumentu wystarczającego, nawet przy wyposażeniu pracowników wchodzących w jej skład w atrybuty takie jak gwarancja nieusuwalności z pracy i z pełnionej funkcji bez zgody organu nadzorującego daną instytucję. Bez wprowadzenia instrumentów kontroli zewnętrznej, kontrola nad zakresem wykorzystania tego środka będzie spoczywać nadal de facto w rękach podmiotów uprawnionych do pozyskiwania danych telekomunikacyjnych.

W projekcie przewidziano również zwiększenie nadzoru prokuratury nad działaniami Policji i służb. Miałby być on realizowany poprzez kontrolę materiału zebranego na potrzeby konkretnego postępowania karnego. Należy jednak zauważyć, że kontrola w tym zakresie ograniczona byłaby jedynie do spraw, którym nadano dalszy bieg procesowy. Kontrolą nieobjęty byłby więc cały wachlarz spraw, które z różnych względów, nie zakończyły się skierowaniem aktu oskarżenia.

Ważnym instrumentem kontroli powinno być rozwiązanie, zgodnie z którym informacja o fakcie pozyskania danych telekomunikacyjnych jest przekazywane osobie, której dane zostały udostępnione. W obecnie obowiązującym stanie prawnym pozyskiwanie danych, o których mowa w art. 180c i d ustawy jest wyłączone zarówno spod kontroli samego zainteresowanego (nie jest on powiadamiany o gromadzeniu dotyczących go danych), jak i spod jakiejkolwiek kontroli innej kontroli zewnętrznej. Budzi to wątpliwości, co do zgodności omawianych przepisów z art. 45 ust. 1 i art. 77 ust. 2 Konstytucji. Wyjątkiem są tu przepisy postępowania karnego. Podmioty prowadzące działalność telekomunikacyjną obowiązane są wydać sądowi lub prokuratorowi, na żądanie

zawarte w postanowieniu, dane telekomunikacyjne, jeżeli mają one znaczenie dla toczącego się postępowania (art. 218 § 1 k.p.k.). Postanowienie w tej sprawie doręcza się abonentowi telefonu lub nadawcy, którego dane telekomunikacyjne zostały pozyskane. Doręczenie postanowienia może być odroczone na czas oznaczony, niezbędny ze względu na dobro sprawy, lecz nie później niż do czasu prawomocnego zakończenia postępowania (art. 218 § 2 k.p.k.). Na postanowienie prokuratora przysługuje zażalenie do sądu właściwego do rozpoznania sprawy (art. 465 § 2 k.p.k.). W świetle powyższego, w ramach prowadzonego postępowania karnego wkroczenie w sferę tajemnicy komunikowania się podlega kontroli sądowej[98]. Taka kontrola jest natomiast wyłączona wtedy, gdy ingerencja w ową sferę ma miejsce poza ramami postępowania karnego. W ocenie NIK, należy wprowadzić rozwiązania, zgodnie z którym każdy ma prawo uzyskać informację o pozyskaniu jego danych telekomunikacyjnych (z zastrzeżeniem możliwości odroczenia przekazania tej informacji ze względu na dobro toczącego się postępowania) bez względu na to, w związku z jakim postępowaniem dane te uzyskano. Jakiekolwiek wyjątki od tej zasady powinny być wskazane wprost w ustawie. Należy przy tym jednakże zauważyć, iż wprowadzenie tego instrumentu będzie mogło w pełni osiągnąć swój cel, gdy zostanie utworzony (wskazany) podmiot wyposażony w kompetencje do kontroli prawidłowości działania służb w tym zakresie[99].

Niszczenie danych

Istotnym elementem oceny obecnie obowiązujących rozwiązań jest kryterium niezbędności. Powinno być ono weryfikowane nie tylko, jak już powyżej wskazano, w sytuacji wystąpienia o udostępnienie danych, ale również pod kątem dalszego przechowywania pozyskanych danych. Zgodnie z art. 30 ust. 6 ustawy o Żandarmerii Wojskowej, art. 20c ust. 7 ustawy o Policji oraz art. 10b ust. 6 ustawy o Straży Granicznej pozyskane dane telekomunikacyjne, jeśli nie zawierają informacji mających znaczenie dla postępowania karnego, podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu. Natomiast stosownie do postanowień art. 36b ust. 5 ustawy o kontroli skarbowej, minister właściwy do spraw finansów publicznych nakazuje niezwłoczne, komisyjne i protokolarne zniszczenie danych uzyskanych od podmiotu prowadzącego działalność telekomunikacyjną w przypadku, gdy uzna wystąpienie z wnioskiem o te dane za nieuzasadnione. W odróżnieniu więc do ww. przepisów art. 36b ust. 5 ustawy o kontroli skarbowej nie przewiduje zniszczenia danych, jeśli nie zawierają one informacji mających znaczenie dla prowadzonego przez organy skarbowe postępowania, lecz tylko wtedy, gdy sam wniosek o ich udostępnienie okazał się niezasadny. W związku z tym ustawodawca w tym przypadku w istocie dopuszcza taką sytuację, kiedy sam wniosek o udostępnienie danych był uzasadniony, zaś zgromadzone w wyniku jego realizacji dane nie zostaną zniszczone, pomimo że nie mają one znaczenia z punktu widzenia prowadzonego postępowania.

Natomiast przepisy ustawy o ABW i AW, ustawy o SKW i SWW, a także ustawy o CBA w ogóle nie przewidują obowiązku usunięcia pozyskanych przez nie danych telekomunikacyjnych, gdy przestały być one niezbędne dla prowadzonego postępowania. Należy zwrócić uwagę, że z art. 51 ust. 2 Konstytucji RP wynika zakaz gromadzenia danych innych, niż niezbędne w demokratycznym państwie prawnym. Dane te więc powinny być obligatoryjnie niszczone. W przygotowywanej

[98] Zobacz jednakże uwagi NIK do realizacji tego obowiązku informowania o pozyskaniu danych telekomunikacyjnych opisane w pkt 3.2.10. na str. 54 Informacji.

[99] Należy wspomnieć, że znana jest możliwość tzw. sprawdzania pośredniego przez podmiot zaufania publicznego, który po fakcie zawiadamia zainteresowanego, że jego dane gromadzono.

nowelizacji przepisów proponuje się wprowadzenie w ustawach określających kompetencje podmiotów uprawnionych do pozyskiwania i wykorzystywania danych telekomunikacyjnych – w tych, w których jeszcze nie przewidziano takiej regulacji – obowiązku niezwłocznego, protokolarnego i komisyjnego niszczenia pozyskanych danych telekomunikacyjnych, które nie zawierają dowodów potwierdzających zaistnienie przestępstwa. Powyżej opisany obowiązek niszczenia danych nie będzie dotyczył informacji istotnych dla bezpieczeństwa państwa. Decyzję o zachowaniu danych istotnych dla bezpieczeństwa państwa miałby podejmować odpowiednio upoważniony członek kierownictwa służby.
W ocenie NIK, konieczne jest pilne wprowadzenie przepisów w zakresie obowiązku niszczenia zbędnych danych telekomunikacyjnych będących w posiadaniu służb. Przepisy powinny nie tylko określić sam obowiązek niszczenia danych, ale również precyzować tryb i sposób jego realizacji. Powinny również definiować (bezpośrednio lub poprzez odesłanie do innych przepisów) pojęcie „informacji istotnych dla bezpieczeństwa państwa".

Sprawozdawczość

Wiarygodne dane jakościowe i ilościowe mają zasadnicze znaczenie dla wykazania konieczności i wartości środków bezpieczeństwa, takich jak zatrzymywanie danych. Dlatego konieczne jest opracowanie nadających się do praktycznego stosowania wskaźników pomiarowych oraz procedur sprawozdawczych, które umożliwiają przejrzyste i rzeczowe monitorowanie zatrzymywania danych, i które nie nakładają nadmiernych obciążeń na systemy wymiaru sprawiedliwości w sprawach karnych oraz organy ścigania. Należy zwrócić uwagę, iż Komisja Europejska rozważa wprowadzenie obowiązku szczegółowego raportowania – czyli rozliczania się przez państwa (i ich służby) z tego, w jakich celach, jak często i z jaki skutkiem retencja danych jest stosowana.

