Dariusz Adamski

Zasady wykorzystywania przez służby specjalne danych telekomunikacyjnych w aspekcie obowiązującego stanu prawnego

1. Wprowadzenie

Na **dane telekomunikacyjne**, do których niejawny dostęp mogą mieć organy państwa, składają się dwie podstawowe kategorie informacji. Pierwszą są **przekazy telekomunikacyjne**, czyli treść rozmów bądź wiadomości wymienianych przez użytkowników sieci telekomunikacyjnych. Do drugiej należą wszelkiego rodzaju **dane związane z przekazami i użytkownikami sieci**, które generowane są w sieci telekomunikacyjnej lub zostały ujawnione przez użytkownika na etapie zawierania umowy z dostawcą usług telekomunikacyjnych. Kwestia ta ma duże znaczenie, ponieważ organy państwa uzyskują dostęp do każdej z tych dwóch kategorii danych na innych zasadach.

Kolejne istotne rozróżnienie, które musi zostać uczynione na wstępie, dotyczy podziału dostępu organów państwa na realizowany w ramach toczącego się postępowania karnego (**czynności procesowe**) oraz realizowany przez uprawnione organy w sytuacji, kiedy w żadnej sprawie i przeciwko żadnemu oskarżonemu nie toczy się postępowanie karne (**pozaprocesowe czynności operacyjno-rozpoznawcze**). W ramach czynności procesowych dostęp do danych telekomunikacyjnych uzyskuje prokurator lub sąd. W ramach czynności operacyjno-rozpoznawczych dostęp do danych telekomunikacyjnych uzyskać mogą:

1. Policja,
2. Straż Graniczna,
3. Agencja Bezpieczeństwa Wewnętrznego,
4. Służba Kontrwywiadu Wojskowego,
5. Żandarmeria Wojskowa,
6. Centralne Biuro Antykorupcyjne,
7. Wywiad skarbowy.

Dalsza część omówienia dostosowana jest to wskazanych podziałów. Składa się na nią analiza zasad dostępu:

- do treści przekazu w ramach czynności procesowych;
- do danych związanych z przekazami i użytkownikami sieci w ramach czynności procesowych;
- do treści przekazu w ramach pozaprocesowych czynności operacyjno-rozpoznawczych;
- do danych związanych z przekazami i użytkownikami sieci w ramach pozaprocesowych czynności operacyjno-rozpoznawczych;

Katalog ten uzupełniają zasady dostępu do **danych o użytkownikach serwisów świadczących usługi drogą elektroniczną**. Omówione zostaną one oddzielnie, w następnej kolejności.

Wcześniej jednak odnieść się należy do sposobu sformułowania – w ustawie z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz.U. z 2004 r. Nr 171 poz. 1800 z późn. zm.), dalej: Pr. tel. – generalnego obowiązku przedsiębiorców telekomunikacyjnych ujawniania danych telekomunikacyjnych wspólnie we wszystkich wskazanych wyżej czterech sytuacjach.

2. Dostęp do danych telekomunikacyjnych na gruncie Prawa telekomunikacyjnego

Art. 179 ust. 3 Prawa telekomunikacyjnego stanowi:

> Przedsiębiorca telekomunikacyjny, z zastrzeżeniem ust. 12 pkt 2[1], jest obowiązany do:
> 1) zapewnienia warunków technicznych i organizacyjnych dostępu i utrwalania, zwanych dalej „warunkami dostępu i utrwalania", umożliwiających jednoczesne i wzajemnie niezależne:
> a) uzyskiwanie przez Policję, Straż Graniczną, Agencję Bezpieczeństwa Wewnętrznego, Służbę Kontrwywiadu Wojskowego, Żandarmerię Wojskową, Centralne Biuro Antykorupcyjne i wywiad skarbowy, zwane dalej „uprawnionymi podmiotami", w sposób określony w ust. 4b[2], dostępu do:
> − przekazów telekomunikacyjnych, nadawanych lub odbieranych przez użytkownika końcowego lub telekomunikacyjne urządzenie końcowe,
> − posiadanych przez przedsiębiorcę danych związanych z przekazami telekomunikacyjnymi, o których mowa w ust. 9[3], art. 159 ust. 1 pkt 1 i pkt 3–5[4],
> b) uzyskiwanie przez uprawnione podmioty danych związanych ze świadczoną usługą telekomunikacyjną i danych, o których mowa w art. 161[5],
> c) utrwalanie przez uprawnione podmioty przekazów telekomunikacyjnych i danych, o których mowa w lit. a i b;
> 2) utrwalania na rzecz sądu i prokuratora przekazów telekomunikacyjnych i danych, o których mowa w pkt 1 lit. a i b.

Wskazane na początku zacytowanego przepisu zastrzeżenie art. 179 ust. 12 pkt 2 Pr. tel. pozwala wyłączyć, rozporządzeniem Rady Ministrów, niektóre kategorie działalności telekomunikacyjnej lub rodzaje przedsiębiorców telekomunikacyjnych z obowiązku udzielenia

---

[1] Szerzej: tekst dalej.

[2] Szerzej: tekst dalej.

[3] Zgodnie z ust. 9: „Przedsiębiorca telekomunikacyjny świadczący publicznie dostępne usługi telekomunikacyjne jest obowiązany prowadzić elektroniczny wykaz abonentów, użytkowników lub zakończeń sieci, uwzględniając w nim dane uzyskiwane przy zawarciu umowy".

[4] Tj. „1) dane dotyczące użytkownika; (...) 3) 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; 4) dane o lokalizacji, które oznaczają dane lokalizacyjne wykraczające poza dane niezbędne do transmisji komunikatu lub wystawienia rachunku; 5) 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".

[5] Znaczenie mają w tej materii zwłaszcza ust. 2 i 3 tego artykułu: „2. Dostawca publicznie dostępnych usług telekomunikacyjnych jest uprawniony do przetwarzania następujących danych dotyczących użytkownika będącego osobą fizyczną: 1) nazwisk i imion; 2) imion rodziców; 3) miejsca i daty urodzenia; 4) adresu miejsca zameldowania na pobyt stały; 5) numeru ewidencyjnego PESEL – w przypadku obywatela Rzeczypospolitej Polskiej; 6) nazwy, serii i numeru dokumentów potwierdzających tożsamość, a w przypadku cudzoziemca, który nie jest obywatelem państwa członkowskiego albo Konfederacji Szwajcarskiej – numeru paszportu lub karty pobytu; 7) zawartych w dokumentach potwierdzających możliwość wykonania zobowiązania wobec dostawcy publicznie dostępnych usług telekomunikacyjnych wynikającego z umowy o świadczenie usług telekomunikacyjnych. 3. Oprócz danych, o których mowa w ust. 2, 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 identyfikacji podatkowej NIP, 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".

dostępu do danych telekomunikacyjnych organom państwa, kierując się zakresem i rodzajem świadczonych usług telekomunikacyjnych lub wielkością sieci telekomunikacyjnych. Rozporządzenie, do wydania którego podstawą jest właśnie art. 179 ust. 12 pkt 2 Pr. tel., określać ma także wymagania i sposób zapewnienia warunków dostępu i utrwalania, kierując się zasadą osiągania celu przy jak najniższych nakładach. Rozporządzenie to nie zostało dotychczas wydane i w jego miejsce stosuje się rozporządzenie wydane na podstawie – nieobowiązującego już – art. 181 Pr. tel., tj. rozporządzenie Rady Ministrów z dnia 13 września 2005 r. w sprawie wypełniania przez przedsiębiorców telekomunikacyjnych zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego (Dz.U. z 2005 r. Nr 187 poz. 1568), dalej: rozporządzenie z 2005 r.[6] Przepis § 9 tego ostatniego zawiera następujące dwa wyłączenia z zakresu obowiązku dostępu i utrwalenia: „wykonywanie działalności telekomunikacyjnej polegającej na:

1) dostarczaniu udogodnień towarzyszących;
2) rozpowszechnianiu lub rozprowadzaniu programów radiofonicznych lub telewizyjnych".

Taki zakres wyłączeń oznacza w praktyce, iż obowiązkiem utrwalenia i udzielenia dostępu objęta jest wszelka działalność telekomunikacyjna polegająca na przekazywaniu komunikatów (słownych lub tekstowych) pomiędzy użytkownikami końcowymi. W żaden sposób działalności tej nie dotyczy bowiem wskazane wyłączenie[7].

Po drugie, art. 179 ust. 3 Prawa telekomunikacyjnego, choć w pierwszej części nie wspomina o sądzie (karnym) ani o prokuratorze, w ostatnim ustępie nawiązuje również do tych organów, których uprawnienia w zakresie wykorzystywania danych telekomunikacyjnych regulowane są oddzielnie (w ustawie z dnia 6 czerwca 1997 r. Kodeks postępowania karnego, Dz.U. z 1997 r. Nr 89 poz. 555, dalej: k.p.k.) od wcześniej wskazanych kategorii „uprawnionych podmiotów". Z zawartego w art. 179 Pr. tel. uregulowania wynika, że o ile w przypadku utrwalania i udostępniania przekazów telekomunikacyjnych i danych na rzecz sądu i prokuratora – w ramach prowadzonych przez nich czynności procesowych – działania podejmowane są przez przedsiębiorcę telekomunikacyjnego, o tyle w przypadku czynności operacyjno-rozpoznawczych prowadzonych przez siedem wskazanych powyżej kategorii podmiotów zarówno dostęp, jak i utrwalanie przekazów i danych powinno pozostać poza jego kontrolą i wpływem. W związku z tym pozostaje art. 179 ust. 4b Pr. tel., zgodnie z którym „Zapewnienie warunków dostępu i utrwalania powinno umożliwiać uprawnionym podmiotom dostęp do przekazów telekomunikacyjnych i danych bez udziału pracowników przedsiębiorcy telekomunikacyjnego. Za zgodą uprawnionego podmiotu warunki dostępu i utrwalania mogą być zapewnione przy niezbędnym współudziale upoważnionych pracowników przedsiębiorcy telekomunikacyjnego gwarantujących prawidłową realizację przedmiotowych czynności w zakresie określonym przez uprawniony podmiot". Zgodnie z brzmieniem art. 179 ust. 3 pkt 1 unormowanie to dotyczy czynności operacyjno-rozpoznawczych, czyli dokonywanych poza procedurą regulowaną k.p.k.

---

[6] Dalsze stosowanie tego rozporządzenia wynika z art. 14 ust. 1 ustawy z dnia 24 kwietnia 2009 r. o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw, Dz.U. z 2009 r. Nr 85 poz. 716.

