Alfred Staszak

Prawne podstawy dopuszczalności żądania bilingów

W ostatnim okresie w mediach i w piśmiennictwie fachowym rozgorzała dyskusja na temat prawnej dopuszczalności pozyskiwania, a następnie przetwarzania i gromadzenia przez organy ścigania danych dotyczących połączeń telefonicznych, uzyskanych od operatorów usług telefonicznych[1]. Szczególną uwagę należy przy tej dyskusji zwrócić na pytania podnoszone przez przedstawicieli środków masowego przekazu dotyczące prawnej dopuszczalności pozyskiwania wykazów połączeń telefonów należących do dziennikarzy, w sytuacji gdy są oni „chronieni" przed takim żądaniem tajemnicą dziennikarską.

I. Wzorce Europejskiego Trybunału Praw Człowieka i norm konstytucyjnych

Punktem wyjścia wszelkich rozważań dotyczących prawnej dopuszczalności pozyskiwania, a następnie przetwarzania i gromadzenia przez organy ścigania uzyskanych od operatorów usług telefonicznych danych dotyczących połączeń telefonicznych, wśród których mogą znaleźć się wykazy połączeń należące do dziennikarzy, w demokratycznym państwie prawa musi być zawsze powszechnie akceptowany standard gwarancji praw człowieka i podstawowych swobód obywatelskich. W krajach europejskich takim punktem odniesienia jest *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności* (dalej: *Konwencja*) oraz orzecznictwo Europejskiego Trybunału Praw Człowieka (dalej: ETPCz).

Artykuł 5 wyżej przytoczonej *Konwencji* stwierdza, że każdy ma prawo do wolności i bezpieczeństwa osobistego. Artykuł 8 natomiast odnosi się do konieczności poszanowania życia prywatnego i rodzinnego, mieszkania i korespondencji. Ten sam artykuł stanowi, że: *Niedopuszczalna jest ingerencja władzy publicznej w korzystanie z tego prawa, z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności innych osób*[2]. W ten sposób wyżej wymieniona *Konwencja* z jednej strony wskazuje podstawowe prawa obywatelskie, a z drugiej przewiduje możliwość – po spełnieniu określonych przesłanek – ingerencji organów władzy państwowej, a w tym i organów ścigania,

[1] Zob.: rs, amk/fac [podpis autora pod przytoczonym dalej artykułem – przyp. red.], *Oświadczenie przewodniczącego speckomisji. Kontrola dziennikarzy „zgodna z prawem", ale „niedopuszczalna"*, www.tvn24.pl/12690,1677636,0,1,kontrola-dziennikarzy-zgodna-z-prawem--ale-niedopuszczalna,wiadomosc.html [dostęp: 18.05.2011]; W. Czuchnowski, *Wpadka speckomisji*, „Gazeta Wyborcza" z 14.10.2010; D. Barski, *Tajemnica dziennikarska nie chroni bilingów*, „Rzeczpospolita" z 15.10.2010; J. Kondracki, K. Stępiński, *Bilingi pod osłoną tajemnicy dziennikarskiej*, „Rzeczpospolita" z 11.10.2010; es [podpis autora pod przytoczonym dalej artykułem – przyp. red.], *Jak śledzić podsłuchy*, http://wyborcza.pl/1,75478,8758667,Jak_sledzic_podsluchy.html.

[2] *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności* sporządzona w Rzymie dnia 4 listopada 1950 r., Dz.U. z 1993 r., Nr 61, poz. 284.

w te prawa. Uznaje także, że istnieje możliwość interwencji państwa, jeżeli tylko organy władzy będą działały:
- na podstawie ustaw i w ich granicach,
- w sytuacjach koniecznych *z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności innych osób.*

Konwencja zawiera także normę, choć nie wyrażoną wprost, odnoszącą się do działalności dziennikarskiej poprzez zagwarantowanie obywatelom prawa do wolności wyrażania opinii, która obejmuje *wolność posiadania poglądów oraz otrzymywania i przekazywania informacji i idei*[3].

Podobne uregulowania znajdujemy w *Konstytucji Rzeczypospolitej Polskiej z 2 kwietnia 1997 roku* (dalej: *Konstytucja*). Art. 49 tej ustawy zasadniczej gwarantuje *wolność i ochronę tajemnicy komunikowania się*, jednak następne zdanie tego artykułu stwierdza, że ograniczenie tych praw jest możliwe *w przypadkach określonych w ustawie i w sposób w niej określony*. Podobnie art. 31 zawiera zapis, że: *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.*

Stwierdzić zatem należy, że zarówno *Konwencja*, jak i *Konstytucja*, wyraźnie wskazują na to, że wolność komunikowania się i swobodnego przepływu informacji należy do fundamentalnych praw obywatelskich w państwach demokratycznych. Prawa te podlegają ochronie przewidzianej dla tajemnicy komunikowania się, a ingerencja organów władzy państwowej w to prawo jest możliwa jedynie wtedy, gdy te organy będą działały w granicach ustawowego umocowania i w sytuacjach koniecznych dla zapewnienia bezpieczeństwa lub porządku publicznego.

II. Zakres pojęć: kontrola korespondencji, kontrola operacyjna i wykaz połączeń

Aktualnie obowiązujące przepisy rozróżniają takie pojęcia jak: korespondencja i przesyłka, kontrola i utrwalanie treści rozmów telefonicznych, kontrola operacyjna, wykaz połączeń. Z każdym z tych pojęć związana jest różna regulacja prawna dotyczącą możliwości zapoznania się przez organy władzy państwowej z treścią informacji przekazywanej w jeden ze wskazanych sposobów komunikowania się. Tylko część tej regulacji zawarta jest w *Kodeksie postępowania karnego*, zdecydowana większość zaś – w przepisach innych ustaw.

Zawartość semantyczna pojęcia korespondencja i przesyłka wynika z definicji legalnej zawartej w *Prawie pocztowym*, zgodnie z którą przesyłka to *rzeczy opatrzone adresem, przedłożone do przyjęcia lub przyjęte przez operatora w celu przemieszczenia i doręczenia adresatowi*[4].

Pojęcie kontroli i utrwalania treści rozmów telefonicznych jest tożsame, w myśl art. 237 kpk, z pojęciem podsłuch, które w tym przypadku

[3] Art. 10 *Konwencji*.
[4] *Ustawa z dnia 12 czerwca 2003 r. Prawo pocztowe* (Dz.U. z 2003 r., Nr 130, poz. 1188 z późn. zm.).

jest pojęciem procesowym. Przepis tego artykułu nie może, i faktycznie nie stanowi, prawnej podstawy do stosowania podsłuchu pozaprocesowego[5]. Procesowa kontrola oraz utrwalanie przy użyciu środków technicznych treści innych rozmów lub przekazów informacji, w tym korespondencji przesyłanej pocztą elektroniczną, uregulowana została w art. 241 kpk. Warto przy tym zauważyć, że Sąd Najwyższy w uchwale z 21 marca 2001 r. uznał, że określenie treści przekazów innych niż rozmowy telefoniczne oznacza *nie mające charakteru rozmowy telefonicznej przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej, tj. przez przewody, systemy radiowe, optyczne lub jakiekolwiek inne urządzenia wykorzystujące energię elektromagnetyczną*[6].

