POZYSKIWANIE DANYCH TELEKOMUNIKACYJNYCH PRZEZ AGENCJĘ BEZPIECZEŃSTWA WEWNĘTRZNEGO PO WYROKU TRYBUNAŁU KONSTYTUCYJNEGO Z 30 LIPCA 2014 ROKU

BARTŁOMIEJ OPALIŃSKI*

1. WPROWADZENIE

Rzeczpospolita Polska jest państwem demokratycznym, co wynika zarówno z deklaracji zawartej w Konstytucji RP z 2 kwietnia 1997 roku[1], jak również z praktyki ustrojowej. W każdej demokracji jednym z kluczowych zagadnień jest zakres ingerencji aparatu państwowego w różne obszary aktywności obywateli. Jednym z tych obszarów są wolności i prawa obywatelskie, w ramach których funkcjonuje ważkie zagadnienie pozyskiwania danych telekomunikacyjnych, w szczególności tzw. billingów telekomunikacyjnych[2]. Zagadnienie to jest związane z zapewnieniem skutecznego zapobiegania przestępczości i stanowi jedno z narzędzi wykorzystywanych w tym calu przez organy ścigania i organy wymiaru sprawiedliwości[3].

* dr, adiunkt w Katedrze Nauki o Administracji Wydziału Prawa i Administracji Uczelni Łazarskiego

[1] Jak wynika z art. 2 Konstytucji RP, Rzeczpospolita Polska jest demokratycznym państwem prawnym, urzeczywistniającym zasady sprawiedliwości społecznej.

[2] Zob. L. Garlicki, *Uwaga nr 3 do art. 49 Konstytucji RP*, [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, L. Garlicki (red.), t. II, Warszawa 2002, s. 1.

[3] Wydaje się, że istotnym asumptem do wprowadzania prawnych regulacji pozwalających na zatrzymywanie danych telekomunikacyjnych oraz na ich udostępnianie służbom policyjnym i służbom ochrony państwa oraz organom wymiaru sprawiedliwości stały się liczne zamachy terrorystyczne, w szczególności dokonany w dniu 11 września 2001 r. zamach na World Trade Center, jak również zamachy terrorystyczne w Madrycie (11 marca 2004 r.) i w Londynie (7 lipca 2005 r.). Tamten okres zapoczątkował światową wojnę z terroryzmem. Skuteczne jej prowadzenie wymagało przygotowania odpowiedniego prawnego instrumentarium do podejmowania działań w tym zakresie. Zob. M. Kiziński, *Retencja danych telekomunikacyjnych*, „Prokuratura i Prawo"

Jak wynika 180a ustawy z dnia 16 lipca 2004 r. prawo telekomunikacyjne (Dz.U. z 2014, poz. 243, ze zm., dalej jako „p.t."), na operatorze publicznej sieci telekomunikacyjnej oraz dostawcy publicznie dostępnych usług telekomunikacyjnych spoczywa obowiązek retencji, tj. gromadzenia i udostępniania danych telekomunikacyjnych[4]. Z przepisu tego wynika wprost, że adresatami obowiązku retencji danych telekomunikacyjnych są operator publicznej sieci telekomunikacyjnej oraz dostawca publicznie dostępnych usług telekomunikacyjnych[5]. Definicje każdego

---

2016, nr 1, s. 138; Fundacja Panoptykon, *Telefoniczna Kopalnia Informacji. Przewodnik*, s. 20, w serwisie Internetowym: http://panoptykon. org/biblio/telefoniczna–kopalnia–informacji–przewodnik.

[4] Powstaje w tym miejscu pytanie, czym są owe dane telekomunikacyjne, podlegające gromadzeniu i – ewentualnie – udostępnieniu. Odpowiedź na to pytanie ma dość złożony charakter, bowiem wymaga analizy wielu przepisów. Zgodnie z art. 180c ust. 1 p.t., udostępnieniu podlegają dane dotyczące ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego inicjującego połączenie i do którego kierowane jest połączenie, a także określające datę i godzinę połączenia oraz czas jego trwania, rodzaj połączenia, a także lokalizację telekomunikacyjnego urządzenia końcowego. Z kolei art. 180d p.t. nie określa katalogu danych podlegających udostępnieniu służbom. Odsyła on do innych przepisów tej ustawy, tj. art. 159 ust. 1 pkt 1 i 3–5, art. 161 oraz art. 179 ust. 9 p.t. Ustawodawca, na podstawie wskazanych przepisów zezwolił na pozyskiwanie przez uprawnione podmioty danych dotyczących użytkownika, danych transmisyjnych (tj. danych przetwarzanych 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), danych o lokalizacji, które oznaczają dane lokalizacyjne wykraczające poza dane niezbędne do transmisji komunikatu lub wystawienia rachunku, danych o próbach uzyskania połączenia między zakończeniami sieci, w tym 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.mJak wynika z art. 161 p.t., dostawca publicznie dostępnych usług telekomunikacyjnych może także gromadzić dane osobowe abonenta obejmujące nazwisko i imiona; imiona rodziców; miejsce i datę urodzenia; adres miejsca zamieszkania i adres korespondencyjny, jeżeli jest on inny niż adres miejsca zamieszkania; numer PESEL – w wypadku obywatela polskiego; nazwę, serię i numer dokumentu potwierdzającego tożsamość, a w wypadku cudzoziemca niebędącego obywatelem państwa członkowskiego UE albo Konfederacji Szwajcarskiej – numer paszportu lub karty pobytu; dane zawarte w dokumentach potwierdzających możliwość wykonania zobowiązania wobec dostawcy publicznie dostępnych usług telekomunikacyjnych wynikającego z umowy o świadczenie usług telekomunikacyjnych. Ponadto, jeśli dostawca publicznie dostępnych usług telekomunikacyjnych uzyskał zgodę użytkownika będącego osobą fizyczną na przetwarzanie innych danych tego użytkownika w związku ze świadczoną usługą, w szczególności numer konta bankowego lub karty płatniczej, adres korespondencyjny użytkownika (jeżeli jest on inny niż adres miejsca zamieszkania), a ponadto adres poczty elektronicznej oraz numery telefonów kontaktowych, również i tego rodzaju dane, znajdujące się w dyspozycji dostawcy publicznie dostępnych usług telekomunikacyjnych, mogą być pozyskiwane i przetwarzane przez służby policyjne i służby ochrony państwa w celach określonych w ustawach. Co więcej, służby te mogą otrzymywać dane wskazane w art. 179 ust. 9 p.t., czyli zawarte w prowadzonym obligatoryjnie przez każdego przedsiębiorcę telekomunikacyjnego wykazie abonentów, użytkowników lub zakończeń sieci, dane uzyskiwane podczas zawarcia umowy. Podsumowując, możliwe jest więc pozyskanie danych trojakiego rodzaju: o abonencie, o ruchu (tzw. dane bilingowe) oraz o lokalizacji.

[5] Wprowadzenie do polskiego systemu prawnego przepisów dotyczących retencji danych telekomunikacyjnych stanowiło pokłosie implementacji dyrektywy 2006/24/WE. Wypada jednak zauważyć, że mechanizmy prawne umożliwiające sięganie przez organy policyjne i organy ochrony państwa do danych gromadzonych przez przedsiębiorców telekomunikacyjnych,

z tych podmiotów zostały określone w art. 2 pkt 27 p.t.. Zgodnie z tym przepisem operatorem jest przedsiębiorca telekomunikacyjny uprawniony do dostarczania publicznych sieci telekomunikacyjnych lub świadczenia usług towarzyszących, zaś dostawcą usług jest przedsiębiorca telekomunikacyjny uprawniony do świadczenia usług telekomunikacyjnych. Podkreślenia wymaga – zaakcentowana przez ustawodawcę w każdej z tych definicji – odmienna płaszczyzna działalności przedsiębiorcy telekomunikacyjnego. Działalność operatora koncentruje się na dostarczaniu sieci telekomunikacyjnej przez co należy rozumieć przygotowanie tej sieci w sposób umożliwiający świadczenie w niej usług. Natomiast działalność dostawcy usług telekomunikacyjnych polega na świadczeniu usług telekomunikacyjnych przy pomocy własnej sieci telekomunikacyjnej albo sieci telekomunikacyjnej należącej do innego operatora[6].

Korelatem wspomnianego obowiązku retencji danych telekomunikacyjnych jest możliwość żądania ich udostępnienia przez uprawnione do tego podmioty (art. 180a ust. 1 pkt 2 p.t. i art. 180d p.t.). Krąg tych podmiotów został określony szeroko. Dostęp do danych telekomunikacyjnych posiadają bowiem sąd i prokuratura[7] oraz osiem służb policyjnych i ochrony państwa, tj.: Policja[8], Straż Graniczna[9], Żandarmeria Wojskowa[10], Agencja Bezpieczeństwa Wewnętrznego[11], Służba Kontrwywiadu Wojskowego[12], Centralne Biuro Antykorupcyjne[13], Służba Celna[14], a także organy kontroli skarbowej[15].

---

co prawda w znacznie mniej rozbudowanej formie niż współcześnie, istniały w polskim systemie prawnym również przed implementacją dyrektywy 2006/24/WE. Wprowadzono je w dniu 24 stycznia 2003 roku na podstawie rozporządzenia Ministra Infrastruktury w sprawie wykonywania przez operatorów zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, Dz.U. nr 19, poz. 166, ze zm. Ustanowienie dyrektywy 2006/24/WE zapewniło jednak prawne doprecyzowanie obowiązków przedsiębiorców w zakresie zatrzymywania danych retencyjnych.

