

Robert Rynkun Werner*

Tajemnica danych telekomunikacyjnych a prawo do obrony

I. Tytułem wstępu

W demokratycznym państwie prawnym działania służb specjalnych, a w szczególności ich działania operacyjne, muszą być poddane ścisłej reglamentacji prawnej, a co za tym idzie, także ścisłej kontroli. Powodem tej reglamentacji, czy też kontroli, jest dążenie do maksymalnego ograniczenia, mogących powstać w trakcie wykonywania tych działań, bezprawnych naruszeń szeregu podstawowych praw człowieka, takich jak, prawo do prywatności, prawo do swobody, jak i tajemnicy komunikowania się, czy też prawo do obrony. Nie kwestionując jednak, co do zasady, konieczności zapewnienia ochrony interesów państwa przez podległe mu służby specjalne, do których w kontekście niniejszego opracowania zaliczam także Policję, nie można jednocześnie nie zauważyć, iż istniejące w tym zakresie regulacje prawne, tworzą całkowicie niespójny system prawa, stwarzający tym samym, realne możliwości wystąpienia nadużyć. Bez wątpienia przyczynić się do tego mogą również, obowiązujące przepisy prawne, a dotyczące tzw. retencji danych telekomunikacyjnych, które nakładają na operatorów telekomunikacyjnych gros obowiązków, nie znajdujących w demokratycznym państwie prawnym, żadnego racjonalnego uzasadnienia. Mało pomocna w tym zakresie jest również regulacja Parlamentu Europejskiego i Rady z 15 marca 2006 roku w postaci Dyrektywy o retencji danych¹, której celem miała być kontrola przesyłek, niejawną rejestracja obrazu i dźwięku, prowokacja, czy w końcu podsłuch telefoniczny, badanie bilingów, jak i poczty elektronicznej, to narzędzia prawne, jak i techniczne, za pomocą których organy państwa, w sposób swobodny zdobywają gros informacji dotyczących życia prywatnego obywateli.

* Robert Rynkun Werner, adwokat, Warszawa, doktorant na Wydziale Prawa i Nauk Społecznych, w Szkole Wyższej Psychologii Społecznej.

¹ Dyrektywa 2006/24/WE 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 zmieniającą dyrektywę 2002/58/WE, Dziennik Urzędowy Unii Europejskiej L 105 z dnia 13.04.2006 r.

Do najczęściej stosowanych przez służby czynności operacyjnych, a jednocześnie wzbudzających największe kontrowersje społeczne, bez wątpienia zaliczyć można stosowanie podsłuchu telefonicznego, zarówno w formie procesowej, jak i pozaprocessowej, oraz praktycznie nieograniczoną, możliwość pozyskiwania bilingów telefonicznych.

Na tle powyższych uprawnień, a wskazanych z uwagi na ograniczone ramy opracowania tylko przykładowo, dochodzi w sposób wręcz oczywisty do konfliktu norm prawnych natury konstytucyjnej. Ta swoista konfrontacja regulacji prawnych sprowadza się do odpowiedzi na podstawowe pytanie, o prawną dopuszczalność samej kontroli i utrwalania, a następnie procesowego wykorzystania treści rozmów telefonicznych, w tym także korespondencji przesyłanej pocztą elektroniczną, jak i pozyskiwania wykazu połączeń – bilingów, w szczególności, w kontekście niniejszego opracowania, osób zobowiązanych do zachowania tajemnicy zawodowej, takich jak adwokat, dziennikarz, czy lekarz.

Problem dopuszczalności ingerencji służb specjalnych w tajemnicę zawodową w szczególności adwokatów i dziennikarzy jest od dawna podnoszony w środkach masowego przekazu, jak i w wypowiedziach samorządu adwokackiego. Uchwałą Prezydium Naczelnej Rady Adwokackiej z listopada 2009 roku², zwrócono uwagę, iż „...szczególne zaniepokojenie środowiska adwokackiego budzi nadużywanie przez służby specjalne środków kontroli operacyjnej, w tym podsłuchów [...]. Szczególne zaś zaniepokojenie budzi stosowanie podsłuchów wobec adwokatów, pełniących funkcję obrońców w sprawach karnych, [...] podczas których obie strony ustalały linię obrony w procesie karnym...”