Kontrola operacyjna, rozumiana także jako podsłuchiwanie treści rozmów i przekazów utrwalanych na odpowiednich nośnikach, została unormowana – zgodnie z wymogami konstytucyjnymi – w ustawach regulujących funkcjonowanie odpowiedniej służby stosującej ten sposób pozyskiwania informacji. W poszczególnych ustawach wskazane zostały prawne przesłanki dopuszczalności stosowania podsłuchu, przy czym zawsze muszą się one mieścić w zakresie kompetencyjnym danej służby, a nadto spełniać zasadę subsydiarności wyrażającą się w stwierdzeniu, że inne formy pracy operacyjnej są lub mogą być bezskuteczne.

Każda ze służb uprawnionych do stosowania podsłuchów (tj. Policja, Straż Graniczna, Agencja Bezpieczeństwa Wewnętrznego, Centralne Biuro Antykorupcyjne, Kontrola Skarbowa, Służba Kontrwywiadu Wojskowego, Żandarmeria Wojskowa) ma inny katalog przestępstw, w których ściganiu dopuszczalne jest stosowanie kontroli operacyjnej[7].

Wspólną dla wszystkich służb stosujących podsłuch formą pracy operacyjnej jest, podobnie jak w przypadku podsłuchu procesowego, sądowa kontrola podejmowanych działań, która wyraża się w wydaniu stosownego postanowienia przez sąd okręgowy, po uprzednim uzyskaniu zgody właściwego prokuratora[8].

---

[5] Zob. Komentarz do art. 237 kpk (Dz.U. z 1997 r., Nr 89, poz. 555), w: J. Grajewski, L. K. Paprzycki, S. Steinborn, *Kodeks postępowania karnego. Komentarz*, tom I (art. 1 - 424), LEX 2010, wyd. II.

[6] Uchwała SN z 21 marca 2001 r. o sygn. I KZP 60/99, OSNKW 2000, nr 3 - 4, poz. 26.

[7] Obecnie dochodzi do sytuacji wręcz paradoksalnych w tym zakresie. Przykładowo można wskazać postanowienie Sądu Apelacyjnego w Warszawie z 18.05.2007 r., II AKz 288/07, które dotyczy korzystania w postępowaniu karnym z dowodów zebranych przez CBA podczas stosowania kontroli operacyjnej. Służba ta ujawniła okoliczności popełnienia zbrodni zabójstwa, którego to przestępstwa nie ma w katalogu przestępstw ściganych przez tę służbę. Sąd Apelacyjny w orzeczeniu stwierdził wprost: *Uzyskane w trybie niejawnym przez CBA materiały nie mogą stanowić dowodu w sprawie o zabójstwo. Ustawa o CBA wprowadza prawo korzystania z dowodów uzyskanych przez Centralne Biuro Antykorupcyjne w trybie art. 17 ust. 1 ustawy w sprawach wskazanych w zamkniętym katalogu przestępstw wymienionych w art. 17 ust. 1 pkt pkt 1 i 2 tej ustawy. Przepisy te nie wymieniają zbrodni zabójstwa, ani nieumyślnego spowodowania śmierci. Sprawia to, że uzyskane w tym trybie dowody nie mogą być podstawą ustaleń, jako zgromadzone w sposób sprzeczny z prawem, a tym samym nielegalne.*

[8] Na temat prawnych podstaw dopuszczalności stosowania kontroli operacyjnej szerzej zobacz m.in. w: L. Paprzycki, Z. Rau (red.), *Praktyczne elementy zwalczania przestępczości zorganizowanej i terroryzmu*, A. Biernaczyk, *Zarys problematyki czynności operacyjnych realizowanych w trybie art. 19, 19a i 19b ustawy z dnia 6 kwietnia 1990 r. o Policji*; J. Kudła, *Wybrana problematyka czynności operacyjnych na tle uwag de lege ferenda projektu ustawy o czynnościach operacyjno-rozpoznawczych*, K. Olejnik, *Zakres stosowania czynności operacyjnych (...)*; A. Taracha, *Czynności operacyjno-rozpoznawcze – aspekty kryminalistyczne i prawno-porównawcze*, czy inne publikacje, szczególnie Jacka Kudły.

Ani w *Kodeksie postępowania karnego*, ani w ustawach regulujących funkcjonowanie służb uprawnionych do prowadzenia pracy operacyjnej nie ma zdefiniowanego pojęcia bilingu, które potocznie rozumiane jest jako wykaz połączeń. Legalnej definicji tego terminu nie można również znaleźć w *Prawie telekomunikacyjnym*[9].

W próbie zdefiniowania terminu b i l i n g pomocny może być jedynie tzw. słowniczek zawarty w art. 2 *Prawa telekomunikacyjnego*. Artykuł ten definiuje m.in. dwa interesujące z tego punktu widzenia podobne pojęcia, tj. p o ł ą c z e n i e i p o ł ą c z e n i e t e l e f o n i c z n e. Pierwszy z tych terminów (połączenie) definiowane jest jako: *fizyczne lub logiczne połączenie telekomunikacyjnych urządzeń końcowych pozwalające na przesłanie przekazów telekomunikacyjnych*, drugie zaś (połączenie telefoniczne) jako *połączenie ustanowione za pomocą publicznie dostępnej usługi telefonicznej, pozwalające na dwukierunkową łączność w czasie rzeczywistym.*

Ważna z tego punktu widzenia jest także treść art. 80 wyżej wymienionej ustawy, gdyż zgodnie z ust. 1 tego artykułu: *Dostawca publicznie dostępnych usług telekomunikacyjnych dostarcza abonentowi nieodpłatnie z każdą fakturą podstawowy wykaz wykonanych usług telekomunikacyjnych zawierający informację o zrealizowanych płatnych połączeniach z podaniem, dla każdego typu połączeń, liczby jednostek rozliczeniowych odpowiadającej wartości zrealizowanych przez abonenta połączeń.*

Z cytowanych przepisów wynika zatem, że pojęcie b i l i n g musi być rozumiane jako wykaz wykonanych połączeń telefonicznych. Na operatorów sieci telefonicznych został przez ustawodawcę nałożony szereg obowiązków istotnych z punktu widzenia obronności i szeroko rozumianego bezpieczeństwa państwa. Obowiązki te wynikają wprost z treści ustawowych przepisów. W tym miejscu można jedynie zaznaczyć, że operator został zobowiązany przez *Prawo telekomunikacyjne* (na własny koszt) między innymi do:

- niezwłocznego blokowania na żądanie uprawnionych podmiotów połączeń telekomunikacyjnych lub przekazów informacji, jeżeli połączenia te mogą zagrażać obronności, bezpieczeństwu państwa oraz bezpieczeństwu i porządkowi publicznemu,
- przechowywania przez okres 24 miesięcy danych generowanych w sieci telekomunikacyjnej lub przez nich przetwarzanych, licząc od dnia połączenia lub nieudanej próby połączenia,
- udostępniania danych uprawnionym podmiotom, a także sądowi i prokuratorowi, na zasadach i w trybie określonym w odrębnych przepisach.