[6] W literaturze dostrzega się również trzecią opcję. Mianowicie działalność dostawcy usług telekomunikacyjnych może również opierać się na odsprzedaży usług zakupionych u innego dostawcy. Zob. K. Kawałek, M. Rogalski red., *Prawo telekomunikacyjne. Komentarz*, Warszawa 2010, s. 64.

[7] Zob. art. 218 ustawy z dnia 6 czerwca 1997 r. Kodeks postępowania karnego, Dz.U. nr 89, poz. 555, ze zm., dalej jako: k.p.k.

[8] Zob. art. 20c ustawy z dnia 6 kwietnia 1990 r. o Policji, Dz.U. z 2015, poz. 355, ze zm., dalej jako: ustawa o Policji.

[9] Zob. art. art. 10b ustawy z dnia 12 października 1990 r. o Straży Granicznej, Dz.U. z 2014, poz. 1402, ze zm., dalej jako: ustawa o SG.

[10] Zob. art. 30 ust. 1 ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych, Dz.U. z 2016, poz. 96, ze zm., dalej jako: ustawa o ŻW.

[11] Zob. art. 28 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu, Dz.U. z 2015, poz. 1929, ze zm., dalej jako: ustawa o ABW i AW.

[12] Zob. art. 32 ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, Dz.U. z 2016, poz. 1318, ze zm., dalej jako: ustawa o SKW i SWW.

[13] Zob. art. 18 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym, Dz.U. z 2016, poz. 1310, ze zm., dalej jako ustawa o CBA.

[14] Zob. art. 75d ustawy z dnia 27 sierpnia 2009 r. o Służbie Celnej, Dz.U. z 2015, poz. 990, ze zm., dalej jako: ustawa o SC.

[15] Zob. art. 36b ustawy z dnia 28 września 1991 r. o kontroli skarbowej, Dz.U. z 2016, poz. 720, ze zm., dalej jako: ustawa o KS.

Jedną ze służb specjalnych, posiadającą prawo do pozyskiwania danych telekomunikacyjnych jest Agencja Bezpieczeństwa Wewnętrznego. Jak to wzmiankowano, kwestia ta została uregulowana w art. 28 ustawy o AWB i AW. Zgodnie z tym przepisem obowiązek uzyskania zgody sądu, o której mowa w art. 27 ust. 1 ustawy (chodzi tu o zgodę na prowadzenie kontroli operacyjnej), nie dotyczy informacji niezbędnych do realizacji przez ABW zadań, o których mowa w art. 5 ust. 1 ustawo o ABW i AW, w postaci danych o których mowa w art. 180c i 180d p.t. oraz danych identyfikujących podmiot korzystający z usług pocztowych oraz dotyczących faktu, okoliczności świadczenia usług pocztowych lub korzystania z tych usług (ust. 1). Zastrzeżono również, że podmiot wykonujący działalność telekomunikacyjną lub operator świadczący usługi pocztowe udostępnia nieodpłatnie dane, o których mowa w ust. 1, odpowiednio funkcjonariuszowi ABW wskazanemu w pisemnym wniosku Szefa ABW lub osoby upoważnionej przez ten organ, na ustne żądanie funkcjonariusza ABW posiadającego pisemne upoważnienie Szefa ABW, a także za pośrednictwem sieci telekomunikacyjnej funkcjonariuszowi ABW posiadającemu pisemne upoważnienie Szefa ABW (ust. 2). W ostatnim ze wskazanych przypadków udostępnianie danych telekomunikacyjnych odbywa się bez udziału pracowników podmiotu wykonującego działalność telekomunikacyjną lub przy ich niezbędnym współudziale, jeżeli możliwość taką przewiduje porozumienie zawarte pomiędzy Szefem ABW a tym podmiotem (ust. 3). Udostępnienie danych, o których mowa w art. 180c i 180d p.t. oraz danych identyfikujących podmiot korzystający z usług pocztowych oraz dotyczących faktu, okoliczności świadczenia usług pocztowych lub korzystania z tych usług może nastąpić za pośrednictwem sieci telekomunikacyjnej, jeżeli sieć ta zapewnia możliwość ustalenia funkcjonariusza ABW uzyskującego dane, ich rodzaju oraz czasu, w którym zostały uzyskane, a także zabezpieczenie techniczne i organizacyjne uniemożliwiające osobie nieuprawnionej dostęp do tych danych (ust. 4).

Od chwili ich wejścia w życie regulacje prawne dotyczące retencji danych telekomunikacyjnych oraz ich udostępniania zarówno przez ABW jak też inne uprawnione do tego podmioty wzbudzały kontrowersje[16]. Spowodowało to, że sposób pozyskiwania i przetwarzania przez uprawnione podmioty danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180c i w art. 180d p.t., został poddany weryfikacji ze przez Najwyższą Izbę Kontroli. W informacji pokontrolnej NIK zaznaczyła, że konieczne jest określenie katalogu spraw, na potrzeby których dane telekomunikacyjne mogą być pozyskiwane. Zwrócono także uwagę na potrzebę wprowadzenia rozwiązań prawnych stwarzających dodatkowe gwarancje wobec osób wykonujących zawody zaufania publicznego. Uznano ponadto, że zasadne jest wprowadzenie mechanizmów kontroli zewnętrznej procesu pozyskiwania danych, ich weryfikacji oraz mechanizmu niszczenia zbędnych danych[17].

---

[16] Dotyczyły one rozmaitych kwestii, m.in. w zatrzymywania danych dotyczących użytkowników wszystkich usług telekomunikacyjnych czy zasadności przechowywania danych przez okres 24 miesięcy. Zob. M. Wach, *Zatrzymywanie danych telekomunikacyjnych przez dwa lata w celach bliżej nieokreślonych a prawo do prywatności*, „Radca Prawny" Dodatek naukowy 2011, nr 115–116.

[17] Informacja o wynikach kontroli NIK w serwisie Internetowym: http://www.nik.gov.pl/plik/id, 5421,vp,7038.pdf [dostęp: 16.06.2016].

Konsekwencją i niejako podsumowaniem kontrowersji w zakresie przepisów dotyczących retencji danych telekomunikacyjnych jest wyrok Trybunału Konstytucyjnego z dnia 30 lipca 2014 r., w sprawie o sygn. akt K 23/11 (tzw. wyrok w sprawie „bilingów i podsłuchów"). Wyrok ten został wydany na podstawie wniosków skierowanych do TK przez Rzecznika Praw Obywatelskich i Prokuratora Generalnego o zbadanie zgodności z Konstytucją RP przepisów regulujących pozyskiwanie danych telekomunikacyjnych przez uprawnione podmioty, w tym przez Agencję Bezpieczeństwa Wewnętrznego. Jego konsekwencją była potrzeba wprowadzenia zmian w poszczególnych ustawach pragmatycznych, nakierowanych na dostosowanie regulacji zezwalających na retencję i udostępnianie danych telekomunikacyjnych do standardów wyznaczonych przez Trybunał Konstytucyjny. Z tym wiąże się cel tego opracowania. Jest nim analiza wspomnianego wyroku TK w sprawie billingów i podsłuchów w zakresie dotyczącym Agencji Bezpieczeństwa Wewnętrznego oraz reakcja legislacyjna ustawodawcy na jego treść i wytyczne trybunalskie w zakresie, w jakim odnosi się on do pozyskiwania danych telekomunikacyjnych przez tę właśnie służbę.

2. ZAKRES WNIOSKU RZECZNIKA PRAW OBYWATELSKICH I PROKURATORA GENERALNEGO

Dokonana przez Trybunał Konstytucyjny kontrola pozyskiwania przez uprawnione podmioty danych telekomunikacyjnych została formalnie zainicjowana przez Rzecznika Praw Obywatelskich oraz Prokuratora Generalnego. We wniosku z dnia 1 sierpnia 2011 r., na podstawie przeprowadzonej analizy przepisów art. 180c i 180d p.t., regulujących dostęp poszczególnych służb do danych objętych tajemnicą komunikowania się, Rzecznik Praw Obywatelskich zakwestionował zgodność z Konstytucją RP dwóch przepisów ustawy o AWB[18]. Pierwszym z nich jest art. 28 ust. 1 pkt 1 ustawy o ABW i AW. Wnioskodawca zakwestionował zgodność tego przepisu z art. 49 w związku z art. 31 ust. 3 Konstytucji RP oraz z art. 8 KOPCPW. Drugim przepisem jest art. 28 ustawy o ABW i AW w zakresie, w jakim – zezwalając na pozyskiwanie danych, o jakich mowa w art. 180c i art. 180d p.t. – nie przewiduje zniszczenia tych spośród pozyskanych danych, które pozbawione są znaczenia dla

[18] Treść wniosku była szersza. Stosownie do celu tego opracowania dla dalszych rozważań istotne są jedynie te kwestie, które dotyczą przepisów ustawy o ABW i AW. Jednakże poza przepisami tej ustawy we wskazanym wniosku RPO zakwestionował również przepisy innych ustaw, tj. art. 36b ust. 5 ustawy o KS, art. 18 ustawy o CBA oraz art. 32 ustawy o SKW i SWW, w zakresie, w jakim – zezwalając na pozyskiwanie danych, o jakich mowa w art. 180c i art. 180d p.t. – nie przewidują zniszczenia tych spośród pozyskanych danych, które pozbawione są znaczenia dla prowadzonego postępowania. W ocenie RPO przepisy te są sprzeczne z art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji RP. Treść zakwestionowanych przepisów jest zbliżona. Na ich podstawie służby policyjne oraz służby ochrony państwa uzyskały kompetencje do pozyskiwania i przetwarzania danych, o których mowa w art. 180c i art. 180d p.t. w celu zapobiegania i wykrywania przestępstw albo realizacji ustawowych zadań służb.

prowadzonego postępowania. W ocenie RPO przepis ten jest sprzeczny z art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji RP[19].