W ramach obowiązujących reguł prawnych, odnoszących się do tajemnicy zawodowej adwokata, która stanowi jednocześnie tajemnicę obrończą, możliwość podejmowania przez służby specjalne czynności operacyjnych, o których wspomniano powyżej, rodzi szereg wątpliwości co do ich legalności. W konflikcie pozostają bowiem normy zasadnicze dla demokratycznego państwa prawnego. Z jednej strony, prawo do wolności i ochrony tajemnicy komunikowania się (art. 49 Konstytucji), którego materialnoprawnym rozwinięciem są m.in. zapisy ustawy *Prawo telekomunikacyjne*³, w której tajemnica komunikowania się w sieciach telekomunikacyjnych obejmuje dane dotyczące użytkownika, treść indywidualnych komunikatów, dane transmisyjne, dane

² Uchwała Prezydium NRA z 17 stycznia 2009 r., Nr 51/2009, „Palestra” 1–2/2010

³ Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, Dz.U. 2004.171.1800 z późn. zm.

o lokalizacji, które oznaczają dane lokalizacyjne wykraczające poza dane niezbędne do transmisji komunikatu lub wystawienia rachunku, dane o próbach uzyskania połączenia między zakończeniami sieci, w tym próbach nieudanych połączeń (art. 159 ust. 1). Z drugiej zaś strony, prawna, tj. przewidziana ustawą, możliwość ingerencji organów państwa w podstawowe prawa człowieka, w sytuacjach nadzwyczajnych, których celem jest zachowanie szeroko rozumianego bezpieczeństwa publicznego. W tym zakresie, trzymając się w dalszym ciągu regulacji prawa telekomunikacyjnego, można przykładowo wskazać ust. 2 pkt 4 art. 159, który zakazuje zapoznawania się, utrwalania, przechowywania, przekazywania lub inne wykorzystywania treści lub danych objętych tajemnicą telekomunikacyjną przez osoby inne niż nadawca lub odbiorca komunikatu, chyba że będzie to konieczne z innych powodów przewidzianych ustawą lub przepisami odrębnymi. Z wyjątkiem przypadków określonych ustawą, ujawnianie lub przetwarzanie treści albo danych objętych tajemnicą telekomunikacyjną narusza obowiązek zachowania tajemnicy telekomunikacyjnej (ust. 3 art. 159). Bez wątplenia zakazem takim objęte powinny być wszelkie dane telekomunikacyjne, związane z wykonywanym zawodem, przez dziennikarza, lekarza, jak i w interesującym nas zakresie przez adwokata. W szczególności, jeżeli dotyczą realizacji prawa do obrony, na które składa się m.in. prawo do zachowania tajemnicy obrończej.

Konstytucyjne prawo do obrony uznawane jest za fundament procesu karnego jak i demokratycznego państwa prawnego. Art. 42. ust. 2 Konstytucji RP⁴, określa to prawo w dwojaki sposób. Po pierwsze, jako prawo w znaczeniu materialnym, czyli prawo oskarżonego (a także podejrzanego) do podejmowania faktycznych czynności obrony w postępowaniu karnym, w szczególności w postaci np. osobistego inicjowania działań natury dowodowej, czy też osobistego uczestnictwa w czynnościach procesowych, przeprowadzanych przez organy wymiaru sprawiedliwości⁵. Po drugie zaś, obrony w znaczeniu formalnym, czyli jako prawa do skorzystanie z pomocy obrońcy z wyboru lub z urzędu, którą co do zasady, w postępowaniu karnym, pełnić może jedynie osoba uprawniona do obrony według przepisów o ustroju adwokatury, czyli adwokat i aplikant adwokacki (art. 82 k.p.k.). W tym miejscu należy zwrócić uwagę,

⁴ Konstytucja RP ustawa z dnia 2 kwietnia 1997 r. Dz.U. Nr 78, poz. 483, art. 42 ust. 2. "Każdy, przeciw komu prowadzone jest postępowanie karne, ma prawo do obrony we wszystkich stadiach postępowania. Może on w szczególności wybrać obrońcę lub na zasadach określonych w ustawie korzystać z obrońcy z urzędu".

