Miłosz Kiziński

Retencja danych telekomunikacyjnych

Streszczenie

Przedmiotem opracowania są ramy prawne systemu retencjonowania danych telekomunikacyjnych i ich udostępniania uprawnionym podmiotom, Służbie Celnej, sądowi i prokuratorowi. Artykuł przedstawia zakres przedmiotowy i podmiotowy obowiązku zatrzymywania danych, zasady udostępniania danych, kontrowersje związane z retencją danych oraz znaczenie wyroku Trybunału Konstytucyjnego w sprawie o sygn. K 23/11.

Wstęp

Zgodnie z art. 180a ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne[1], na operatorze publicznej sieci telekomunikacyjnej oraz dostawcy publicznie dostępnych usług telekomunikacyjnych ciąży obowiązek retencji danych telekomunikacyjnych. Obecne przepisy dotyczące retencji danych zostały wprowadzone do polskiego systemu prawnego wskutek implementacji dyrektywy Parlamentu Europejskiego i Rady 2006/24/WE[2].

Celem przepisów ustanawiających retencję danych jest zwalczanie przestępczości i zapobieganie terroryzmowi. Potrzeba wprowadzania do systemów prawnych regulacji dotyczących zatrzymywania danych telekomunikacyjnych i ich udostępniania służbom policyjnym i ochrony państwa oraz organom wymiaru sprawiedliwości zaczęła być podkreślana po zamachu na World Trade Center w dniu 11 września 2001 r. i rozpoczęciu „wojny z terroryzmem". Na gruncie europejskim istotnym czynnikiem wpływającym na wprowadzenie powszechnego obowiązku retencji były zamachy terrory-

[1] Dz. U. z 2014 r., poz. 243 ze zm. O ile w artykule nie wskazano innego aktu prawnego, powoływane przepisy dotyczą tejże ustawy.

[2] 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 zmieniająca dyrektywę 2002/58/WE (Dz. U. UE. L. z 2006 r., Nr 105, poz. 54, dalej jako „Dyrektywa retencyjna"). Należy nadmienić, iż rozwiązania prawne umożliwiające sięganie przez organy policyjne i ochrony państwa do danych gromadzonych przez przedsiębiorców telekomunikacyjnych, jakkolwiek mniej rozbudowane, istniały w polskim systemie prawnym również przed implementacją Dyrektywy retencyjnej.

styczne w Madrycie (11 marca 2004 r.) i w Londynie (7 lipca 2005 r.)[3]. W uzasadnieniu projektu ustawy z dnia 24 kwietnia 2009 r. o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw[4], która implementowała do nowelizowanego aktu prawnego regulacje z Dyrektywy retencyjnej, wskazano na położenie geograficzne Polski na szlakach wschód – zachód i północ – południe jako na czynnik powodujący bardzo duże prawdopodobieństwo wykorzystania terytorium naszego kraju jako zaplecza logistycznego lub punktu tranzytowego dla ugrupowań terrorystycznych. Zwrócono również uwagę na ryzyko utworzenia nowego szlaku przerzutu heroiny do Europy przez terytorium Polski za pośrednictwem żołnierzy służących w Afganistanie. Jako że przemyt heroiny stanowi jedno ze źródeł finansowania al-Kaidy, udział polskich żołnierzy w przemycie mógłby, w opinii autora projektu nowelizacji z 2009 r., mieć negatywny wpływ na sojuszniczą wiarygodność Polski.

Zakres przedmiotowy obowiązku retencji danych

Obowiązek retencji danych obejmuje cztery powiązane ze sobą czynności: zatrzymywanie danych, przechowywanie ich przez okres wskazany przepisami prawa, udostępnianie podmiotom uprawnionym do ich uzyskania oraz ochronę danych (art. 180a ust. 1). Przepisy dotyczące retencji danych telekomunikacyjnych są elementem kompleksu przepisów określających obowiązki, jakie przedsiębiorcy telekomunikacyjni realizują na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego. Przedsiębiorcy telekomunikacyjni są zobowiązani m.in. do zapewnienia dostępu i utrwalania przekazów telekomunikacyjnych i tzw. danych towarzyszących (art. 179 ust. 3) oraz do udostępniania uprawnionym podmiotom, Służbie Celnej, sądowi i prokuratorowi – oprócz danych retencyjnych – również szeregu innych przetwarzanych przez siebie danych telekomunikacyjnych (art. 180d).

Operator oraz dostawca usług telekomunikacyjnych są zobowiązani zatrzymywać i przechowywać dane retencyjne, generowane w sieci telekomunikacyjnej lub przez nich przetwarzane, na terytorium Rzeczypospolitej Polskiej, przez okres 12 miesięcy, licząc od dnia połączenia lub nieudanej próby połączenia (art. 180a). Z upływem tego okresu dane retencyjne podlegają zniszczeniu, o ile nie podlegały zabezpieczeniu zgodnie z przepisami odrębnymi. Okres retencji został skrócony do 12 miesięcy ustawą nowelizacyjną

[3] Fundacja Panoptykon, „Telefoniczna Kopalnia Informacji. Przewodnik", s. 20; http://panoptykon.org/biblio/telefoniczna–kopalnia–informacji–przewodnik.
[4] Dz. U. Nr 85, poz. 716.

z 2012 r.[5]; poprzednio wynosił 24 miesiące. Dyrektywa retencyjna pozwalała na implementację do krajowych systemów prawnych okresu zatrzymywania danych nie krótszego niż 6 miesięcy oraz nie dłuższego niż dwa lata od daty połączenia[6]. Przechowywane dane podlegają udostępnieniu uprawnionym podmiotom, a także Służbie Celnej, sądowi i prokuratorowi, na zasadach określonych w przepisach odrębnych. Katalog uprawnionych podmiotów, zawarty w art. 179 ust. 3, obejmuje Policję, Straż Graniczną, Agencję Bezpieczeństwa Wewnętrznego, Służbę Kontrwywiadu Wojskowego, Żandarmerię Wojskową, Centralne Biuro Antykorupcyjne i wywiad skarbowy. Dane podlegające retencji powinny być chronione przez przypadkowym lub bezprawnym zniszczeniem, utratą lub zmianą, nieuprawnionym lub bezprawnym przechowywaniem, przetwarzaniem, dostępem lub ujawnieniem. Ochrona powinna być sprawowana z uwzględnieniem przepisów art. 159–175a, art. 175c i art. 180e. Zastosowanie mają przed wszystkim przepisy dotyczące ochrony tajemnicy telekomunikacyjnej, gdyż praktycznie całość danych retencyjnych to jednocześnie dane stanowiące tajemnicę telekomunikacyjną[7]. Zgodnie z art. 180e, w celu ochrony danych podlegających retencji przedsiębiorca telekomunikacyjny stosuje właściwe środki techniczne i organizacyjne oraz zapewnia dostęp do tych danych jedynie upoważnionym pracownikom. Wydaje się, iż chodzi o osoby zatrudnione na podstawie umowy o pracę w rozumieniu Kodeksu pracy, a nie o osoby, z którymi zawarto np. umowę o świadczenie usług w rozumieniu art. 750 k.c.[8]. Za takim stanowiskiem przemawia zarówno wynik wykładni językowej, jak i względy celowościowe – *ratio legis* tego przepisu jest bowiem zapewnienie właściwych standardów ochrony danych. Czynności retencyjne powinny być realizowane w taki sposób, aby nie powodować ujawnienia przekazu telekomunikacyjnego, czyli np. treści rozmowy telefonicznej lub wiadomości SMS (art. 180a ust. 7).