Rzecznik Praw Obywatelskich sformułował pięć zarzutów pod adresem ww. regulacji. Po pierwsze, powołane przepisy nie regulują w sposób precyzyjny celu gromadzenia danych. Odwołują się bowiem jedynie do zakresu zadań ABW bądź ogólnego stwierdzenia, że 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, istotna część danych gromadzonych przez ABW nie podlega zniszczeniu także wtedy, gdy dane te okazały się nieprzydatne z punktu widzenia realizowanych zadań[20].

W skierowanym do TK w dniu 21 czerwca 2012 r. wniosku Prokurator Generalny zakwestionował zgodność z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 KOPCPW przepisów art. 28 ust. 1 pkt 1 w związku z art. 5 ust. 1 pkt 2 lit. a ustawy o ABW i AW w zakresie, w jakim odnosi się do zwrotu „i innych przestępstw godzących w bezpieczeństwo państwa", a także art. 28 ust. 1 pkt 1 w związku z art. 5 ust. 1 pkt 2 lit. b oraz c, jak również pkt 5 ustawy o ABW i AW[21]. Zakwestionowane

---

[19] Warto odnotować, że w dniu 27 kwietnia 2012 r. RPO skierował do TK kolejny wniosek dotyczący jednak retencji danych i udostępniania ich Służbie Celnej. Zarządzeniami Prezesa Trybunału Konstytucyjnego z 1 września 2011 r. oraz z 8 maja 2012 r. oba wskazane wnioski Rzecznika Praw Obywatelskich zostały połączone w celu łącznego ich rozpoznania.

[20] Zob. wniosek RPO do TK z dnia 1 sierpnia 2011 r., s. 15; w serwisie internetowym: 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 [dostęp: 10.06.2016].

[21] Podobnie jak wniosek Rzeczni uwagi na cel tego opracowania przedmiot badania inny niż przepisy ustawy o ABW i AW nie jest istotny i nie podlega analizie. Z rzetelności należy wskazać, że Prokurator generalny w złożonym w tej sprawie wniosku zakwestionował również zgodność z art. 2, art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji oraz z art. 8 KOPCPW następujących przepisów: art. 20c ust. 1 ustawy o Policji w związku z: art. 212 § 1 i 2, art. 216 § 1 i 2, art. 217 § 1, art. 221, art. 278 § 1–3 i 5, art. 284 § 1–3, art. 288 § 1 i 2 oraz art. 290 § 1 k.k., art. 45, art. 46 ust. 1, art. 49 i art. 49a ustawy z dnia 26 stycznia 1984 r. – Prawo prasowe, Dz.U. Nr 5, poz. 24, ze zm.; z art. 34 pkt 2, 3 i 4 ustawy z dnia 16 kwietnia 2004 r. o wyrobach budowlanych, Dz.U. Nr 92, poz. 881, ze zm.; art. 33 ustawy z dnia 25 lutego 2011 r. o substancjach chemicznych i ich mieszaninach, Dz.U. Nr 63, poz. 332, ze zm.; art. 77 pkt 2, 2a i 3 ustawy z dnia 11 marca 2004 r. o ochronie zdrowia zwierząt oraz zwalczaniu chorób zakaźnych zwierząt, Dz.U. z 2008 r., Nr 213, poz. 1342, ze zm. i w związku z art. 52 pkt 2 i 4 ustawy z dnia 13 października 1995 r. – Prawo łowieckie, Dz.U. z 2005 r., Nr 127, poz. 1066 ze zm.; art. 10b ust. 1 ustawy o SG w związku z: art. 212 § 1 i 2, art. 216 § 1 i 2, art. 217 § 1, art. 221, art. 278 § 1–3 i 5, art. 284 § 1–3, art. 288 § 1 i 2 oraz art. 290 § 1 k.k., art. 45, art. 46 ust. 1, art. 49 i art. 49a prawa prasowego, art. 34 pkt 2, 3 i 4 ustawy o wyrobach budowlanych, art. 33 ustawy substancjach chemicznych, art. 77 pkt 2, 2a i 3 ustawy o ochronie zdrowia zwierząt i w związku z art. 52 pkt 2 i 4 prawa łowieckiego; art. 30 ust. 1 ustawy o ŻW w związku z: art. 212 § 1 i 2, art. 216 § 1 i 2, art. 217 § 1, art. 221, art. 278 § 1–3 i 5, art. 284 § 1-3, art. 288 § 1 i 2 oraz art. 290 § 1 k.k., z art. 60 § 2 i 3, art. 61 § 1, art. 62 § 1, 3 i 4, art. 80 § 1 i 2, art. 93 § 2 i 3, art. 95 § 1, art. 108 § 2 oraz art. 109 k.k.s., art. 45, art. 46 ust. 1, art. 49 i art. 49a prawa prasowego, z art. 34 pkt 2, 3 i 4 ustawy o wyrobach budowlanych, art. 33 ustawy o substancjach chemicznych, art. 77 pkt 2, 2a i 3 ustawy o ochronie zdrowia zwierząt i w związku z art. 52 pkt 2 i 4 prawa łowieckiego; art. 36b ust. 1 pkt 1 ustawy o KS w związku

przepisy przyznają Agencji Bezpieczeństwa Wewnętrznego uprawnienia do gromadzenia i przetwarzania danych telekomunikacyjnych osób podejrzewanych o popełnienie drobnych przestępstw o niskiej społecznej szkodliwości. W ocenie Prokuratora Generalnego stanowią one nieproporcjonalną ingerencję w konstytucyjnie chroniony status jednostki. Wskazany katalog czynów nie uzasadnia bowiem ograniczenia konstytucyjnego prawa do prywatności i tajemnicy komunikowania się.

3. TREŚĆ WYROKU TRYBUNAŁU KONSTYTUCYJNEGO W ZAKRESIE ABW I AW

Ukształtowany przepisami polskiego prawa system retencji danych przez przedsiębiorców telekomunikacyjnych jest istotnym narzędziem walki organów państwowych z przestępczością. Jako taki wpisuje się w europejskie regulacje dotyczące tego zagadnienia. System ten nie jest jednak narzędziem bez wad. Przeciwnie, nie-

---

z art. 60 § 2 i 3, art. 61 § 1, art. 62 § 1, 3 i 4, art. 80 § 1 i 2, art. 93 § 2 i 3, art. 95 § 1, art. 108 § 2 oraz art. 109 k.k.s.; art. 36b ust. 1 pkt 1 w związku z art. 2 ust. 1 pkt 12 ustawy o KS, w związku z art. 85 § 4, art. 86 § 4, art. 87 § 4, art. 88 § 3, art. 89 § 3, art. 90 § 3, art. 91 § 4, art. 92 § 3, art. 94 § 3, art. 95 § 2 i art. 96 § 1 k.k.s. oraz w związku z art. 100 ust. 1 i art. 101 ust. 1 ustawy z dnia 19 marca 2004 r. – Prawo celne, Dz.U. z 2004 r., Nr 68, poz. 662 ze zm.; art. 32 ust. 1 pkt 1 w związku z art. 5 ust. 1 pkt 1 lit. a ustawy o SKW i SWW w zakresie, w jakim odnosi się do zwrotu „a także innych ustawach i umowach międzynarodowych"; art. 32 ust. 1 pkt 1 w związku z art. 5 ust. 1 pkt 1 lit. g ustawy o SKW i SWW w zakresie, w jakim odnosi się do zwrotu „oraz innych niż wymienione w lit. a–f, godzących w bezpieczeństwo potencjału obronnego państwa, SZ RP oraz jednostek organizacyjnych MON, a także państw, które zapewniają wzajemność"; art. 32 ust. 1 pkt 1 w związku z art. 5 ust. 1 pkt 9 ustawy o SKW i SWW; art. 18 ust. 1 pkt 1 w związku z art. 2 ust. 1 pkt 2 ustawy o CBA w związku z art. 4, art. 12 ust. 3–6, art. 13 oraz art. 15 ustawy z dnia 21 sierpnia 1997 r. o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne, Dz.U. z 2006 r., Nr 216, poz. 1584 ze zm.; art. 18 ust. 1 pkt 1 w związku z art. 2 ust. 1 pkt 5 ustawy o CBA w związku z art. 8 ust. 1 i 3 oraz art. 10 ust. 1, 2, 5 i 6 ustawy o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne, z art. 35 ust. 1 ustawy z dnia 9 maja 1996 r. o wykonywaniu mandatu posła i senatora, Dz.U. z 2011 r., Nr 7, poz. 29 ze zm.; z art. 87 § 1 ustawy z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych, Dz.U. z 2001 r., Nr 98, poz. 1070 ze zm.; z art. 38 ustawy z dnia 23 listopada 2002 r. o Sądzie Najwyższym, Dz.U. z 2002 r., Nr 240, poz. 2052 ze zm.; z art. 49a ust. 1 ustawy z dnia 20 czerwca 1985 r. o prokuraturze, Dz.U. z 2011 r., Nr 270, poz. 1599 ze zm.; z art. 24h ust. 1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym, Dz.U. z 2001 r., Nr 142, poz. 1591 ze zm.; z art. 25c ust. 1 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym, Dz.U. z 2001 r., Nr 142, poz. 1592 ze zm. oraz w związku z art. 27c ust. 1 ustawy z dnia 5 czerwca 1998 r. o samorządzie województwa, Dz.U. z 2001 r., Nr 142, poz. 1590 ze zm.; art. 18 ust. 1 pkt 1 w związku z art. 2 ust. 1 pkt 3 ustawy o CBA w związku z art. 1 ust. 1 i 2 ustawy z dnia 21 czerwca 1990 r. o zwrocie korzyści uzyskanych niesłusznie kosztem Skarbu Państwa lub innych państwowych osób prawnych, Dz.U. z 1990 r., Nr 44, poz. 255 ze zm.; art. 18 ust. 1 pkt 1 w związku z art. 2 ust. 1 pkt 4 ustawy o CBA w związku z art. 200 ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych, Dz.U. z 2010 r., Nr 113, poz. 759 ze zm.; art. 46 ust. 1, art. 75 ust. 1-4 i art. 110 ust. 1 ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej, Dz.U. z 2010 r., Nr 220, poz. 1447 ze zm. oraz w związku z art. 3 ust. 1, art. 20a ust. 1–3, art. 3la, art. 36 ust. 1, art. 39 ust. 1 i art. 69e ustawy z dnia 30 sierpnia 1996 r. o komercjalizacji i prywatyzacji, Dz.U. z 2002 r., Nr 171, poz. 1397 ze zm.; art. 18 ust. 1 pkt 1 w związku z art. 2 ust. 1 pkt 6 i 7 ustawy o CBA; art. 75d ust. 1 w związku z ust. 5 ustawy o SC w związku z art. 108 § 2 i art. 109 k.k.s.