Jak wykazała kontrola NIK, funkcjonujący obecnie system gromadzenia informacji o pozyskiwaniu danych retencyjnych nie zapewnia rzetelnej informacji o liczbie tego rodzaju przypadków[100]. Brak jest precyzyjnie określonych wskaźników pomiarowych, a ustanowione procedury nie zapobiegają wystąpieniu rażących błędów. Również zakres gromadzonych danych sprawozdawczych nie pozwala na ocenę, dla jakich celów, jak często i z jakim skutkiem retencja danych jest wykorzystywana. Przygotowywany projekt zmian przewiduje nałożenie na wszystkie podmioty uprawnione do pozyskiwania i wykorzystywania danych telekomunikacyjnych obowiązku sprawozdawczego w zakresie opracowywania i podawania do publicznej wiadomości do końca stycznia danego roku statystyk przetwarzanych danych telekomunikacyjnych. Statystyki obejmowałyby w szczególności:

- liczbę przypadków, w których uprawnione organy uzyskiwały od przedsiębiorców telekomunikacyjnych wyłącznie dane osobowe użytkownika;
- liczbę przypadków (rozumianych jako liczbę numerów telefonicznych lub numerów IP), w których uprawnione organy uzyskiwały dane telekomunikacyjne (z wyłączeniem ustaleń danych abonenckich);
- łączną liczbę przypadków, w których wniosek uprawnionego podmiotu nie mógł być zrealizowany (w rozbiciu na 2 ww. kategorie);
- liczbę osób, których dane telekomunikacyjne były pozyskiwane i wykorzystywane przez uprawnione organy (z wyłączeniem ustaleń danych abonenckich).

[100] Kwestia ta została szczegółowo omówiona w pkt 3.2.8. Informacji na str. 48.

W ocenie NIK, proponowane zmiany, jakkolwiek stanowiące znaczny postęp w stosunku do obecnie obowiązujących rozwiązań, nie są wystarczające. Dla oceny funkcjonowania systemu retencji danych niezbędne jest gromadzenie również danych na temat rodzaju spraw, w których środek ten wykorzystywano oraz o jego skuteczności.

3.3 Dobre praktyki

Najwyższa Izba Kontroli, mając na celu propagowanie dobrych praktyk, zwróciła uwagę na niżej przedstawione rozwiązanie, którego zastosowanie w innych służbach może przyczynić się do poprawy realizacji zadań w zakresie pozyskiwania i przetwarzania danych telekomunikacyjnych.

Pozyskiwanie danych od operatorów za pośrednictwem wyspecjalizowanej komórki

Pozyskiwania danych od operatorów za pośrednictwem innej komórki, niż komórka merytoryczna, tj. komórki pośredniczącej, znacznie ogranicza ryzyko związane z nieuprawnionym lub niecelowym pozyskiwaniem danych telekomunikacyjnych. Rozwiązania takie wdrożyła Żandarmeria Wojskowa i Ministerstwo Finansów. Natomiast w przypadku pozostałych jednostek kontrolowanych, oprócz komórki pośredniczącej, zapytania mogą również kierować upoważnieni pracownicy komórek merytorycznych.

Rozwiązanie polegające na pozyskiwaniu danych za pośrednictwem jednostek „wsparcia", w sposób istotny redukuje ryzyko wystąpienia nieprawidłowości. Dokonanie ustaleń wymaga w tym wypadku przekazania zapytania jednostce „wsparcia", w której jest ono dodatkowo weryfikowane pod względem zgodności z obowiązującymi przepisami. Rozwiązanie takie znacznie ogranicza ryzyko nadużycia kompetencji przez osoby prowadzące postępowanie, bądź naruszenia obowiązujących w tym zakresie przepisów. Potwierdzają to ustalenia kontroli np. w centrali CBA, zgodnie z którymi Biuro Techniki Operacyjnej (BTO) – jednostka wsparcia – kieruje zapytanie do operatora dopiero po uprzedniej weryfikacji wniosku o dokonanie ustaleń telekomunikacyjnych i usunięciu przez komórkę wnioskującą braków lub uchybień. Należy podkreślić, iż dokonywanie ustaleń telekomunikacyjnych przez służby stanowi znaczną ingerencję w sferę praw i wolności obywatelskich. Obejmują one, bowiem nie tylko ustalenie danych abonenta, ale zazwyczaj również wykazy połączeń, czy szczegółowe informacje o miejscach pobytu. Biorąc pod uwagę powyższe uwarunkowania, przestrzeganie zasady rozdzielenia kluczowych kompetencji stanowi istotny element kontroli procesu pozyskiwania danych telekomunikacyjnych przez uprawnione służby. Jak pokazuje praktyka, wprowadzenie komórki pośredniczącej w dokonywaniu zapytań, nie tylko pozwala wyeliminować szereg nieprawidłowości w zapytaniach, ale niejednokrotnie pozwala skrócić czas na uzyskanie żądanych danych, zmniejszając ryzyko odmowy przekazania danych przez operatora ze względów formalnych. Należy przy tym zauważyć, iż jego realizacja nie wymaga poniesienia dodatkowych nakładów, czy wprowadzenia szeroko zakrojonych zmian organizacyjnych, a w sposób istotny ogranicza ryzyko wystąpienia nieprawidłowości.

W ocenie NIK, celowe byłoby wdrożenie analogicznych rozwiązań we wszystkich podmiotach pozyskujących dane telekomunikacyjne[101]. W przypadku Sądów i Prokuratur nie ma wprawdzie

[101] Należałoby tu jednak przewidzieć wyjątek dla „biur spraw wewnętrznych", które ze względu na charakter realizowanych zadań, wymagających zachowania najwyższego stopnia poufności prowadzonych w stosunku do innych funkcjonariuszy postępowań oraz niewielką liczbę kierowanych zapytań, powinny pozyskiwać dane telekomunikacyjne z pominięciem „jednostek wsparcia", przy zachowaniu jednakże odpowiednich procedur wewnętrznych w zakresie kontroli i nadzoru nad realizowanym zadaniami.

możliwości kontroli merytorycznej wniosków (również w podmiotach stosujących to rozwiązanie jest to kontrola zasadniczo o charakterze formalnym), jednakże jak pokazuje wysoki wskaźnik odmów udostępnienia danych telekomunikacyjnych przez operatorów ze względów formalnych (szczególnie dotyczy to Sądów), wprowadzenie zbliżonych rozwiązań organizacyjnych ułatwiłoby sędziom i prokuratorom prawidłową realizację zadań w tym zakresie.

4 INFORMACJE DODATKOWE

4.1 Przygotowanie kontroli

Organizacja kontroli

Najwyższa Izba Kontroli nie przeprowadzała dotychczas kontroli organów, służb i formacji mogących pozyskiwać dane telekomunikacyjne. Kontrolę planową poprzedziła analiza obowiązujących przepisów, dokumentów otrzymanych od podmiotów pozyskujących dane telekomunikacyjne, a także od operatorów telekomunikacyjnych.
Kontrolę planową przeprowadzili kontrolerzy z Departamentów Porządku i Bezpieczeństwa Wewnętrznego NIK, Obrony Narodowej, Budżetu i Finansów oraz Delegatur NIK w Bydgoszczy, Katowicach, Rzeszowie, Szczecinie i Wrocławiu.
Szczegółowy wykaz jednostek kontrolujących i kontrolowanych zamieszczono w zał. nr 5.1 na str. 76 Informacji.

Metodyka prowadzenia kontroli

Kontrola została w całości przeprowadzona wg nowej procedury kontrolnej, wprowadzonej ustawą o zmianie ustawy o Najwyższej Izbie Kontroli oraz związanymi z nią przepisami wykonawczymi. Część dokumentacji postępowania kontrolnego, w tym wystąpienie pokontrolne dotyczące ABW jest niejawna.

Postępowanie kontrolne zostało poprzedzone pozyskaniem od 8 największych operatorów telekomunikacyjnych baz danych dotyczących zapytań o dane telekomunikacyjne. Bazy te, po zanonimizowaniu danych zostały wykorzystane do badania rzetelności rejestrów prowadzonych przez poszczególne podmioty kontrolowane. Ogółem próbę kontrolną stanowiło 2413 wniosków o przekazanie danych telekomunikacyjnych. Ponadto badaniu poddano zbiór dokumentów/zapisów ujętych w ewidencji, dotyczących żądania udostępnienia danych telekomunikacyjnych przez kontrolowaną jednostkę w okresie od 1 stycznia 2011 r. do 30 czerwca 2012 r.[102]

Kontroli w zakresie pozyskiwania danych telekomunikacyjnych podlegały m.in.: regulaminy i inne akty prawa wewnętrznego regulujące kwestie pozyskania tych danych; wytworzona w związku z dokonywaniem zapytań o ww. dane dokumentacja; instrukcje, procedury i inne dokumenty opisujące funkcjonowanie systemów teleinformatycznych służących pozyskiwaniu danych telekomunikacyjnych; procedury zabezpieczenia i niszczenia zbędnych danych. Kontroli nie podlegała dokumentacja prowadzonych czynności operacyjno-rozpoznawczych. Z badania wyłączono również dokumenty wchodzące w skład toczących się postępowań sądowych lub prokuratorskich.

4.2 Postępowanie kontrolne i działania podjęte po zakończeniu kontroli

Postępowanie kontrolne

Postępowania kontrolne zostały przeprowadzone w poszczególnych jednostkach w okresie od 5 września do 21 grudnia 2012 r.