[7] Art. 179 ust. 6–6b przyznaje prezesowi UKE uprawnienie do zawieszenia, w całości lub w części, w drodze decyzji, obowiązku dostępu i utrwalenia na wniosek indywidualnych przedsiębiorców i na okres nie dłuższy niż 6 miesięcy. Wniosek uzasadniony musi być wszakże obiektywnymi i niezależnymi od przedsiębiorcy technicznymi lub organizacyjnymi przyczynami uniemożliwiającymi dalsze wykonywanie obowiązku zapewnienia warunków dostępu i utrwalania. O ile wiadomo autorowi, prezes UKE nie skorzystał dotychczas z uprawnień przysługującego mu na mocy wskazanych przepisów.

Powyższe reguły rozwijane są w wyżej wskazanym rozporządzeniu z 2005 r. Do jego najważniejszych postanowień należą:

> § 2.1. (…) przedsiębiorca zapewnia techniczne i organizacyjne warunki wykonywania zadań przez przygotowanie, uruchomienie i utrzymanie gotowości eksploatacyjnej zestawu współdziałających urządzeń technicznych, zwanego dalej „systemem", oraz przygotowanie pracowników i zorganizowanie ich pracy, zapewniające:
> 1) dostęp do treści komunikatu i innych danych, o których mowa w art. 159 ust. 1 ustawy, przekazywanych w sieci telekomunikacyjnej przedsiębiorcy, wysyłanych lub odbieranych w zakończeniach tej sieci wskazanych przez podmioty, o których mowa w art. 179 ust. 3 pkt 1 ustawy, zwane dalej „uprawnionymi podmiotami";
> 2) dostęp do posiadanych lub przetwarzanych przez przedsiębiorcę danych:
> a) określonych w art. 159 ust. 1 pkt 3 i 5 ustawy, dotyczących wskazanego przez uprawnione podmioty zakończenia sieci tego przedsiębiorcy,
> b) określających zakończenia sieci, użytkownika lub abonenta, zwanych dalej „podmiotem kontrolowanym", w przypadku zastosowania środków służących przekierowywaniu połączeń do sieci innych przedsiębiorców lub innych zakończeń sieci,
> c) określonych w art. 159 ust. 1 pkt 4 ustawy, dotyczących wskazanych przez uprawnione podmioty zakończeń sieci tego przedsiębiorcy,
> d) dotyczących rodzajów usług telekomunikacyjnych, z których korzysta wskazany przez uprawnione podmioty użytkownik lub abonent,
> e) określonych w art. 161 ust. 2 i 3 ustawy lub zgromadzonych w wykazie, o którym mowa w art. 179 ust. 9 ustawy[8], dotyczących podmiotu kontrolowanego;
> 3) dokonywanie utrwalania przez uprawnione podmioty:
> a) treści komunikatu i danych, o których mowa w pkt 1,
> b) danych, o których mowa w pkt 2 lit. a i b,
> c) danych, o których mowa w pkt 2 lit. c, wraz z czasem ich zaistnienia.
> 2. Warunki, o których mowa w ust. 1, zapewnia się w sposób umożliwiający:
> 1) rozpoczęcie dostępu, o którym mowa w ust. 1 pkt 1 i 2, lub utrwalania, o którym mowa w ust. 1 pkt 3, niezwłocznie po wskazaniu przez uprawnione podmioty zakończeń sieci;
> 2) całodobowy, równoczesny z wysyłaniem lub odbiorem komunikatu, dostęp i utrwalanie treści komunikatu i danych, o których mowa w ust. 1 pkt 1, a jeżeli dostęp równoczesny nie jest możliwy – niezwłoczne dostarczenie treści komunikatu lub danych, które nie mogły być dostarczone;
> 3) dostęp i utrwalanie treści komunikatu lub danych w sposób pozwalający na ich odtworzenie przy pomocy standardowych urządzeń odtwarzających lub powszechnie stosowanego sprzętu komputerowego, w postaci:
> a) wysyłanej lub odbieranej we wskazanych zakończeniach sieci przedsiębiorcy – w przypadku treści komunikatu, o którym mowa w ust. 1 pkt 1,
> b) występującej w sieci telekomunikacyjnej, jak również przetwarzanej przez przedsiębiorcę, a jeżeli ich nie przetwarza – w postaci, w jakiej występują w sieci telekomunikacyjnej – w przypadku danych, o których mowa w ust. 1 pkt 1 i 2 lit. a–c;
> 4) dostęp i utrwalanie treści komunikatu lub danych, tak aby na skutek zastosowania systemu jakość oraz zakres usługi telekomunikacyjnej świadczonej kontrolowanemu abonentowi lub użytkownikowi nie uległy zmianie.
> 3. Sprawność i niezawodność systemu nie może być mniejsza od sprawności i niezawodności urządzeń telekomunikacyjnych wykorzystywanych do świadczenia usług telekomunikacyjnych abonentom lub użytkownikom. (…)
> § 4. 1. Zapewnienie dostępu do treści komunikatu i danych oraz ich utrwalanie realizuje się w miejscach uzgodnionych w drodze odrębnych pisemnych porozumień, zawartych przez przedsiębiorcę z Ministrem Obrony Narodowej, ministrem właściwym do spraw wewnętrznych, ministrem właściwym do spraw finansów publicznych, Szefem Agencji Bezpieczeństwa Wewnętrznego i Szefem Agencji Wywiadu.
> 2. W przypadku braku uzgodnienia, na wniosek organu lub przedsiębiorcy, o których mowa w ust. 1, miejsca wybiera Prezes Urzędu Regulacji Telekomunikacji i Poczty.

[8] Ten ostatni przepis dotyczy elektronicznego wykazu abonentów.

§ 5. 1. System przygotowuje się w sposób zapewniający upoważnionemu funkcjonariuszowi, żołnierzowi lub pracownikowi uprawnionego podmiotu wykonanie w miejscach, o których mowa w § 4, czynności powodujących rozpoczęcie i zakończenie dostępu lub utrwalania.
2. Udział pracowników przedsiębiorcy w realizowaniu zadań powinien być ograniczony do niezbędnego minimum. (…)
§ 7. 1. System przygotowuje się w sposób zapewniający uprawnionym podmiotom jednoczesny i wzajemnie niezależny dostęp lub utrwalanie treści komunikatu i danych (…).
2. Maksymalna liczba zakończeń sieci, które mogą być wskazane przez uprawnione podmioty w celu zapewnienia przez system dostępu lub utrwalania, o których mowa w ust. 1, jest uzgadniana, w drodze odrębnych pisemnych porozumień zawartych przez przedsiębiorcę z Ministrem Obrony Narodowej, ministrem właściwym do spraw wewnętrznych, ministrem właściwym do spraw finansów publicznych, Szefem Agencji Bezpieczeństwa Wewnętrznego i Szefem Agencji Wywiadu.
3. W przypadku braku uzgodnienia, liczba zakończeń sieci dla każdego z organów, o których mowa w ust. 2, powinna wynosić co najmniej:
1) 0,05 % pojemności każdej centrali wchodzącej w skład sieci przedsiębiorcy lub
2) 0,03 % zakończeń sieci przedsiębiorcy, w których wykonywana jest działalność telekomunikacyjna, podlegająca obowiązkowi wykonywania zadań
– z tym że nie może być mniejsza niż jeden.

W swoich najważniejszych postanowieniach powyższe przepisy zakładają, że sposób dostępu i utrwalania danych telekomunikacyjnych kontrolowany ma być w całości przez uprawniony podmiot i uruchamiany na skutek (jedynie) wskazania przez uprawniony organ zakończenia sieci, którego dotyczyć będzie kontrola (§ 2). Przedsiębiorca telekomunikacyjny musi zrealizować żądanie uprawnionego organu, i to w sposób minimalizujący udział w tym pracowników owego przedsiębiorcy. Co więcej, przygotowanie i wykonywanie zadań przewidzianych rozporządzeniem objęte jest klauzulą niejawności, co wynika z (niecytowanego wyżej) § 3 rozporządzenia. Tym samym przedsiębiorcy telekomunikacyjni nie mogą ujawniać osobom trzecim jakichkolwiek informacji dotyczących dostępu uprawnionych podmiotów do danych telekomunikacyjnych. Niejawność ta z jednej strony uzasadniona jest koniecznością zagwarantowania poufności technik operacyjnych stosowanych przez organy państwa korzystające z dostępu do sieci telekomunikacyjnych na potrzeby przeciwdziałania i zwalczania przestępstw. Z drugiej jednak strony uniemożliwia uzyskanie pełnego obrazu skali i sposobów inwigilacji społeczeństwa przez władze publiczne.

Zacytowane przepisy nie wprowadzają niemal jakichkolwiek mechanizmów ograniczenia możliwości wykorzystywania sieci telekomunikacyjnych przez uprawnione organy. Pamiętać należy jednak, że regulują one jedynie specyficzną relację pomiędzy uprawnionym organem a przedsiębiorcą telekomunikacyjnym. O dopuszczalności i zakresie kontroli decydują inne przepisy, niezwiązane z Prawem telekomunikacyjnym. Zanalizowane zostaną one poniżej, z rozbiciem na reguły dotyczące dostępu do treści przekazu i innych danych telekomunikacyjnych.

3. Czynności procesowe

3.1. Dostęp do treści przekazu

W ramach postępowania karnego zarządzenie „kontroli oraz utrwalania przy użyciu środków technicznych treści rozmów lub przekazów informacji, w tym korespondencji przesyłanej pocztą elektroniczną” możliwe jest tylko:

1) po wszczęciu postępowania, przez sąd na wniosek prokuratora[9];
2) w celu wykrycia i uzyskania dowodów dla toczącego się postępowania lub zapobieżenia popełnieniu nowego przestępstwa (art. 237 § 1 k.p.k. oraz art. 241 k.p.k.);
3) gdy toczące się postępowanie lub uzasadniona obawa popełnienia nowego przestępstwa dotyczy (art. 237 § 3):
   - 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;
   - 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 ustawy z dnia 6 czerwca 1997 r. Kodeks karny (Dz.U. Nr 88 poz. 553 z późn. zm.) oraz w art. 5–8 Rzymskiego Statutu Międzynarodowego Trybunału Karnego, sporządzonego w Rzymie 17 lipca 1998 r. (Dz.U. z 2003 r. Nr 78 poz. 708), zwanego dalej: Statutem;
4) w stosunku do osoby podejrzanej, oskarżonego oraz w stosunku do pokrzywdzonego lub innej osoby, z którą może się kontaktować oskarżony albo która może mieć związek ze sprawcą lub z grożącym przestępstwem (art. 237 § 4 k.p.k.);
5) jest ograniczona czasowo do maksymalnie 6 miesięcy[10], a po jej zakończeniu sąd zarządza zniszczenie utrwalonych zapisów, jeżeli nie mają znaczenia dla postępowania karnego (art. 238 k.p.k.);

[9] Na zasadzie wyjątku, w wypadkach niecierpiących zwłoki, kontrolę i utrwalanie rozmów telefonicznych może zarządzić prokurator, który obowiązany jest zwrócić się w terminie 3 dni do sądu z wnioskiem o zatwierdzenie postanowienia. Sąd wydaje postanowienie w przedmiocie wniosku w terminie 5 dni na posiedzeniu bez udziału stron (art. 237 § 2 k.p.k.).