Retencji podlegają dane niezbędne do ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego i użytkownika końcowego inicjującego połączenie oraz do którego kierowane jest połączenie, jak również dane niezbędne do określenia daty i godziny połączenia, czasu jego trwania, rodzaju połączenia i lokalizacji telekomunikacyjnego urządzenia końcowego (art. 180c ust. 1). Rozporządzenie Ministra Infrastruktury, wydane na podstawie delegacji zawartej w art. 180c ust. 2, konkretyzuje zakres obowiązku

[5] Ustawa z dnia 16 listopada 2012 r. o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw, Dz. U. z 2012 r., poz. 1445.
[6] Art. 6 Dyrektywy retencyjnej.
[7] S. P i ą t e k, Prawo telekomunikacyjne. Komentarz, Warszawa 2013, s. 1090.
[8] A. K r a s u s k i, Prawo telekomunikacyjne. Komentarz, Warszawa 2010, s. 695.

poprzez wskazanie szczegółowego wykazu danych podlegających retencji[9]. Zakres zatrzymywanych danych został określony odrębnie w odniesieniu do stacjonarnej publicznej sieci telekomunikacyjnej, ruchomej publicznej sieci telekomunikacyjnej, usług polegających na przekierowaniu lub przełączaniu połączenia, usługi dostępu do Internetu, usługi poczty elektronicznej oraz usługi telefonii internetowej. Dane podlegające retencji można podzielić na 4 grupy. Oto przykładowy wykaz danych podlegających zatrzymaniu w ruchomej publicznej sieci telekomunikacyjnej:

1) Dane niezbędne do ustalenia zakończenia sieci (telekomunikacyjnego urządzenia końcowego, użytkownika końcowego) inicjującego połączenie albo do którego kierowane jest połączenie. W przypadku ruchomej publicznej sieci telekomunikacyjnej będzie to numer MSISDN[10] użytkownika końcowego, inicjującego połączenie, albo wywoływanego, imię i nazwisko albo nazwa oraz adres użytkownika końcowego, inicjującego połączenie, albo wywoływanego (jeżeli udostępnił te dane), numer IMSI[11] użytkownika końcowego, inicjującego połączenie, albo wywoływanego, pierwsze 14 cyfr numeru IMEI[12] albo numer ESN[13] telekomunikacyjnego urządzenia końcowego inicjującego połączenie, albo wywoływanego, data i godzina pierwszego zalogowania telekomunikacyjnego urządzenia końcowego do ruchomej publicznej sieci telefonicznej, zgodnie z czasem lokalnym oraz współrzędne geograficzne lokalizacji stacji BTS, poprzez którą dokonano tego zalogowania – w przypadku użytkownika usługi przedpłaconej.

2) Dane niezbędne do ustalenia daty i godziny połączenia oraz czasu jego trwania. W przypadku ruchomej publicznej sieci telekomunikacyjnej będzie to data i godzina nieudanej próby połączenia lub zestawienia i zakończenia połączenia zgodnie z czasem lokalnym oraz czas trwania połączenia z dokładnością do 1 sekundy.

3) Dane niezbędne do ustalenia rodzaju połączenia. W przypadku ruchomej publicznej sieci telekomunikacyjnej będzie to określenie wykorzystanej usługi.

---

[9] 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).

[10] Numer MSISDN (*Mobile Subscriber Integrated Services Digital Network*) – numer przydzielony użytkownikowi końcowemu ruchomej publicznej sieci telekomunikacyjnej.

[11] Numer IMSI (*International Mobile Subscriber Identity*) – międzynarodowy numer przydzielony karcie identyfikującej użytkownika w ruchomej publicznej sieci telekomunikacyjnej.

[12] Numer IMEI (*International Mobile Equipment Identity*) – indywidualny międzynarodowy numer identyfikujący telekomunikacyjne urządzenie końcowe, używane w ruchomej publicznej sieci telekomunikacyjnej.

[13] Numer ESN (*Electronic Serial Number*) – indywidualny numer identyfikujący telekomunikacyjne urządzenie końcowe, używane w ruchomej publicznej sieci telekomunikacyjnej wykorzystującej technologię CDMA (*Code Division Multiple Access*).

4) Dane niezbędne do ustalenia lokalizacji telekomunikacyjnego urządzenia końcowego inicjującego połączenie albo do którego kierowane jest połączenie. W przypadku ruchomej publicznej sieci telekomunikacyjnej będzie to: identyfikator anteny stacji BTS[14] (w czasie inicjowania albo rozpoczęcia odbioru połączenia) oraz współrzędne geograficzne stacji BTS, w obszarze której znajdowało się telekomunikacyjne urządzenie końcowe i azymut, wiązka i zasięg roboczy anteny stacji BTS (w czasie, przez który zatrzymywane są dane odnośnie połączenia) – jeśli telekomunikacyjne urządzenie końcowe znajduje się na terytorium Rzeczypospolitej Polskiej albo identyfikator MCC[15] i identyfikator sieci MNC[16], w której zainicjowano albo do której skierowano połączenie – jeśli telekomunikacyjne urządzenie końcowe znajduje się poza granicami Rzeczypospolitej Polskiej.

Artykuł 180a ust. 5 precyzuje, iż retencji podlegają dane dotyczące zarówno połączeń zrealizowanych, jak i nieudanych prób połączenia. Dyrektywa retencyjna odróżniała nieudaną próbę połączenia od przypadku nieuzyskania połączenia telefonicznego (połączenie nieskuteczne). Nieudana próba połączenia była definiowana jako nawiązanie łączności, w którym połączenie nie zostało odebrane lub nastąpiła interwencja sieci. Jeśli połączenie w ogóle nie zostało uzyskane, Dyrektywa retencyjna nie wymagała zatrzymywania danych[17]. Zakres danych podlegających retencji wynika z przepisów prawa i nie jest uzależniony od sposobu prowadzenia działalności gospodarczej przez przedsiębiorcę telekomunikacyjnego ani od stosowanej technologii. Przedsiębiorcy telekomunikacyjni wykonują obowiązki w zakresie retencji danych na własny koszt[18].

Zakres podmiotowy obowiązku retencji danych

Ustawa wskazuje operatora publicznej sieci telekomunikacyjnej oraz dostawcę publicznie dostępnych usług telekomunikacyjnych jako adresatów obowiązku retencji. Zgodnie z art. 2 pkt 27, operatorem jest przedsiębiorca telekomunikacyjny uprawniony do dostarczania publicznych sieci telekomu-

[14] Stacja BTS (*Base Transceiver Station*) – urządzenie umożliwiające połączenie telekomunikacyjnego urządzenia końcowego, używanego w ruchomej publicznej sieci telekomunikacyjnej z częścią stałą tej sieci.