Zgodnie z ustawą obowiązkiem gromadzenia i przechowywania objęte są dane niezbędne do:

1) ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego i użytkownika końcowego:
   a) inicjującego połączenie,
   b) do którego kierowane jest połączenie;
2) określenia:
   a) daty i godziny połączenia oraz czasu jego trwania,
   b) rodzaju połączenia,
   c) lokalizacji telekomunikacyjnego urządzenia końcowego.

Korzystając z przyznanej w art. 180c ust. 2 ustawy *Prawo telekomunikacyjne* delegacji ustawowej, minister infrastruktury wydał *Rozporządzenie z dnia 28 grudnia 2009 r. w sprawie szczegółowego wykazu danych oraz rodzajów operatorów publicznej*

[9] *Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne*, Dz.U. z 2004 r., Nr 171, poz. 1800 z późn. zm.

sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do ich zatrzymywania i przechowywania[10]. W rozporządzeniu tym przyjęto między innymi[11], że danymi niezbędnymi do ustalenia w ruchomej publicznej sieci telekomunikacyjnej, a więc w sieciach telefonii komórkowej, są dane dotyczące:

- numeru MSISDN użytkownika końcowego, inicjującego połączenie i do którego połączenie jest kierowane,
- imienia i nazwiska albo nazwy oraz adresu użytkowników końcowych,
- numerów IMSI użytkowników końcowych,
- pierwszych 14 cyfr numeru IMEI albo numeru ESN telekomunikacyjnego urządzenia końcowego,
- daty i godziny pierwszego zalogowania telekomunikacyjnego urządzenia końcowego do ruchomej publicznej sieci telefonicznej, zgodnie z czasem lokalnym, oraz współrzędnych geograficznych lokalizacji stacji BTS,
- daty i godziny połączenia (lub jego próby) oraz czasu jego trwania z dokładnością do 1 sekundy,
- lokalizacji telekomunikacyjnego urządzenia końcowego poprzez identyfikator anteny stacji BTS.

W przypadku stacji bazowych dane identyfikujące anteny stacji BTS obejmować muszą, zgodnie z tym rozporządzeniem, nie tylko współrzędne geograficzne tej stacji, ale także azymut, wiązkę i zasięg roboczy tego typu anteny. W konsekwencji dane te pozwalają na bardzo dużą dokładność ustalenia miejsca pobytu użytkownika telefonu komórkowego zarówno wykonującego, jak i odbierającego połączenie telefoniczne.

Wynikające z omawianych przepisów obowiązki wskazane zostały również w postanowieniu Sądu Najwyższego z dnia 25 marca 2010 r., w sprawie o sygn. I KZP 37/09. W postanowieniu tym Sąd stwierdził, że: *Przepis art. 180a ust. 1 pkt 2 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. z 2004 r., Nr 171, poz. 1800 ze zm.) nakłada na operatorów publicznej sieci telekomunikacyjnej oraz dostawców ogólnie dostępnych usług telekomunikacyjnych obowiązek udostępniania, to jest wyszukiwania, tworzenia stosownych zestawień i przesyłania za pomocą sieci telekomunikacyjnej uprawnionym podmiotom, w tym sądowi i prokuratorowi danych, o których mowa w art. 180c ust. 1 ustawy. Tak rozumiane koszty udostępniania tych danych obciążają operatora lub dostawcę* (...)[12].

W świetle obowiązującej i przedstawionej regulacji prawnej, a w szczególności jednoznacznej treści znowelizowanego art. 218 kpk, nie jest konieczne uzyskanie postanowienia sądu na otrzymanie od operatora na potrzeby toczącego się postępowania przygotowawczego wykazu połączeń telefonicznych, czyli tzw. bilingu. W myśl tego przepisu bowiem: *Urzędy, instytucje i podmioty prowadzące działalność w dziedzinie poczty lub działalność telekomunikacyjną, urzędy celne oraz instytucje i przedsiębiorstwa transportowe obowiązane są wydać sądowi lub prokuratorowi, na żądanie zawarte w postanowieniu, korespondencję i przesyłki oraz dane, o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne* (Dz.U. z 2004 r., Nr 171, poz. 1800 z późn. zm.), *jeżeli mają znaczenie dla toczącego się postępowania. Tylko sąd lub prokurator mają prawo je otwierać lub zarządzić ich otwarcie.* Warun-

[10] Dz.U. z 2009 r., Nr 226, poz. 1828.
[11] Zob. załącznik nr 2 do przedmiotowego rozporządzenia.
[12] Zob. System Informacji Prawnej Lex - 564521.

kiem koniecznym otrzymania tych danych jest zatem jedynie wydanie postanowienia przez prokuratora na etapie postępowania przygotowawczego, a przez sąd na etapie postępowania sądowego.

III. Dopuszczalność uzyskiwania, analizowania i gromadzenia wykazu połączeń dla potrzeb pracy operacyjnej

Nadal otwarta pozostaje jednak kwestia, czy dopuszczalne jest uzyskiwanie, analizowanie i gromadzenie bilingów w ramach pracy operacyjnej wykonywanej przez uprawnione do tego służby. Jako punkt wyjścia do dalszych rozważań należy przyjąć, że każdy z uprawnionych podmiotów prowadzących tego typu pracę będzie działał w ramach swoich zadań i ustawowych kompetencji.

1. Ustawa o Policji

Kwestia uzyskiwania bilingów na potrzeby Policji została uregulowana z dniem 6 lipca 2009 r. w art. 20c *Ustawy o Policji* w brzemieniu, co jest ważne, nadanym mu ustawą z dnia 24 kwietnia 2009 r. *o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw* (Dz.U. z 2009 r., Nr 85, poz. 716). Przepis ten wskazuje, że: *W celu zapobiegania lub wykrywania przestępstw Policja może mieć udostępniane dane, o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. z 2004 r., Nr 171, poz. 1800 z późn. zm.), zwane dalej „danymi telekomunikacyjnymi", oraz może je przetwarzać*[13].