[10] Jak stanowi art. 238 k.p.k., „§ 1. Kontrola i utrwalanie rozmów telefonicznych mogą być wprowadzone najwyżej na okres 3 miesięcy, z możliwością przedłużenia, w szczególnie uzasadnionym wypadku, na okres najwyżej dalszych 3 miesięcy. § 2. Kontrola powinna być zakończona niezwłocznie po ustaniu przyczyn wymienionych w art. 237 § 1–3, najpóźniej jednak z upływem okresu, na który została wprowadzona. § 3. Po zakończeniu kontroli sąd zarządza

6) jest ogłaszana osobie kontrolowanej; ogłoszenie postanowienia o kontroli i utrwalaniu rozmów telefonicznych osobie, której ono dotyczy, może być odroczone na czas niezbędny ze względu na dobro sprawy (art. 239 § 1 k.p.k.), jednak jeśli zarządzono je w trakcie postępowania przygotowawczego (co jest regułą), ogłoszenie nie może nastąpić później niż na etapie zakończenia tego postępowania (art. 239 § 2 k.p.k.)

Na postanowienie dotyczące kontroli i utrwalania rozmów telefonicznych przysługuje zażalenie (art. 240 k.p.k.). Osoba, której dotyczy postanowienie, może w zażaleniu domagać się zbadania zasadności oraz legalności kontroli i utrwalania rozmów telefonicznych.

Wskazane reguły mocno i w zróżnicowany sposób przeciwdziałają nadużywaniu uprawnienia do kontroli przekazów informacji. Niezwykle istotnym kolejnym mechanizmem tego samego rodzaju jest zawarte w art. 237 § 5 k.p.k. postanowienie, zgodnie z którym urzędy, instytucje oraz podmioty prowadzące działalność w dziedzinie poczty lub działalność telekomunikacyjną obowiązane są nie tylko „umożliwić wykonanie postanowienia sądu lub prokuratora w zakresie przeprowadzenia kontroli rozmów telefonicznych", ale także „zapewnić rejestrowanie faktu przeprowadzenia takiej kontroli". Dzięki temu podmiot niezależny od uprawnionego organu nie tylko posiada świadomość zarządzonej kontroli, ale przede wszystkim wytwarza jej ślad, co pozwala sądowi dokonać weryfikacji skali, rodzaju i zasadności kontroli[11]. Kwestia ta rozwijana jest w rozporządzeniu Ministra Sprawiedliwości z dnia 24 czerwca 2003 r. w sprawie sposobu technicznego przygotowania sieci służących do przekazywania informacji, do kontroli przekazów informacji oraz sposobu dokonywania, rejestracji, przechowywania, odtwarzania i niszczenia zapisów z kontrolowanych przekazów, Dz.U. z 2003 r. Nr 110 poz. 1052 (dalej: rozporządzenie z 2003 r.). Reguluje ono między innymi kwestie technicznego systemu rejestracji kontroli przekazów informacji oraz niszczenia zapisów z tych przekazów:

> § 11. 1. Podmiot obowiązany zapewnia rejestrację faktu przeprowadzenia kontroli przekazów informacji, gromadząc dane o przeprowadzonych kontrolach.
> 2. Dane, o których mowa w ust. 1, obejmują:
> 1) sygnaturę akt sprawy i datę wydania postanowienia sądu lub prokuratora;
> 2) datę przeprowadzenia kontroli;
> 3) informację o podmiocie uprawnionym;
> 4) imię i nazwisko użytkownika sieci lub nazwę podmiotu będącego użytkownikiem, w stosunku do którego zarządzono kontrolę;
> 5) czas dokonywania kontroli.
> 3. Gromadzenie, przechowywanie i udostępnianie danych, o których mowa w ust. 1 i 2, odbywa się przy zastosowaniu przepisów dotyczących ochrony informacji niejawnych stanowiących tajemnicę państwową. (…)
> § 15. 1. Zapis z kontroli przekazów informacji, którego zniszczenie sąd zarządził (…), podlega usunięciu w sposób trwale uniemożliwiający jego odtworzenie.
> 2. Jeżeli mimo usunięcia zapisu zachodzi możliwość jego odtworzenia, należy zarządzić fizyczne zniszczenie nośnika.
> 3. Z czynności usunięcia zapisu lub zniszczenia nośnika sporządza się protokół.

---

zniszczenie utrwalonych zapisów, jeżeli nie mają znaczenia dla postępowania karnego; zniszczenie utrwalonych zapisów następuje także wówczas, gdy sąd nie zatwierdził postanowienia prokuratora, o którym mowa w art. 237 § 2".

[11] Art. 237 § 7 k.p.k. stanowi, że „prawo zapoznawania się z rejestrem przeprowadzonych kontroli rozmów telefonicznych ma sąd, a w postępowaniu przygotowawczym – prokurator".

3.2. Dostęp do danych związanych z przekazami i użytkownikami sieci

Kodeks postępowania karnego określa reguły dotyczące wydania i zabezpieczenia danych niebędących treścią indywidualnych komunikatów w – odpowiednio – art. 218 i 219.

> Art. 218 § 1. Urzędy, instytucje i podmioty prowadzące działalność w dziedzinie poczty lub działalność telekomunikacyjną, urzędy celne oraz instytucje i przedsiębiorstwa transportowe obowiązane są wydać sądowi lub prokuratorowi, na żądanie zawarte w postanowieniu, korespondencję i przesyłki oraz dane, o których mowa w art. 180c i 180d ustawy (...) Prawo telekomunikacyjne (...)[12], jeżeli mają znaczenie dla toczącego się postępowania. Tylko sąd lub prokurator mają prawo je otwierać lub zarządzić ich otwarcie.
> § 2. Postanowienie, 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.
> Art. 218a § 1. Urzędy, instytucje i podmioty prowadzące działalność telekomunikacyjną obowiązane są niezwłocznie zabezpieczyć, na żądanie sądu lub prokuratora zawarte w postanowieniu, na czas określony, nieprzekraczający jednak 90 dni, dane informatyczne przechowywane w urządzeniach zawierających te dane na nośniku lub w systemie informatycznym. Przepis art. 218 § 2 zdanie drugie stosuje się odpowiednio.
> § 2. Pozbawione znaczenia dla postępowania karnego dane informatyczne, o których mowa w § 1, należy niezwłocznie zwolnić spod zabezpieczenia.

Zacytowane przepisy nie ograniczają co prawda przedmiotowo ani podmiotowo zakresu spraw, w których zarządzone może zostać wydanie lub zabezpieczenie danych (jedyną wskazówką jest „znaczenie dla toczącego się postępowania"). Jednak – po pierwsze – warunkują wydanie lub zabezpieczenie danych od postanowienia prokuratora lub sądu. Po drugie – nakazują poinformować (po fakcie) o kontroli osobę kontrolowaną. Po trzecie – obowiązek zabezpieczenia jest ograniczony czasowo. Po czwarte – zdefiniowane zostały zasady i sposoby usuwania zapisów danych zbędnych dla danego postępowania.

Dodać do tego należy, że wydanie i zabezpieczenie danych niebędących treścią indywidualnych komunikatów – podobnie jak treści komunikatów – rejestrowane jest przez przedsiębiorcę telekomunikacyjnego. Ostatnia ze wskazanych kwestii rozwinięta została w § 6 rozporządzenia 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. z 2004 r. Nr 100 poz. 1023). Zgodnie z tym przepisem przedsiębiorca telekomunikacyjny

> gromadzi dane o dokonanych zabezpieczeniach danych zapisanych. Gromadzone dane, o których mowa w ust. 1, obejmują:
> 1) sygnaturę akt sprawy i datę wydania postanowienia o zabezpieczeniu danych zapisanych;
> 2) nazwę podmiotu uprawnionego;
> 3) datę dokonania zabezpieczenia;
> 4) imię i nazwisko użytkownika systemu lub sieci albo nazwę podmiotu będącego użytkownikiem, w stosunku do którego zarządzono zabezpieczenie danych zapisanych;
> 5) czas trwania zabezpieczenia,
> 6) dane identyfikujące miejsce zabezpieczenia danych zapisanych.

Wskazany przepis zawiera dość istotną wadę, ponieważ wyraźnie odnosi się jedynie do zabezpieczenia danych (kwestia regulowana w art. 218a k.p.k.). Tymczasem delegacja ustawowa

[12] Tj. wszelkie dane telekomunikacyjne i o użytkownikach sieci, poza treścią indywidualnych komunikatów.

dla cytowanego rozporządzenia nawiązuje do art. 218 k.p.k., czyli przypadków wydania tych danych uprawnionym organom przez przedsiębiorcę telekomunikacyjnego. Odniesienie obowiązku określonego w § 6 rozporządzenia do tych przypadków byłoby też dużo bardziej racjonalne. Pozwalałoby bowiem na weryfikację przypadków, kiedy dane indywidualnych użytkowników są ujawniane organom państwa, a zatem tych sytuacji, kiedy dochodzi do skonkretyzowania zagrożenia dla prywatności użytkownika sieci (na etapie zabezpieczenia danych zagrożenie to jest zawieszone do momentu ujawnienia tych danych właściwemu organowi – sądowi lub prokuratorowi). Kwestia ta nie ma wszakże znaczenia pierwszoplanowego, ponieważ całość procesowych działań prokuratora w ramach postępowania kontrolnego znajduje się pod kontrolą sądową.

4. Pozaprocesowe czynności operacyjno-rozpoznawcze

4.1. Dostęp do treści przekazu

Przepisy regulujące działalność Policji i służb specjalnych zawierają odrębnie szczegółowe unormowania dotyczące dopuszczalności i zasad wykonywania podstawowego rodzaju czynności operacyjno-rozpoznawczych, jakim jest kontrola operacyjna. Przepisy te odnoszą się wszakże jedynie do dostępu i przetwarzania treści przekazów. Nie dotyczą natomiast reguł dotyczących dostępu i przetwarzania danych telekomunikacyjnych innych niż treść przekazu. Kwestia ta ma bardzo duże znaczenie, ponieważ przepisy pierwszego z owych dwóch rodzajów przewidują szereg mechanizmów przeciwdziałających nadużyciom władzy, drugie zaś nie zawierają ich właściwie wcale.

Jako przykład pierwszego ze wskazanych rodzajów przepisów powołać można art. 19 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz.U. z 2007 r. Nr 43 poz. 277).