[15] Identyfikator MCC (*Mobile Country Code*) – wskaźnik (kod) kraju, w którym działa dana, ruchoma publiczna sieć telekomunikacyjna.

[16] Identyfikator sieci MNC (*Mobile Network Code*) – identyfikator ruchomej publicznej sieci telekomunikacyjnej na terytorium danego kraju.

[17] Art. 3 ust. 2 *in fine* Dyrektywy retencyjnej.

[18] S. P i ą t e k, Prawo…, *op. cit.*, s. 1088; por. uzasadnienie wyroku SN z dnia 25 marca 2010 r., sygn. I KZP 37/09, OSNKW 2010, nr 5, poz. 43, LEX nr 564521, w którym wyrażony został pogląd, iż koszty udostępnienia danych drogą inną niż za pomocą sieci telekomunikacyjnej (np. drogą pocztową) nie powinny obciążać operatora.

nikacyjnych lub świadczenia usług towarzyszących, zaś dostawcą usług jest przedsiębiorca telekomunikacyjny uprawniony do świadczenia usług telekomunikacyjnych. Każda z definicji akcentuje inny aspekt działalności przedsiębiorcy telekomunikacyjnego. Istotą działalności operatora jest dostarczanie sieci telekomunikacyjnej, przez co należy rozumieć przygotowanie sieci telekomunikacyjnej w sposób umożliwiający świadczenie w niej usług, jej eksploatację, nadzór nad nią lub dający możliwość dostępu telekomunikacyjnego. Natomiast istotą działalności dostawcy usług jest świadczenie usług telekomunikacyjnych, co może się odbywać z wykorzystaniem własnej sieci telekomunikacyjnej lub sieci telekomunikacyjnej należącej do innego operatora. Działalność dostawcy usług może się również opierać na odsprzedaży usług zakupionych u innego dostawcy usług telekomunikacyjnych[19].

Ten sam przedsiębiorca telekomunikacyjny może być zarówno operatorem (w jednym obszarze działalności), jak i dostawcą usług (w innym obszarze działalności). W niektórych modelach biznesowych może dochodzić do oddzielenia funkcji operatora i dostawcy usług. Przykładem takiej sytuacji jest działalność tzw. wirtualnych operatorów (MVNO[20]), czyli przedsiębiorców telekomunikacyjnych oferujących usługi telekomunikacyjne w swoim imieniu, ale z wykorzystaniem infrastruktury telekomunikacyjnej należącej do innego operatora telekomunikacyjnego (tzw. operator infrastrukturalny – MNO[21]). Operator wirtualny pozbawiony możliwości technicznych pozwalających na samodzielne retencjonowanie danych może, na podstawie art. 180b ust. 2, powierzyć realizację tego obowiązku operatorowi infrastrukturalnemu, na którego sieci funkcjonuje. Powołany przepis dopuszcza możliwość powierzenia realizacji obowiązku retencji danych w drodze umowy innemu przedsiębiorcy telekomunikacyjnemu (*outsourcing*). Takie sformułowanie przepisu ogranicza krąg podmiotów, którym przedsiębiorca telekomunikacyjny może powierzyć wykonywanie obowiązków z art. 180a, do innych przedsiębiorców telekomunikacyjnych, co wydaje się uzasadnione ze względu na specyfikę działalności telekomunikacyjnej i konieczność zapewnienia odpowiedniego standardu ochrony danych retencyjnych. Wykładnia literalna przepisu art. 180b ust. 1 oraz względy celowościowe zdają się wskazywać, iż możliwe jest powierzenie realizacji obowiązków retencyjnych jednemu podmiotowi, a nie np. podział tych obowiązków między kilku zleceniobiorców. Wydaje się również, iż nie ma przeszkód, by umowa powierzenia realizacji obowiązków retencyjnych, zawarta z jednym zleceniobiorcą, obejmowała część, a nie całość obowiązków ciążących na przedsiębiorcy telekomunikacyjnym (*argumentum a maiori ad minus*). Niezależnie od zakresu zle-

[19] K. Kawałek, M. Rogalski, Prawo telekomunikacyjne. Komentarz, Warszawa 2010, s. 64.
[20] *Mobile Virtual Network Operator*.
[21] *Mobile Network Operator*.

cenia, zawarcie umowy, o której mowa w art. 180b ust. 2, nie zwalnia zleceniodawcy z odpowiedzialności za realizację obowiązków retencyjnych. Zleceniobiorca ponosi natomiast odpowiedzialność kontraktową wobec zleceniodawcy. Konstrukcja powierzenia realizacji obowiązków w zakresie retencji danych jest też przewidziana w ofercie ramowej określającej warunki dostępu telekomunikacyjnego do sieci Orange Polska S.A., skierowanej do przedsiębiorców telekomunikacyjnych świadczących usługi z wykorzystaniem infrastruktury tego operatora i zatwierdzanej przez Prezesa Urzędu Komunikacji Elektronicznej[22]. Ustawa dopuszcza ponadto możliwość wspólnego wykonywania obowiązków retencyjnych przez dwóch lub więcej operatorów lub dostawców usług (art. 180b ust. 1), np. w celu minimalizacji kosztów działalności[23].

Przedsiębiorca telekomunikacyjny, który zaprzestaje działalności telekomunikacyjnej, powinien przekazać dane retencyjne innemu przedsiębiorcy telekomunikacyjnemu do dalszego przechowywania, udostępniania oraz ochrony (art. 180a ust. 2). W przypadku ogłoszenia upadłości przedsiębiorcy telekomunikacyjnego dane retencyjne należy przekazać do dalszego przechowywania, udostępniania oraz ochrony Prezesowi Urzędu Komunikacji Elektronicznej (art. 180a ust. 3).

Z obowiązku retencji danych zwolnieni są przedsiębiorcy telekomunikacyjni, których działalność polega wyłącznie na dostarczaniu udogodnień towarzyszących lub rozpowszechnianiu lub rozprowadzaniu programów radiofonicznych lub telewizyjnych[24].