Udostępnienie żądanych przez policję danych telekomunikacyjnych następuje nieodpłatnie. Przekazuje się je policjantowi wskazanemu w pisemnym wniosku skierowanym do operatora przez Komendanta Głównego Policji lub komendanta wojewódzkiego Policji albo osobie przez nich upoważnionej.

Przepis ten bardzo ogólnie wskazuje, że udostępnienie bilingów może nastąpić jedynie w celu zapobieżenia lub wykrycia przestępstw, ale już w żaden sposób ich nie wartościuje (nie kataloguje, jak w przypadku kontroli operacyjnej). Możliwe jest zatem żądanie bilingu zarówno w sprawie dotyczącej zabójstwa, jak i kradzieży lub przywłaszczenia mienia ruchomego o wartości nie większej niż 250 złotych. Policja nie ma jedynie możliwości występowania z tego typu żądaniem w sprawach o wykroczenia.

Ważne jest przy tym, że materiały uzyskane od operatora w postaci bilingów i ich analiza (jako forma ich przetworzenia), w sytuacji gdy zawierają informacje mające znaczenie dla postępowania karnego, przekazywane są właściwemu miejscowo i rzeczowo prokuratorowi do prowadzonego postępowania karnego. Nie ma zatem potrzeby ponownego zwracania się o nie w trybie art. 218 § 1 kpk, co jednak w praktyce bardzo często się zdarza.

Ustawa reguluje również sytuację, gdy uzyskane w ten sposób materiały nie zawierają informacji mających znaczenie dla postępowania karnego. Podlegają one wówczas niezwłocznemu zniszczeniu komisyjnemu i protokolarnemu, przy czym w ustawie brak definicji tego terminu i określenia, jak należy go rozumieć. Nie można nawet w sposób wiążący w tym przypadku powołać się, stosując analogię, na dwumiesięczny termin z art. 19 ust. 17, to jest na sytuację, gdy w wyniku stosowania kontroli operacyjnej nie uzyskano materiału pozwalającego na wszczęcie postępowa-

[13] *Ustawa z dnia 6 kwietnia 1990 r. o Policji*; tekst jednolity – Dz.U. z 2007 r., Nr 43, poz. 277 z późn. zm.

nia karnego, gdyż termin tam określony, jak i cały ten przepis, odnosi się jedynie do tej kontroli[14].

2. Ustawy o: Straży Granicznej, Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, Centralnym Biurze Antykorupcyjnym i Kontroli Skarbowej

Regulacja prawna, bardzo podobna do tej obowiązującej w przypadku Policji, została nadana nowelizacją *Prawa telekomunikacyjnego* z 2009 r. ustawie o Straży Granicznej, o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu i o Kontroli Skarbowej[15]. Rozwiązanie przyjęte w ustawie powołującej w 2006 r. Centralne Biuro Antykorupcyjne przeniesione zostało w 2009 r. do *Ustawy o ABW oraz AW.*

Pozyskiwanie bilingów, danych BTS, danych personalnych użytkowników inicjujących połączenie i je odbierających zostało uregulowane w:
- art. 10b *Ustawy z dnia 12 października 1990 r. o Straży Granicznej* (tekst jednolity Dz.U.05.234.1997 z późn. zm.),
- art. 28. *Ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (tekst jednolity Dz.U.10.29.154),
- art. 18 *Ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym* (Dz.U.06.104.708 z późn. zm.),
- art. 36b *Ustawy z dnia 28 września 1991 r. o kontroli skarbowej* (tekst jednolity Dz.U.04.8.65 z późn. zm.).

Tożsama regulacja dotycząca uzyskiwania danych od operatora telefonicznego zawarta w Ustawie o Policji, o Straży Granicznej i o Kontroli Skarbowej nieznacznie różni się od regulacji zawartej w ustawach o ABW oraz AW i o CBA. W obu ostatnich ustawach bowiem w sposób nie budzący żadnych wątpliwości wskazano, że: *Obowiązek uzyskania zgody sądu*, o której mowa w art. 27 ust. 1 *Ustawy o ABW oraz AW* i w art. 17 *Ustawy o CBA* (to jest koniecznej dla kontroli operacyjnej), *nie dotyczy informacji niezbędnych do realizacji ich zadań (...) w postaci danych:*
1) *o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. z 2004 r., Nr 171, poz. 1800 z późn. zm.),*
2) *identyfikujących podmiot korzystający z usług pocztowych oraz dotyczących faktu, okoliczności świadczenia usług pocztowych lub korzystania z tych usług.*

IV. Tajemnice prawnie chronione

M. i R. Taradejna w książce pt. *Dostęp do informacji publicznej, a prawna ochrona informacji dotyczących działalności gospodarczej, społecznej i zawodowej oraz życia prywatnego*[16] wskazują na istnienie w polskim systemie ponad 120 różnego rodzaju prawnie (ustawowo) uregulowanych tajemnic. Ich waga dla bezpieczeństwa państwa zależy oczywiście nie od zakresu i obszerności ustawowego uregulowania, ale od tre-

[14] Nie oznacza to oczywiście, że termin dwóch miesięcy nie może być jakimś odnośnikiem realizacji ustawowego obowiązku *niezwłocznego zniszczenia*, które jednak powinno nastąpić wcześniej.

[15] W analizie celowo pominięto *Ustawę z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych*, a także *Ustawę z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego*, gdyż regulacja jest podobna, a praktycznie niespotykana w powszechnych jednostkach prokuratury.

[16] M. i R. Taradejna, *Dostęp do informacji publicznej, a prawna ochrona informacji dotyczących działalności gospodarczej, społecznej i zawodowej oraz życia prywatnego,* Toruń 2003, Adam Marszałek.

ści informacji niejawnych objętych tą tajemnicą. Przykładowo, jako mające największe znaczenie dla pracy operacyjnej organów ścigania, a jednocześnie uregulowane np. w *Ustawie o Policji* (a więc w ustawie regulującej funkcjonowanie tej służby) traktowane są dane objęte tajemnicą pocztową, ubezpieczeniową i bankową. Tajemnica pocztowa uregulowana jest w art. 39 ustawy z dnia 12 czerwca 2003 r. – *Prawo pocztowe* (Dz.U. z 2003 r., Nr 130, poz. 1188 z późn. zm.). Obejmuje ona *informacje przekazywane w przesyłkach, informacje dotyczące realizacji przekazów pocztowych, dane dotyczące podmiotów korzystających z usług pocztowych oraz dane dotyczące faktu i okoliczności świadczenia usług pocztowych lub korzystania z tych usług*[17]. Do zachowania tajemnicy pocztowej zobowiązany jest nie tylko operator pocztowy, czyli podmiot prowadzący działalność gospodarczą polegającą na dostarczaniu przesyłek, ale także każda inna osoba, która z racji wykonywanej działalności uzyskała dostęp do tajemnicy pocztowej.