⁵ Patrz orzeczenie TK z dnia 17 lutego 2004 r., SK 39/02, OTK-A 2004 Nr 2, poz. 7, Wyrok SN z 4 lutego 2003 r., IV KK 379/02,

iż uprawnienie aplikanta adwokackiego, do wykonywania funkcji obrońcy, spełnia przesłanki ustawowe, pod warunkiem posiadania stosowanego upoważnienia adwokata,⁶ w oparciu o art. 77 ustawy *Prawo o adwokaturze*⁷. Na gruncie przepisów procedury karnej, konstytucyjną zasadę prawa do obrony realizuje art. 6 k.p.k., którego treść stanowi, iż oskarżonemu przysługuje prawo do obrony, w tym prawo do korzystania z pomocy obrońcy, o czym należy go pouczyć. Przedmiotowy zapis jest praktycznie tożsamy z konstytucyjną gwarancją prawa do obrony, którą określa w tym zakresie wspomniany powyżej art. 42 ust. 2 Konstytucji. Na gruncie standardów europejskich, podobne uregulowania, w zakresie podstawowych gwarancji procesowych oskarżonego, zawiera Europejska Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności⁸, jak i Międzynarodowy Pakt Praw Obywatelskich i Politycznych⁹. W myśl tych regulacji prawo do obrony jest jednym ze standardów rzetelnego procesu sądowego, do których przestrzegania zobowiązane jest każde z państw sygnatariuszy konwencji. W kontekście niniejszej publikacji zasadnicze znaczenie mieć będzie prawo do obrony w znaczeniu formalnym, a więc prawo do swobodnego, niczym nie skrzepowanego kontaktu klienta z adwokatem, a co się dalej z tym wiąże, również z prawem do swobodnego przepływu informacji na linii obrońca klient, ale również klient obrońca. Trudno wyobrazić sobie w demokratycznym państwie prawnym, kontakt adwokata z klientem, który pozbawiony byłby pełnej swobody i zarazem ochrony, przed ingerencją osób trzecich. Wynika to nie tylko z istoty tajemnicy adwokackiej, w tym konstytucyjnej gwarancji prawa do obrony, ale również z konstytucyjnej ochrony prawa do tajemnicy i wolności komunikacji. W myśl art. 49 Konstytucji RP „Zapewnia się wolność i ochronę tajemnicy komunikowania się. Ich ograniczenie może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej określony.” Oznacza to, iż każdy obywatel ma prawo do wolności komunikowania się oraz zapewniona jest mu, co do zasady, ochrona tajemnicy informacji.

Podobnie art. 8 ust. 1 EKPCz, który wskazuje, iż każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji. Według ust. 2 tegoż artykułu, niedopuszczalna jest ingerencja

⁶ Postanowienie SN z dnia 26 października 2011 roku, I KZP 12/11.

⁷ Ustawa.

⁸ Dz.U. 1993 r., Nr 61, poz. 284 ze zm., dokładnie chodzi o art. 6 ust. 3 lit. b, czyli prawo do posiadania odpowiedniego czasu i możliwości do przygotowania obrony, jak i ust. 3 lit. c, czyli prawo do bronięcia się osobiście lub przez ustanowionego adwokata.