Obowiązki dotyczące retencji danych dotyczą podmiotów działających w sferze komunikacji publicznej[25]. Adresatami obowiązku retencyjnego są operator publicznej sieci telekomunikacyjnej i dostawca publicznie dostępnych usług telekomunikacyjnych. Publiczna sieć telekomunikacyjna to sieć telekomunikacyjna wykorzystywana głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych (art. 2 pkt 29). Publicznie dostępną usługą telekomunikacyjną nazywa ustawodawca taką usługę telekomunikacyjną, która jest dostępna dla ogółu użytkowników (art. 2 pkt 31). Kryterium publiczności jest więc istotne dla określenia kręgu adresatów obowiązku z art. 180a. Obowiązek retencyjny ciąży niewątpliwie na przedsiębiorcy telekomunikacyjnym świadczącym usługi telekomunikacyjne dostępne dla każdego podmiotu, który wyrazi wolę skorzystania z takiej usługi. Ograniczenie

[22] http://uke.gov.pl/zmiana–oferty–ramowej–dla–tp–13177.
[23] K. K a w a ł e k, M. R o g a l s k i, Prawo…, *op. cit.*, s. 961–962.
[24] Paragraf 13 rozporządzenia 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).
[25] S. P i ą t e k, Prawo…, *op. cit.*, s. 1087.

zakresu podmiotowego oferty poprzez skierowanie jej do określonej grupy użytkowników (np. do przedsiębiorców, do konsumentów) nie pozbawia usługi cechy publiczności i nie znosi obowiązku retencji.[26] Również terytorialne ograniczenie obszaru, na jakim przedsiębiorca telekomunikacyjny świadczy usługi, nie jest wystarczające do stwierdzenia, że nie jest to usługa publicznie dostępna[27]. Obowiązek retencyjny nie ciąży natomiast na podmiotach eksploatujących własne (wewnętrzne, prywatne) sieci telekomunikacyjne, wyłącznie dla własnych potrzeb, jak również na podmiotach dysponujących siecią telekomunikacyjną w celu świadczenia usług telekomunikacyjnych innych niż publicznie dostępne[28]. Zastrzegając, że każdy stan faktyczny powinien być poddany odrębnej ocenie, można wyrazić pogląd, iż obowiązek retencyjny nie dotyczy niektórych sieci telekomunikacyjnych o charakterze prywatnym (np. domowych) oraz w przedsiębiorstwach[29].

Tryb udostępniania danych retencyjnych

Kwestia gromadzenia i dostępu do danych retencyjnych została uregulowana na dwóch płaszczyznach. Przepisy przywoływanej ustawy określają zakres obowiązków retencyjnych nałożonych na przedsiębiorców telekomunikacyjnych, natomiast zasady i tryb udostępniania danych podlegających retencji uprawnionym podmiotom, Służbie Celnej, sądowi i prokuratorowi określone są w większości w przepisach odrębnych (art. 180a ust. 1 pkt 2).

Zgodnie z art. 180a ust. 7, udostępnianie danych retencyjnych może nastąpić za pomocą sieci telekomunikacyjnej, chyba że przepisy odrębne stanowią inaczej. Taką szczególną regulacją są np. przepisy ustawy o Policji[30]. Zasady udostępniania danych retencyjnych funkcjonariuszom Policji w ramach czynności operacyjno-rozpoznawczych określa art. 20c ustawy o Policji. Dane, o których mowa w art. 180c i art. 180d, mogą być udostępniane Policji i przez nią przetwarzane w celu zapobiegania lub wykrywania przestępstw. Podmiot prowadzący działalność telekomunikacyjną udostępnia dane nieodpłatnie policjantowi wskazanemu w pisemnym wniosku Komendanta Głównego Policji lub komendanta wojewódzkiego Policji albo osoby przez nich upoważnionej bądź na ustne żądanie policjanta posiadającego pisemne upoważnienie takich osób oraz temuż policjantowi za pośrednictwem sieci telekomunikacyjnej. W przypadku wykorzystywania sieci telekomunikacyjnej udostępnianie danych odbywa się bez udziału pracowników

[26] K. K a w a ł e k, M. R o g a l s k i, Prawo…, *op. cit.*, s. 68.
[27] Por. A. K r a s u s k i, Prawo…, *op. cit.*, s. 78.
[28] S. P i ą t e k, Prawo…, *op. cit.*, s. 76.
[29] Por. M. S i w i c k i, Retencja danych transmisyjnych na podstawie art. 180a Prawa telekomunikacyjnego, Prokuratura i Prawo 2011, nr 9, s. 121–122.
[30] Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2011 r., Nr 287, poz. 1687 ze zm.).

przedsiębiorcy telekomunikacyjnego lub przy niezbędnym ich udziale, jeżeli możliwość taka jest przewidziana w porozumieniu zawartym pomiędzy Komendantem Głównym Policji a tym przedsiębiorcą (art. 20c ust. 2a ustawy o Policji). Udostępnianie Policji danych retencyjnych może nastąpić za pośrednictwem sieci telekomunikacyjnej, jeśli wykorzystywane sieci zapewniają możliwość ustalenia osoby uzyskującej dane, rodzaju tych danych oraz czasu, w którym zostały uzyskane, oraz zabezpieczenie techniczne i organizacyjne uniemożliwiające osobie nieuprawnionej dostęp do tych danych, jak również wtedy, gdy jest to uzasadnione specyfiką lub zakresem zadań wykonywanych przez jednostki organizacyjne Policji albo prowadzonych przez nie czynności (art. 20c ust. 5 ustawy o Policji).

Podobne unormowania znajdują się w ustawach regulujących działalność pozostałych organów i służb stanowiących uprawnione podmioty w rozumieniu art. 179 ust. 3 oraz Służby Celnej[31].

Unormowania te różnią się przede wszystkim celem pozyskiwania danych oraz zasadami ich niszczenia. Policja oraz Straż Graniczna uzyskują dane, o których mowa w art. 180c i 180d, w celu zapobiegania lub wykrywania przestępstw, z zastrzeżeniem przepisów ustawy o Straży Granicznej regulujących zakres zadań tej formacji. Wywiad skarbowy uzyskuje takie dane w celu zapobiegania lub wykrywania przestępstw skarbowych, przestępstw określonych w art. 228–231 k.k. popełnianych przez osoby zatrudnione lub pełniące służbę w jednostkach organizacyjnych podległych ministrowi właściwemu do spraw finansów publicznych oraz dotyczących naruszeń krajowych i unijnych przepisów celnych, Służba Celna – w celu zapobiegania lub wykrywania przestępstw skarbowych, o których mowa w rozdziale 9 Kodeksu karnego skarbowego, zaś Centralne Biuro Antykorupcyjne, Służba Kontrwywiadu Wojskowego i Agencja Bezpieczeństwa Wewnętrznego – po prostu w celu realizacji określonych ustawowo zadań tych służb. Zwraca uwagę, że w odniesieniu do trzech ostatnich formacji ustawodawca *expressis verbis* przewidział brak konieczności uzyskania zgody sądu na pozyskiwanie omawianych tu danych, natomiast w przypadku pozostałych służb nie wprowadził przepisów, które by takiej zgody wymagały.

[31] Art. 10b ustawy z dnia 12 października 1990 r. o Straży Granicznej, Dz. U. z 2011 r., Nr 116 poz. 675 z późn. zm.; art. 28 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, Dz. U. z 2010 r., Nr 29 poz. 154 z późn. zm.; art. 32 ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, Dz. U. z 2014 r., poz. 253 z późn. zm.; art. 30 ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych, Dz. U. z 2013 r., poz. 568 z późn. zm.; art. 18 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym, Dz. U. z 2012 r., poz. 621 z późn. zm.; art. 36b ustawy z dnia 28 września 1991 r. o kontroli skarbowej, Dz. U. z 2011 r., Nr 41 poz. 214 z późn. zm.; art. 75d ustawy z dnia 27 sierpnia 2009 r. o Służbie Celnej, Dz. U. z 2013 r., poz. 1404 z późn. zm.