Ustawa wskazuje także na sytuacje stanowiące naruszenie obowiązku zachowania tajemnicy pocztowej, wymieniając w szczególności jako jej przykłady: ujawnianie lub przetwarzanie informacji albo danych objętych tajemnicą pocztową i otwieranie zamkniętych przesyłek lub zapoznawanie się z ich treścią czy umożliwianie osobom nieuprawnionym działań mających na celu wykonywanie którejkolwiek z tych czynności[18].

Ustawa o Policji w art. 20d reguluje sytuacje legalnego dostępu do danych objętych tajemnicą pocztową. Wskazuje ona, podobnie jak w przypadku danych telekomunikacyjnych, że informacje dotyczące osób korzystających z usług pocztowych oraz dotyczące faktu i okoliczności świadczenia lub korzystania z tych usług mogą być ujawnione Policji i przez nią przetwarzane wyłącznie w celu zapobiegania lub wykrywania przestępstw oraz ich sprawców. Także i w tym przypadku ujawnienie tych danych na potrzeby operacyjne odbywa się na pisemny wniosek skierowany do operatora usług pocztowych przez Komendanta Głównego Policji lub Komendanta Wojewódzkiego lub na żądanie policjanta posiadającego pisemne upoważnienie tych osób.

Policja, a także inne służby, posiadają uprawnienia do niejawnego (ale legalnego) pozyskiwania określonych danych chronionych tajemnicą ubezpieczeniową i bankową, oczywiście po spełnieniu wszystkich ustawowych przesłanek takiej dopuszczalności[19].

Regulacja prawna dotycząca pozyskiwania na potrzeby pracy operacyjnej przez policję (podobnie jak i przez CBA i Straż Graniczną) danych objętych tajemnicą ubezpieczeniową i bankową jest szczególnie ważna z punktu widzenia potrzeby pozyskiwania ewentualnej zgody sądu, gdyż wprost do tej zgody się odnosi[20].

Omawiana ustawa wyraźnie wskazuje, że: *Jeżeli jest to konieczne dla skutecznego zapobieżenia przestępstwom określonym w art. 19 ust. 1 lub ich wykrycia albo ustalenia sprawców i uzyskania dowodów, Policja może korzystać z informacji dotyczących*

[17] Art. 39 ust. 1 *Ustawy z dnia 12 czerwca 2003 r. – Prawo pocztowe* (Dz.U. z 2003 r., Nr 130, poz. 1188 z późn. zm.).

[18] Tamże, ust. 2.

[19] Przesłanki dopuszczalności pozyskiwania informacji objętych tajemnicą ubezpieczeniową i bankową zawarte zostały także w:
- art. 10c *Ustawy o Straży Granicznej*,
- art. 23 *Ustawy o Centralnym Biurze Antykorupcyjnym*.

[20] Szerzej zob.: J. Kudła, A. Staszak, *Praktyczne aspekty tajemnicy bankowej. Przetwarzanie i wykorzystanie informacji zgromadzonych na etapie czynności operacyjno-rozpoznawczych*, w: „Policja" 2010, nr 1 lub strona internetowa Prokuratury Okręgowej w Zielonej Górze: *http://www.zielona-gora.po.gov.pl/esi-admin/upload/lektury_elektroniczne/2-praktyczne-aspekty-tajemnicy-bankowej.pdf*.

umów ubezpieczenia, a w szczególności z przetwarzanych przez zakłady ubezpieczeń danych podmiotów, w tym osób, które zawarły umowę ubezpieczenia, a także przetwarzanych przez banki informacji stanowiących tajemnicę bankową[21].

Informacje te na podstawie postanowienia wydanego na pisemny wniosek Komendanta Głównego Policji albo Komendanta Wojewódzkiego Policji udostępnia sąd okręgowy właściwy miejscowo ze względu na siedzibę organu wnioskującego. Po rozpatrzeniu wniosku sąd, w drodze postanowienia, wyraża zgodę na przekazanie informacji i danych wskazanego podmiotu, określając ich rodzaj i zakres oraz podmiot (konkretnego ubezpieczyciela lub bank) zobowiązany do ich udostępnienia.

Charakter gwarancyjny w zakresie przestrzegania praw i wolności obywatelskich ma przepis art. 20 ust. 10 *Ustawy o Policji*, zgodnie z którym w terminie do 90 dni od dnia przekazania danych objętych tajemnicą ubezpieczeniową i bankową podmiot, którego te dane dotyczyły – a więc konkretny człowiek lub konkretny podmiot gospodarczy – jest informowany przez policję o treści postanowienia sądu, wyrażającego zgodę na udostępnienie tych danych.

Pozornie trudniejsza sytuacja prawna może dotyczyć tajemnic wskazanych w art. 180 kpk, który odnosi się do osób zobowiązanych do zachowania tajemnicy notarialnej, adwokackiej, radcy prawnego, doradcy podatkowego, lekarskiej lub dziennikarskiej. Takie osoby mogą być przesłuchiwane co do faktów objętych tą tajemnicą tylko wtedy, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność (na jaką mają być przesłuchane te osoby) nie może być ustalona na podstawie innego dowodu. Wówczas w trakcie postępowania przygotowawczego konieczna jest decyzja sądu zezwalająca na przesłuchanie i określająca jego przedmiot. Warunkiem procesowego zwolnienia tych osób z tajemnicy jest konieczność przeprowadzenia tego przesłuchania dla dobra wymiaru sprawiedliwości i to pod warunkiem wyczerpania wszelkich innych środków dowodowych odnoszących się do okoliczności mających być ujawnionymi w trakcie przesłuchania[22].

W przypadku tajemnicy dziennikarskiej *zwolnienie dziennikarza od obowiązku zachowania tajemnicy nie może dotyczyć danych umożliwiających identyfikację autora materiału prasowego, listu do redakcji lub innego materiału o tym charakterze, jak również identyfikację osób udzielających informacji opublikowanych lub przekazanych do opublikowania, jeżeli osoby te zastrzegły nieujawnianie powyższych danych*[23].

Pojęcie t a j e m n i c y d z i e n n i k a r s k i e j zostało jednak sformułowane nie w przepisach kpk, ale w *Ustawie z dnia 26 stycznia 1984 r. – Prawo prasowe*[24], a dokładnie w art. 15 tej ustawy. Tajemnica ta dotyczy danych umożliwiających identyfikację:

1. Autora materiału prasowego,
2. Listu do redakcji lub innego materiału o tym charakterze,
3. Innych osób udzielających informacji opublikowanych albo przekazanych do opublikowania,

[21] Art. 20c ust. 3 *Ustawy o Policji*.

[22] J. Grajewski, L. Paprzycki, S. Steinborn, *Komentarz do art.180 kodeksu postępowania karnego* (Dz.U. z 1997 r., Nr 89, poz. 555), w: J. Grajewski, L. K. Paprzycki, S. Steinborn, *Kodeks postępowania karnego. Komentarz*, tom I (art. 1 - 424), wyd. II, LEX 2010.