[102] Badaniami obejmowano całą populację lub w przypadku populacji zawierających dużą liczbę żądań wielkość próby ustalano od 150 do 300 dokumentów/zapisów wybranych z zastosowaniem metod statystycznych.

Działania podjęte po zakończeniu kontroli

Po kontroli, w 17 wystąpieniach pokontrolnych skierowanych do kierowników kontrolowanych jednostek zawarto oceny kontrolowanej działalności, w tym: 12 ocen pozytywnych, 4 oceny pozytywne, pomimo stwierdzonych nieprawidłowości oraz 1 ocenę negatywną. Oceny te zostały wydana w oparciu o badanie strony organizacyjno-formalnej uzyskiwania przez uprawnione podmioty danych telekomunikacyjnych – ze względu na ograniczenia ustawowe kompetencji kontrolnych NIK, przedmiotem kontroli nie mogła być ocena zasadności pozyskiwania przez uprawnione podmioty danych telekomunikacyjnych. Ponadto, formułując oceny, NIK uwzględniła, iż obowiązujące przepisy w sposób nieprecyzyjny regulują kwestie związane z pozyskiwaniem danych telekomunikacyjnych. W przypadku kontrolowanych jednostek terenowych, ich kierownicy, działając w zhierarchizowanej strukturze swoich służb i formacji, realizowali zadania postawione przez przełożonych, mając ograniczone uprawnienia decyzyjne. Wewnętrzne akty prawne oraz stosowane rozwiązania informatyczne były wprowadzane centralnie, co istotnie rzutowało na swobodę decyzji kierowników jednostek kontrolowanych, a tym samym zakres ich odpowiedzialności za stwierdzone nieprawidłowości – kwestia ta nie mogło pozostać bez wpływu na formułowane oceny.

Szczegółowe zestawienie ustaleń i ocen kontrolowanych jednostek zawarto w zał. nr 5.3 na str. 80 Informacji.

Zastrzeżenia do wystąpienia pokontrolnego zgłosili: Szef CBA oraz Prezes UKE. Zastrzeżenia Prezesa UKE zostały, z przyczyn formalnych, oddalone przez Prezesa NIK[103]. Łącznie, z 12 zgłoszonych przez Szefa CBA zastrzeżeń, Kolegium NIK uwzględniło częściowo jedno.

W 17 wystąpieniach pokontrolnych skierowanych do kierowników skontrolowanych jednostek sformułowano łącznie 34 wnioski pokontrolne zmierzające do wyeliminowania stwierdzonych nieprawidłowości. Wszyscy adresaci wystąpień pokontrolnych poinformowali Najwyższą Izbę Kontroli o zrealizowaniu wniosków pokontrolnych, bądź o podjęciu działań celem ich realizacji. Na szczególne podkreślenie zasługuje podjęcie przez Prezesa Sądu Okręgowego w Bydgoszczy, w ramach posiadanych przez siebie kompetencji, kompleksowych działań w celu zapobieżenia występowania naruszeń przepisów w zakresie pozyskiwania danych telekomunikacyjnych również w stosunku do sądów rejonowych funkcjonujących na terenie podległego mu okręgu.

[103] Zostały złożone po upływie terminu ustawowego.

5.1. Wykaz podmiotów objętych kontrolą oraz jednostek organizacyjnych NIK, które przeprowadziły kontrolę

Lp.	Wyszczególnienie	Jednostka kontrolująca
1.	Agencja Bezpieczeństwa Wewnętrznego	Departament Porządku i Bezpieczeństwa Wewnętrznego
2.	Centralne Biuro Antykorupcyjne	
3.	Komenda Główna Policji	
4.	Komenda Główna Straży Granicznej	
5.	Prokuratura Okręgowa w Warszawie	
6.	Sąd Okręgowy w Warszawie	
7.	Urząd Komunikacji Elektronicznej	
8.	Służba Kontrwywiadu Wojskowego	Departament Obrony Narodowej
9.	Komenda Główna Żandarmerii Wojskowej	
10.	Ministerstwo Finansów	Departament Budżetu i Finansów
11.	Sąd Okręgowy w Bydgoszczy	Delegatura NIK w Bydgoszczy
12.	Prokuratura Okręgowa w Katowicach	Delegatura NIK w Katowicach
13.	Komenda Wojewódzka Policji w Katowicach	
14.	Sąd Okręgowy w Szczecinie	Delegatura NIK w Szczecinie
15.	Prokuratura Okręgowa we Wrocławiu	Delegatura NIK we Wrocławiu
16.	Komenda Wojewódzka Policji we Wrocławiu	
17.	Prokuratura Okręgowa w Rzeszowie	Delegatura NIK w Rzeszowie
18.	Komenda Wojewódzka Policji w Rzeszowie	

5.2. Wykaz osób zajmujących w latach 2010–2012 stanowiska kierownicze w kontrolowanych jednostkach[104]

Lp.	Wyszczególnienie	Osoby odpowiedzialne za kontrolowaną działalność w latach 2010–2012
1.	Agencja Bezpieczeństwa Wewnętrznego w Warszawie	Szef – generał brygady Krzysztof Bondaryk 1 grudnia 2007 r. – 15 stycznia 2013 r.
2.	Centralne Biuro Antykorupcyjne	Szef: – Paweł Wojtunik 13 września 2009 r. – nadal
3.	Komenda Główna Policji w Warszawie	Komendanci: – nadinspektor Marek Działoszyński 10 stycznia 2012 r. – nadal – generalny inspektor Andrzej Matejuk 6 marca 2008 r. – 9 stycznia 2012 r.
4.	Komenda Wojewódzka Policji w Katowicach	Komendant – nadinspektor Dariusz Działo 9 lutego 2012 r. – nadal – nadinspektor Dariusz Biel od 2008 r. – 8 lutego 2012 r.
5.	Komenda Wojewódzka Policji w Rzeszowie	Komendant – inspektor Zdzisław Stopczyk 14 lutego 2012 r. – nadal – nadinspektor Józef Gdański od 2008 r. – 13 lutego 2012 r.
6.	Komenda Wojewódzka Policji we Wrocławiu	Komendanci: – nadinspektor Dariusz Biel 9 lutego 2012 r. – luty 2013 r. – nadinspektor Zbigniew Maciejewski od 2008 r. – 6 lutego 2012 r.
7.	Służba Kontrwywiadu Wojskowego	Szef: – generał brygady Janusz Nosek 20 maja 2008 r. – nadal
8.	Komenda Główna Straży Granicznej	Komendanci: – generał brygady SG Dominik Tracz 11 kwietnia 2012 r. – nadal – generał brygady SG Leszek Elas 17 stycznia 2008 r. – 10 kwietnia 2012 r.
9.	Komenda Główna Żandarmerii Wojskowej	Komendant – generał dywizji Mirosław Rozmus 17 grudnia 2010 r. – nadal
10.	Ministerstwo Finansów	Minister Finansów Jan Vincent-Rostowski 16 listopada 2007 r. – nadal
11.	Sąd Okręgowy w Bydgoszczy	Prezes Sądu – sędzia sądu okręgowego Danuta Flinik od 2009 r. – nadal
12.	Sąd Okręgowy w Szczecinie	Prezes Sądu – sędzia sądu apelacyjnego Halina Zarzeczna 1 lipca 2011 r. – nadal – sędzia sądu okręgowego Henryk Sobociński 1 lipca 2005 r. – 30 czerwca 2011 r.
13.	Sąd Okręgowy w Warszawie	Prezes Sądu – sędzia sądu okręgowego Małgorzata Kluziak 12 września 2011 r. – nadal – sędzia sądu okręgowego Małgorzata Kosicka 8 sierpnia 2011 r. – 11 września 2011 r. – sędzia sądu okręgowego Beata Waś 1 stycznia 2011 r. – 8 sierpnia 2011 r.
14.	Prokuratura Okręgowa w Katowicach	Prokurator Okręgowy w Katowicach Krzysztof Kołaczek 7 października 2010 r. – nadal
15.	Prokuratura Okręgowa w Rzeszowie	Prokurator Okręgowy w Rzeszowie Bogdan Gunia 28 października 2010 r. – nadal
16.	Prokuratura Okręgowa w Warszawie	Prokurator Okręgowy w Warszawie Ryszard Rogatko 14 grudnia 2010 r. – nadal
17.	Prokuratura Okręgowa we Wrocławiu	Prokurator Okręgowy we Wrocławiu Katarzyna Boć-Orzechowska 21 lutego 2008 r. – nadal
18.	Urząd Komunikacji Elektronicznej	Prezes: Magdalena Gaj 7 lutego 2012 r. – nadal Anna Streżyńska 14 stycznia 2006 r. – 6 lutego 2012 r.

[104] Aktualizacja na 31 grudnia 2012 r.