Ustawa o Policji przewiduje niezwłoczne komisyjne i protokolarne zniszczenie uzyskanych materiałów, jeśli nie zawierają informacji mających znaczenie dla postępowania karnego. Ustawy: o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, jak też ustawa o Centralnym Biurze Antykorupcyjnym nie przewidują możliwości likwidacji uzyskanych danych, nawet jeśli są nieprzydatne z punktu widzenia celu, dla którego zostały zebrane. Pośrednie rozwiązanie zawiera ustawa o kontroli skarbowej, zgodnie z którą minister właściwy do spraw finansów publicznych nakazuje niezwłoczne, komisyjne i protokolarne zniszczenie uzyskanych danych, jeśli uzna wystąpienie z wnioskiem o ich udostępnienie przez przedsiębiorcę telekomunikacyjnego za nieuzasadnione. Z kolei, zgodnie z art. 75d ustawy o Służbie Celnej, materiały udostępnione Służbie Celnej w wyniku realizacji uprawnienia do pozyskiwania danych z art. 180c i art. 180d, które nie zawierają informacji mających znaczenie dla postępowania w sprawach o wykroczenia skarbowe lub przestępstwa skarbowe, podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu.

W uzupełnieniu uwag dotyczących udostępniania danych retencyjnych uprawnionym podmiotom i Służbie Celnej należy zauważyć, iż zgodnie z art. 180d przedsiębiorcy telekomunikacyjni są obowiązani do zapewnienia warunków dostępu i utrwalania oraz do udostępniania uprawnionym podmiotom, a także Służbie Celnej, sądowi i prokuratorowi, na własny koszt, przetwarzanych przez siebie danych, o których mowa w art. 159 ust. 1 punkty 1 i 3–5, w art. 161 oraz w art. 179 ust. 9, związanych ze świadczoną usługą telekomunikacyjną, na zasadach i przy zachowaniu procedur określonych w przepisach odrębnych. Przepis ten stanowi uzupełnienie regulacji zawartej w art. 179 ust. 3, dotyczącej zapewnienia warunków dostępu i utrwalania przekazów telekomunikacyjnych i tzw. danych towarzyszących. Udostępnianie danych, o których mowa w art. 180d, może następować przy wykorzystaniu interfejsów według art. 179 ust. 4a, czyli interfejsów przeznaczonych do realizacji obowiązku zapewnienia dostępu i utrwalania przekazów telekomunikacyjnych i tzw. danych towarzyszących (art. 179 ust. 3)[32]. Wymagania techniczne i eksploatacyjne interfejsów określa rozporządzenie wydane na podstawie delegacji zawartej w art. 182[33]. Obowiązek z art. 180d obejmuje dane dotyczące użytkownika[34] (art. 159 ust. 1 pkt 1), dane transmisyjne[35]

[32] Uzasadnienie rządowego projektu ustawy z dnia 24 kwietnia 2009 r. o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw, druk nr 1448 Sejmu VI kadencji.

[33] Rozporządzenie Rady Ministrów w sprawie wymagań technicznych i eksploatacyjnych dla interfejsów umożliwiających wykonywanie zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego z dnia 20 stycznia 2012 r. (Dz. U. z 2012 r., poz. 200).

[34] Użytkownik – podmiot korzystający z publicznie dostępnej usługi telekomunikacyjnej lub żądający świadczenia takiej usługi.

(art. 159 ust. 1 pkt 3), dane o lokalizacji[36] (art. 159 ust. 1 pkt 4), dane o próbach uzyskania połączenia, w tym o próbach nieudanych (art. 159 ust. 1 pkt 5), dane o użytkownikach będących osobami fizycznymi, które mogą być przetwarzane przez dostawcę usług telekomunikacyjnych (art. 161), oraz dane zawarte w elektronicznym wykazie abonentów, użytkowników lub zakończeń sieci (art. 179 ust. 9). Porównanie zakresu danych wskazanych w art. 180c (dotyczącym danych retencyjnych) i w art. 180d prowadzi do wniosku, iż zakres danych wskazanych w obu tych przepisach częściowo się pokrywa[37]. W wielu przypadkach te same dane mogą stanowić dane retencyjne, zatrzymywane i udostępniane na podstawie art. 180c, oraz dane udostępniane na podstawie art. 180d (np. za pomocą interfejsów[38]). Przepisy ustaw regulujących działalność uprawnionych podmiotów i Służby Celnej, powołane we wcześniejszej części artykułu (jak również art. 218 § 1 Kodeksu postępowania karnego), odnoszą się zresztą łącznie do danych, o których mowa w art. 180c i art. 180d.

Podstawą prawną udostępniania danych retencyjnych sądom i prokuratorom w sprawach karnych są przepisy Kodeksu postępowania karnego. Podmioty prowadzące działalność telekomunikacyjną obowiązane są wydać sądowi lub prokuratorowi, na żądanie zawarte w postanowieniu, dane, o których mowa w art. 180c i art. 180d, jeżeli dane te mają znaczenie dla toczącego się postępowania (art. 218 § 1 k.p.k.). Tylko sąd lub prokurator mają prawo otwierać lub zarządzić otwarcie wykazów zawierających takie dane. Postanowienie, o którym mowa w art. 218 § 1 k.p.k., może być wydane w postępowaniu przygotowawczym zarówno w fazie *in rem*, jak i *in personam*[39]. Postanowienie to doręcza się abonentowi telefonu lub nadawcy, któ-

[35] Dane transmisyjne – 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 lub w ramach usług telekomunikacyjnych wskazujące położenie geograficzne urządzenia końcowego użytkownika publicznie dostępnych usług telekomunikacyjnych.

[36] Dane o lokalizacji – dane lokalizacyjne wykraczające poza dane niezbędne do transmisji komunikatu lub wystawienia rachunku.

[37] S. P i ą t e k, Prawo..., *op. cit.*, s. 1099–1100; K. K a w a ł e k, M. R o g a l s k i, Prawo..., *op. cit.*, s. 967.

[38] Jak wynika z uzasadnienia rządowego projektu ustawy z dnia 24 kwietnia 2009 r. o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw (druk sejmowy nr 1448), dane, o których mowa w art. 180d, mogą być również udostępniane za pomocą oddzielnego interfejsu, uwzględniającego wymagania zawarte w rozporządzaniu Rady Ministrów wydanym na podstawie delegacji z art. 182 albo z wykorzystaniem posiadanych przez przedsiębiorców telekomunikacyjnych rozwiązań technicznych oraz rozwiązań planowanych w związku z koniecznością udostępnienia danych retencyjnych. Wymagania techniczne i eksploatacyjne interfejsu dedykowanego do udostępniania danych, o których mowa w art. 180d, zawarte są w powołanym rozporządzeniu Rady Ministrów z dnia 20 stycznia 2012 r. (tzw. interfejs HI A–B).