[23] Art. 180 § 3 kpk.

[24] Dz.U. z 1984 r., Nr 5, poz. 24 z późn. zm.

4. Wszelkich informacji, których ujawnienie mogłoby naruszać chronione prawem interesy osób trzecich.

Anonimizacja autora materiału prasowego, listu do redakcji lub innego materiału o tym charakterze, a także osób udzielających informacji opublikowanych albo przekazanych do opublikowania może nastąpić tylko wtedy, gdy osoby te zastrzegły nieujawnianie powyższych danych. Jest to zatem warunek sine qua non objęcia danych personalnych tych osób ochroną.

Obowiązek przestrzegania tajemnicy dziennikarskiej dotyczy wszystkich osób zatrudnionych w redakcjach, wydawnictwach prasowych i innych prasowych jednostkach organizacyjnych, które z racji wykonywanej pracy zapoznały się z treścią podlegających tej ochronie danych[25]. Punktem wyjścia do określenia zakresu tajemnicy dziennikarskiej jest jednak treść art. 15 *Prawa prasowego* w kontekście art. 7 tejże ustawy. Wymaga to szczególnego podkreślenia, gdyż art. 15 stwierdza, że dziennikarzowi przysługuje prawo zobowiązujące do zachowania tajemnicy dziennikarskiej tylko jako *autorowi materiału prasowego*, a nie w związku z wykonywanym zawodem. W art. 7 zaś zawarta jest definicja legalna materiału prasowego. Przepis ten stwierdza, że: *Materiałem prasowym jest każdy opublikowany lub przekazany do opublikowania w prasie tekst albo obraz o charakterze informacyjnym, publicystycznym, dokumentalnym lub innym, niezależnie od środków przekazu, rodzaju, formy, przeznaczenia czy autorstwa*[26].

W konsekwencji można powiedzieć, że art. 7 *Prawa prasowego* w sposób istotny zawęża przedmiot i zakres tajemnicy dziennikarskiej. Obecnie jednak próbuje się nadać tej tajemnicy bardziej pojemny charakter, szczególnie w środowiskach reprezentujących dziennikarzy, a więc żywotnie zainteresowanych maksymalnym rozszerzeniem jej stosowania. Warto jednak zwrócić uwagę na to, że definiowanie pojęcia t a j e m n i c a d z i e n n i k a r s k a jedynie przez pryzmat art. 15, w oderwaniu od kontekstu innych przepisów (choćby tylko tej jednej ustawy) powoduje, że mamy do czynienia z zakresem wręcz wykraczającym poza dopuszczalne ramy prawne. O znaczeniu praktycznym tego zawężonego zakresu pojęcia t a j e m n i c y d z i e n n i k a r s k i e j może świadczyć to, że również dziennikarze dopuszczają się popełniania przestępstw, nawet bardzo poważnych. Ograniczenie możliwości dowodowych w zakresie analizy bilingów z tego powodu, że sprawcą poważnego przestępstwa jest dziennikarz, prowadzi do wypaczenia powagi wymiaru sprawiedliwości, czyniąc określoną grupę zawodową niemal bezkarną.

Prawo prasowe nie zawiera norm pozwalających na uchylenie tajemnicy dziennikarskiej. Zawiera je natomiast przepis art. 180 § 3 kpk, który *stanowi lex specialis w stosunku do art. 15 ust. 2 ustawy z 26 stycznia 1984 r. - Prawo prasowe, Dz. U. Nr 5, poz. 24 z późn. zm. (SN I KZP 15/94, OSNKW 1995, nr 1 - 2, poz. 1* [27] i daje częściowo taką możliwość.

W uzasadnieniu tego orzeczenia SN wskazał, iż *generalny charakter regulacji zawartej w art. 15 prawa prasowego. wynika z ustanowienia w nim zarówno przedmiotu, jak i zakresu tajemnicy zawodowej obejmującej wszystkich dziennikarzy.* (...) *Natomiast*

[25] Zob. E. Ferenc-Szydełko, *Komentarz do art. 15 ustawy z dnia 26 stycznia 1984 r. Prawo prasowe*, (Dz.U. z 1984 r., Nr 5, poz. 24), Oficyna 2010, LEX, wyd. III.

[26] Art. 7 ust. 2 pkt 4 *Prawa prasowego.*

[27] J. Grajewski, L. Paprzycki, S. Steinborn, *Komentarz do art. 180...*, s. 448; podobnie J. Sobczak, *Komentarz do art.15 ustawy z dnia 26 stycznia 1984 r. – Prawo prasowe* (Dz.U. z 1984 r., Nr 5, poz. 24), LEX 2008.

regulacja art. 163 d. kpk dotyczy jedynie sytuacji wycinkowej obejmującej kwestię składania zeznań w procesie karnym i uwarunkowanej ponadto zwolnieniem przez określony organ od obowiązku zachowania tajemnicy. Stanowisko Sądu Najwyższego spotkało się zarówno z krytyką (Z. Gostyński), jak i z pełną aprobatą glosujących to orzeczenie (E. Łętowska i J. Łętowski oraz M. Filar)[28].

Orzeczenie to jest o tyle ważne, że wskazuje na to, iż zakaz dowodowy sformułowany w dyspozycji art. 180 § 2 kpk w zw. z art. 15 *Prawa prasowego* nie ma charakteru bezwzględnego, a nadto możliwa jest interpretacja tych przepisów według ogólnie przyjętych zasad wykładni. Warto wspomnieć również, że zgodnie z art. 12 tegoż *Prawa* dziennikarz obowiązany jest zachować szczególną staranność i rzetelność przy zbieraniu i wykorzystywaniu materiałów prasowych. Powinien w szczególności sprawdzić zgodność z prawdą uzyskanych wiadomości lub podać ich źródło, chronić dobra osobiste, a ponadto interesy działających w dobrej wierze informatorów i innych osób, które okazują mu zaufanie. Od obowiązku zachowania tajemnicy notarialnej, adwokackiej, radcowskiej, lekarskiej i dziennikarskiej może bowiem zwolnić jedynie sąd, po spełnieniu odpowiednich przesłanek.

W literaturze przedmiotu można znaleźć informację, że co najmniej od 2004 r. żywy był w doktrynie spór o to, czy istnieje bezwzględny zakaz stosowania podsłuchu rozmów telefonicznych i kontroli przekazów e-mailowych dziennikarzy i innych osób wymienionych w art. 180 § 2 kpk. Tak zdefiniowany problem może być kontrowersyjny nadal.