zbędne jest wprowadzenie w tym systemie daleko idących zmian tak, aby regulacje ustawowe swym kształtem odpowiadały przepisom Konstytucji RP. Liczne wnioski w tym zakresie płyną z wydanego w dniu 30 lipca 2014 r. wyroku Trybunału Konstytucyjnego w sprawie o sygn. akt K 23/11. Po zbadaniu połączonych wniosków Rzecznika Praw Obywatelskich i Prokuratora Generalnego orzekł, że art. 28 ust. 1 pkt 1 ustawy o ABW i AW, jest niezgodny z art. 47 i art. 49 w zw. z art. 31 ust. 3 Konstytucji przez to, że nie przewiduje niezależnej kontroli udostępniania danych telekomunikacyjnych, o których mowa w art. 180c i 180d p.t. Ponadto, Trybunał orzekł również że 28 ustawy o ABW i AW, w zakresie, w jakim nie przewiduje zniszczenia danych niemających znaczenia dla prowadzonego postępowania, jest niezgodny z art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji. Jednocześnie utrata mocy obowiązującej przez przepisy uznane za niezgodne z Konstytucją RP została odroczona na okres 18 miesięcy od ogłoszenia wyroku w Dzienniku Ustaw.

W uzasadnieniu tego wyroku, Trybunał Konstytucyjny wyjaśnił, że w art. 28 ust. 1 pkt 1 ustawy o ABW i AW w przeciwieństwie do przepisów innych ustaw (m.in. ustawy o Policji czy ustawy o kontroli skarbowej) wprost wyłączono obowiązek uzyskania zgody sądu, a dokładnie rzecz biorąc – obowiązek wydania postanowienia wyrażającego zgodę na udostępnienie funkcjonariuszom ABW danych telekomunikacyjnych. Jednocześnie ustawodawca nie przewidział żadnego alternatywnego mechanizmu niezależnej kontroli nad pozyskiwaniem tych danych przez funkcjonariuszy ABW, który mógłby zostać uznany za spełniający standardy konstytucyjne.

Trybunał Konstytucyjny nie przesądził, jak kontrola taka powinna przebiegać i przez jaki organ powinna być sprawowana. W tym zakresie Trybunał ograniczył się jedynie do sugestii, że nie jest wykluczone wprowadzenie jako zasady kontroli następczej. Zatrzymywanie i udostępnianie różnych rodzajów danych może bowiem powodować różną intensywność ingerencji w wolności i prawa człowieka, a przez to uzasadniać pewne zróżnicowanie mechanizmu kontroli w odniesieniu do poszczególnych rodzajów danych. 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. Trybunał dostrzegł jednak argumenty przemawiające za wprowadzeniem – w pewnych przypadkach – kontroli uprzedniej. Tytułem przykładu, wskazać należy dostęp do danych telekomunikacyjnych osób wykonujących zawody zaufania publicznego lub sytuacje, kiedy brak jest konieczności pilnego działania służb.

Jak zauważył to Trybunał, ustawodawca przyznał ABW uprawnienie do pozyskania danych telekomunikacyjnych w bardzo szerokim zakresie. Dotyczy to bowiem nie tylko rozpoznawania, wykrywania i ścigania przestępstw (które są uregulowane w art. 5 ust. 1 pkt 2 ustawy o ABW i AW), ale również innych zadań, o których mowa w art. 5 ust. 1 ustawy o ABW i AW. Należą do nich: rozpoznawanie i zwalczanie zagrożeń godzących w bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny, a w szczególności w suwerenność i międzynarodową pozycję, niepodległość i nienaruszalność jego terytorium, a także obronność państwa oraz zapobieganie takim zagrożeniom (pkt 1), realizowanie, w granicach

swojej właściwości, zadań związanych z ochroną informacji niejawnych oraz wykonywanie funkcji krajowej władzy bezpieczeństwa w zakresie ochrony informacji niejawnych w stosunkach międzynarodowych (pkt 3), uzyskiwanie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć istotne znaczenie dla ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego (pkt 4) oraz podejmowanie innych działań określonych w odrębnych ustawach i umowach międzynarodowych (pkt 5). Jednocześnie niektóre zadania w postaci rozpoznawania i wykrywania przestępstw wymienionych w art. 5 ust. 1 pkt 2 ustawy o ABW i AW i zapobiegania takim przestępstwom zostały sformułowane na wysokim stopniu ogólności, w związku z czym nie można na ich podstawie zdefiniować konkretnych okoliczności, w których dane telekomunikacyjne mogą być udostępniane funkcjonariuszom ABW.

Trybunał Konstytucyjny podkreślił również, że kontrola udostępniania danych telekomunikacyjnych nie musi być sprawowana przez sądy. Niezbędne jest jednak, aby organ sprawujący taką kontrolę był niezależny od rządu i nie pozostawał w bezpośredniej lub pośredniej relacji zwierzchności z funkcjonariuszami pozyskującymi dane.

Uzasadniając swoje orzeczenie, Trybunał Konstytucyjny podkreślił, że relatywnie ogólne wskazanie zadań organu władzy publicznej (w tym wypadku ABW) samo w sobie nie jest niezgodne z Konstytucją. Problem powstaje natomiast wówczas, gdy w ramach takich zadań, organy władzy publicznej mogą podejmować działania ingerujące w wolności i prawa jednostek polegające na niejawnym pozyskiwaniu informacji. Ilekroć organ władzy publicznej jest uprawniony do pozyskiwania informacji o życiu prywatnym jednostek, w tym danych telekomunikacyjnych, niezbędne jest precyzyjne określenie przez ustawodawcę przedmiotowego zakresu możliwości realizacji tego zadania. Mając na uwadze niezwykle szeroki zakres okoliczności, w jakich ABW mogą zostać udostępnione dane telekomunikacyjne, a zarazem jednoznaczne wyłączenie obowiązku uzyskania zgody sądu oraz braku obowiązku uzyskania na to zgody jakiegokolwiek niezależnego organu, Trybunał stwierdził, że zakwestionowany przepis nie zawiera nawet minimalnych gwarancji proceduralnych, koniecznych z punktu widzenia poszanowania przepisów Konstytucji. W ocenie TK okoliczność ta jest wystarczająca do stwierdzenia niezgodności art. 28 ust. 1 pkt 1 ustawy o ABW i AW z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucją przez to, że nie przewiduje on niezależnej kontroli udostępniania danych telekomunikacyjnych, o których mowa w art. 180c i art. 180d p.t.

Wymaga odnotowania, że w swoim rozstrzygnięciu Trybunał Konstytucyjny nie odniósł się do wszystkich zarzutów podniesionych przez Rzecznika Praw Obywatelskich i Prokuratora Generalnego. Bez refleksji orzeczniczej pozostawiony został zarzut, zgodnie z którym pozyskiwanie danych telekomunikacyjnych nie ma charakteru subsydiarnego. Jest ono dopuszczalne w każdym przypadku, gdy tylko zwrócą się o to odpowiednie służby. Warunkiem uzyskania dostępu do tych danych nie jest bowiem wyczerpanie innych środków prawnych, mniej ingerujących w sferę prywatności oraz w tajemnicę komunikowania się.