[39] J. G r a j e w s k i, Komentarz do art. 218 Kodeksu postępowania karnego, LEX 2014.

rego wykaz połączeń lub innych przekazów informacji został wydany, przy czym 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.). Przedsiębiorca telekomunikacyjny udostępnia dane z uwzględnieniem postanowień rozporządzenia Ministra Sprawiedliwości z dnia 28 kwietnia 2004 r.[40], które zachowuje moc na podstawie przepisów przejściowych wspomnianej ustawy nowelizacyjnej z 2009 r. do czasu wydania nowego rozporządzenia z upoważnienia art. 218b k.p.k.

Warto odnotować, iż naruszenie przez przedsiębiorcę telekomunikacyjnego obowiązków dotyczących retencjonowania, udostępniania oraz chronienia danych telekomunikacyjnych może skutkować nałożeniem przez Prezesa Urzędu Komunikacji Elektronicznej kary pieniężnej na podstawie art. 209 ust. 1 pkt 10 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne. Przepis ten umożliwia nałożenie kary pieniężnej w wysokości do 3% przychodu ukaranego podmiotu, osiągniętego w poprzednim roku kalendarzowym, jeżeli podmiot ten nie wypełnia lub nienależycie wypełnia obowiązki lub zadania na rzecz obronności i bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, w zakresie i na warunkach określonych w ustawie lub decyzjach wydanych na jej podstawie. Prezes Urzędu Komunikacji Elektronicznej może również nałożyć karę pieniężną na osobę kierującą przedsiębiorstwem telekomunikacyjnym, w szczególności na osobę pełniącą funkcję kierowniczą lub wchodzącą w skład organu zarządzającego przedsiębiorcy telekomunikacyjnego lub związku takich przedsiębiorców, w wysokości do 300% jego miesięcznego wynagrodzenia, naliczanego jak dla celów ekwiwalentu za urlop wypoczynkowy.

Kontrowersje dotyczące ram prawnych retencji danych

Regulacje prawne w przedmiocie retencji danych od chwili wejścia w życie budziły kontrowersje[41]. Sama idea zatrzymywania danych dotyczących wszystkich użytkowników usług telekomunikacyjnych – niezależnie od tego, czy dana osoba ma jakikolwiek związek z przestępstwem – bywa postrze-

[40] 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).

[41] Retencja danych – list otwarty, http://prawo.vagla.pl/node/5812; por. również A. A d a m s k i, The telecommunication data retention in Poland: does the legal regulation pass the proportionality test?, Przegląd Prawa Technologii Informacyjnych. ICT Law Review 2013, nr 1, s. 4–11.

gana jako odwrócenie zasady domniemania niewinności[42]. W zamian proponuje się mechanizm tzw. *quick freeze*, zakładający szybkie i selektywne „zamrażanie" danych w związku z konkretnymi postępowaniami[43]. Kwestionowano również zasadność przechowywania danych przez 24 miesiące[44]. Jakkolwiek ingerencja w prywatność abonentów w przypadku retencjonowania danych jest mniejsza niż w przypadku utrwalania treści komunikatów, to analiza tzw. metadanych, czyli informacji o rozmowie innych niż sama treść rozmowy, może być wystarczająca do zbudowania szczegółowego profilu aktywności abonenta. Jak dowiódł eksperyment przeprowadzony przez niemieckiego polityka Malte Spitza, który pozyskał od dostawcy usług telekomunikacyjnych bazę danych gromadzonych na swój temat, analiza danych retencyjnych pozwala na ustalenie szlaków komunikacyjnych abonenta i częstotliwości jego telefonicznych interakcji, a w zestawieniu z danymi publicznie dostępnymi (np. Twitter, media) umożliwia odtworzenie nadto celów podróży[45].

Sygnalizowane kontrowersje spowodowały, iż niektóre państwa Unii Europejskiej długo uchylały się od implementowania Dyrektywy retencyjnej (np. Szwecja zrobiła to dopiero w 2012 r. pod presją kary finansowej, jaką nałożył na nią Trybunał Sprawiedliwości Unii Europejskiej[46]), zaś implementowane regulacje były zaskarżane na poziomie krajów członkowskich. Sądy konstytucyjne Bułgarii, Rumunii, Niemiec, Czech, Austrii i Słowenii uznały krajowe przepisy implementujące Dyrektywę retencyjną za niezgodne z ustawami zasadniczymi[47]. Wątpliwości powzięte przez sądy w Irlandii i Austrii dały z kolei asumpt do zajęcia stanowiska w sprawie retencji danych przez Trybunał Sprawiedliwości Unii Europejskiej (dalej: TSUE), który w wyroku z dnia 8 kwietnia 2014 r.[48] w sprawie „Digital Rigths Ireland" stwierdził nieważność Dyrektywy retencyjnej. Zdaniem TSUE, Dyrektywa retencyjna w sposób nieproporcjonalny ingerowała w gwarantowane w Karcie Praw Podstawowych UE prawo do prywatności i ochrony danych osobowych z uwagi na m.in. objęcie obowiązkiem retencji danych dotyczących wszystkich bez

[42] Fundacja Panoptykon, „Telefoniczna kopalnia informacji. Przewodnik", s. 26; zob. przypis 3.
[43] http://panoptykon.org/wiadomosc/komisja-europejska-przygotowuje-ocene-skutkow-regulacji-dla-nowej-dyrektywy-o-retencji-dan.
[44] M. W a c h, Zatrzymywanie danych telekomunikacyjnych przez dwa lata w celach bliżej nieokreślonych a prawo do prywatności, Radca Prawny 2011, nr 115–116, dodatek naukowy, s. 22.
[45] Fundacja Panoptykon, „Telefoniczna kopalnia…, *op. cit.*, s. 16.
[46] Tamże, s. 25.
[47] Tamże; zob. też uzasadnienie wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r., sygn. K 23/11, OTK-A 2014, nr 7, poz. 80, s. 67.
[48] Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 8 kwietnia 2014 r., sygn. C–293/12 i C–594/12, http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc 30dd28ad261c4cca444bac72badb467ed752.e34KaxiLc3qMb40Rch0SaxuPaNf0?text=&docid=153045&pageIndex=0&doclang=PL&mode=req&dir=&occ=first&part=1&cid=537102.

wyjątku użytkowników, w tym pozostających bez związku z działalnością przestępczą, jak również zobowiązanych do zachowania tajemnicy zawodowej, a także na brak ograniczenia retencji do przypadków „ciężkich" przestępstw. Trybunał zwrócił również uwagę na brak w Dyrektywie retencyjnej jasnych wymogów co do standardów technicznych i organizacyjnych przechowywania danych, w tym brak obowiązku przechowywania danych na terytorium Unii Europejskiej, jak też na fakt, iż Dyrektywa retencyjna nie różnicuje długości okresu przechowywania danych w odniesieniu do poszczególnych kategorii danych[49]. Należy zaznaczyć, iż wyrok stwierdzający nieważność Dyrektywy retencyjnej na płaszczyźnie prawa Unii Europejskiej nie ma bezpośredniego przełożenia na ważność aktu implementującego tę dyrektywę w prawie krajowym[50].