⁹ Dz.U. 1977 r., Nr 38, poz.167; dokładanie chodzi o art. 14 ust. 3, który zapewnia szereg gwarancji procesowych w tym prawo do obrony.

władzy publicznej w korzystanie z tego prawa, z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie w szczególności z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne, ochronę porządku i zapobiegania przestępstwom lub ochronę praw i wolności innych osób. Oznacza to, iż powyższe prawa, a więc prawo do prywatności, wolności komunikowania się i zachowania jej tajemnicy, nie mają charakteru bezwzględnego, i na mocy stosownych przepisów ustawy, o czym dalej, mogą być w znacznym stopniu ograniczane. Przy czym, ustawodawca dopuszczając możliwość ograniczenia praw i wolności konstytucyjnych, ma jednocześnie obowiązek przestrzegania odpowiednich reguł, w szczególności zachowania przy tym zasad proporcjonalności, zgodnie z ogólną dyspozycją art. 31 ust. 3 Konstytucji. Ograniczenia te muszą być równocześnie wprowadzane tylko w formie ustawy, dodatkowo ustawy, która w jasny sposób, sprecyzuje konkretne zapisy, dotyczące m.in. kategorii spraw – przestępstw, osób, czy też celu ochrony, odnośnie których możliwa jest ingerencja państwa w prawa i wolności obywatelskie (art. 51 § 5 w zw. z art. 93 ust. 2 zdanie 2 Konstytucji RP). Równie ważne, jeżeli nie najważniejsze, jest także określenie sposobu kontroli nad tymi działaniami, ze strony niezależnych organów, ale przede wszystkim niezależnego sądu. Szczególne zagrożenie ingerencją w prawa i wolności jednostki dotyczyć może stosowania przez organy ochrony porządku i bezpieczeństwa publicznego tzw. kontroli operacyjnej, czyli pozaprocesowej, polegającej na uzyskiwaniu w sposób niejawni informacji i dowodów oraz ich utrwalaniu. W szczególności zaś, dotyczy to uzyskiwania wykazu połączeń telefonicznych tzw. bilingów oraz podsłuchiwanie i utrwalania rozmów telefonicznych, czy kontroli i utrwalania treści przekazu przesyłanego drogą elektroniczną. Na tej płaszczyźnie dochodzi w sposób zasadniczy do konfliktu pomiędzy prawem do prywatności i autonomii informacyjnej, a interesem (bezpieczeństwem) publicznym w demokratycznym państwie prawnym¹⁰. Konflikt ten, w omawianym zakresie, sprowadza się do braku respektowania przestrzegania tajemnicy zawodowej adwokatów poprzez pozyskiwanie przez stosowne służby, danych objętych zakazami dowodowymi, wprost, czy też niejako przy okazji, przeprowadzania przez nie działań operacyjnych. Przy czym tajemnicę zawodową związaną z wykonywaniem zawodu lub funkcją stanowią wiadomości, które zostały uzyskane w związku z wykonywanym zawodem lub pełnioną funkcją¹¹. Każda więc rozmowa adwokata z klientem o sprawie,

¹⁰ Wyrok TK z 12.12.2005 r., sygn. akt K 32/04 – uzasadnienie.

¹¹ J. Sobczak, *Prawo Prasowe – komentarz*, Warszawa 2008.

w trakcie której może dochodzić w szczególności do ustalania linii obrony bądź podejmowanie innych ważkich decyzji przed procesowych, a równie istotnych z punktu widzenia prawa do obrony, powinna być zabezpieczona gwarancją pełnej poufności. A co za tym idzie, powinna być wyłączona od jakiegokolwiek ingerencji ze strony organów państwa.