Natomiast w sposób szczegółowy Trybunał odniósł się do zarzutu nieuwzględnienia przez ustawodawcę szczególnych rygorów ochrony informacji objętych

tajemnicami zawodowymi (adwokacką, notarialną, radcy prawnego, dziennikarską, lekarską)[22]. Trybunał Konstytucyjny wyjaśnił w tej kwestii, że nie znajduje uzasadnienia bezwarunkowe wyodrębnienie jakiejkolwiek kategorii podmiotów spod dopuszczalności objęcia czynnościami operacyjno-rozpoznawczymi, w tym pozyskiwania informacji w trybie kontroli operacyjnej.

W ocenie Trybunału Konstytucja RP nie przewiduje w tym zakresie jakichkolwiek podmiotowych wyłączeń. Nie oznacza to jednak dopuszczalności pozyskiwania informacji w takim trybie od wszystkich osób w jednakowym stopniu i na jednakowych zasadach. Wyższe standardy konstytucyjności regulacji niejawnego pozyskiwania informacji o jednostkach dotyczą wiadomości przekazywanych osobom, które wykonują zawody zaufania publicznego. Jednym z instrumentów ochrony zaufania jest tajemnica zawodowa i gwarancje jej poszanowania w postępowaniach sądowych. Zaliczają się do nich m.in. bezwarunkowe i warunkowe zakazy dowodowe w postępowaniu karnym. Trybunał Konstytucyjny zwrócił uwagę, że ochrona tajemnicy zawodowej, jak i ściśle związane z nią zakazy dowodowe w postępowaniu karnym nie są wartościami autotelicznymi.

Jakkolwiek zachowanie poufności przez podmioty wykonujące zawody zaufania publicznego musi być zawsze widziane jako integralna wartość demokratycznego państwa prawa, to jednak podstawową ich funkcją jest ochrona wolności i praw konstytucyjnych jednostek przekazujących w dyskrecji pewne informacje na swój temat osobom wykonującym zawody zaufania publicznego (por. wyrok TK z 2 lipca 2007 r., sygn. K 41/05, cz. III, pkt 7). Ochrona tajemnicy zawodowej powinna być zatem każdorazowo widziana jako przejaw ochrony wolności i praw jednostki, zwłaszcza jej prywatności (art. 47), autonomii informacyjnej (art. 51 ust. 1), prawa do obrony (art. 42 ust. 2), prawa do sądu (art. 45 ust. 1), wolności sumienia i wyznania (art. 53) czy wolności pozyskiwania informacji, w tym wolności prasy (art. 54 ust. 1 Konstytucji). Z tego powodu Trybunał podkreślał – odnosząc się do tajemnicy radcy prawnego – że prawo do prywatności i poufności informacji przysługuje nie radcom prawnym, ale ich klientom; natomiast na radcach prawnych spoczywa obowiązek respektowania tego prawa (zob. wyrok TK z 22 listopada 2004 r., sygn. SK 64/03, OTK ZU nr 10/A/2004, poz. 107, cz. III, pkt 3). TK wyjaśnił, że stanowisko to zachowuje aktualność w odniesieniu do pozostałych tajemnic zawodowych. Wyjaśnił ponadto, że kolizja obydwu wartości nie przesądza o tym, że pierwszeństwo ma zawsze zyskiwać ochrona wolności i praw jednostki,

[22] W odniesienie do zarzutu sformułowanego przez Rzecznika Praw Obywatelskich, Trybunał wyjaśnił w uzasadnieniu swojego wyroku, że nie zostały w tym zakresie przedstawione żadne argumenty na jego poparcie. Wniosek Rzecznika Praw Obywatelskich nie spełnia – w ocenie TK – wymagań formalnych wynikających z art. 32 ust. 1 pkt 4 ustawy o TK, czyli nie zawiera uzasadnienia z powołaniem dowodów na poparcie postawionego zarzutu. Tym samym postępowanie w tym zakresie także podlega umorzeniu na podstawie art. 39 ust. 1 pkt 1 ustawy o TK. Z kolei odnosząc się do analogicznego zarzutu postawionego przez Prokuratora Generalnego, Trybunał, pomimo dostrzeżonych mankamentów w argumentacji, stwierdził, że jego intencje są dostatecznie czytelne. Z treści wniosku wynika bowiem, że istotą postawionych zarzutów jest uregulowanie kontroli operacyjnej w sposób nieprecyzyjny i niegwarantujący dostatecznej ochrony konstytucyjnych wolności oraz praw osób, w interesie których ustanowiono obowiązek zachowania tajemnicy zawodowej i tak zwane zakazy dowodowe.

a pośrednio sama tajemnica zawodowa. W tym zakresie Trybunał odwołał się do swojego wcześniejszego orzecznictwa[23]. Na tej podstawie Trybunał Konstytucyjny wyjaśnił, że „ogólne wyłączenie spod kontroli operacyjnej podmiotów zobowiązanych w ustawie do zachowania tajemnicy zawodowej, a nawet wyłączenie informacji uznawanych za stanowiące tajemnicę zawodową, jako bezwzględnie niedopuszczalnych do pozyskania w tym trybie, prowadziłoby do istotnych utrudnień w gromadzeniu materiału dowodowego niektórych rodzajów przestępstw, popełnianych np. z wykorzystaniem nowych technologii".

Na tej podstawie TK wywiódł, że „punkt ciężkości przesuwa się więc na zapewnienie stosownych gwarancji proceduralnych, eliminujących nieuprawnione pozyskanie przez służby policyjne oraz służby ochrony państwa informacji, które – z uwagi na ich treść i okoliczności przekazania – powinny podlegać ochronie prawnej". W ocenie Trybunału modelowym rozwiązaniem tego konfliktu pomiędzy dwoma dobrami jest przewidziany w art. 180 § 2 k.p.k. mechanizm zwolnienia z tajemnicy zawodowej przez sąd w sytuacji, gdy jest to konieczne dla dobra wymiaru sprawiedliwości, zaś dana okoliczność nie może zostać wykazana w inny sposób. Zbliżone rozwiązania legislacyjne powinny – w ocenie TK – dotyczyć również ochrony tajemnicy zawodowej w trakcie czynności operacyjno-rozpoznawczych, w tym kontroli operacyjnej. Nie istnieją bowiem jakiekolwiek uzasadnione podstawy do tego, aby na tym etapie postępowania stosować łagodniejsze standardy, aniżeli przewidują to przepisy procedury karnej. Przeciwnie, uznać należy, że standardy te – z uwagi na ponadprocesowy, niejawny charakter kontroli – powinny być co najmniej tożsame ze standardami w postępowaniu karnym.

Jak już wyjaśniono, na podstawie wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r., w sprawie o sygnaturze K 23/11, przepis art. 28 ustawy o ABW i AW, w poprzednim brzmieniu, w zakresie w jakim nie przewidywał zniszczenia danych niemających znaczenia dla prowadzonego postępowania, został uznany za niezgodny z art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji. Trybunał Konstytucyjny wyjaśnił, że warunkiem niejawnego uzyskiwania informacji o jednostkach, w tym dotyczących ich danych telekomunikacyjnych, jest ustanowienie procedury niezwłocznej selekcji oraz niszczenia materiałów zbędnych i niedopuszczalnych. Rozwiązanie to zapobiega nieuprawnionemu wykorzystaniu przez organy państwa zebranych legalnie informacji i ich przechowywaniu na wszelki wypadek, gdyby w przyszłości okazały się przydatne do innych celów. Ingerencją w sferę prywatności jednostek będzie nie tylko jednorazowe pozyskanie danych o jednostce (m.in. w trybie określonym w art. 28 ust. 1 ustawy o ABW), ale również każde kolejne operacje na tych danych, w tym przechowywanie czy wtórne wykorzystywanie w toku innych postępowań. Ustawodawca dodał do art. 28 nowy ustęp – ust. 7. Zgodnie z jego treścią dane, o których mowa w ust. 1, które nie mają znaczenia dla postępowania karnego albo nie są istotne dla bezpieczeństwa państwa, podlegają niezwłocznemu, komisyjnemu i protokolarnemu zniszczeniu. Ustawodawca

[23] Zob. wyroki TK z dnia: 22 listopada 2004 r., sygn. SK 64/03, cz. III, pkt 3; 2 lipca 2007 r., sygn. K 41/05, cz. III, pkt 7; 13 grudnia 2011 r., sygn. K 33/08, OTK ZU nr 10/A/2011, poz. 116, cz. III, pkt 6.4.

nie przewidział więc zniszczenia wszelkich innych danych telekomunikacyjnych, pocztowych i internetowych niż tylko tych, które nie posiadają znaczenia dla prowadzonego postępowania karnego. W ten sposób ustawodawca zezwolił na zachowanie danych, określonych jako „istotne dla bezpieczeństwa państwa".