W Polsce sposób uzyskiwania i przetwarzania przez uprawnione podmioty danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180c i w art. 180d, był przedmiotem weryfikacji ze strony Najwyższej Izby Kontroli. W informacji o wynikach wzmiankowanej kontroli wskazano na potrzebę określenia katalogu spraw, na potrzeby których mogą być pozyskiwane dane telekomunikacyjne, ponadto na konieczność wprowadzenia rozwiązań stwarzających dodatkowe gwarancje dla osób wykonujących zawody zaufania publicznego (np. dziennikarzy, adwokatów). Za zasadne uznano także stworzenie rozwiązań zapewniających zewnętrzną kontrolę nad procesem pozyskiwania danych, weryfikację ich wykorzystania oraz mechanizm niszczenia danych, które okazały się zbędne[51].

Retencja danych po wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r. (sygn. K 23/11)

Na gruncie prawa krajowego swoistym podsumowaniem krytycznych głosów na temat przepisów regulujących retencję danych były wnioski skierowane do Trybunału Konstytucyjnego przez Rzecznika Praw Obywatelskich i Prokuratora Generalnego, poddające w wątpliwość zgodność ze standardami konstytucyjnymi przepisów regulujących pozyskiwanie danych reten-

[49] M. Gutowska, T. Krzywański, Ł. Lasek, Wyrok TSUE w sprawie Digital Rights – co dalej z retencją?, Biuletyn praktyki nowych technologii kancelarii Wardyński i Wspólnicy, maj 2014 r., s. 27; http://www.wardynski.com.pl/publikacje/biuletyny/ biuletyn–praktyki–prawa–nowych–technologii.

[50] M. Taborowski, Skutki wyroku Trybunału Sprawiedliwości Unii Europejskiej stwierdzającego nieważność dyrektywy retencyjnej, s. 4, http://www.hfhr.pl/wp–content/uploads/ 2014/04/skutki_wyroku_TSUE_MTaborowski–3.pdf.

[51] Informację o wynikach kontroli NIK zamieszczono na stronie http://www.nik.gov.pl/plik/id, 5421,vp,7038.pdf; zob. też artykuł „NIK o bilingach", http://www.nik.gov.pl/aktualnosci/nik–o–billingach.html.

cyjnych przez uprawnione podmioty i Służbę Celną. Jak podniesiono we wniosku RPO z dnia 1 sierpnia 2011 r., przeprowadzona analiza przepisów regulujących materię dostępu poszczególnych służb do danych objętych tajemnicą komunikowania się, wskazanych w art. 180c i art. 180d Prawa telekomunikacyjnego, pozwala na sformułowanie pięciu wniosków natury ogólnej. I tak, po pierwsze, omawiane przepisy nie regulują w sposób precyzyjny celu gromadzenia danych, gdyż odwołują się jedynie do zakresu zadań poszczególnych służb bądź ogólnego stwierdzenia, iż dane te są pozyskiwane w celu zapobiegania lub wykrywania przestępstw. Po drugie, przepisy te nie wskazują kategorii osób, w stosunku do których niezbędne jest respektowanie ich tajemnicy zawodowej. Po trzecie, warunkiem uzyskania dostępu do tych danych nie jest wyczerpanie innych, mniej ingerujących w sferę praw i wolności obywatelskich, możliwości pozyskania niezbędnych informacji. Po czwarte, dziedzina dotycząca pozyskiwania w tym trybie danych nie podlega żadnej zewnętrznej kontroli. Po piąte wreszcie, istotna część danych gromadzonych przez służby nie podlega zniszczeniu także wtedy, gdy dane te okazały się nieprzydatne z punktu widzenia realizowanych zadań[52]. Obaj wnioskodawcy kwestionowali zgodność z Konstytucją i Konwencją o ochronie praw człowieka i podstawowych wolności przepisów ustaw regulujących działalność uprawnionych podmiotów i Służby Celnej, odnoszących się do zbierania informacji o jednostce za pomocą środków technicznych w działaniach operacyjnych, w tym informacji stanowiących dane podlegające retencji[53].

Wyrokiem z dnia 30 lipca 2014 r.[54] Trybunał Konstytucyjny, po zbadaniu połączonych wniosków wymienionych organów, stwierdził niezgodność z Konstytucją części przepisów ustaw regulujących działalność uprawnionych podmiotów i Służby Celnej, związanych z obowiązkiem retencji danych. Orzekł mianowicie, iż przepisy art. 20c ust. 1 ustawy o Policji, art. 10b ust. 1 ustawy o Straży Granicznej, art. 36 ust. 1 pkt 1 ustawy o kontroli skarbowej, art. 30 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28 ust. 1 pkt 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 32 ust. 1 pkt 1 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, art. 18 ust. 1 pkt 1 ustawy o Centralnym Biurze Antykorupcyjnym oraz art. 75 d ustawy o Służbie Celnej są niezgodne z art. 47 i art. 49 w zw. z art. 31 ust. 3 Konstytucji przez to, że nie przewidują niezależnej kontroli udostępniania

[52] Wniosek Rzecznika Praw Obywatelskich do Trybunału Konstytucyjnego z dnia 1 sierpnia 2011 r., s. 15; http://db.trybunal.gov.pl/sprawa/sprawa_pobierz_plik62.asp?plik=F–274604174/K_23_11_Wns_2011_06_29.pdf&syg=K%2023/11.

[53] Skarżący nie kwestionowali konstytucyjności przepisów dotyczących udostępniania danych retencyjnych w toku postępowania karnego.

[54] Wyrok Trybunału Konstytucyjnego z dnia 30 lipca 2014 r., sygn. K 23/11, OTK-A 2014, nr 7, poz. 80.

danych telekomunikacyjnych, o których mowa w art. 180c i 180d. Ponadto, w ocenie Trybunału, art. 28 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 32 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego oraz art. 18 ustawy o Centralnym Biurze Antykorupcyjnym w zakresie, w jakim nie przewidują zniszczenia danych niemających znaczenia dla prowadzonego postępowania, są niezgodne z art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji, zaś art. 75d ust. 5 ustawy o Służbie Celnej w zakresie, w jakim zezwala na zachowanie materiałów innych niż zawierające informacje mające znaczenie dla postępowania w sprawach wykroczeń skarbowych lub przestępstw skarbowych, określonych w rozdziale 9 Kodeksu karnego skarbowego, jest niezgodny z art. 51 ust. 4 Konstytucji. Przepisy uznane za niezgodne z ustawą zasadniczą stracą moc obowiązującą po upływie 18 miesięcy od ogłoszenia wyroku w Dzienniku Ustaw.