Czy zatem działania służb specjalnych posiadają cechę legalności, wkraczając w zagwarantowane konstytucyjnie oraz ustawowo, prawo obywatela do obrony, w szczególności, gdy źródłem pozyskanych informacji są działania operacyjne – niejawnie, przeprowadzone wobec adwokata lub/i jego klienta? Aby spróbować odpowiedzieć na tak sformułowane pytanie, w pierwszej kolejności należy określić, od którego momentu możemy mówić o realnym prawie do obrony. Czy jest to data formalnego postawienia zarzutów w postępowaniu przygotowawczym, a więc etap postępowania *in personam*. Co wydaje się być oczywiste. Czy też, o prawie do obrony możemy mówić już od chwili podjęcia przez organy procesowe pierwszych czynności nakierowanych na ściganie danej osoby, jeszcze w fazie prowadzenia postępowania *in rem*. O ile w pierwszym przypadku sytuacja taka nie budzi żadnych wątpliwości, o tyle w drugim, w kontekście wykonywania czynności operacyjnych, mogą się one pojawić. Praktyka organów ścigania jest taka, iż najpierw osobę podejrzewaną, co nie jest tożsame z osobą podejrzaną, przesłuchuje się w charakterze świadka. Jest to oczywiście celowe działanie, które nakierowane jest na uzyskanie szeregu informacji, które w sytuacji podejrzanego mogłyby być chronione prawem do obrony przejawiającym się w np. odmowie składania wyjaśnień. Każdy zaś, kto jako świadek składa zeznania, mające służyć za dowód w postępowaniu sądowym zobowiązany jest mówić prawdę. W przypadku, kiedy zeznania świadka są fałszywe, rodzi to po jego stronie, co do zasady, odpowiedzialność karną (art. 233 § 1 k.k.), oczywiście po wcześniejszym stosownym uprzedzeniu o takiej odpowiedzialności. Świadek ma jednak, co do zasady, ograniczone możliwości w zakresie korzystania z prawa do obrony w porównaniu z podejrzanym, a przejawiające się np. koniecznością mówienia prawdy, czy też brakiem możliwości odmowy udzielenia odpowiedzi na pytania, jak i w ogóle odmowy zeznań, oczywiście poza przypadkami opisanymi w art. 182, 183 i 185 k.p.k. Podejrzanym, w przeciwieństwie do świadka, może więc mówić nawet nieprawdę, jeżeli służy to jego linii obrony. Nie ponosi za to żadnej odpowiedzialności. Nie oznacza to jednak, iż świadek, który jest potencjalnym podejrzanym – sprawcą czynu zabronionego, nie może korzystać z prawa do obrony, już w tym stadium postępowania. Nie popełnia bowiem fałszywych zeznań, kto umyślnie składa nieprawdziwe zeznania dotyczące okoliczności mają-

cych znaczenie dla realizacji jego prawa do obrony¹². Nie ma przy tym znaczenia, uprzedzenie przesłuchiwanej osoby, w trybie art. 183 § 1 k.p.k., o prawie do odmowy udzielania odpowiedzi na zadawane pytania. Tym samym wydaje się być oczywistym, iż faktyczna realizacja prawa do obrony, może nastąpić już od momentu popełnienia czynu zabronionego. W konsekwencji prowadzi to do sytuacji, w której nawiązanie kontaktu z obrońcą, powoduje, iż wszelkie ustalenia związane z daną sprawą, pomiędzy adwokatem, a klientem, powinny korzystać z ochrony, m.in. konstytucyjnej gwarancji prawa do obrony, jak i zakazem dowodowym, o którym mowa w art. 178 k.p.k. Wzmocnieniem przedmiotowego prawa, chociaż lepiej można byłoby powiedzieć jego uzupełnieniem, bądź też realizacją¹³, jest obowiązek leżący po stronie obrońcy, zachowania w tajemnicy wszystkiego, o czym dowiedział się w związku z udzieleniem pomocy prawnej (art.6 Prawa o adw.)¹⁴. Nie bez znaczenia dla samego obrońcy jak i jego klienta, w kwestii dochowania tajemnicy adwokackiej, a więc zawodowej, pozostaje również regulacja § 19 Zbioru Zasad Etyki Adwokackiej i Godności Zawodu¹⁵. Na gruncie procedury karnej gwarancją zachowania w tajemnicy okoliczności związanych z prowadzeniem danej sprawy, zapewniają dodatkowo oprócz wspomnianego już art. 178 k.p.k., tkzw. zakazy dowodowe, o których mowa m.in. w art.171 i 180 k.p.k.. O ile art. 178 k.p.k. wyraża bezwzględny zakaz przesłuchi-