> 1. Przy wykonywaniu czynności operacyjno-rozpoznawczych, podejmowanych przez Policję w celu zapobieżenia, wykrycia, ustalenia sprawców, a także uzyskania i utrwalenia dowodów ściganych z oskarżenia publicznego, umyślnych przestępstw:
> 1) przeciwko życiu, określonych w art. 148-150 Kodeksu karnego,
> 2) określonych w art. 134, art. 135 § 1, art. 136 § 1, art. 156 § 1 i 3, art. 163 § 1 i 3, art. 164 § 1, art. 165 § 1 i 3, art. 166, art. 167, art. 173 § 1 i 3, art. 189, art. 189a, art. 200, art. 200a, art. 211a, art. 223, art. 228 § 1 i 3-5, art. 229 § 1 i 3-5, art. 230 § 1, art. 230a § 1, art. 231 § 2, art. 232, art. 245, art. 246, art. 252 § 1-3, art. 258, art. 269, art. 280-282, art. 285 § 1, art. 286 § 1, art. 296 § 1-3, art. 296a § 1, 2 i 4, art. 299 § 1-6 oraz art. 310 § 1, 2 i 4 Kodeksu karnego,
> 2a) określonych w art. 46 ust. 1, 2 i 4, art. 47 oraz art. 48 ust. 1 i 2 ustawy z dnia 25 czerwca 2010 r. o sporcie (Dz.U. Nr 127, poz. 857),
> 3) przeciwko obrotowi gospodarczemu, określonych w art. 297-306 Kodeksu karnego, powodujących szkodę majątkową lub skierowanych przeciwko mieniu, jeżeli wysokość szkody lub wartość mienia przekracza pięćdziesięciokrotną wysokość najniższego wynagrodzenia za pracę określonego na podstawie odrębnych przepisów,
> 4) skarbowych, jeżeli wartość przedmiotu czynu lub uszczuplenie należności publicznoprawnej przekraczają pięćdziesięciokrotną wysokość najniższego wynagrodzenia za pracę określonego na podstawie odrębnych przepisów,
> 4a) skarbowych, o których mowa w art. 107 § 1 Kodeksu karnego skarbowego,
> 5) nielegalnego wytwarzania, posiadania lub obrotu bronią, amunicją, materiałami wybuchowymi, środkami odurzającymi lub substancjami psychotropowymi albo ich prekursorami oraz materiałami jądrowymi i promieniotwórczymi,
> 6) określonych w art. 8 ustawy z dnia 6 czerwca 1997 r. – Przepisy wprowadzające Kodeks karny (…),

7) określonych w art. 43-46 ustawy z dnia 1 lipca 2005 r. o pobieraniu, przechowywaniu i przeszczepianiu komórek, tkanek i narządów (...),
8) ściganych na mocy umów i porozumień międzynarodowych,
gdy inne środki okazały się bezskuteczne albo zachodzi wysokie prawdopodobieństwo, że będą nieskuteczne lub nieprzydatne, sąd okręgowy, na pisemny wniosek Komendanta Głównego Policji, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego albo na pisemny wniosek komendanta wojewódzkiego Policji, złożony po uzyskaniu pisemnej zgody właściwego miejscowo prokuratora okręgowego, może, w drodze postanowienia, zarządzić kontrolę operacyjną.
2. Postanowienie, o którym mowa w ust. 1, wydaje sąd okręgowy właściwy miejscowo ze względu na siedzibę składającego wniosek organu Policji.
3. W przypadkach niecierpiących zwłoki, jeżeli mogłoby to spowodować utratę informacji lub zatarcie albo zniszczenie dowodów przestępstwa, Komendant Główny Policji lub komendant wojewódzki Policji może zarządzić, po uzyskaniu pisemnej zgody właściwego prokuratora, o którym mowa w ust. 1, kontrolę operacyjną, zwracając się jednocześnie do właściwego miejscowo sądu okręgowego z wnioskiem o wydanie postanowienia w tej sprawie. W razie nieudzielenia przez sąd zgody w terminie 5 dni od dnia zarządzenia kontroli operacyjnej, organ zarządzający wstrzymuje kontrolę operacyjną oraz dokonuje protokolarnego, komisyjnego zniszczenia materiałów zgromadzonych podczas jej stosowania.
5. W przypadku potrzeby zarządzenia kontroli operacyjnej wobec osoby podejrzanej lub oskarżonego, we wniosku organu Policji, o którym mowa w ust. 1, o zarządzenie kontroli operacyjnej zamieszcza się informację o toczącym się wobec tej osoby postępowaniu.
6. Kontrola operacyjna prowadzona jest niejawnie i polega na:
1) kontrolowaniu treści korespondencji;
2) kontrolowaniu zawartości przesyłek;
3) stosowaniu środków technicznych umożliwiających uzyskiwanie w sposób niejawny informacji i dowodów oraz ich utrwalanie, a w szczególności treści rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych.
7. Wniosek organu Policji, o którym mowa w ust. 1, o zarządzenie przez sąd okręgowy kontroli operacyjnej powinien zawierać w szczególności:
1) numer sprawy i jej kryptonim, jeżeli został jej nadany;
2) opis przestępstwa z podaniem, w miarę możliwości, jego kwalifikacji prawnej;
3) okoliczności uzasadniające potrzebę zastosowania kontroli operacyjnej, w tym stwierdzonej albo prawdopodobnej bezskuteczności lub nieprzydatności innych środków;
4) dane osoby lub inne dane, pozwalające na jednoznaczne określenie podmiotu lub przedmiotu, wobec którego stosowana będzie kontrola operacyjna, ze wskazaniem miejsca lub sposobu jej stosowania;
5) cel, czas i rodzaj prowadzonej kontroli operacyjnej, o której mowa w ust. 6.
8. Kontrolę operacyjną zarządza się na okres nie dłuższy niż 3 miesiące. Sąd okręgowy może, na pisemny wniosek Komendanta Głównego Policji lub komendanta wojewódzkiego Policji, złożony po uzyskaniu pisemnej zgody właściwego prokuratora, na okres nie dłuższy niż kolejne 3 miesiące, wydać postanowienie o jednorazowym przedłużeniu kontroli operacyjnej, jeżeli nie ustały przyczyny zarządzenia tej kontroli.
9. W uzasadnionych przypadkach, gdy podczas stosowania kontroli operacyjnej pojawią się nowe okoliczności istotne dla zapobieżenia lub wykrycia przestępstwa albo ustalenia sprawców i uzyskania dowodów przestępstwa, sąd okręgowy, na pisemny wniosek Komendanta Głównego Policji, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, może wydać postanowienie o kontroli operacyjnej przez czas oznaczony również po upływie okresów, o których mowa w ust. 8.
10. Do wniosków, o których mowa w ust. 3, 4, 8 i 9, stosuje się odpowiednio przepis ust. 7. Sąd przed wydaniem postanowienia, o którym mowa w ust. 3, 4, 8 i 9, może zapoznać się z materiałami uzasadniającymi wniosek, zgromadzonymi podczas stosowania kontroli operacyjnej zarządzonej w tej sprawie.
11. Wnioski, o których mowa w ust. 1, 3-5, 8 i 9, sąd okręgowy rozpoznaje jednoosobowo, przy czym czynności sądu związane z rozpoznawaniem tych wniosków powinny być realizowane w warunkach przewidzianych dla przekazywania, przechowywania i udostępniania informacji niejawnych (...). W posiedzeniu sądu może wziąć udział wyłącznie prokurator i przedstawiciel organu Policji wnioskującego o zarządzenie kontroli operacyjnej.

12. Podmioty wykonujące działalność telekomunikacyjną oraz podmioty świadczące usługi pocztowe są obowiązane do zapewnienia na własny koszt warunków technicznych i organizacyjnych umożliwiających prowadzenie przez Policję kontroli operacyjnej.
13. Kontrola operacyjna powinna być zakończona niezwłocznie po ustaniu przyczyn jej zarządzenia, najpóźniej jednak z upływem okresu, na który została wprowadzona.
14. Organ Policji, o którym mowa w ust. 1, informuje właściwego prokuratora o wynikach kontroli operacyjnej po jej zakończeniu, a na jego żądanie również o przebiegu tej kontroli.
15. W przypadku uzyskania dowodów pozwalających na wszczęcie postępowania karnego lub mających znaczenie dla toczącego się postępowania karnego, Komendant Główny Policji lub komendant wojewódzki Policji przekazuje właściwemu prokuratorowi wszystkie materiały zgromadzone podczas stosowania kontroli operacyjnej, w razie potrzeby z wnioskiem o wszczęcie postępowania karnego (…).
16. Osobie, wobec której kontrola operacyjna była stosowana, nie udostępnia się materiałów zgromadzonych podczas trwania tej kontroli. Przepis nie narusza uprawnień wynikających z art. 321 Kodeksu postępowania karnego[13].
17. Zgromadzone podczas stosowania kontroli operacyjnej materiały niezawierające dowodów pozwalających na wszczęcie postępowania karnego przechowuje się po zakończeniu kontroli przez okres 2 miesięcy, a następnie dokonuje się ich protokolarnego, komisyjnego zniszczenia. Zniszczenie materiałów zarządza organ Policji, który wnioskował o zarządzenie kontroli operacyjnej. (…)
20. Na postanowienia sądu w przedmiocie kontroli operacyjnej, o których mowa w ust. 1, 3, 8 i 9, przysługuje zażalenie organowi Policji, który złożył wniosek o wydanie tego postanowienia. Do zażalenia stosuje się odpowiednio przepisy Kodeksu postępowania karnego.
22. Prokurator Generalny przedstawia corocznie Sejmowi i Senatowi informację o działalności określonej w ust. 1–21 (…).

Jak wskazano wprost w ust. 6 pkt 3 cytowanego przepisu, kontrola operacyjna polega na stosowaniu środków technicznych umożliwiających „uzyskiwanie w sposób niejawny informacji i dowodów oraz ich utrwalanie, a w szczególności treści rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych". Przepis ten dotyczy zatem między innymi dostępu do treści przekazu dokonywanego za pomocą sieci.

Wskazane przepisy zawierają nie tylko szereg ograniczeń podmiotowych, przedmiotowych i czasowych stosowania kontroli operacyjnej, ale też tworzą mechanizmy nadzoru organów niezależnych od Policji nad sposobem korzystania przez tą ostatnią z przysługujących jej uprawnień.