5.3. Zasadnicze ustalenia kontroli i oceny jednostek[105]

Lp.	Jednostka	Zasadnicze ustalenia kontroli	Ocena[105]
1.	Agencja Bezpieczeństwa Wewnętrznego	Działalność ABW w zakresie uzyskiwania i przetwarzania przez nie danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180c i d ustawy Prawo telekomunikacyjne została oceniona pozytywnie. Stwierdzone uchybienia dotyczyły braku skutecznej reakcji ABW na fakt otrzymywania od operatorów danych telekomunikacyjnych w szerszym zakresie, niż wynikało to ze stosownego zapytania.	pozytywna
2.	Centralne Biuro Antykorupcyjne	Zasady uzyskiwania i przetwarzania w CBA danych, o których mowa w art. 180c i d Prawa telekomunikacyjnego były prawidłowo unormowane. Pozyskane dane zostały zabezpieczone przed nieuprawnionym dostępem lub zniszczeniem. Zapewniono także poufność przekazywania danych pomiędzy uprawnionymi komórkami organizacyjnymi CBA. Nieprawidłowości dotyczyły pozyskiwania danych za pośrednictwem sieci telekomunikacyjnej i systemów teleinformatycznych oraz naruszenia obowiązujących przepisów wewnętrznych, przy udzielaniu upoważnień do występowania o udostępnienie danych telekomunikacyjnych. Stwierdzono również, że Szef CBA nie posiadał informacji niezbędnych dla zapewnienia rzetelnego nadzoru nad pozyskiwaniem danych telekomunikacyjnych w przypadku zapytań kierowanych za pomocą systemów teleinformatycznych.	pozytywna, pomimo stwierdzonych nieprawidłowości
3.	Komenda Główna Policji	W KGP prawidłowo uregulowano sposób udzielania pisemnych upoważnień do uzyskiwania danych telekomunikacyjnych oraz zapewnił nadzór nad ich pozyskiwaniem i przetwarzaniem. Pozyskane dane zostały prawidłowo zabezpieczone przed nieuprawnionym dostępem. Zapewniono także poufność przekazywania danych pomiędzy uprawnionymi komórkami organizacyjnymi KGP. Nieprawidłowości dotyczyły pozyskiwania danych za pośrednictwem sieci telekomunikacyjnej i systemów teleinformatycznych oraz usuwania zbędnych danych telekomunikacyjnych. NIK zwróciła również uwagę na brak odpowiednich procedur wewnętrznych, które zapobiegłyby wystąpieniu nieprawidłowości lub pozwoliłyby na bieżąco je eliminować.	pozytywna, pomimo stwierdzonych nieprawidłowości
4.	Komenda Wojewódzka Policji w Katowicach	Prawidłowo sformułowano wewnętrzne uregulowania i utworzono odpowiednie struktury organizacyjne w obszarze pozyskiwania i przetwarzania danych telekomunikacyjnych. Przestrzegano obowiązujące przepisy w zakresie uzyskiwania, przetwarzania i niszczenia danych telekomunikacyjnych.	pozytywna
5.	Komenda Wojewódzka Policji w Rzeszowie	W KWP działania dotyczące uzyskiwania, przetwarzania, wykorzystania i niszczenia były prowadzono w sposób zapewniający bezpieczeństwo, poufność, oraz integralność i rozliczalność pozyskanych danych.	pozytywna

[105] Przy formułowaniu oceny realizacji zadań przez kierowników jednostek terenowych ABW, Policji i Straży Granicznej uwzględniono ich ograniczone kompetencje wynikające z funkcjonowania w formacji scentralizowanej.

Lp.	Jednostka	Zasadnicze ustalenia kontroli	Ocena[105]
6.	Komenda Wojewódzka Policji we Wrocławiu	Zasady uzyskiwania i przetwarzania danych telekomunikacyjnych zostały w sposób prawidłowy uregulowane aktami wewnętrznymi. Pozyskane dane zostały prawidłowo zabezpieczone przed nieuprawnionym dostępem. Nie stwierdzono nieprawidłowości dotyczących pozyskiwania, przetwarzania i niszczenia danych. Zapewniono także poufność przekazywania danych pomiędzy uprawnionymi komórkami organizacyjnymi KGP. NIK zwróciła uwagę na niespójności w uregulowaniach wewnętrznych dotyczące zatwierdzania wniosków o stosowanie technicznych środków wsparcia.	pozytywna
7.	Służba Kontrwywiadu Wojskowego	Zasady pozyskiwania i przetwarzania danych telekomunikacyjnych w SKW były prawidłowo uregulowane aktami wewnętrznymi. Pozyskane dane były zabezpieczone przed nieuprawnionym dostępem, zapewniono także poufność ich przekazywania pomiędzy uprawnionymi komórkami organizacyjnymi SKW.	pozytywna
8.	Komenda Główna Straży Granicznej	System uzyskiwania i przetwarzania danych telekomunikacyjnych był prawidłowo zorganizowany. Ustanowiono zabezpieczenia techniczne i organizacyjne uniemożliwiające wykorzystanie danych telekomunikacyjnych niezgodnie z celem ich uzyskania, ustalono środki zaradcze w celu eliminacji ryzyka wystąpienia zdarzeń niepożądanych, określono procedury niszczenia danych telekomunikacyjnych nie mających znaczenia dla postępowania karnego. Uchybienia dotyczyły braku rejestru osób upoważnionych do uzyskiwania danych za pomocą sieci telekomunikacyjnej, nieokreślenia zadań w zakresie pozyskiwania danych telekomunikacyjnych w regulaminach wewnętrznych niektórych komórek organizacyjnych i zakresach obowiązków funkcjonariuszy. Stwierdzono również pojedyncze przypadki naruszenia obowiązujących przepisów i procedur. NIK zwróciła ponadto uwagę, na konieczność zapewnienia zewnętrznego, w stosunku do komórek organizacyjnych wnioskujących i realizujących zapytania o dane telekomunikacyjne, nadzoru i kontroli nad realizacją przez poszczególnych funkcjonariuszy uprawnień związanych z uzyskiwaniem i przetwarzaniem danych telekomunikacyjnych.	pozytywna
9.	Komenda Główna Żandarmerii Wojskowej	Przyjęte w Komendzie Głównej Żandarmerii Wojskowej rozwiązania organizacyjno-prawne oraz techniczne zapewniały bezpieczeństwo pozyskiwania i przetwarzania danych telekomunikacyjnych. Stosowany tryb postępowania z pozyskanymi danymi telekomunikacyjnymi eliminował ryzyko wystąpienia zdarzeń niepożądanych w zakresie nieuprawnionego dostępu do danych telekomunikacyjnych.	pozytywna
10.	Ministerstwo Finansów	Zasady uzyskiwania i przetwarzania danych, o których mowa w art. 180c i d Prawa telekomunikacyjnego zostały w sposób prawidłowy uregulowane aktami wewnętrznymi. Pozyskane dane zostały zabezpieczone przed nieuprawnionym dostępem lub zniszczeniem. Zapewniono także poufność przekazywania danych pomiędzy uprawnionymi komórkami organizacyjnymi.	pozytywna