Przeciwko możliwości stosowania podsłuchu (procesowego lub w formie kontroli operacyjnej), a także samej możliwości żądania bilingów dziennikarza wypowiedzieli się W. Gontarski i J. Sobczak. Gontarski stwierdził nawet, że *prokurator nie ma prawa żądać bilingu rozmów dziennikarza ani od niego, ani od operatora, gdyż postępowanie takie stanowi przestępstwo nadużycia władzy prokuratorskiej. Wyjątkowo z takim żądaniem mógłby wystąpić dopiero po zwolnieniu dziennikarza z obowiązku zachowania tajemnicy przez sąd, ale jedynie w przypadku, gdy chodzi o informacje, których przedmiotem są najcięższe przestępstwa* (zob. W. Gontarski, *Prokurator nadużywa władzy*, „Rzeczpospolita" z dnia 13 grudnia 2004 r.)[29].

Zdaniem A. Bajończyka, R. Stefańskiego i G. Musialik natomiast istnieje prawna możliwość żądania bilingów, a nawet stosowania podsłuchu, gdyż nigdy nie można z całą pewnością przewidzieć, jakie informacje zostaną uzyskane dzięki uruchomieniu kontroli rozmów telefonicznych dziennikarza, a tym bardziej, czy będą one objęte tajemnicą dziennikarską, która w dużej mierze zależna jest od woli osoby udzielającej informacji lub od autora listu do redakcji. Bajończyk dowodzi dalej, iż w zasadzie na żądanie prokuratora czy sądu operator musi wydać biling, jeżeli ma on znaczenie dla toczącego się postępowania, ponieważ art. 218 § 1 kpk nie przewiduje żadnych ograniczeń w tym zakresie[30].

Podobne stanowisko prezentuje J. A. Śliwa, który uważa, że *wykaz rozmów prowadzonych z telefonu używanego przez dziennikarza nie jest objęty tajemnicą dziennikarską* (...). *W związku z tym wykaz nie może być wystarczającym dowodem na przeka-*

[28] J. Sobczak, *Komentarz do art.15 ustawy z dnia 26 stycznia 1984 r. – Prawo prasowe* (Dz.U. z 1984 r., Nr 5, poz. 24), LEX 2008.

[29] Tamże.

[30] Tamże.

zanie określonych informacji, chroniony jest natomiast tajemnicą telekomunikacyjną, podobnie jak relacja między organem procesowym a operatorem[31].

Stanowisku wskazującemu na dopuszczalność żądania i analizowania bilingów osób, co do których potencjalnie konieczne jest uzyskanie zwolnienia z zachowania tajemnicy i zgoda sądu, nie przeczy często przywoływane orzeczenie Sądu Najwyższego z 22 listopada 2002 r. W uchwale tej SN stwierdził, że: *Sformułowany w art. 180 § 3 k.p.k. zakaz zwalniania dziennikarza od obowiązku zachowania w tajemnicy danych umożliwiających identyfikację autora materiału prasowego, listu do redakcji lub innego materiału o tym charakterze, jak również identyfikację osób udzielających informacji opublikowanych lub przekazanych do opublikowania, jeżeli osoby te zastrzegły nieujawnianie tych danych - konkretyzuje treść tajemnicy dziennikarskiej określonej w art. 15 ustawy z 26 stycznia 1984 r. – Prawo prasowe. Zakaz ten ma charakter bezwzględny i nie może być naruszany poprzez zastosowanie art. 2 § 1 pkt 1 k.p.k. i art. 9 k.p.k.*[32]. Zakaz ten bowiem odnosi się do poprawnie zdefiniowanej tajemnicy dziennikarskiej, a nie do osoby wykonującej zawód dziennikarza.

V. Analiza aktualnego stanu prawnego

Jako wystarczającą podstawę do żądania bilingu na etapie postępowania przygotowawczego (przez prokuratora) należy wskazać treść art. 218 kpk.

W przypadku uzyskiwania, gromadzenia i przetwarzania (a więc i analizowania) danych telekomunikacyjnych oraz pozyskiwania tych danych w ramach niejawnej pracy operacyjnej danej służby taką samoistną podstawę prawną stanowić będą, jako *lex specialis,* przepisy art. 10b *Ustawy z dnia 12 października 1990 r. o Straży Granicznej,* art. 28 *Ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu,* art. 18 *Ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym* czy art. 36b *Ustawy z dnia 28 września 1991 r. o kontroli skarbowej.*

Ogólne zasady wykładni, a w szczególności zasada *lex posterior derogat legi priori,* a więc, że pierwszeństwo należy zawsze przypisać prawu ustanowionemu później, jednoznacznie wskazują na to, że prym musi wieść prawo ustanowione później dla zwalczania zjawisk patologicznych. Chodzi więc o to, że, przepisy dotyczące możliwości gromadzenia danych telekomunikacyjnych w zakresie pracy operacyjnej zostały wprowadzone w 2009 r., a więc później niż te wprowadzone w okresie, z którego wywodzi się nie tylko prawna definicja tajemnicy dziennikarskiej, ale także chroniąca ją norma art. 180 § 2 i 3 kpk. Przy czym należy wskazać, że przepisy dotyczące prawnej dopuszczalności uzyskiwania danych objętych tajemnicą telekomunikacyjną zostały wprowadzone w celu realizacji fundamentalnego prawa obywateli do bezpiecznego życia[33], wolnego od przemocy. Racjonalny ustawodawca, wprowadzając przepisy pozwalające przykładowo policji żądać danych objętych tajemnicą ubezpieczeniową czy bankową na podstawie postanowienia sądu, mógł, gdyby widział taką potrzebę, objąć kontrolą sądową również dane telekomunikacyjne.

Oczywiste jest też, że ingerencja władzy publicznej w korzystanie z tego prawa nastąpiła na podstawie ustawy i jest konieczna *z uwagi na bezpieczeństwo państwowe,*

[31] Tamże.

[32] Uchwała SN o sygn. I KZP 26/02 z 22 listopada 2002 r. OSNKW 2003/1 - 2/6.

[33] Art. 5 *Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności.*

bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności innych osób[34].

VI. Postulaty *de lege ferenda*

Z orzecznictwa ETPCz dotyczącego prawnej dopuszczalności działań państwa i jego służb policyjnych czy specjalnych wynika, że systemy niejawnej inwigilacji muszą zawierać proceduralne gwarancje skutecznej kontroli działań tych służb, która to powinna być sprawowana przez organy zewnętrzne wobec nich. Jednocześnie zawarte jest tu stwierdzenie o charakterze postulatywnym, że kontrola sądowa jest najlepszą gwarancją niezależności, bezstronności i stosowania właściwych procedur.

Niezależnie od tego, czy działania służb państwowych o charakterze policyjnym, które żądały bilingów dziennikarzy, o ile oczywiście takie sytuacje występowały, były w świetle obowiązujących przepisów dopuszczalne, należy wskazać, że powinny one ulec zmianie. Potrzebna jest bowiem większa niż dotychczas ochrona podstawowych praw i swobód obywatelskich.