Po pierwsze, zakres dopuszczalnej kontroli operacyjnej jest zawężony jedynie do przypadków przestępstw enumeratywnie wskazanych w ust. 1 (zasada *numerus clausus*) i może mieć miejsce tylko, jeśli inne środki okazały się bezskuteczne albo byłyby nieprzydatne (zasada subsydiarności). Do najnowszej nowelizacji przepisów dotyczących kontroli operacyjnej, dokonanej ustawą z dnia 4 lutego 2011 r. o zmianie ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw (Dz.U. z 2011 r. Nr 53 poz. 273), dalej: ustawa z 4 lutego 2011 r. – która weszła w życie 11 czerwca 2011 r., zastosowanie kontroli operacyjnej możliwe było już wówczas, gdy zachodziło „wysokie prawdopodobieństwo", że inne środki będą nieskuteczne lub nieprzydatne. Tym samym zastosowanie kontroli operacyjnej było w praktyce łatwiejsze niż obecnie, ponieważ jej dopuszczalność wynikała z założenia w dużej mierze hipotetycznego.

Po drugie, do przeprowadzenia kontroli operacyjnej niezbędne jest wydanie postanowienia przez sąd okręgowy, na pisemny wniosek komendanta głównego Policji, złożony po uzyskaniu pisemnej zgody prokuratora generalnego, albo na pisemny wniosek komendanta wojewódzkiego Policji, złożony po uzyskaniu pisemnej zgody prokuratora okręgowego

[13] Prawo do zaznajomienia się z materiałami postępowania.

właściwego ze względu na siedzibę składającego wniosek organu Policji. Ustawa z 4 lutego 2011 r. uzupełniła wskazane uregulowania o bardzo ważne postanowienie zawarte w ust. 1(a). Zgodnie z nim do wniosku załączone powinny zostać materiały uzasadniające potrzebę zastosowania kontroli operacyjnej. Przedstawienie sądowi owych dokumentów jest istotne dla umożliwienia sądowi kontroli twierdzeń Policji o nieskuteczności lub nieprzydatności innych środków, a zatem o zasadności zastosowania kontroli operacyjnej.

Zarządzenie kontroli operacyjnej możliwe jest też bez uprzedniej zgody sądu. Jednak zgoda ta następczo uzyskana musi zostać w ciągu najdalej pięciu dni od zarządzenia kontroli, a sama kontrola bez owej uprzedniej zgody możliwa jest tylko w wyjątkowych sytuacjach (w przypadkach niecierpiących zwłoki, jeżeli mogłoby to spowodować utratę informacji lub zatarcie albo zniszczenie dowodów przestępstwa). Wskazane uregulowanie szczególne ma wszakże ten mankament, iż nie wymaga przekazania sądowi materiałów uzasadniających zastosowanie kontroli operacyjnej. Tym samym sądowa (następcza) akceptacja odbywa się jedynie na podstawie wniosku przedstawionego przez komendanta głównego Policji lub komendanta wojewódzkiego Policji i pisemnej zgody właściwego prokuratora.

Po trzecie, ustawa określa treść wniosku o zarządzenie kontroli operacyjnej, w tym wymaga uzasadnienia spełnienia przesłanek sięgnięcia po ten środek.

Po czwarte, w wyniku nowelizacji dokonanej ustawą z 4 lutego 2011 r. kontrola operacyjna może zostać zarządzona na okres zasadniczo nie dłuższy niż 6 miesięcy. Dalsze jej stosowanie – przez czas oznaczony w tym postanowieniu – wymaga postanowienia sądu okręgowego, które wydane może zostać tylko „w uzasadnionych przypadkach, gdy podczas stosowania kontroli operacyjnej pojawią się nowe okoliczności istotne dla zapobieżenia lub wykrycia przestępstwa albo ustalenia sprawców i uzyskania dowodów przestępstwa" i wyłącznie na pisemny wniosek komendanta głównego Policji, złożony po uzyskaniu pisemnej zgody prokuratora generalnego.

Po piąte, wykorzystanie dowodów popełnienia przestępstwa innego niż określone we wniosku o zarządzenie kontroli operacyjnej lub przeciwko innej osobie możliwe jest tylko, kiedy wydane zostanie w tej materii (następcze) postanowienie sądu pierwotnie zarządzającego kontrolę operacyjną, przy czym postanowienie w tej materii wydane może zostać jedynie, jeśli wniosek prokuratora trafi do sądu nie później (w przypadku skrajnym) niż trzy miesiące po zakończeniu kontroli.

Po szóste, materiały, które nie są przydatne w postępowaniu karnym, mają zostać niezwłocznie, protokolarnie i komisyjnie zniszczone, a o wykonaniu zarządzenia w tej sprawie poinformowany ma zostać właściwy prokurator.

Po siódme, w wyniku nowelizacji z 4 lutego 2011 r. prokurator generalny został zobowiązany do przedstawiania rokrocznie Sejmowi i Senatowi – do 30 czerwca – informacji o praktyce prowadzenia kontroli operacyjnej przez Policję. Obowiązek ten znajduje swoje odzwierciedlenie w art. 10ea ust. 1 ustawy z dnia 20 czerwca 1985 r. o prokuraturze (Dz.U. z 2008 r. Nr 7 poz. 39), zgodnie z którym prokurator generalny przedstawia Sejmowi i Senatowi do 30 czerwca każdego roku

> jawną roczną informację o łącznej liczbie osób, wobec których został skierowany wniosek o zarządzenie kontroli i utrwalania rozmów lub wniosek o zarządzenie kontroli operacyjnej, ze wskazaniem liczby osób, co do których:
> 1) sąd zarządził kontrolę i utrwalanie rozmów lub kontrolę operacyjną,

2) sąd odmówił zarządzenia kontroli i utrwalania rozmów lub kontroli operacyjnej,
3) wniosek o kontrolę operacyjną nie uzyskał zgody prokuratora,
z wyszczególnieniem liczby osób w wymienionych kategoriach, co do których o kontrolę operacyjną wnioskował organ Policji.

Pierwsza tego rodzaju informacja przekazana została Sejmowi i Senatowi 21 czerwca 2011 r. (http://www.senat.gov.pl/k7/dok/dr/1250/1267.pdf).

Powyższe uregulowania są co do zasady standardem regulacji zasad prowadzenia czynności operacyjnych przez służby specjalne. Analogiczne brzmienie mają:

- art. 9e ustawy z dnia 12 października 1990 r. o Straży Granicznej, Dz.U. z 2005 r. Nr 234 poz. 1997 ze zm. (ustawa o SG);
- art. 27 ustawy 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 ABW i AW);
- art. 31 ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, Dz.U. Nr 104 poz. 709 ze zm. (ustawa o SKW i SWW);
- art. 31 ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych, Dz.U. Nr 123 poz. 1353 ze zm. (ustawa o ŻW);
- art. 17 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym, Dz.U. Nr 104 poz. 708 ze zm. (ustawa o CBA);
- art. 36c ustawy z dnia 28 września 1991 r. o kontroli skarbowej, Dz.U. z 2011 r. Nr 41 poz. 214 (UKS).

Różnią się one jednak od ustawy o Policji niektórymi uregulowaniami szczegółowymi.

Jedno z nich, zawarte w UKS, przyczynia się do poprawy stanu ochrony prywatności. Wynika z niego, że informacje zebrane w trakcie kontroli operacyjnej przez służby kontroli skarbowej nie mogą zostać w żadnym przypadku wykorzystane przez inne organy (na potrzeby postępowań innych niż karne skarbowe).

Z drugiej strony – żaden ze wskazanych aktów prawnych nie przewiduje obowiązku zwierzchnika służb (ministra spraw wewnętrznych i administracji – przełożonego komendanta głównego Straży Granicznej, ministra obrony narodowej – przełożonego komendanta głównego Żandarmerii Wojskowej i szefa Służby Kontrwywiadu Wojskowego, prezesa Rady Ministrów – przełożonego szefów ABW, AW i CBA, ministra finansów – przełożonego generalnego inspektora kontroli skarbowej) lub prokuratora generalnego przedstawiania parlamentowi informacji o sposobie wykonywania kontroli operacyjnej przez podległe im służby. To z kolei utrudnia nadzór polityczny i społeczny nad kontrolą operacyjną realizowaną przez służby specjalne.

Dodać należy w tym kontekście, że jedynie ustawa o CBA zawiera uregulowanie zobowiązujące jej szefa do przekazywania parlamentowi sprawozdania z działalności podległej mu agencji[14]. Ukształtowane jest ono jednak (art. 12 ust. 4) bardzo specyficznie: „Szef CBA przedstawia corocznie do dnia 31 marca Sejmowi oraz Senatowi informację o wynikach działalności CBA, z wyjątkiem informacji, do których stosuje się przepisy o ochronie informacji niejawnych". Takie unormowanie nie może być podstawą ujawnienia informacji o statystykach dotyczących kontroli operacyjnej dokonywanej przez CBA, ponieważ nie jest to informacja o wynikach działalności.

[14] Publicznie dostępne nie są też sprawozdania z działalności CBA, przekazywane prezesowi Rady Ministrów oraz Sejmowej Komisji do Spraw Służb Specjalnych przez Szefa CBA na podstawie art. 12 ust. 3 ustawy o CBA.

W jednej ze spraw sądowych (wyrok NSA z 7 lipca 2010 r., Sygn. Akt I OSK 592/10) przyjęto, że niedopuszczalność ujawnienia informacji o praktyce stosowania kontroli operacyjnej wynika również z wyłączenia dopuszczalności udzielania informacji o środkach i formach realizacji zadań służb specjalnych.

I tak, art. 9d ustawy o SG stanowi: „Udzielenie informacji o szczegółowych formach, zasadach i organizacji, a także o prowadzonych czynnościach operacyjno-rozpoznawczych oraz o stosowanych środkach i metodach ich realizacji może nastąpić wyłącznie w przypadku, gdy istnieje uzasadnione podejrzenie popełnienia przestępstwa ściganego z oskarżenia publicznego w związku z wykonywaniem tych czynności…". Z kolei art. 35 ust. 1 ustawy o ABW i AW, art. 39 ust. 1 ustawy o SKW i SWW, art. 40 ust. 1 ustawy o ŻW oraz art. 24 ust. 1 ustawy o CBA ogólnie nakładają na służby specjalne obowiązek zapewnienia ochrony „środków, form i metod realizacji zadań, zgromadzonych informacji oraz własnych obiektów i danych identyfikujących funkcjonariuszy". Art. 37 ust. 1 ustawy o kontroli skarbowej zawiera uregulowanie łączące obydwa wskazane powyżej.

Podkreślić należy wszakże, iż brzmienie bardzo zbliżone do powyższych ma art. 20a ust. 1 ustawy o Policji („W związku z wykonywaniem zadań wymienionych w art. 1 ust. 2 Policja zapewnia ochronę form i metod realizacji zadań, informacji oraz własnych obiektów i danych identyfikujących policjantów"), co trafnie uznano za niesprzeczne z obowiązkami informacyjnymi prokuratora generalnego określonymi w art. 19 ust. 22 tej samej ustawy. Przemawia to – wbrew stanowisku NSA – przeciwko dopuszczalności ujawniania statystyk o skali i sposobach korzystania ze służb specjalnych z przysługujących im uprawnień kontrolnych.