Lp.	Jednostka	Zasadnicze ustalenia kontroli	Ocena[105]
11.	Sąd Okręgowy w Bydgoszczy	Administracyjno-organizacyjna działalność sądu w zakresie uzyskiwania i przetwarzania danych telekomunikacyjnych oceniona została pozytywnie. Wszystkie uzyskane dane telekomunikacyjne zabezpieczone były poprzez wyłączenie ich z akt spraw, których dotyczyły. Stwierdzono przypadki odmowy udostępnienia danych przez operatorów z uwagi na brak podstawy od sformułowania takiego żądania. NIK zwróciła ponadto uwagę na brak odrębnej ewidencji spraw i zapytań z jakimi występowano do operatorów, co powodowało trudności w ustaleniu ich ogólnej liczby i przebiegu procesu pozyskiwania tych danych.	pozytywna
12.	Sąd Okręgowy w Szczecinie	Administracyjno-organizacyjna działalność sądu w zakresie uzyskiwania i przetwarzania danych telekomunikacyjnych oceniona została pozytywnie. Wszystkie uzyskane dane telekomunikacyjne zabezpieczone były poprzez wyłączenie ich z akt spraw, których dotyczyły. Stwierdzono przypadki kierowania wniosków o udostępnienie danych telekomunikacyjnych w sprawach cywilnych, bez uzyskania uprzednio zgody abonenta; wskazywania niewłaściwych przepisów, jako podstawy udostępnienia danych telekomunikacyjnych; żądania treści sms-ów oraz powoływania się na przepisy postępowania karnego w sprawach cywilnych; występowania o dane telekomunikacyjne za okres przekraczający 24 miesiące, odmowy udostępnienia przez operatorów danych telekomunikacyjnych, ze względu na brak podstawy prawnej do takiego wystąpienia i uchylenia tajemnicy telekomunikacyjnej lub na niewykonalność postanowienia Sądu z innych formalno-prawnych przyczyn; nie realizowania obowiązku informacyjnego, w stosunku do osób, których dane telekomunikacyjne pozyskiwano.	pozytywna
13.	Sąd Okręgowy w Warszawie	Kontrola nie została zakończona – po stwierdzeniu przez kontrolę niezgodności prezentowanych danych ze stanem faktycznym, Prezes Sądu uniemożliwiła dalsze prowadzenie czynności kontrolnych, powołując się na zasadę niezawisłości sędziowskiej.	-
14.	Prokuratura Okręgowa w Katowicach	Prokurator Okręgowy określił zasady bezpieczeństwa oraz organizacji pracy przy uzyskiwaniu danych telekomunikacyjnych oraz zapewnił przekazywanie prokuratorom danych telekomunikacyjnych udostępnionych za pomocą systemu teleinformatycznego zgodnie z treścią wydanych przez nich postanowień. Nieprawidłowości dotyczyły wydawania zarządzeń o doręczeniu postanowień i doręczania postanowień z naruszeniem terminu określonego w art. 218 § 2 zd. 2 ustawy z dnia 6 czerwca 1997 r. Kodeks postępowania karnego.	pozytywna, pomimo stwierdzonych nieprawidłowości
15.	Prokuratura Okręgowa w Rzeszowie	Obowiązujące w Prokuraturze procedury wewnętrzne dotyczące zabezpieczenia w aktach postępowania przygotowawczego danych telekomunikacyjnych przed ich udostępnieniem osobom nieupoważnionym regulowały wszystkie istotne kwestie, z punktu widzenia realizacji celów dla których dane te są uzyskiwane. Nieprawidłowości dotyczyły przypadków niedoręczania abonentom telefonów postanowień, na podstawie których uzyskano wykaz połączeń z ich telefonów, mimo prawomocnego zakończenia postępowań przygotowawczych.	pozytywna

Lp.	Jednostka	Zasadnicze ustalenia kontroli	Ocena[105]
16.	Prokuratura Okręgowa w Warszawie	Prokurator Okręgowy określił zasady bezpieczeństwa oraz organizacji pracy przy uzyskiwaniu danych telekomunikacyjnych oraz zapewnił przekazywanie prokuratorom danych telekomunikacyjnych udostępnionych za pomocą systemu teleinformatycznego zgodnie z treścią wydanych przez nich postanowień. Nieprawidłowości dotyczyły wydawania zarządzeń o doręczeniu postanowień i doręczania postanowień z naruszeniem terminu określonego w art. 218 § 2 zd. 2 ustawy z dnia 6 czerwca 1997 r. Kodeks postępowania karnego.	pozytywna, pomimo stwierdzonych nieprawidłowości
17.	Prokuratura Okręgowa we Wrocławiu	W Prokuraturze w sposób prawidłowy zorganizowano system pozyskiwania danych telekomunikacyjnych. Dane te uzyskiwano na właściwej podstawie prawnej, wyłącznie przez uprawnione osoby, a ich zabezpieczone przed dostępem osób nieuprawnionych było należyte.	pozytywna
18.	Urząd Komunikacji Elektronicznej	Prezes UKE nie sprawował, pomimo posiadania stosownych kompetencji ustawowych, skutecznego nadzoru nad wywiązywaniem się przez przedsiębiorców telekomunikacyjnych z nałożonych na nich obowiązków. W efekcie opracowywane przez Prezesa UKE informacje w zakresie wykorzystania przez służby danych retencyjnych nie odpowiadały stanowi rzeczywistemu. Stwierdzono również brak nadzoru nad przetwarzaniem i niszczeniem danych retencyjnych.	negatywna

5.4. Charakterystyka obszaru objętego kontrolą

5.4.1. Charakterystyka stanu prawnego

Implementacja dyrektywy 2006/24/WE została dokonana poprzez zmianę ustawy Prawo telekomunikacyjne, ustawą z dnia 24 kwietnia 2009 r.[106] Art. 180c ust. 2 znowelizowanej ustawy zawiera upoważnienie dla ministra właściwego do spraw łączności, działającego w porozumieniu z ministrem właściwym do spraw wewnętrznych, do określenia w drodze rozporządzenia szczegółowego wykazu danych, które zgodnie z treścią ustawy podlegają retencji[107] przez operatorów telekomunikacyjnych oraz rodzajów operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do zatrzymywania i przechowywania tych danych. Wzmiankowane rozporządzenie zostało wydane przez Ministra Infrastruktury w dniu 28 grudnia 2009 r.[108], z datą wejścia w życie od 1 stycznia 2010 r. Zgodnie z art. 180a Prawa telekomunikacyjnego, na operatorze publicznej sieci telekomunikacyjnej oraz dostawcy publicznie dostępnych usług telekomunikacyjnych ciąży obowiązek zatrzymywania i przechowywania przez okres 12 miesięcy[109] danych o ruchu w sieciach telekomunikacyjnych (art. 180c Prawa telekomunikacyjnego) w celu zapobiegania, dochodzenia, wykrywania i ścigania przestępstw.

Dostawcą usług, zgodnie z definicją sformułowaną w art. 2 pkt 27 Prawa telekomunikacyjnego, jest przedsiębiorca, jak też inny podmiot uprawniony do wykonywania działalności gospodarczej na podstawie odrębnych przepisów, świadczący usługi telekomunikacyjne, a więc usługi polegające głównie na przekazywaniu sygnałów w sieci telekomunikacyjnej. Operatorem natomiast jest przedsiębiorca lub inny podmiot uprawniony do wykonywania działalności gospodarczej na podstawie odrębnych przepisów, uprawniony do dostarczania publicznych sieci telekomunikacyjnych lub udogodnień towarzyszących. Oznacza to, że obowiązek zachowywania danych ciąży również na podmiotach świadczących różnego rodzaju usługi telekomunikacyjne, w szczególności usługę bezprzewodowego dostępu do Internetu (tzw. WLAN-Hotspots)[110].

Należy zauważyć, że podmioty, o których mowa art. 180a Prawa telekomunikacyjnego zostały zobowiązane na własny koszt zarówno zatrzymywać i przechowywać ww. dane, udostępniać je uprawnionym podmiotom, jak również je chronić.[111]Jednocześnie podmioty te zostały

[106] Ustawa z dnia 24 kwietnia 2009 r. o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw (Dz. U. Nr 85, poz. 716).

[107] Retencja danych sprowadza się do obowiązku zapisywania przez dostawców ogólnie dostępnych usług łączności elektronicznej lub publicznych sieci łączności, przez określony czas (od 6 miesięcy do dwóch lat), danych niezbędnych do ustalenia źródła połączenia; danych niezbędnych do ustalenia odbiorcy połączenia; danych niezbędnych do określenia daty, godziny i czasu trwania połączenia; danych niezbędne do określenia rodzaju połączenia; dane niezbędne do określenia narzędzia komunikacji lub tego, co może służyć za narzędzie komunikacji; danych niezbędnych do identyfikacji lokalizacji urządzenia komunikacji ruchomej. Obowiązek ten wynika z dyrektywy 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r., zwanej też *dyrektywą w sprawie retencji danych telekomunikacyjnych*.

[108] Rozporządzenie Ministra Infrastruktury z dnia 28 grudnia 2009 r. w sprawie szczegółowego wykazu danych oraz rodzajów operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do ich zatrzymywania i przechowywania (Dz. U. Nr 226, poz. 1828).

[109] Do 21 stycznia 2013 obowiązywał 24 miesięczny okres retencji danych.

[110] M. Siwicki, Retencja danych transmisyjnych na podstawie art. 180a Prawa telekomunikacyjnego, Prokuratura i Prawo, Nr 9/2011, str. 112 i nast.

[111] Zob. postanowienie Sądu Najwyższego z dnia 25 marca 2010 r. (sygn. I KZP 37/09) oraz rozporządzenie Prezesa Rady Ministrów z dnia 22 marca 2010 r. w sprawie sposobu przekazywania i udostępniania danych w przypadku ogłoszenia upadłości operatora publicznej sieci telekomunikacyjnej lub dostawcy publicznie dostępnych usług telekomunikacyjnych (Dz. U. z dnia 29 marca 2010 r.).

zobowiązane do udostępniania wskazanych danych uprawnionym służbom, a także sądowi i prokuratorowi. Nie udzielenie informacji wskazanym służbom, a także sądowi i prokuratorowi podlega karom, o których mowa w art. 209 ust. 1 Prawa telekomunikacyjnego. Może to również skutkować nałożeniem przez prezesa UKE kary pieniężnej na osobę kierującą przedsiębiorstwem telekomunikacyjnym na podstawie art. 209 ust. 2 Prawa telekomunikacyjnego. Kary pieniężne nakładane przez organy regulacji rynku nie mają jednakże charakteru sankcji karnych[112].