4. NOWE BRZMIENIE ART. 28 USTAWY O ABW I AW

Stanowiący przedmiot trybunalskiego orzeczenia, przepis art. 28 ustawy o ABW i AW nie regulował postępowania z danymi telekomunikacyjnymi, po ich zgromadzeniu na podstawie art. 28 ust. 1 ustawy o ABW i AW. Kwestia postępowania ze zgromadzonymi w tym trybie danymi została przez ustawodawcę pominięta. Nie ma zarazem prawnych podstaw do odpowiedniego stosowania przepisów regulujących niszczenie danych zgromadzonych w kontroli operacyjnej czy przepisów k.p.k. regulujących kontrolę i utrwalanie treści rozmów (art. 237 i n. k.p.k.). Oznaczało to, że na gruncie art. 28 ustawy o ABW nie było żadnych regulacji dotyczących weryfikacji oraz niszczenia danych zbędnych. Nie można więc było wykluczyć przechowywania danych nieprzydatnych w prowadzonym postępowaniu, w toku którego wystąpiono o te dane, ani nawet do innych usprawiedliwionych konstytucyjnie celów. Trybunał Konstytucyjny nie neguje dopuszczalności dalszego przechowywania (to jest po ich analizie i stwierdzeniu ewentualnej nieprzydatności w prowadzonym postępowaniu w konkretnej sprawie) danych telekomunikacyjnych dotyczących cudzoziemców znajdujących się pod władzą Rzeczypospolitej Polskiej, w szczególności jeśli istnieją poważne i uzasadnione podejrzenia co do ich zaangażowania w działalność zagrażającą bezpieczeństwu państwa, w tym w terroryzm i przestępczość zorganizowaną. Takie zróżnicowanie stopnia ochrony ma swe umocowanie przede wszystkim w art. 51 ust. 2 i art. 37 ust. 2 Konstytucji.

Chcąc dostosować uchylone przez TK przepisy p.t. do standardów konstytucyjnych, w dniu 15 stycznia 2016 r. została uchwalona ustawa o zmianie ustawy o Policji oraz niektórych innych ustaw[24]. Ustawa ta nadała nowe brzmienie art. 28 ust. 2–3 ustawy o ABW i AW. Zgodnie z art. 28 ust. 2 ustawy o ABW i AW, przedsiębiorca telekomunikacyjny, operator pocztowy lub usługodawca świadczący usługi drogą elektroniczną udostępnia nieodpłatnie dane, o których mowa w art. 28 ust. 1 ustawy o ABW i AW, odpowiednio:

1) funkcjonariuszowi ABW wskazanemu w pisemnym wniosku Szefa ABW lub osoby upoważnionej przez ten organ;
2) na ustne żądanie funkcjonariusza ABW posiadającego pisemne upoważnienie Szefa ABW;
3) za pośrednictwem sieci telekomunikacyjnej funkcjonariuszowi ABW posiadającemu upoważnienie, o którym mowa w pkt 2.

W przypadku udostępnienia danych na ustne żądanie funkcjonariusza ABW posiadającego pisemne upoważnienie Szefa ABW, udostępnianie danych odbywa się bez udziału pracowników przedsiębiorcy telekomunikacyjnego, operatora pocz-

[24] Dz.U. z 2016, poz. 147.

towego lub usługodawcy świadczącego usługi drogą elektroniczną, lub przy ich niezbędnym współudziale, jeżeli możliwość taką przewiduje porozumienie zawarte pomiędzy Szefem ABW a tym podmiotem (art. 28 ust. 3 ustawy o ABW i AW).

Udostępnienie ABW danych, o których mowa w art. 180c i 180d p.t., może nastąpić za pośrednictwem sieci telekomunikacyjnej, jeżeli sieć ta zapewnia:
1) możliwość ustalenia funkcjonariusza ABW uzyskującego dane, ich rodzaju oraz czasu, w którym zostały uzyskane;
2) zabezpieczenie techniczne i organizacyjne uniemożliwiające osobie nieuprawnionej dostęp do tych danych (art. 28 ust. 4 ustawy o ABW i AW).

5. SĄDOWA KONTROLA UZYSKIWANIA PRZEZ ABW DANYCH TELEKOMUNIKACYJNYCH

Jednym z zarzutów, które Trybunał Konstytucyjny skierował wobec ustawy o ABW i AW w zakresie prowadzonych badań objętych wnioskami RPO i PG był brak sądowej kontroli nad uzyskiwaniem przez funkcjonariuszy ABW danych telekomunikacyjnych. Wydaje się, że jest to najistotniejsza kwestia, nad którą pochylił się Trybunał Konstytucyjny w swoim orzeczeniu. Zagadnienie to z uwagi na swój istotny charakter, wymaga odrębnego potraktowania. Udostępnianie danych telekomunikacyjnych służbom specjalnym jest bowiem doniosłe z perspektywy ingerowania w konstytucyjne wolności i prawa, m.in. tajemnicę korespondencji i wolność komunikowania się. Tak więc uznać należy, że pozbawienie sądu kontroli tych procedur, a *de facto* – na co zwrócił uwagę Trybunał – brak regulacji zapewniających jakąkolwiek niezależną od rządu kontrolę tego procesu, jest zjawiskiem dalece niepożądanym. Nie mieści się to bowiem w konstytucyjnych standardach wyznaczonych przez polskiego ustrojodawcę. W ustawodawstwie zwykłym nie przewidziano jakiegokolwiek sądowego, ani nawet alternatywnego do sądowego mechanizmu niezależnej kontroli nad pozyskiwaniem danych telekomunikacyjnych przez funkcjonariuszy ABW. Z uwagi więc na fakt, że katalog okoliczności pozwalających funkcjonariuszom ABW uzyskać dane telekomunikacyjne jest szeroki, należy stwierdzić, że nie istniała w tym zakresie żadna, choćby minimalna proceduralna gwarancja poszanowania standardów konstytucyjnych.

Chcąc rozwiązać ten problem, na podstawie wspomnianej ustawy z dnia 15 stycznia 2016 r. dodano do ustawy o ABW i AW nowy przepis – art. 28a. Zgodnie z tym przepisem kontrolę nad uzyskiwaniem przez ABW danych telekomunikacyjnych, pocztowych lub internetowych sprawuje Sąd Okręgowy w Warszawie (ust. 1). Szef ABW przekazuje, z zachowaniem przepisów o ochronie informacji niejawnych, wskazanemu sądowi, w okresach półrocznych, sprawozdanie obejmujące:
1) liczbę przypadków pozyskania w okresie sprawozdawczym danych telekomunikacyjnych, pocztowych lub internetowych oraz rodzaj tych danych;
2) kwalifikacje prawne czynów, w związku z zaistnieniem których wystąpiono o dane telekomunikacyjne, pocztowe lub internetowe (ust. 2).

W ramach tej kontroli, sąd może zapoznać się z materiałami uzasadniającymi udostępnienie ABW danych telekomunikacyjnych, pocztowych lub internetowych

Sąd informuje Szefa ABW o wyniku kontroli w terminie 30 dni od jej zakończenia (ust. 3).

Ustawodawca, na podstawie art. 28a ustawy o ABW i AW, wprowadził więc – preferowaną przez ustrojodawcę – następczą kontrolę udostępniania ABW danych telekomunikacyjnych. W wyroku z dnia 30 lipca 2014 r., w sprawie o sygnaturze K 23/11 TK wskazał, że ogólny standard konstytucyjny nie przesądza, jak dokładnie ma wyglądać procedura dostępu do danych telekomunikacyjnych, a w szczególności czy konieczne ma być w odniesieniu do każdego rodzaju zatrzymywanych danych, o których mowa w art. 180c i art. 180d p.t. uzyskanie zgody na ich udostępnienie. Nie wszystkie dane tego rodzaju powodują taką samą intensywność ingerencji w wolności i prawa człowieka. Zdaniem Trybunału nie jest wykluczone – w odniesieniu do udostępniania danych telekomunikacyjnych w toku czynności operacyjno-rozpoznawczych – wprowadzenie, jako zasady, kontroli następczej. Regulując ten mechanizm, ustawodawca powinien uwzględnić m.in. specyfikę działania i ustawowy zakres zadań poszczególnych służb, sytuacje niecierpiące zwłoki, w których szybkie pozyskanie danych telekomunikacyjnych może być niezbędne do zapobieżenia popełnieniu przestępstwa lub jego wykrycia. Zgodnie z wyrażoną w preambule, konstytucyjną zasadą sprawności działania instytucji publicznych należy wykreować mechanizm, który umożliwiłby służbom odpowiedzialnym za bezpieczeństwo państwa i porządek publiczny efektywną walkę z zagrożeniami. Trybunał dostrzega jednak argumenty za wprowadzeniem kontroli uprzedniej w pewnych wypadkach. W szczególności chodzić może o dostęp do danych telekomunikacyjnych osób wykonujących zawody zaufania publicznego lub jeśli nie ma koniecznego pilnego działania służb. Kwestie te musi jednak odpowiednio wyważyć ustawodawca.

Na tle nowej regulacji ustawowej jawi się kilka pytań. Po pierwsze, należy zastanowić się nad efektywnością przyjętego rozwiązania. Istotne jest bowiem to, na ile kontrola sprawowana przez sąd będzie miała charakter rzeczywisty, a nie wyłącznie pozorny. Prowadzenie kontroli nie jest bowiem obligatoryjne tylko fakultatywne. Dane podlegające kontroli będą przekazywane periodycznie – w okresach półrocznych. Sprawujący kontrolę sąd okręgowy, może w ramach swoich uprawnień zapoznać się z materiałami uzasadniającymi udostępnienie ABW danych telekomunikacyjnych, efektem czego będą wyniki kontroli przekazywane przez ten sąd organowi ABW. Po przekazaniu wyników kontroli aktywność sądu nakierowana na zweryfikowanie prawidłowości udostępnienia danych telekomunikacyjnych ABW w zasadzie zostanie zakończona. Ustawodawca nie określił procesowych zagadnień związanych z ewentualnymi dalszymi działaniami sądu w przypadku wykrycia, że udostępnienie danych nastąpiło z naruszeniem obowiązujących przepisów. Sąd po przeprowadzeniu kontroli będzie mógł w zasadzie jedynie poinformować kontrolowaną służbę o wynikach kontroli. Nie dysponuje natomiast kompetencją do zarządzenia zniszczenia zgromadzonych danych[25].