4.2. Dostęp do danych związanych z przekazami i użytkownikami sieci

Ustawy regulujące działalność Policji i służb specjalnych zawierają przepisy szczególne, które wyłączają stosowanie gwarancji ochrony praworządności zawartych zarówno w uregulowaniach dotyczących kontroli operacyjnej, jak i określonych w k.p.k. w odniesieniu do danych związanych z przekazami i użytkownikami sieci.

Znów za punkt odniesienia przyjąć można przepis ustawy o Policji (art. 20c):

> 1. W celu zapobiegania lub wykrywania przestępstw Policja może mieć udostępniane dane, o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne[15], zwane dalej „danymi telekomunikacyjnymi", oraz może je przetwarzać.
> 2. Podmiot prowadzący działalność telekomunikacyjną udostępnia nieodpłatnie dane telekomunikacyjne:
> 1) policjantowi wskazanemu w pisemnym wniosku Komendanta Głównego Policji lub komendanta wojewódzkiego Policji albo osoby przez nich upoważnionej;
> 2) na ustne żądanie policjanta posiadającego pisemne upoważnienie osób, o których mowa w pkt 1;
> 3) za pośrednictwem sieci telekomunikacyjnej policjantowi posiadającemu pisemne upoważnienie osób, o których mowa w pkt 1.
> 2a. W przypadku, o którym mowa w ust. 2 pkt 3, udostępnianie danych telekomunikacyjnych odbywa się bez udziału pracowników podmiotu prowadzącego działalność telekomunikacyjną lub przy niezbędnym

[15] Tj. wszelkie dane telekomunikacyjne i o użytkownikach sieci, poza treścią indywidualnych komunikatów.

ich udziale, jeżeli możliwość taka jest przewidziana w porozumieniu zawartym pomiędzy Komendantem Głównym Policji a tym podmiotem. (…)

5. Udostępnienie Policji danych telekomunikacyjnych może nastąpić za pośrednictwem sieci telekomunikacyjnej jeżeli:

1) wykorzystywane sieci telekomunikacyjne zapewniają:

a) możliwość ustalenia osoby uzyskującej dane, ich rodzaju oraz czasu, w którym zostały uzyskane,

b) zabezpieczenie techniczne i organizacyjne uniemożliwiające osobie nieuprawnionej dostęp do danych;

2) jest to uzasadnione specyfiką lub zakresem zadań wykonywanych przez jednostki organizacyjne Policji albo prowadzonych przez nie czynności.

6. Materiały uzyskane w wyniku czynności podjętych na podstawie ust. 2, które zawierają informacje mające znaczenie dla postępowania karnego, Policja przekazuje właściwemu miejscowo i rzeczowo prokuratorowi.

7. Materiały uzyskane w wyniku czynności podjętych na podstawie ust. 2, które nie zawierają informacji mających znaczenie dla postępowania karnego, podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu.

Zacytowany przepis nie zawiera żadnych mechanizmów nadzoru jakiegokolwiek organu zewnętrznego (sądu lub prokuratora) nad działaniami Policji i służb specjalnych, ograniczeń zakresu przestępstw, w przypadku których może zostać zastosowane udostępnienie danych telekomunikacyjnych, ani maksymalnego okresu kontroli danych. Jednocześnie, o czym była mowa wcześniej, kontrola może się odbywać bez udziału przedsiębiorcy telekomunikacyjnego, a do uzyskania dostępu do danych przez policjanta wystarcza już posiadanie pisemnego upoważnienia wydanego przez komendanta wojewódzkiego Policji. Upoważnienie to siłą rzeczy nie dotyczy indywidualnej sprawy, lecz ogólnie – inwigilowania abonentów i innych użytkowników danej sieci. Co więcej, z kontroli nie sporządza się protokołu ani notatki, a zatem po dostępie może nie pozostać żaden ślad. Nawet w przypadku dostępu bezpośrednio za pomocą sieci telekomunikacyjnej ustawa jedynie przewiduje, że sieć ma zapewnić możliwość ustalenia osoby uzyskującej dane, ich rodzaju oraz czasu, w którym zostały uzyskane. Nie oznacza to jednak, iż sieć ma także rejestrować i utrwalać powyższe informacje, a weryfikacja sposobu stosowania wskazanego przepisu w praktyce jest niemożliwa, ponieważ stanowi informację niejawną. W konsekwencji dostęp Policji i służb specjalnych do danych telekomunikacyjnych (poza treścią przekazu) jest kontrolowany jedynie szczątkowo.

Niemal identyczne unormowania zawarte są w:

- art. 10b ustawy o SG,
- art. 28 ustawy o ABW i AW,
- art. 32 ustawy o SKW i SWW,
- art. 30 ustawy o ŻW,
- art. 18 ustawy o CBA,
- art. 36b UKS.

Różnica polega głównie na tym, że art. 28 ustawy o ABW i AW, art. 32 ustawy o SKW i SWW, a także art. 18 ustawy o CBA nie przewidują w ogólne możliwości usunięcia zgromadzonych przez te służby danych operacyjnych, także wówczas, gdy dane te są nieprzydatne z punktu widzenia realizacji celu, dla którego zostały zebrane. Z kolei art. 36b ust. 5 UKS przewiduje zniszczenie danych tylko wtedy, gdy minister właściwy do spraw finansów publicznych uzna

wystąpienie o te dane za nieuzasadnione. Zniszczenie danych jest więc uzależnione od, w dużej mierze dyskrecjonalnej, decyzji ministra finansów[16].

5. Dostęp do danych o odbiorcach usług świadczonych drogą elektroniczną

Art. 18 ust. 6 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, (Dz.U. Nr 144 poz. 1204 ze zm.) – dalej: uśude – postanawia, iż każdy podmiot świadczący usługi objęte tą ustawą (w pewnym uproszczeniu: usługi online) udziela informacji o wszystkich posiadanych przez siebie danych użytkowników „organom państwa na potrzeby prowadzonych przez nie postępowań". Innymi słowy dane te udostępniane mają być wszelkim organom państwowym, bez żadnych mechanizmów zewnętrznego nadzoru nad proporcjonalnością lub zasadnością tego rodzaju żądań. W praktyce jedynym warunkiem żądania ich ujawnienia pozostaje związek pomiędzy nimi a już toczącym się (jakimkolwiek) postępowaniem prowadzonym przez wnioskujący organ. Usługodawca oczywiście nie jest przy tym w stanie zweryfikować, czy wniosek realizuje także drugą przesłankę ujawnienia – istnienie „potrzeby" ich ujawnienia – czyli nie może ustalić znaczenia owych danych dla prowadzonego postępowania.

6. Podsumowanie

Wykorzystywanie przez Policję i służby specjalne danych telekomunikacyjnych wymaga wyważenia przeciwstawnych interesów, z jednej strony:

- społeczeństwa w zapewnieniu bezpieczeństwa publicznego;
- uprawnionych organów ścigania w maksymalnie sprawnej realizacji ich obowiązków ustawowych;

oraz z drugiej strony:

- społeczeństwa w zagwarantowaniu praworządności działań organów państwa (art. 7 Konstytucji);
- społeczeństwa w zagwarantowaniu ochrony prywatności, wolności wypowiedzi i danych osobowych (art. 8 EKPCzł, art. 31 ust. 3 Konstytucji – konieczność ograniczeń konstytucyjnych wolności i praw z punktu widzenia społeczeństwa demokratycznego, art. 47 – zasada ochrony życia prywatnego, art. 49 – zasada wolności i ochrony tajemnicy komunikowania się, art. 51 – ochrona informacji o sobie);
- przedsiębiorców telekomunikacyjnych i dostawców usług świadczonych drogą elektroniczną w minimalizacji przerzucanych na nich kosztów współpracy z organami ścigania i nakładania obowiązków prowadzących do inwigilacji własnych klientów.

Najważniejsza kwestia dotycząca wartości branych pod uwagę, gdy chodzi o wykorzystywanie przez Policję i służby specjalne danych telekomunikacyjnych, dotyczy ustalenia, jakie mechanizmy kontrolne są **konieczne w społeczeństwie demokratycznym**. „Konieczność" zastosowania ograniczenia oznacza przy tym obowiązek ustawodawcy wyboru najmniej uciążliwego środka (por. wyrok TK z 26 kwietnia 1999 r., sygn. akt K 33/98; wyrok TK z 11 maja 1999 r., sygn. akt K 13/98) oraz nakaz „skonstruowania takiego systemu zabezpieczeń

[16] Por. także Raport Komisji Praw Człowieka przy Naczelnej Radzie Adwokackiej pt. *Retencja Danych: Troska o bezpieczeństwo czy inwigilacja obywateli* z 21 maja 2011 r., dostępny na http://adwokatura.pl/wp-content/uploads/2011/05/Raport-pdf.pdf, s. 36.

proceduralnych, który w skuteczny sposób zabezpieczałby przed ekscesami w postaci zbierania danych wykraczających poza rzeczywisty cel, niewłaściwe zabezpieczenie czy wykorzystanie zebranych danych" (wyrok TK z 12 grudnia 2005 r., sygn. akt K 32/04).

Ponadto, zgodnie z orzecznictwem ETPCzł, środki kontroli stosowane przez władze publiczne mogą być dopuszczalne z perspektywy podstawowego prawa do prywatności jedynie, jeśli są oparte na przewidywalnej dla jednostki podstawie prawnej[17]. Wymóg ten potwierdzony został w sprawach dotyczących zapisów informacji (przechowywanie przez służby specjalne akt zawierających informacje osobowe)[18], zapisów z kamer przemysłowych[19], a także podsłuchów[20]. ETPCzł podkreślił wszakże, że „przewidywalność (*foreseeability*) w szczególnym kontekście niejawnych środków kontroli, takich jak przechwytywanie komunikatów, nie może oznaczać, że jednostka powinna być w stanie przewidzieć, kiedy prawdopodobne jest przechwycenie jej komunikatu przez władze i móc stosownie dostosować swoje postępowanie (…). Niemniej jednak, zwłaszcza kiedy władza przyznana organom wykonawczym realizowana jest niejawnie, aktualne staje się niebezpieczeństwo arbitralności (…). Niezbędne jest zatem stworzenie jasnych, szczegółowych reguł (…), zwłaszcza biorąc pod uwagę coraz większe wyrafinowanie stosowanych technologii (…). Prawo krajowe musi być wystarczająco jasne w swoich postanowieniach, by dać obywatelom adekwatną wskazówkę co do okoliczności i warunków, w których władze publiczne władne są uciekać się do takich środków (…)"[21]. Jeden z komentatorów podsumował orzecznictwo ETPCzł w tym zakresie stwierdzeniem, że środki kontroli, aby były zgodne z prawem do prywatności, muszą być „dopuszczone prawnie, dostępne dla wiedzy społecznej, z wystarczająco precyzyjnymi postanowieniami, aby wyeliminować arbitralne działania władz i by poinformować obywateli o możliwych atakach na ich sferę prywatną"[22].