Dane, o których mowa w art. 180c Prawa telekomunikacyjnego, to zgodnie z ust. 1 pkt 1 dane niezbędne do: ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego (inicjującego połączenia oraz do którego kierowane jest połączenie) oraz zgodnie z pkt 2 przywołanego przepisu: określenia daty i godziny połączenia oraz czasu jego trwania, rodzaju połączenia, lokalizacji telekomunikacyjnego urządzenia końcowego.

Należy zauważyć, że dane wymienione w treści cytowanego wyżej art. 180c stanowią odwołanie do katalogu definiującego tajemnicę telekomunikacyjną (art. 159 ust. pkt 1 Prawa telekomunikacyjnego), w tym danych precyzujących sposób gromadzenia informacji dotyczących użytkownika (art. 161 i 179 ust. 9 Prawa telekomunikacyjnego) i są danymi osobowymi, w związku z czym podlegają również ochronie na podstawie ustawy o ochronie danych osobowych. Dane osobowe, to według art. 6 ust. 1 ustawy o ochronie danych osobowych wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej[113]. Do danych osobowych zaliczane są przede wszystkim: imię i nazwisko, dane adresowe, wizerunek (zdjęcie), miejsce urodzenia, miejsce zamieszkania. Niewątpliwie art. 180a Prawa telekomunikacyjnego stanowi przesłankę zgodnego z prawem przetwarzania danych osobowych użytkowników końcowych. Jednakże powinna tu znaleźć zastosowanie zasada adekwatności i proporcjonalności przechowywania danych, według której dane należy gromadzić w sposób proporcjonalny i adekwatny do celu, dla jakiego są one gromadzone (art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych). Nieuprawnione gromadzenie danych o charakterze osobowym stanowi według art. 49 ust. 1 ustawy o ochronie danych osobowych czyn przestępczy[114].

Na mocy cytowanej już ustawy z dnia 24 kwietnia 2009 r. nowelizującej Prawo telekomunikacyjne, wprowadzono do ustaw regulujących zadania i kompetencje organów ścigania, właściwych służb oraz jednostek organizacyjnych podległych ministrowi właściwemu do spraw finansów publicznych, niżej wymienione przepisy rozszerzające możliwość uzyskiwania danych identyfikacyjnych abonentów sieci telekomunikacyjnych:

a) art. 218 § 1 k.p.k.;
b) art. 20 c ustawy o Policji;
c) art. 10 b ustawy o Straży Granicznej;

---

112 Por. np. wyrok Sądu Najwyższego z dnia 14 kwietnia 2010 r. (sygn. III SK 1/10).

113 Według tej definicji pojęcie danych osobowych obejmuje zarówno informacje pozwalające na określenie tożsamości konkretnej osoby, jak też informacje, które nie pozwalają na jej natychmiastową identyfikację, ale są przy pewnym nakładzie kosztów, czasu i działań, wystarczające do jej ustalenia. Pojęcie danych osobowych obejmuje zatem zbiór jakichkolwiek informacji umożliwiających identyfikację osoby co do tożsamości. Ocena taka wynika również z Dyrektywy 2002/58/WE z dnia 12 lipca 2002 r. o przetwarzaniu danych osobowych i ochronie prywatności w sektorze komunikacji elektronicznej oraz wzorowanych na tej Dyrektywie przepisów rozdziału 4 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną.

114 Według tego przepisu, kto przetwarza w zbiorze dane osobowe, choć ich przetwarzanie nie jest dopuszczalne, albo do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności, albo pozbawienia wolności do lat 2. W sytuacji, kiedy określony powyżej czyn dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, sprawca podlega grzywnie, karze ograniczenia wolności, albo pozbawienia wolności do lat 3.

d) art. 36b ustawy o kontroli skarbowej;
e) art. 30 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych;
f) art. 28 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu;
g) art. 18 ustawy o Centralnym Biurze Antykorupcyjnym;
h) art. 31 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego.

Podobne zmiany wprowadzono ustawą z dnia 26 maja 2011 r. o zmianie ustawy o grach hazardowych oraz niektórych innych ustaw[115], gdzie został dodany do ustawy o Służbie Celnej art. 75d. Zgodnie z treścią art. 75d ust. 1 ustawy o Służbie Celnej, w celu zapobiegania lub wykrywania przestępstw skarbowych, o których mowa w rozdziale 9 Kodeksu karnego skarbowego (a więc przestępstw skarbowych przeciwko organizacji gier hazardowych), Służbie Celnej mogą być udostępniane dane, o których mowa w art. 180c i art. 180d Prawa telekomunikacyjnego.

Odnosząc się do trybu żądania przez sądy i prokuratury udostępnienia danych, o których mowa w art. 180 c Prawa telekomunikacyjnego, należy stwierdzić, iż kluczowe dla oceny prawnej jest brzmienie § 1 art. 218 k.p.k., który stanowi, iż urzędy, instytucje i podmioty prowadzące działalność w dziedzinie poczty lub działalność telekomunikacyjną, urzędy celne oraz instytucje i przedsiębiorstwa transportowe obowiązane są wydać sądowi i prokuratorowi, na żądanie zawarte w postanowieniu, korespondencję i przesyłki oraz dane, o których mowa w art. 180c i 180d Prawa telekomunikacyjnego.

Żądanie przez uprawnione służby udostępnienia danych, o których mowa w art. 180 c Prawa telekomunikacyjnego wymaga spełnienia określonych przesłanek ustawowych. W szczególności omawiane dane są udostępniane:

a) *w celu zapobiegania lub wykrywania przestępstw* (art. 20c ust. 1 ustawy o Policji oraz art. 10 b ust. 1 ustawy o Straży Granicznej);
b) *w celu zapobiegania lub wykrywania przestępstw skarbowych lub przestępstw, o których mowa w art. 2 ust. 1 pkt 14b, oraz naruszeń przepisów, o których mowa w art. 2 ust. 1 pkt 12*, tj. także w celu zapobiegania i ujawniania przestępstw, o których mowa w art. 228-231 k.k., popełnianych przez osoby zatrudnione lub pełniące służbę w jednostkach organizacyjnych podległych ministrowi właściwemu do spraw finansów publicznych oraz w celu zapobiegania i wykrywania naruszeń krajowych przepisów celnych oraz ścigania naruszeń krajowych lub wspólnotowych przepisów celnych (art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej);
c) *w celu zapobiegania lub wykrywania przestępstw, w tym skarbowych* (art. 30 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych);
d) *w celu realizacji przez ABW zadań, o których mowa w art. 5 ust. 1*, tj. rozpoznawania, zapobiegania i zwalczania zagrożeń godzących w bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny, rozpoznawania, zapobiegania i wykrywania przestępstw określonych w art. 5 ust. 1 pkt 2; realizowania, w granicach swojej właściwości, zadań związanych z ochroną informacji niejawnych oraz wykonywania funkcji krajowej władzy bezpieczeństwa w zakresie ochrony informacji niejawnych w stosunkach międzynarodowych; uzyskiwania, analizowania, przetwarzania i przekazywania właściwym organom informacji mogących mieć istotne znaczenie dla ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego, podejmowania innych działań określonych w odrębnych ustawach i umowach międzynarodowych (art. 28 ust. 1 pkt 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu);

[115] Dz. U. Nr 134, poz. 779, akt wygasł z dniem 15 marca 2012 r.