[25] Analogiczne rozwiązanie przyjęto w przypadku pozostałych podmiotów uprawnionych do przeprowadzania kontroli operacyjnej. Zob. art. 18a ustawy o CBA; art. 36ba ustawy o KS; art. 20ca ustawy o Policji; 75da ustawy o SC; art. 10ba ustawy o Straży Granicznej; art. 32a ustawy o SKW oraz SWW; art. 30b ustawy o ŻW.

Po drugie, trzeba się zastanowić, czy z perspektywy ochrony praw i wolności obywatelskich, ale także uwzględnienia interesów służb, lepszym rozwiązaniem nie byłoby wprowadzenie – jako reguły – uprzedniej kontroli sądu. Nie oznacza to rezygnacji z kontroli następczej, ale stosowanie jej w nie cierpiących zwłoki przypadkach, wymagających działania ABW. Takie rozwiązanie z pewnością przyczyniłoby się zarówno do zwiększenia poprawności przygotowywanych przez organy ABW i inne służby wniosków, jak również do zwiększenia ich liczby.

Zaprezentowane powyżej wątpliwości znajdują również oparcie w wyroku TSUE z 8 kwietnia 2014 r. Trybunał zauważył, że uzyskanie przez właściwe organy krajowe dostępu do danych nie podlega uprzedniej kontroli sądu lub niezależnego organu administracyjnego. Sąd lub niezależny organ administracyjny powinien kontrolować, aby udostępnianie i wykorzystywanie danych ograniczało się do przypadków, gdy jest to ściśle konieczne do realizacji zamierzonego celu[26]. TSUE mówi więc wyraźnie o uprzedniej kontroli niezależnego organu.

Warto również zwrócić uwagę na to, że zgodnie z art. 28a ust. 5 ustawy o ABW i AW, nie podlega kontroli uzyskiwanie danych na podstawie art. 28b ust. 1 ustawy o ABW i AW. Zgodnie z tym przepisem chodzi więc o szerokie spektrum informacji obejmujące dane:

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

6. WNIOSKI

Waga orzecznictwa dla praktyki stosowania określonych instytucji prawnych nie budzi wątpliwości. Można wręcz powiedzieć, że orzecznictwo stanowi drugie dno każdej regulacji prawnej, bowiem kształtuje ono stosowanie prawa w praktyce. Dotyczy to nie tylko orzecznictwa sądowego, ale również orzecznictwa Trybunału Konstytucyjnego, któremu ustrojodawca przypisał podstawową rolę w postaci badania i orzekania w kwestii hierarchicznej zgodności aktów prawnych[27].

Trybunał Konstytucyjny nie tylko ustala, ale częstokroć wypełnia treścią normy konstytucyjne, które z założenia mają wyższy stopień ogólności, niż w przypadku ustawodawstwa zwykłego. Należy więc uznać, że Trybunał nie jest wyłącznie rekonstruktorem treści normy prawnej, ale – w związku z walorem powszechnego obowiązywania orzeczeń tego organu – faktycznie współtworzy treść normy na

[26] Tezy 60–62 wyroku z dnia 8 kwietnia 2014 r. Trybunał Sprawiedliwości Unii Europejskiej, Dz. Urz. UE z 2014 r., L 105.

[27] Zob. M. Zubik, *Status prawny sędziego Trybunału Konstytucyjnego*, Warszawa 2011, s. 22.

potrzeby praktyki konstytucyjnej. Co więcej, w przypadku oceny konstytucyjności ustaw posiada on w tym zakresie monopol kompetencyjny. Te uprawnienia Trybunału nabierają szczególnego znaczenia w sytuacji, gdy badana przez Trybunał ustawa stanowi wykonanie konstytucyjnych przepisów. Nie budzi wątpliwości, że ustawa o ABW i AW w zakresie gromadzenia i udostępniania danych telekomunikacyjnych należy do tej właśnie kategorii. Wprowadza bowiem ograniczenia w korzystaniu z konstytucyjnej wolności komunikowania się, która – podobnie jak każda inna wolność – nie może mieć charakteru nieograniczonego. Przeczyłoby to jej istocie, mogąc doprowadzić do konfliktów polegających na ingerencji jednej osoby w wolność innej czy na instrumentalnym traktowaniu, a w konsekwencji nadużywaniu przysługującej wolności. Ustawodawca konstytucyjny, mając świadomość tych zagrożeń, przewidział dwie podstawy ustrojowe ograniczenia wolności komunikowania się. Pierwsza z nich została określona w art. 49 Konstytucji RP, tj. w przepisie ustanawiającym tę wolność. Z jego treści wynika, że ograniczenie wolności komunikowania się jest dopuszczalne jedynie w przypadkach określonych w ustawie i w sposób w niej określony[28]. Ustawowe graniczenia konstytucyjnej wolności komunikowania się mogą więc zostać ustanowione wówczas, gdy korzystanie z tej wolności prowadziłoby do naruszenia praw i wolności jednostki oraz innych konstytucyjnie chronionych wartości.

Drugą podstawę stanowi art. 31 ust. 3 Konstytucji RP, formułujący generalne ograniczenie korzystania z konstytucyjnych wolności i praw[29]. Przepis ten składa się z dwóch części. Część pierwsza stanowi klauzulę generalną odnoszącą się do ograniczeń sformułowanych w niej praw i wolności. Ustawodawca konstytucyjny przyjął zasadę powszechnie uznaną w demokratycznych konstytucjonalizmach, zgodnie z którą ustalenie granic konstytucyjnych wolności i praw może być dokonane tylko w ustawie[30]. Część druga art. 31 ust. 3 Konstytucji RP stanowi określenie

---

[28] Z takiego unormowania zawartego w art. 49 zd. 2 Konstytucji RP wynikają trojakie konsekwencje. Po pierwsze, ustawodawca zwykły dysponuje konstytucyjnie przyznanym prawem decydowania o zakresie wolności komunikowania się. Po drugie, jedynym aktem, przy pomocy którego dopuszczalna jest ingerencja w wolność komunikowania się jest ustawa. Po trzecie, z ustawy zwykłej wynikać mają określone przypadki i sposoby ograniczenia. Istnieje zatem w tym zakresie wymóg konkretności, wyłączając możliwość zastosowania klauzul generalnych. Zob. wyrok TK z dnia 12 grudnia 2005 r., sygn.. akt K 32/04, OTK-A 2005, nr 11, poz. 132.

[29] Brzmi on następująco: „Ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Ograniczenia te nie mogą naruszać istoty wolności i praw".

[30] Zarówno w piśmiennictwie jak i w orzecznictwie zwrot ten jest interpretowany podobnie. Ustawa nie musi stanowić jedynego źródła ograniczeń. Dopuszczalne są bowiem sytuacje, kiedy na poziomie ustawy określone są jedynie podstawowe elementy ograniczeń. Ich rozwinięcie i uzupełnienie może zaś zostać dokonane w akcie podustawowym, np. w rozporządzeniu czy w akcie prawa miejscowego. Regulacja ustawowa musi jednak nadawać tym ograniczeniom zasadniczy kształt oraz wyznaczać ich zakres. Zob. K. Wojtyczek, *Granice ingerencji ustawodawczej w sferę praw człowieka w Konstytucji RP,* Kraków 1999, s. 110; wyrok TK z dnia 12 stycznia 2000 r., sygn. akt P 11/98, OTK 2000, nr 1, poz. 3.

materialnoprawnych przesłanek dopuszczających ograniczenie praw i wolności[31]. Są nimi: bezpieczeństwo lub porządek publiczny, ochrona środowiska, zdrowia i moralności publicznej oraz ochrona wolności i praw innych osób.

Jak wyjaśniono w toku wywodu, w wyroku z dnia 30 lipca 2014 r., sygn. akt K 23/11 Trybunał Konstytucyjny zakwestionował przepisy ustawy o ABW i AW w zakresie w jakim ustawodawca nie przewidział niezależnej kontroli udostępniania danych telekomunikacyjnych, jak również w zakresie, w jakim nie przewidziano zniszczenia danych niemających znaczenia dla prowadzonego postępowania. Rozstrzygnięcie to należy uznać za słuszne. Po pierwsze, każde ograniczenie konstytucyjnej wolności komunikowania się jest odstępstwem od ustrojowej zasady i jako takie powinno być poddane kontroli. Należy w tym zakresie przychylić się do postulatu formułowanego w literaturze, zgodnie z którym regulacja ograniczeń w zakresie wolności komunikowania się oraz ich realizacja powinny zostać poddane kontroli sądowej[32]. Po drugie, mając na uwadze to, że pozyskiwanie danych telekomunikacyjnych stanowi odstępstwo od – będącej zasadą – tajemnicy komunikowania się, niezbędne wydaje się niezwłoczne niszczenie danych, które nie mają znaczenia dla postępowania.