Przepisy regulujące procedurę dostępu do komunikatów przekazywanych za pomocą sieci telekomunikacyjnych (treść rozmów, wiadomości tekstowe itp.) zawierają szereg gwarancji ochrony prawa do prywatności. O ile jednak bezspornie gwarantują one ochronę praw podstawowych w swoim modelu procesowym (wynikającym z k.p.k.), to ich odpowiedniki pozaprocesowe z ustawy o Policji i służbach specjalnych stały się w ostatnim czasie przedmiotem wniosku RPO do Trybunału Konstytucyjnego w sprawie stosowania przez poszczególne służby w ramach kontroli operacyjnej środków technicznych umożliwiających uzyskiwanie w sposób niejawny informacji i dowodów oraz ich utrwalanie (wystąpienie z 29 czerwca 2011 r., Sygn. RPO/666037/11/II/208 RZ)[23]. Wcześniej, 28 stycznia 2011 r., bardzo zbliżony wniosek został złożony przez grupę posłów SLD. Obydwa wnioski o stwierdzenie niekonstytucyjności dotyczą art. 19 ust. 6 pkt 3 ustawy o Policji oraz identycznych przepisów w ustawach regulujących działalność służb specjalnych. Zgodnie z tymi przepisami kontrola operacyjna może polegać generalnie na „stosowaniu środków technicznych umożliwiających uzyskiwanie w sposób niejawny informacji i dowodów oraz ich utrwalanie". Zarzut dotyczy braku precyzji tego rodzaju normy, która nie konkretyzuje, o jakie środki techniczne, informacje i dowody w niej chodzi.

---

17 Sunday Times p. Zjednoczone Królestwo, sygn. 6538/74, Eur. Ct. H.R. § 49 (1979).
18 Np. Rotaru p. Rumunia, sygn. 28341/95, Eur. Ct. H.R. (2000).
19 Peck p. Zjednoczone Królestwo, sygn. 44647/98, Eur. Ct. H.R. (2003).
20 Np. Amann p. Szwajcaria, sygn. 27798/95, Eur. Ct. H.R. (2000).
21 Weber i Saravia p. Niemcy, sygn. 54934/00, Eur. Ct. H.R. § 93 (2006).
22 F. Bignami, *Privacy and Law Enforcement in the EU: The Data Retention Directive*, 8 Chi. J. Int'l L. 233, 242 (2007).
23 http://www.sprawy-generalne.brpo.gov.pl/pdf/2011/01/666037/1576197.pdf

Najpoważniejszym zarzutem zawartym w obydwu wnioskach jest to, że działania operacyjne podejmowane w trybie k.p.k. obejmują wyłącznie kontrolę i utrwalanie treści rozmów telefonicznych (art. 237 § 1 k.p.k.) oraz kontrolę i utrwalanie treści innych rozmów lub przekazów informacji (art. 241 k.p.k.). Trudno w związku z tym uzasadnić, dlaczego w przypadku analogicznych czynności prowadzonych przez Policję i służby specjalne w trybie pozaprocesowym środki kontroli konieczne w społeczeństwie demokratycznym zostały zakreślone szerzej. Logicznie nasuwa się wniosek, że skoro konieczne w społeczeństwie są węższe ramy uprawnień przewidziane w k.p.k., a ustawy o Policji i służbach specjalnych zakreślają te ramy szerzej, to te ostatnie są zbędne w zakresie, w jakim wykraczają poza wzorzec kodeksowy.

Z drugiej strony nie jest prawdziwe stwierdzenie zawarte w skardze konstytucyjnej RPO, iż „wbrew regule konstytucyjnej, to nie ustawodawca, lecz same służby nieskrępowane w tym zakresie postanowieniami ustawy, określają rodzaje danych o jednostce, które chcą pozyskać w ramach prowadzonej przez siebie kontroli operacyjnej" (s. 13). Kontrola operacyjna w każdym przypadku wymaga zgody prokuratora i sądu, a celem warunkowania jej od stanowiska tych organów jest eliminacja nieproporcjonalnych środków i zagrożenia arbitralnością w działaniu Policji i służb specjalnych. Kwestia ta ma znaczenie zwłaszcza z perspektywy tego, że zagrożenie dla praw jednostki stanowi nie tyle szerokość gamy instrumentów przeciwdziałania przestępczości, co raczej niebezpieczeństwo zastosowania ich wobec osób innych niż przestępcy. Skuteczna kontrola sądowa realizuje ten cel lepiej i bardziej proporcjonalnie – z perspektywy bezpieczeństwa publicznego – niż zamknięty katalog dopuszczalnych technik operacyjnych.

Zamknięty katalog rodzajów kontroli operacyjnej jest też mało racjonalny z perspektywy dynamiki postępu technologicznego. Tempo postępu jest bowiem dużo większe niż możliwości adaptacyjne procesu legislacyjnego. Z tego powodu każdy zamknięty katalog środków kontroli operacyjnej musi w krótkim czasie okazać się nieadekwatny do wymogów skutecznej realizacji nadrzędnego interesu publicznego każdego społeczeństwa w skutecznym zwalczaniu przestępczości. Tym samym model kodeksowy postrzegany może być jako zakreślony węziej niż to, co jest konieczne dla skutecznego zwalczania przestępczości w społeczeństwie demokratycznym.

Kolejną różnicą pomiędzy kodeksowym modelem kontroli operacyjnej a modelem pozakodeksowym jest istnienie tylko w tym pierwszym przypadku obowiązku doręczanie kontrolowanemu podmiotowi zaskarżalnego postanowienia o zarządzeniu kontroli operacyjnej (art. 239 i 240 k.p.k.). Rodzi to pytanie o zasadność rozszerzenia rozwiązania kodeksowego na model pozakodeksowy. Argumentować można bowiem, że kontrolowanemu zagwarantowano by w ten sposób prawo do sądu i rozciągnięto na niego kodeksowe gwarancje procesowe. Wniosek taki oparty jest jednak na fałszywych przesłankach. W przypadku – po pierwsze – zniszczenia materiałów z kontroli operacyjnej lub – po drugie – wszczęcia postępowania karnego takie rozwiązanie okazałoby się nieistotne z punktu widzenia ochrony prywatności, natomiast utrudniałoby zwalczanie przestępczości. W pierwszej bowiem z tych dwóch sytuacji osoba kontrolowana dowiedziałaby się, że była kontrolowana, ale wynik kontroli nie pozwala na wszczęcie postępowania karnego i – w konsekwencji – materiały z kontroli zostały prawidłowo usunięte. Osobom przypadkowo kontrolowanym nie przysługiwałoby w takim przypadku wobec podmiotu kontrolującego żadne roszczenie, natomiast przestępcom zwracano by uwagę na to, iż są przedmiotem zainteresowania organów ścigania. Z kolei w przypadku włączenia do akt

postępowania karnego materiału zebranego w wyniku kontroli operacyjnej prawidłowość sposobu zebrania materiału dowodowego może być kwestionowane na zasadach ogólnych.

Wady obowiązujących reguł dotyczących pozaprocesowej kontroli operacyjnej mają charakter drugorzędny.

Po pierwsze, za nieprawidłowe uznać należy obowiązujące rozwiązanie, według którego następcza sądowa zgoda na kontrolę operacyjną udzielana jest jedynie na podstawie wniosku przedstawionego przez komendanta głównego lub wojewódzkiego Policji i pisemnej zgody właściwego prokuratora, bez przekazywania sądowi odnośnego materiału dowodowego.

Po drugie, ochronę praw podstawowych utrudnia niejednoznaczność w zakresie dopuszczalności publikowania raportów o skali kontroli operacyjnej dokonywanej przez służby specjalne. Obowiązku takiego nie przewidują bowiem przepisy regulujące funkcjonowanie tych służb, a – jak była o tym mowa wcześniej – NSA wręcz interpretuje zawarte w nich przepisy jako wykluczające możliwość ujawnienia tych informacji. Z drugiej strony pierwsza informacja prokuratora generalnego o łącznej liczbie osób, wobec których został skierowany wniosek o zarządzenie kontroli i utrwalania rozmów lub wniosek o zarządzenie kontroli operacyjnej (z 21 czerwca 2011 r.) odnosi się do liczby wniosków skierowanych do sądu lub prokuratora przez „wszystkie uprawnione organy" (http://www.senat.gov.pl/k7/dok/dr/1250/1267.pdf), co wyraźnie sugeruje, iż dotyczy też służb specjalnych. Kwestia ta nie może wszakże zostać rozstrzygnięta jednoznacznie, ponieważ omawiana informacja nie uszczegóławia – poza Policją – zakresu objętych nią wnioskodawców.

Z bardzo dużą rezerwą podejść należy natomiast do **gwarancji przestrzegania praw podstawowych wynikających z reguły dostępu do danych związanych z przekazami i użytkownikami sieci (informacji innych niż treść komunikatu)**. To tej kategorii danych dotyczy obowiązek retencji wynikający z dyrektywy 2006/24, w tym zawarty w jej art. 1 ust. 1 wymóg zapewnienia dostępności danych „do celu dochodzenia, wykrywania i ścigania poważnych przestępstw". Tymczasem w art. 218 § 1 k.p.k. dostęp do danych możliwy jest „jeżeli mają znaczenie dla toczącego się postępowania", a według art. 20c ust. 1 ustawy o Policji (i bardzo zbliżonych przepisów zawartych w aktach regulujących funkcjonowanie poszczególnych służb) dane związane z przekazami i użytkownikami sieci udostępniane są „w celu zapobiegania lub wykrywania przestępstw"[24]. Brak zawężenia zakresu przestępstw, w przypadku których wykorzystana może zostać ta kategoria danych, stanowi jawne naruszenie przepisów dyrektywy i godzi w założenie przewidywalności ograniczenia praw podstawowych. Tym samym, jak trafnie zauważyła RPO, poprzez użycie otwartych klauzul generalnych, przepisy te naruszają konstytucyjny wymóg konkretności ograniczenia praw podstawowych (w tym przypadku zawartych w art. 49 Konstytucji)[25].