e) *w celu realizacji przez CBA zadań określonych w art. 2*, tj. w celu: 1) rozpoznawania, zapobiegania i wykrywania przestępstw wymienionych w art. 2 ust. 1 pkt 1, oraz ścigania ich sprawców, 2) ujawniania i przeciwdziałania przypadkom nieprzestrzegania przepisów ustawy o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne, 3) dokumentowania podstaw i inicjowania realizacji przepisów ustawy o zwrocie korzyści uzyskanych niesłusznie kosztem Skarbu Państwa lub innych państwowych osób prawnych, 4) ujawniania przypadków nieprzestrzegania określonymi przepisami prawa procedur podejmowania i realizacji decyzji w przedmiocie: prywatyzacji i komercjalizacji, wsparcia finansowego, udzielenia zamówień publicznych, rozporządzenia mieniem jednostek lub przedsiębiorców oraz przyznawania koncesji, zwolnień, zwolnień podmiotowych i przedmiotowych, ulg, preferencji, kontyngentów, plafonów, poręczeń i gwarancji kredytowych, 5) kontroli prawidłowości i prawdziwości oświadczeń majątkowych lub oświadczeń o prowadzeniu działalności gospodarczej osób pełniących funkcje publiczne, o których mowa w art. 115 § 19 k. k., 6) prowadzenia działalności analitycznej dotyczącej zjawisk występujących w obszarze właściwości CBA oraz przedstawiania w tym zakresie informacji Prezesowi Rady Ministrów, Prezydentowi RP, Sejmowi oraz Senatowi, 7) podejmowania innych działań określonych w odrębnych ustawach i umowach międzynarodowych (art. 18 ust. 1 pkt 1ustawy o Centralnym Biurze Antykorupcyjnym);

f) w celu *realizacji przez SKW zadań określonych w art.* 5, tj.: 1) rozpoznawania, zapobiegania oraz wykrywania popełnionych przez żołnierzy, funkcjonariuszy SKW i SWW oraz pracowników Sił Zbrojnych RP (SZ RP) i innych jednostek organizacyjnych Ministerstwa Obrony Narodowej (MON), przestępstw wymienionych art. 5 ust. 1 pkt 1, 2) realizowania, w granicach swojej właściwości, zadań określonych w przepisach ustawy o ochronie informacji niejawnych, 3) uzyskiwania, gromadzenia, analizowania, przetwarzania i przekazywania właściwym organom informacji mogących mieć znaczenie dla obronności państwa, bezpieczeństwa lub zdolności bojowej Sił Zbrojnych oraz podejmowania działań w celu eliminowania ustalonych zagrożeń, 4) prowadzenia kontrwywiadu radioelektronicznego oraz przedsięwzięć z zakresu ochrony kryptograficznej i kryptoanalizy, 5) uczestniczenia w planowaniu i przeprowadzaniu kontroli realizacji umów międzynarodowych dotyczących rozbrojenia, 6) ochrony bezpieczeństwa jednostek wojskowych i innych jednostek organizacyjnych MON, 7) ochrony bezpieczeństwa badań naukowych i prac rozwojowych, 9) podejmowania innych działań przewidzianych dla Służby Kontrwywiadu Wojskowego (art. 32 ust. 1 pkt 1 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego).

W powołanych wyżej ustawach kompetencyjnych tylko szczątkowo został określony tryb żądania danych telekomunikacyjnych przez uprawnione podmioty. Szczegółowe procedury współpracy uprawnionych podmiotów z operatorami i przedsiębiorcami telekomunikacyjnymi w zakresie udostępnienia danych, o których mowa w art. 180 c, w szczególności środki techniczne i organizacyjne, sposób prowadzenia i zakres dokumentacji, oraz tryb wydawania upoważnień do uzyskiwania danych telekomunikacyjnych, zostały określone w aktach prawa wewnętrznego poszczególnych służb i uprawnionych organów[116].

Przepisy ustawy Prawo telekomunikacyjne określają, że organy administracji łączności, którymi są minister właściwy do spraw łączności (obecnie Minister Administracji i Cyfryzacji) i Prezes Urzędu Komunikacji Elektronicznej prowadzą politykę regulacyjną, mając na celu w szczególności przyczynianie się do zapewnienia wysokiego poziomu ochrony danych osobowych (art. 189 ust. 2

[116] Szczegółowa analiza i porównanie obowiązujących procedur zostanie przeprowadzona w ramach prowadzonej kontroli.

pkt 3 lit. c) oraz zapewnienie integralności i bezpieczeństwa publicznej sieci telekomunikacyjnej (art. 189 ust. 2 pkt 3 lit. f). Prezes UKE, jako centralny organ administracji rządowej, wykonujący zadania z zakresu regulacji i kontroli rynku usług telekomunikacyjnych, jest uprawniony do kontroli przestrzegania przepisów, decyzji i postanowień z zakresu telekomunikacji oraz do nakładania kar pieniężnych.

Przedsiębiorca telekomunikacyjny na podstawie art. 180g ust. 1 Prawa telekomunikacyjnego w terminie do 31 stycznia, składa Prezesowi UKE, za rok poprzedni informacje o:

1) łącznej liczbie przypadków, w których uprawnionym podmiotom, sądowi i prokuratorowi były udostępnione dane, o których mowa w art. 180c ust. 1;
2) czasie, jaki upłynął między datą zatrzymania danych a datą złożenia przez podmioty, o których mowa w pkt 1, wniosku lub ustnego żądania o ich udostępnienie;
3) łącznej liczbie przypadków, w których wniosek lub ustne żądanie, o którym mowa w pkt 2, nie mógł być zrealizowany.

Zgodnie z art. 10 Dyrektywy 2006/24/WE oraz stosownie do postanowień art. 180g ust.2 ustawy Prawo telekomunikacyjne Prezes UKE przygotowuje zbiorcze zestawienie dotyczące żądań udostępnienia danych kierowanych od uprawnionych podmiotów, sądów i prokuratorów do przedsiębiorców telekomunikacyjnych. Jest ono publikowane raz do roku.

5.4.2. Uwarunkowania organizacyjne

Urząd Komunikacji Elektronicznej

Przepisy ustawy Prawo telekomunikacyjne określają m.in., że organy administracji łączności, którymi są minister właściwy do spraw łączności (obecnie Minister Administracji i Cyfryzacji) i Prezes Urzędu Komunikacji Elektronicznej prowadzą politykę regulacyjną, mając na celu w szczególności przyczynianie się do zapewnienia wysokiego poziomu ochrony danych osobowych (art. 189 ust. 2 pkt 3 lit. c) oraz zapewnienie integralności i bezpieczeństwa publicznej sieci telekomunikacyjnej (art. 189 ust. 2 pkt 3 lit. f). Prezes UKE, jako centralny organ administracji rządowej, wykonujący zadania z zakresu regulacji i kontroli rynku usług telekomunikacyjnych, jest uprawniony do kontroli przestrzegania przepisów, decyzji i postanowień z zakresu telekomunikacji oraz do nakładania kar pieniężnych.

Przedsiębiorca telekomunikacyjny na podstawie art. 180g ust. 1 Prawa telekomunikacyjnego w terminie do dnia 31 stycznia, składa Prezesowi UKE, za rok poprzedni informacje o:

1) łącznej liczbie przypadków, w których uprawnionym podmiotom, sądowi i prokuratorowi były udostępnione dane, o których mowa w art. 180c ust. 1;
2) czasie, jaki upłynął między datą zatrzymania danych a datą złożenia przez podmioty, o których mowa w pkt 1, wniosku lub ustnego żądania o ich udostępnienie;
3) łącznej liczbie przypadków, w których wniosek lub ustne żądanie, o którym mowa w pkt 2, nie mógł być zrealizowany.

Agencja Bezpieczeństwa Wewnętrznego

Do kierowania zapytań, celem pozyskania danych telekomunikacyjnych bezpośrednio do operatorów upoważniony był Departament Wsparcia Operacyjno-Technicznego ABW oraz jego odpowiedniki w delegaturach ABW, a także komórki odpowiedzialne za koordynację, analitykę i nadzór Delegaturze Stołecznej, Departamencie Zwalczania Terroryzmu, Departamencie Bezpieczeństwa Wewnętrznego i Audytu oraz Centrum Analiz. Zlecania dotyczące ustaleń

telekomunikacyjnych składały wybrane komórki upoważnionych przez Szefa ABW ośmiu departamentów ABW. Zaakceptowane przez dyrektora departamentu lub upoważnionego wicedyrektora zlecenie kierowane było do komórki realizującej. Po dokonaniu ustalenia przełożony funkcjonariusza dokonującego ustalenia przekazywał odpowiedź do funkcjonariusza zlecającego zapytanie.

Centralne Biuro Antykorupcyjne

Jednostką organizacyjną odpowiedzialną za uzyskiwanie danych telekomunikacyjnych na potrzeby jednostek organizacyjnych usytuowanych w Warszawie oraz w szczególnie uzasadnionych przypadkach, na potrzeby Delegatur CBA, było Biuro Techniki Operacyjnej.[117] W delegaturach CBA za pozyskiwanie danych telekomunikacyjnych, odpowiedzialne były zespoły/sekcje wsparcia lub wydziały operacyjno-śledcze. Ustalenia telekomunikacyjne w trybie art. 18 ust.2 ustawy o CBA dokonywane były na pisemny wniosek szefa CBA lub osoby przez niego upoważnionej, jak również na ustne żądanie funkcjonariusza, realizowane były na podstawie ewidencjonowanych w dziennikach korespondencyjnych zleceń pisemnych. W przypadku uzyskania informacji w trybie zapytania ustnego, sporządzano stosowną notatkę lub adnotację na wniosku. Wyniki sprawdzeń przekazywano za pokwitowaniem osobie upoważnionej w piśmie zlecającym ustalenia, drogą pisemną lub elektroniczną pocztą szyfrowaną.