Korzystając z przyznanej mu w tym zakresie kompetencji, Trybunał orzekł, że utrata mocy obowiązującej przez przepisy uznane za niezgodne z Konstytucją RP nastąpi po upływie maksymalnego okresu 18 miesięcy od ogłoszenia wyroku w Dzienniku Ustaw. W tym czasie ustawodawca powinien podjąć stosowne prace legislacyjne w celu usunięcia przepisów uznanych za niekonstytucyjne. Tak też się stało. Na podstawie art. 7 ustawy z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw, wypełniając swą prawną powinność, ustawodawca wprowadził stosowne zmiany w ustawie o ABW i AW, usuwając z obrotu prawnego przepisy uznane przez Trybunał za niekonstytucyjne.

BIBLIOGRAFIA

Banaszak B., *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2012.

Garlicki L., *Uwagi do art. 49 Konstytucji RP*, [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, L. Garlicki (red.), t. II, Warszawa 2002.

Kawałek K., Rogalski M. (red.), *Prawo telekomunikacyjne. Komentarz*, Warszawa 2010.

Kiziński M., *Retencja danych telekomunikacyjnych*, „Prokuratura i Prawo" 2016, nr 1.

Wach M., *Zatrzymywanie danych telekomunikacyjnych przez dwa lata w celach bliżej nieokreślonych a prawo do prywatności*, „Radca Prawny" Dodatek naukowy 2011, nr 115–116.

Wojtyczek K., *Granice ingerencji ustawodawczej w sferę praw człowieka w Konstytucji RP*, Kraków 1999.

Zubik M., *Status prawny sędziego Trybunału Konstytucyjnego*, Warszawa 2011.

[31] Zob. wyrok TK z dnia 25 lutego 1999 r., sygn. akt K 23/98, OTK 1999, nr 2, poz. 25.

[32] Zob. B. Banaszak, *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2012, s. 256.

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. Urz. UE, L 105.
Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz.U. z 1997, nr 78, poz. 483, ze zm.
Konwencja o ochronie praw człowieka i podstawowych wolności sporządzona w Rzymie dnia 4 listopada 1950 r., Dz.U. z 1993, nr 61, poz. 284, ze zm.
Rozporządzenie Ministra Infrastruktury z dnia 24 stycznia 2003 roku w sprawie wykonywania przez operatorów zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, Dz.U. nr 19, poz. 166, ze zm.
Ustawa z dnia 26 stycznia 1984 r. – Prawo prasowe, Dz.U. Nr 5, poz. 24, ze zm.
Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym, Dz.U. z 2001 r., Nr 142, poz. 1591 ze zm.
Ustawa z dnia 6 kwietnia 1990 r. o Policji, Dz.U. z 2015, poz. 355, ze zm.
Ustawa z dnia 12 października 1990 r. o Straży Granicznej, Dz.U. z 2014, poz. 1402, ze zm.
Ustawa z dnia 28 września 1991 r. o kontroli skarbowej, Dz.U. z 2016, poz. 720, ze zm.
Ustawa z dnia 13 października 1995 r. – Prawo łowieckie, Dz.U. z 2005 r., Nr 127, poz. 1066 ze zm.
Ustawa z dnia 9 maja 1996 r. o wykonywaniu mandatu posła i senatora, Dz.U. z 2011 r., Nr 7, poz. 29 ze zm.
Ustawa z dnia 30 sierpnia 1996 r. o komercjalizacji i prywatyzacji, Dz.U. z 2002 r., Nr 171, poz. 1397, ze zm.
Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego, Dz.U. nr 89, poz. 555, ze zm.
Ustawa z dnia 21 sierpnia 1997 r. o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne, Dz.U. z 2006 r., Nr 216, poz. 1584 ze zm.
Ustawa z dnia 5 czerwca 1998 r. o samorządzie województwa, Dz.U. z 2001 r., Nr 142, poz. 1590 ze zm.
Ustawa z dnia 5 czerwca 1998 r. o samorządzie powiatowym, Dz.U. z 2001 r., Nr 142, poz. 1592 ze zm.
Ustawa z dnia 10 września 1999 r. Kodeks karny skarbowy, Dz.U. z 2013, poz. 186, ze zm.
Ustawa z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych, Dz.U. z 2001 r., Nr 98, poz. 1070 ze zm.
Ustawa z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych, Dz.U. z 2016, poz. 96, ze zm.
Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu, Dz.U. z 2015, poz. 1929, ze zm.
Ustawa z dnia 23 listopada 2002 r. o Sądzie Najwyższym, Dz.U. z 2002 r., Nr 240, poz. 2052 ze zm.
Ustawa z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych, Dz.U. z 2010 r., Nr 113, poz. 759 ze zm.
Ustawa z dnia 11 marca 2004 r. o ochronie zdrowia zwierząt oraz zwalczaniu chorób zakaźnych zwierząt, Dz.U. z 2008 r., Nr 213, poz. 1342, ze zm.
Ustawa z dnia 19 marca 2004 r. – Prawo celne, Dz.U. z 2004 r., Nr 68, poz. 662 ze zm.
Ustawa z dnia 16 kwietnia 2004 r. o wyrobach budowlanych, Dz.U. Nr 92, poz. 881, ze zm.
Ustawa z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej, Dz.U. z 2010 r., Nr 220, poz. 1447 ze zm.
Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym, Dz.U. z 2016, poz. 1310, ze zm.

Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, Dz.U. z 2016, poz. 1318, ze zm.
Ustawa z dnia 27 sierpnia 2009 r. o Służbie Celnej, Dz.U. z 2015, poz. 990, ze zm.
Ustawa z dnia 25 lutego 2011 r. o substancjach chemicznych i ich mieszaninach, Dz.U. Nr 63, poz. 332, ze zm.
Ustawa z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw, Dz.U. z 2016, poz. 147.

Wyrok TK z dnia 25 lutego 1999 r., sygn. akt K 23/98.
Wyrok TK z dnia 12 stycznia 2000 r., sygn. akt P 11/98.
Wyrok TK z dnia 12 grudnia 2005 r., sygn. akt K 32/04.
Wyrok TK z dnia 30 lipca 2014 r., sygn. akt K 23/11.

http://www.nik.gov.pl/plik/id, 5421,vp,7038.pdf [dostęp: 15.08.2016].
Fundacja Panoptykon, *Telefoniczna Kopalnia Informacji. Przewodnik,* w serwisie Internetowym: http://panoptykon. org/biblio/telefoniczna–kopalnia–informacji–przewodnik [dostęp: 15.08.2016].
Wniosek RPO do TK z dnia 1 sierpnia 2011 r., s. 15; w serwisie internetowym: 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 [dostęp: 15.08.2016].

POZYSKIWANIE DANYCH TELEKOMUNIKACYJNYCH PRZEZ AGENCJĘ BEZPIECZEŃSTWA WEWNĘTRZNEGO PO WYROKU TRYBUNAŁU KONSTYTUCYJNEGO Z 30 LIPCA 2014 ROKU

Streszczenie

Celem tego artykułu jest analiza wyroku TK z dnia 30 lipca 2016 r. sygn. akt K 23/11 w sprawie billingów i podsłuchów w zakresie, w jakim dotyczy on pozyskiwania danych telekomunikacyjnych przez Agencję Bezpieczeństwa Wewnętrznego. Wiąże się z tym ustalenie reakcji legislacyjnej ustawodawcy na treść tego wyroku i wytyczne trybunalskie w zakresie, w jakim odnosi się on do pozyskiwania danych telekomunikacyjnych przez tę właśnie służbę. Do przeprowadzenia badań nakierowanych na osiągnięcie założonych celów wykorzystano metodę dogmatyczno-prawną, poprzez badanie treści aktów prawnych oraz wydawanego w tym zakresie orzecznictwa Trybunału Konstytucyjnego. Na podstawie przeprowadzonych rozważań ustalono, że Trybunał Konstytucyjny zasadnie uznał za niezgodne z Konstytucją przepisy ustawy o ABW i AW w zakresie, w jakim ustawodawca nie przewidział niezależnej kontroli udostępniania danych telekomunikacyjnych, jak również w zakresie, w jakim nie przewidziano zniszczenia danych niemających znaczenia dla prowadzonego postępowania. Oba te mankamenty zostały prawidłowo zmodyfikowane w ustawie z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji i niektórych innych ustaw.

Słowa kluczowe: Prawo telekomunikacyjne, dane telekomunikacyjne, retencja danych, Agencja Bezpieczeństwa Wewnętrznego, Trybunał Konstytucyjny

OBTAINING COMMUNICATIONS DATA BY THE INTERNAL SECURITY AGENCY AFTER THE CONSTITUTIONAL TRIBUNAL JUDGEMENT OF 30 JULY 2014

Summary

The article aims to analyse the Constitutional Tribunal judgement of 30 July 2016, file no. K23/11, on the Internal Security Agency obtaining telecommunications billings and intercepting communications in order to obtain communications data. It is connected with the establishment of the legislator's legislative response to the content of the judgement and its recommendations as far as obtaining communications data by this agency is concerned. In order to conduct the analysis and meet the set objectives, the author uses a dogmatic-legal method and examines the content of legal acts and the Constitutional Tribunal judgements issued in relation to them. Based on that, it is established that the Constitutional Tribunal rightly recognised the provisions of Act on the Internal Security Agency and the Intelligence Agency as partly unconstitutional because the legislator did not envisage independent supervision of telecommunications data provision and did not regulate the destruction of data that are insignificant for a proceeding conducted. Both deficiencies were rectified in Act of 15 January 2016 amending Act on the Police and some other acts.

Key words: communications law, communications data, data retention, Internal Security Agency, Constitutional Tribunal