Ponadto, ustawodawca nie wyłączył żadnej kategorii użytkowników z kręgu podmiotów, do których danych telekomunikacyjnych dostęp mogą uzyskać Policja i służby specjalne, chociaż dane te mogą być objęte tajemnicą notarialną, lekarską, radcy prawnego, a zwłaszcza adwokacką

[24] Szerzej wątek ten omówiła Rzecznik Praw Obywatelskich w piśmie do Premiera z 17 stycznia 2011 r., sygn. RPO-662587-II-10/ST, dostępnym na http://www.sprawy-generalne.brpo.gov.pl/pdf/2010/12/662587/1540465.pdf, s. 7–10.

[25] Pismo do Premiera z 17 stycznia 2011 r., s. 17 i Raport Komisji Praw Człowieka przy Naczelnej Radzie Adwokackiej, pt. *Retencja danych: troska o bezpieczeństwo czy inwigilacja obywateli* z 21 maja 2011 r., dostępny na http://adwokatura.pl/wp-content/uploads/2011/05/Raport-pdf.pdf, s. 30.

lub dziennikarską[26]. Tym samym uprawnienie Policji i służb specjalnych nie podlegają ograniczeniu analogicznemu do tego, jaki na gruncie postępowania karnego wynika z art. 180 § 2 k.p.k., zgodnie z którym zniesienie owych tajemnic jest możliwe wyłącznie, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a dana okoliczność nie może być ustalona na podstawie innego dowodu. Tego rodzaju brak godzi w same podstawy porządku demokratycznego.

W przypadku omawianej tu kategorii danych brak jest też wskazania maksymalnej długości kontroli, spójnych reguł usuwania danych zebranych w jej trakcie i rejestrowania faktu jej dokonywania i przebiegu. Przede wszystkim jednak brak jest mechanizmów nadzoru zewnętrznego (sądu lub prokuratora) nad działaniami Policji i służb specjalnych.

Postulować należy zatem odpowiednie stosowanie do dostępu do danych związanych z przekazami i użytkownikami sieci warunków stosowania kontroli operacyjnej (w tym dotyczących maksymalnego czasu kontroli i reguł usuwania danych zebranych w jej trakcie), przy czym dopuszczalność stosowania kontroli danych związanych z przekazami i użytkownikami sieci należałoby uzależnić od wydania postanowienia przez właściwego prokuratora.

Nadzór prokuratorski nad zgodnością z prawem inicjowania i przeprowadzania czynności operacyjno-rozpoznawczych (zawężony jednak do zakresu przewidzianego w ustawach regulujących organizację i przedmiot działania tych organów) został już wprowadzony do ustawy o prokuraturze (art. 3 ust. 1 pkt 7a) ustawą z 4 lutego 2011 r., a znowelizowany tym samym aktem art. 18 ust. 5 ustawy o prokuraturze przyznał ministrowi sprawiedliwości, po zasięgnięciu opinii prokuratora generalnego, uprawnienie do wydania rozporządzenia określającego „sposób realizacji kompetencji prokuratora w zakresie nadzoru nad czynnościami operacyjno-rozpoznawczymi, mając na uwadze zapewnienie merytorycznej i efektywnej kontroli podstaw faktycznych wnioskowanych czynności". Wprowadzenie mechanizmów nadzoru zewnętrznego nad dokonywaną przez Policję i służby specjalne kontrolą danych związanych z przekazami i użytkownikami sieci odbyć się zatem powinno poprzez rozszerzenie powyższych reguł na ten rodzaj kontroli, co powinno zostać powiązane ze stosownymi zmianami w ustawie o Policji i służbach specjalnych.

Niestosownym wydaje się natomiast postulowane przez RPO warunkowanie kontroli danych innych niż treść przekazu od zgody sądu (na wzór rozwiązanie obowiązującego w przypadku kontroli operacyjnej)[27]. Pamiętać należy bowiem, że – jak słusznie zauważył Trybunał Konstytucyjny w wyroku z 23 czerwca 2009 r. (sygn. akt K 54/07, OTK z 2009 r.): „Sfera prywatna jest zbudowana z różnych kręgów w mniejszym lub większym stopniu otwartych (prawnie) na oddziaływanie zewnętrzne, gdzie konstytucyjna aprobata dla władczego wkroczenia przez władze nie jest jednakowa (…)". Innymi słowy inne – wyższe – są niezbędne gwarancje ochrony praw podstawowych w przypadku bardziej inwazyjnego środka stosowanego przez władze publiczne (kontrola operacyjna) niż w przypadku środka mniej inwazyjnego (inne dane)[28]. Nadzór prokuratorski nie jest też instrumentem mniej skutecznym

[26] Por. także Pismo do Premiera z dnia 17 stycznia 2011 r., s. 10–11 i Raport Komisji Praw Człowieka przy Naczelnej Radzie Adwokackiej, s. 32.

[27] Pismo do Premiera z 17 stycznia 2011 r., s. 21.

[28] Tę samą uwagę odnieść można do postulatu stosowania do kontroli omawianej to kategorii danych zasady subsydiarności – dopuszczalności ich kontrolowania tylko o ile inne środki dowodowe byłyby nieprzydatne. Por. Raport Komisji Praw Człowieka przy Naczelnej Radzie Adwokackiej, pt. *Retencja danych: troska o bezpieczeństwo czy*

niż sądowy. Jak bowiem wynika z informacji prokuratora generalnego o łącznej liczbie osób, wobec których został skierowany wniosek o zarządzenie kontroli i utrwalania rozmów lub wniosek o zarządzenie kontroli operacyjnej[29], w 2010 r. prokuratorzy nie wyrazili zgody na kontrolę operacyjną wobec 218 osób, podczas gdy sądy – jedynie wobec 52 osób.

Wniosek o konieczności wprowadzenia nadzoru prokuratorskiego nad działaniami kontrolnymi rozciągnąć należy także na przypadki **kontroli danych o odbiorcach usług świadczonych drogą elektroniczną**. Nadzór ten w pierwszej kolejności obejmować powinien konieczność uzyskania zgody prokuratora na wystąpienie do dostawcy usług świadczonych drogą elektroniczną z wnioskiem o ujawnienie danych użytkowników. Zgoda taka udzielana powinna być tylko wówczas, gdy jak wskazuje to aktualnie uśude, istnieje „potrzeba" dostępu organów państwowych do danych o użytkownikach usług świadczonych drogą elektroniczną.

Dostęp do wszelkich danych telekomunikacyjnych (w tym do danych niebędących treścią przekazu) – realizowany zarówno bezpośrednio za pośrednictwem sieci jak i pośrednio, przy pomocy pracowników przedsiębiorcy telekomunikacyjnego – warunkowany powinien być też od dokonania wpisu kontroli do rejestru odpowiadającego temu, o którym mowa w § 6 rozporządzenia Ministra Sprawiedliwości z dnia 28 kwietnia 2004 r. w sprawie sposobu technicznego przygotowania systemów i sieci służących do przekazywania informacji. Rejestr taki powinien zawierać przynajmniej:

1) sygnaturę akt sprawy i datę wydania postanowienia o kontroli danych;
2) nazwę podmiotu uprawnionego;
3) imię i nazwisko użytkownika systemu lub sieci albo nazwę podmiotu będącego użytkownikiem, w stosunku do którego zarządzono kontrolę danych;
4) czas trwania kontroli.

Kwestia rejestracji faktu kontroli danych jest istotna przede wszystkim ze względu na automatyzację i postępującą niezależność organów państwa od przedsiębiorców telekomunikacyjnych. W konsekwencji powstają bardzo wyraźne wyłomy w mechanizmach potwierdzenia dokonania kontroli. Dla przykładu, jak była o tym mowa wcześniej, z jednej strony udzielony przez przedsiębiorcę telekomunikacyjnego dostęp do sieci ma umożliwiać zarówno kontrolę komunikatu, jak i innych danych telekomunikacyjnych. Z drugiej strony art. 20c ust. 5 ustawy o Policji, określający zakres rejestrowanych informacji o dostępie (oraz jego odpowiedniki w ustawach o służbach specjalnych), dotyczy tylko drugiej z tych kategorii informacji. Oznacza to w praktyce, iż dostęp Policji do treści komunikatu może być nierejestrowany i w żaden sposób niekontrolowany.

Zwrócić należy także uwagę na to, że zgodnie z art. 180g ust. 1 oraz 2 prezesowi UKE oraz Komisji Europejskiej przedstawiane są przez przedsiębiorców telekomunikacyjnych informacje o:

1) łącznej liczbie przypadków, w których uprawnionym podmiotom, sądowi i prokuratorowi były udostępnione dane związane z przekazami i użytkownikami sieci;
2) czasie, jaki upłynął między datą zatrzymania danych a datą złożenia przez te podmioty wniosku lub ustnego żądania o ich udostępnienie;

---

inwigilacja obywateli z 21 maja 2011 r., dostępny na http://adwokatura.pl/wp-content/uploads/2011/05/Raport-pdf.pdf, s. 32–33. Kontrola danych billingowych nie narusza prywatności w takim stopniu, jak kontrola treści przekazu, a tym samym nie wymaga tak dalekich gwarancji ochronnych, by zapewnić porównywalny poziom ochrony prywatności.

[29] Z 21 czerwca 2011 r., dostępna na http://www.senat.gov.pl/k7/dok/dr/1250/1267.pdf.

3) łącznej liczbie przypadków, w których wniosek lub ustne żądanie nie mógł być zrealizowany.

W chwili obecnej informacje te przekazywane są opinii publicznej jedynie fragmentarycznie. Ujawnianie ich powinno być natomiast regułą, ponieważ nie ogranicza zdolności operacyjnych organów państwa, a pozwala na zwiększenie kontroli społecznej nad sposobem korzystania przez władze publiczne z uprawnień kontrolnych.

Jak warto dodać dla porządku, brak mechanizmów kontrolnych nie oznacza, że dane telekomunikacyjne zebrane przez Policję lub służby specjalne mogą być w dowolny sposób wykorzystywane. Policjant lub funkcjonariusz służb specjalnych ujawniający takie dane innej osobie niż prokurator lub sąd karny popełni przestępstwo naruszenia tajemnicy służbowej (typ przestępstwa przeciwko ochronie informacji), za co grozi kara do 3 lat pozbawienia wolności. Jak stanowi art. 266 § 2 ustawy z dnia 6 czerwca 1997 r. Kodeks karny (Dz.U. z 1997 r. Nr 88 poz. 553 z późn. zm.): „Funkcjonariusz publiczny, który ujawnia osobie nieuprawnionej informację niejawną o klauzuli »zastrzeżone« lub »poufne« lub informację, którą uzyskał w związku z wykonywaniem czynności służbowych, a której ujawnienie może narazić na szkodę prawnie chroniony interes, podlega karze pozbawienia wolności do lat 3". Ochrona prywatności jest oczywiście prawnie chronionym interesem, a ujawnienie danych telekomunikacyjnych w każdym przypadku może ten interes narazić na szkodę.