Policja

Dane telekomunikacyjne w Komendzie Głównej Policji w trybie art. 20c ustawy z dnia 6 kwietnia 1990 r. o Policji, były pozyskiwane przez funkcjonariuszy Centralnego Biura Śledczego KGP, Biura Spraw Wewnętrznych KGP, Biura Wywiadu Kryminalnego KGP oraz Biura Kryminalnego KGP. Dane telekomunikacyjne były pozyskiwane na podstawie pisemnych zleceń komórek organizacyjnych (Wydziałów) wchodzących w skład ww. Biur, które miały w zakresie swojej właściwości określone zadania związane z zapobieganiem lub wykrywaniem przestępstw, a także Biura Międzynarodowej Współpracy Policji KGP. W komendach wojewódzkich Policji za pozyskiwanie danych telekomunikacyjnych, odpowiedzialne były wydziały techniki operacyjnej, wydziały wywiadu kryminalnego. Osobami uprawnionymi, do występowania z żądaniem udostępnienia danych telekomunikacyjnych do operatorów byli policjanci wskazani w pisemnym wniosku Komendanta Głównego Policji lub komendanta wojewódzkiego Policji albo osoby przez nich upoważnione.

Służba Kontrwywiadu Wojskowego

Szef SKW na podstawie art. 20 ust. 2 ustawy o SKW i SWW upoważnił dyrektora Biura Techniki i Obserwacji oraz jego zastępców do występowania w jego imieniu do operatorów o dane telekomunikacyjne. Ponadto do korzystania z elektronicznych baz danych operatorów telekomunikacyjnych upoważnione zostały imiennie osoby z dziewięciu jednostek organizacyjnych SKW realizujących czynności operacyjne. Udostępnianie danych telekomunikacyjnych upoważnionemu funkcjonariuszowi SKW, odbywało się na podstawie porozumień zawartych pomiędzy Szefem SKW a operatorem.

[117] § 7 ust. 2 pkt 10 zarządzenia nr N/6/10 z dnia 26 października 2010 r. w sprawie regulaminu organizacyjnego Biura Techniki Operacyjnej.

Straż Graniczna

Podmiotami uprawnionymi do uzyskiwania i przetwarzania danych telekomunikacyjnych w Komendzie Głównej Straży Granicznej były komórki organizacyjne, które regulaminami wewnętrznymi zostały powołane do rozpoznania, zapobiegania i wykrywania przestępstw tj. Zarząd Operacyjno-Śledczy[118] i Zarząd Spraw Wewnętrznych[119]. Ustalenia telekomunikacyjne dokonywane w trybie art. 10b ust. 2 pkt 1 ustawy o Straży Granicznej tj. na pisemny wniosek Komendanta Głównego Straży Granicznej lub osoby przez niego upoważnionej, jak również na ustne żądanie funkcjonariusza, realizowane były na podstawie ewidencjonowanych w rejestrze upoważnień. Występowanie przez upoważnionego funkcjonariusza o ustalenie danych telekomunikacyjnych odbywało się za wiedzą i zgodą kierownika komórki organizacyjnej.

Żandarmeria Wojskowa

Do uzyskiwania danych telekomunikacyjnych uprawnioną komórką był Wydział Zabezpieczenia i Ewidencji w Zarządzie Dochodzeniowo-Śledczym Komendy Głównej Żandarmerii Wojskowej. Z wnioskiem do Szefa tego wydziału mogli występować szefowie wydziałów, komendanci placówek, żołnierze Zarządu Dochodzeniowo-Śledczego po akceptacji przez bezpośredniego przełożonego.

Ministerstwo Finansów

Departament Wywiadu Skarbowego Ministerstwa Finansów, pozyskiwał dane telekomunikacyjne w trybie określonym w art. 36 b ustawy z dnia 28 września 1991 r. o kontroli skarbowej[120]. Dane te uzyskiwano z wykorzystaniem Systemu Elektronicznej Wymiany Informacji (SEWI), z którego mogli korzystać jedynie pracownicy Wywiadu Skarbowego, po złożeniu pisemnej prośby do naczelnika Wydziału Wywiadu Skarbowego. Pozyskiwanie danych telekomunikacyjnych w trybie art. 75 d ustawy z dnia 27 sierpnia 2009 r. o Służbie Celnej[121] powierzono Krajowej Grupie Zadaniowej ds. e-kontroli, funkcjonującej w Izbie Celnej w Opolu, realizującej zadania na rzecz całej Służby Celne.

Sądy

W sądach okręgowych dane telekomunikacyjne uzyskane od operatorów były integralną częścią akt sądowych w ramach procedury, w której zostały uzyskane i podlegały ochronie według zasad przewidzianych dla akt sądowych. Wnioski do operatorów o udostępnienie danych telekomunikacyjnych, kierowały poszczególne wydziały Sądu. Podstawą wystąpienia o dane telekomunikacyjne było postanowienie Sędziego Sądu.

Prokuratury

W prokuraturach dane telekomunikacyjne uzyskiwane były od operatorów na podstawie wydanych postanowień przesyłanych za pośrednictwem Poczty Polskiej lub ze stanowisk dostępowych drogą elektroniczną na podstawie podpisanych porozumień z operatorami.

---

[118] Załącznik do zarządzenia nr 79 Komendanta Głównego Straży Granicznej z dnia 23 października 2009 r. w sprawie regulaminu organizacyjnego Zarządu Operacyjno-Śledczego Komendy Głównej Straży Granicznej (Dz. Urz. KGSG Nr 13, poz. 79 ze zm.).

[119] Załącznik do zarządzenia nr 33 Komendanta Głównego Straży Granicznej z dnia 2 czerwca 2009 r. w sprawie regulaminu organizacyjnego Zarządu Operacyjno-Śledczego Komendy Głównej Straży Granicznej (Dz. Urz. KGSG Nr 6, poz. 36 ze zm.).

[120] Dz. U. z 2011 r. Nr 41, poz. 214 ze zm.

[121] Dz. U. Nr 168, poz. 1323 ze zm.

5.5. Wykaz podstawowych aktów prawnych[122]

1. Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78, poz. 483 ze zm.).
2. Ustawa z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2012 r., poz. 82 ze zm.).
3. Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2011 r. Nr 287, poz. 1687 ze zm.).
4. Ustawa z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2011 r. Nr 116, poz. 675 ze zm.).
5. Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2010 r. Nr 29, poz. 154 ze zm.).
6. Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. z 2012 r., poz. 621).
7. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.).
8. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228).
9. Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. Nr 171 poz. 1800 z późn. zm.).
10. Ustawa z dnia 28 września 1991 r. o kontroli skarbowej (Dz. U. z 2011 r. Nr 41, poz. 214 ze zm.).
11. Ustawa z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. Nr 123, poz. 1353 ze zm.).
12. Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. Nr 104, poz. 709 ze zm.).
13. Ustawa z dnia 27 sierpnia 2009 r. o Służbie Celnej (Dz. U. Nr 168, poz. 1323 ze zm.).
14. Ustawa z dnia 20 czerwca 1985 r. o prokuraturze (Dz. U. z 2011 r., Nr 270, poz. 1599 ze zm.).
15. Rozporządzenie Ministra Infrastruktury z dnia 28 grudnia 2009 r. w sprawie szczegółowego wykazu danych oraz rodzajów operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do ich zatrzymywania i przechowywania (Dz. U. Nr 226, poz. 1828).
16. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).
17. Rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004 r. w sprawie sposobu technicznego przygotowania systemów i sieci służących do przekazywania informacji – do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczania danych informatycznych (Dz. U. Nr 100, poz. 1023).

[122] W brzmieniu obowiązującym w kontrolowanym okresie.

5.6. Wykaz organów, którym przekazano informację o wynikach kontroli

1. Prezydent Rzeczypospolitej Polskiej
2. Marszałek Sejmu Rzeczypospolitej Polskiej
3. Marszałek Senatu Rzeczypospolitej Polskiej
4. Prezes Rady Ministrów Rzeczypospolitej Polskiej
5. Prezes Trybunału Konstytucyjnego
6. Minister Finansów
7. Minister Obrony Narodowej
8. Minister Spraw Wewnętrznych
9. Minister Sprawiedliwości
10. Prokurator Generalny
11. Rzecznik Praw Obywatelskich
12. Generalny Inspektor Ochrony Danych Osobowych
13. Przewodniczący Sejmowej Komisji Spraw Wewnętrznych
14. Przewodniczący Sejmowej Komisji do Spraw Kontroli Państwowej
15. Przewodniczący Sejmowej Komisji do Spraw Służb Specjalnych
16. Szef Biura Bezpieczeństwa Narodowego
17. Szef Agencji Bezpieczeństwa Wewnętrznego
18. Szef Centralnego Biura Antykorupcyjnego
19. Szef Służby Kontrwywiadu Wojskowego
20. Komendant Główny Policji
21. Komendant Główny Straży Granicznej
22. Komendant Główny Żandarmerii Wojskowej
23. Prezes Urzędu Komunikacji Elektronicznej