Podstawy prowadzenia czynności operacyjnych oraz standardy sądowej kontroli ich zasadności i legalności powinny odnosić się do wszystkich działań operacyjnych i procesowych naruszających prawa obywatelskie, a nie tylko do podsłuchu procesowego czy operacyjnego, jak ma to miejsce w tej chwili. Dokonana właśnie przez sejm zmiana przepisów nie zapewnia jednak sądowej kontroli działań operacyjnych innych niż podsłuch, w tym także jedynie sądowej podstawy żądania bilingów co jak się wydaje, powinno być standardem w demokratycznym państwie.

Streszczenie

Niniejszy artykuł podejmuje aktualną obecnie i żywo dyskutowaną w środkach masowego przekazu kwestię prawnych podstaw żądania bilingów przez organy ścigania, zarówno do celów operacyjnych, jak i procesowych. Jako punkt wyjścia rozważań obrano powszechnie akceptowany standard gwarancji praw człowieka i podstawowych swobód obywatelskich wyrażony w *Konwencji o Ochronie Praw Człowieka i Podstawowych wolności*, orzecznictwie Europejskiego Trybunału Praw Człowieka oraz w normach konstytucyjnych.

Opierając się na wymienionych wyżej przepisach, autor stwierdza, że ingerencja organów władzy państwowej w te prawa jest możliwa tylko wtedy, gdy będą one działały:

- na podstawie ustaw i w ich granicach,
- w sytuacjach koniecznych z uwagi na bezpieczeństwo państwa, bezpieczeństwo publiczne, dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności oraz ochronę praw i wolności innych osób.

Dalej autor definiuje pojęcia: k o n t r o l a k o r e s p o n d e n c j i, k o n t r o l a o p e r a c y j n a i w y k a z p o ł ą c z e ń z uwagi na to, że w ustawach regulujących

[34] Art. 8 Konwencji.

funkcjonowanie odpowiedniej służby stosującej niejawny sposób pozyskiwania informacji, wskazane zostały prawne przesłanki dopuszczalności stosowania niejawnych form pracy operacyjnej. Jednocześnie zwraca uwagę, że przesłanki te muszą mieścić w zakresie kompetencyjnym danej służby oraz spełniać zasadę subsydiarności wyrażającą się w stwierdzeniu, że inne formy pracy operacyjnej są lub mogą być bezskuteczne.

Kolejną kwestią podnoszoną w artykule było zdefiniowanie pojecia b i l i n g, które potocznie rozumiane jest jako wykaz połączeń telefonicznych, a tym samym nie może być utożsamiane z kontrolą operacyjną i posłuchem procesowym. Autor artykułu zauważa, że w świetle obowiązujących przepisów, a w szczególności jednoznacznej treści art. 218 § 1 kpk, nie jest konieczne uzyskanie postanowienia sądu w celu otrzymania od operatora na potrzeby toczącego się postępowania przygotowawczego wykazu połączeń telefonicznych.

Podobnie kwestia uzyskiwania bilingów przez Policję, Agencję Bezpieczeństwa Wewnętrznego, Agencję Wywiadu, Straż Graniczną czy Centralne Biuro Antykorupcyjne została uregulowana między innymi w przepisach znowelizowanej w lipcu 2009 r. ustawy *Prawo telekomunikacyjne*. Udostępnienie żądanych przez te instytucje danych telekomunikacyjnych następuje nieodpłatnie, bez potrzeby uzyskiwania postanowienia sądu, ale jedynie w celu zapobiegania przestępstwom lub wykrywania ich.

Dalej autor analizuje treść i zakres tajemnicy dziennikarskiej przez pryzmat brzmienia art. 15 *Prawa prasowego* w kontekście art. 7 tej ustawy. Artykuł 15 przytoczonej ustawy stwierdza bowiem, że dziennikarzowi przysługuje prawo związane z zachowaniem tajemnicy dziennikarskiej tylko jako *autorowi materiału prasowego*, a nie w związku z wykonywanym zawodem. Artykuł 7 natomiast w sposób istotny zawęża znaczenie i zakres tajemnicy dziennikarskiej tylko do materiału opublikowanego lub przekazanego do publikacji.

W konsekwencji autor niniejszej publikacji stoi na stanowisku, że wykaz rozmów prowadzonych z telefonu używanego przez dziennikarza nie jest objęty tajemnicą dziennikarską. Postuluje jednak (*de lege ferenda*), aby systemy niejawnej inwigilacji podlegały kontroli organów zewnętrznych. Obecnie zaś najlepszą gwarancją niezależności, bezstronności i stosowania właściwych procedur jest kontrola sądowa.

Abstract

The article refers to the widely discussed mater of legal basis for the right to claim telephone billings by law enforcement institutions for both operational purposes and prosecution. The starting point for considerations was the publicly accepted standard for guarantees of human rights and fundamental freedoms expressed in the Convention for the Protection of Human Rights and Fundamental Freedoms, the European Court of Human Rights and constitutional norms.

The interference of state authorities in these rights is possible only if the authorities will act:

- accordingly to and strictly within legal regulations and Acts;
- according to the interests of national security, public safety or national prosperity, protection and prevention, health or morals or the protection of the rights and freedoms of others.

Further on, the author defines the concept: *control of correspondence, operational control, the list of telephone connections*. The laws governing the operation of the

appropriate service using a clandestine method of obtaining information are defined in the legal conditions for admissibility of clandestine forms of operational activity. These conditions have to be included within the statutory competences of the service, and fulfill the subsidiary rule that other forms of operational activity are or may be considered as ineffective.

Another issue raised in the article was to define the term *telephone billing*, which is understood to be a form of a list of phone calls, therefore cannot be identified with the operational control and wiretapping.

The existing legislation, in particular the wording of Article 218 § 1 of the Code of Criminal Procedure, it is not necessary to obtain a court order to request for billing from the operator company within the preparatory proceedings.

The issue of obtaining billings by the Police, the Internal Security Agency, the Foreign Intelligence Agency, the Border Guard or the Central Anticorruption Bureau is regulated, inter alia, by the provisions of the amended in July 2009, the Telecommunications Act. Making available telecommunication data is provided free of charge, without the necessity to obtain a court order, but only if used to prevent or detect crime.

Additionally, the author analyzes the content and scope of journalistic confidentiality contained in the articles of the Press Law. Art 15 states that a journalist has the right associated with the confidentiality of journalism only as the 'author of a press release' not in relation to the profession. Article 7 of the Press Law in fact significantly narrows down the scope and range of confidentiality of journalistic materials only to published or communicated for publication.

Consequently, the author presents the view that a list of phone conversations of a journalist cannot be treated as a part of the journalist confidentiality.

The author suggests (de lege ferenda) that classified surveillance systems should fall under the supervision of external institutions. Judicial control is the best guarantee of independence, impartiality and the use of appropriate procedures.