W uzasadnieniu judykatu Trybunał Konstytucyjny zwrócił uwagę, iż ustawodawca nie przewidział żadnego mechanizmu niezależnej kontroli nad udostępnianiem danych retencyjnych. Trybunał Konstytucyjny nie przesądził, jak taka kontrola powinna przebiegać i przez jaki organ powinna być sprawowana, ograniczając się do sugestii, iż nie jest wykluczone wprowadzenie jako zasady kontroli następczej, bowiem zatrzymywanie i udostępnianie różnych rodzajów danych może powodować różną intensywność ingerencji w wolności i prawa człowieka, a przez to uzasadniać pewne zróżnicowanie mechanizmu kontroli w odniesieniu do poszczególnych rodzajów danych. Zaakcentował jednocześnie, że regulując ten mechanizm, ustawodawca powinien uwzględnić w szczególności specyfikę działania i ustawowy zakres zadań poszczególnych rodzajów służb, sytuacje niecierpiące zwłoki, w których szybkie pozyskanie danych telekomunikacyjnych może być niezbędne dla zapobieżenia popełnieniu przestępstwa lub jego wykrycia. Dostrzegł jednak argumenty przemawiające za wprowadzeniem w pewnych wypadkach kontroli uprzedniej. Chodzić może, przykładowo, o dostęp do danych telekomunikacyjnych osób wykonujących zawody zaufania publicznego lub jeśli nie ma konieczności pilnego działania służb. Kwestie te musi jednak odpowiednio wyważyć ustawodawca[55]. Trybunał Konstytucyjny nadto podkreślił, iż kontrola udostępniania danych telekomunikacyjnych nie musi być sprawowana przez sądy, konieczne jest jednak, by organ sprawujący taką kontrolę był niezależny od rządu i nie pozostawał w bezpośredniej lub pośredniej relacji zwierzchności z funkcjonariuszami pozyskującymi dane.

Jak wspomniano, Trybunał Konstytucyjny uznał również za niezgodny z ustawą zasadniczą brak unormowań dotyczących niszczenia danych nie-

[55] Uzasadnienie wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r., sygn. K 23/11, OTK-A 2014, nr 7, poz. 80, s. 11.

mających znaczenia dla prowadzonego postępowania. Zakwestionowane przepisy ustaw o ABW, CBA i SKW nie regulują wszakże postępowania z danymi telekomunikacyjnymi po ich zgromadzeniu i nie ustanawiają procedury usuwania danych zbędnych. Z kolei art. 75d ust. 5 ustawy o Służbie Celnej przewiduje zniszczenie materiałów, które nie zawierają informacji mających znaczenie dla postępowania w sprawach o wykroczenia skarbowe lub przestępstwa skarbowe. Biorąc pod uwagę, iż Służba Celna uzyskuje dane, o których mowa w art. 180c i art. 180d, w celu zapobiegania lub wykrywania przestępstw skarbowych stypizowanych w rozdziale 9 Kodeksu karnego skarbowego, a nie wszystkich przestępstw skarbowych i wykroczeń skarbowych, Trybunał stwierdził niekonstytucyjność art. 75d ust. 5 ustawy o Służbie Celnej jedynie w zakresie, w jakim przepis ów zezwala na zachowanie materiałów innych niż zawierające informacje mające znaczenie dla postępowania w sprawach o właśnie takie czyny zabronione[56].

Podsumowanie

System retencji i udostępniania danych przez przedsiębiorców telekomunikacyjnych stanowi niewątpliwie ważne narzędzie walki z przestępczością, jednakże istniejące regulacje prawne w tym zakresie wymagają daleko idących zmian, uwzględniających wnioski płynące z wyroku Trybunału Konstytucyjnego w sprawie o sygn. K 23/11 oraz wyroku TSUE w sprawie Digital Right Ireland. Warto przy tym pamiętać, iż Trybunał Konstytucyjny, rozpatrując wnioski Rzecznika Praw Obywatelskich i Prokuratora Generalnego, zajął się tylko wycinkiem obszaru retencji danych dotyczącym udostępniania tych danych uprawnionym podmiotom i Służbie Celnej. Poza zakresem zaskarżenia pozostał problem dopuszczalności i proporcjonalności obowiązków retencyjnych spoczywających na przedsiębiorcach telekomunikacyjnych, jakkolwiek Trybunał uwzględnił wyrok TSUE w sprawie Digital Rights Ireland jako tło decyzyjne podczas oceny konstytucyjności przepisów krajowych o udostępnianiu danych telekomunikacyjnych.[57] Jeżeli nowelizacja wymuszona wyrokiem Trybunału Konstytucyjnego w sprawie o sygn. K 23/11 ograniczy się do zmiany przepisów uznanych za niekonstytucyjne, to zapewne nie wpłynie w zasadniczy sposób na kształt systemu retencji danych telekomunikacyjnych, a jedynie zmodyfikuje zasady udostępniania tych danych służbom policyjnym i ochrony państwa. Niemniej jednak należy mieć na uwadze, iż jednym z możliwych scenariuszy jest przyjęcie nowej dyrektywy retencyjnej[58], uwzględniającej wnioski płynące z wyroku w sprawie Digital

[56] *Ibidem*, s. 135–143.
[57] *Ibidem*, s. 65 i 114.
[58] M. G u t o w s k a, T. K r z y w a ń s k i, Ł. L a s e k, Wyrok TSUE…, *op. cit.*, s. 32.

Rights Ireland, co niewątpliwie znalazłoby odzwierciedlenie w regulacji krajowej.

Wydaje się, iż optymalnym rozwiązaniem byłoby utrzymanie systemu retencji i udostępniania danych telekomunikacyjnych z jednoczesnym daleko idącym wzmocnieniem proceduralnych gwarancji ochrony praw osób, których dane dotyczą, oraz zapewnieniem proporcjonalności stosowanych rozwiązań. *De lege ferenda* wskazane jest określenie katalogu czynów zabronionych, których ściganie uzasadnia sięganie po dane retencyjne, przy czym powinny to być przestępstwa poważne, wyliczone enumeratywnie. Nowa regulacja retencji danych powinna przewidywać mechanizm niezależnej kontroli nad ich udostępnianiem i wykorzystaniem, sprawowanej przez organ administracji publicznej. Przepisy prawa powinny precyzyjnie określać procedurę niszczenia udostępnionych danych retencyjnych, które przestały być potrzebne. Dane retencyjne powinny być przechowywane na obszarze Unii Europejskiej; niepożądane wydaje się ich przetwarzanie w chmurze.

Wśród danych podlegających retencji znajdują się dane w różnym stopniu ingerujące w prywatność użytkowników. Wydaje się, iż reżim przechowywania, udostępniania i wykorzystywania poszczególnych kategorii danych powinien być zróżnicowany. Przykładowo, udostępnianie danych lokalizacyjnych i danych o lokalizacji – istotnie ingerujących w prywatność – mogłoby podlegać kontroli apriorycznej, za wyjątkiem wypadków niecierpiących zwłoki, zaś w przypadku pozostałych danych retencyjnych stosowana byłaby kontrola *ex post*. Rozważenia wymaga również ewentualne zróżnicowanie okresu przechowywania danych retencyjnych w odniesieniu do poszczególnych ich kategorii.

Retention of telecommunications data

Abstract

This study deals with the legal framework for retention of telecommunications data and disclosure of such data to authorized agencies, Customs Service, courts and prosecutors. The subjective and objective scope of the obligation to retain data, principles of disclosure, controversies around data retention and consequences of the judgment of the Constitutional Tribunal in case K 23/11 are presented.