¹² Uchwała SN z 26.04.2007 r., I KZP 4/07, OSNKW 2007, nr 6, poz. 45, z dnia 20.09.2007 r., I KZP 26/07, OSNKW 2007, nr 10, poz. 71, w tym szerokie piśmiennictwo zaprezentowane w uzasadnieniach do przedmiotowych uchwał.

¹³ P. Kardas, „Ochrona tajemnicy obrończej. Kilka uwag o dopuszczalności kontroli i utrwalania treści rozmów oraz przekazów informacji realizowanych przy użyciu środków technicznych pomiędzy obrońcą a mandantem”, „Polska Akademia Umiejętności Czasopismo prawa karnego i nauk penalnych”, Rok XV: 2011, z. 4, s. 8.

¹⁴ Ustawa dnia 26.5.1982 r. Prawo o adwokaturze (tj. Dz.U. z 2009 r., Nr 146, poz. 1188 ze zm.). W myśl natomiast art. 6 ust. 3 tegoż prawa adwokata nie można zwolnić od obowiązku zachowania tajemnicy zawodowej co do faktów, o których dowiedział się udzielając pomocy prawnej lub prowadząc sprawę.

¹⁵ Zbiór Zasad Etyki Adwokackiej i Godności Zawodu (Kodeks Etyki), Uchwałą NRA nr 52/2011 z dnia 19.11.2011 r. – tekst jednolity. Najistotniejszym zapisem przedmiotowego paragrafu jest pkt 3. Tajemnicą objęte są nadto wszystkie wiadomości, notatki i dokumenty dotyczące sprawy uzyskane od klienta oraz innych osób, niezależnie od miejsca, w którym się znajdują. Pkt 5. Adwokat posługujący się w pracy zawodowej komputerem lub innymi środkami elektronicznego utrwalania danych zobowiązany jest stosować oprogramowanie i inne środki zabezpieczające dane przed ich niepowołanym ujawnieniem. 6. Przekazywanie informacji objętych tajemnicą zawodową za pomocą elektronicznych i podobnych środków przekazu wymaga zachowania szczególnej ostrożności i uprzedzenia klienta o ryzyku związanym z zachowaniem poufności przy wykorzystaniu tych środków.

wania jako świadka obrońcy lub adwokata działającego w imieniu zatrzymanego, co do faktów, o których dowiedział się udzielając porady prawnej lub prowadząc sprawę, o tyle dyspozycja art. 180 § 2 k.p.k. może nasuwać pewne wątpliwości. Jak wynika bowiem z brzmienia tego zapisu osoba obowiązana do zachowania tajemnicy adwokackiej może być przesłuchiwana co do faktów objętych tą tajemnicą tylko wtedy, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu. Jak widać, zakaz określony w tej regulacji jest zakazem względnym. Wzmocnieniem pozycji adwokata w tej materii, jest jednak zapis art. 6 Prawa o adw., który wyłącza w sposób bezwzględny możliwość jego przesłuchania w tym zakresie. Na podobnym stanowisku stoi również samorząd adwokacki, który stosowną uchwałą Naczelnej Rady Adwokackiej¹⁶, uznał, iż tajemnica adwokacka ma charakter bezwzględnie obowiązujący, i ani sąd ani prokurator, nie są władni zwolnić adwokata od obowiązku zachowania tej tajemnicy. Do zakazu dowodowego odnosi się również m.in. regulacja art. 225 § 3 k.p.k., dotycząca wykonywania zadań obrońcy, która zakazuje wydania na żądanie oraz w trakcie przeszukania, pism i dokumentów związanych z wykonywaniem funkcji obrońcy, a więc zarówno przez adwokata jak i aplikanta adwokackiego, który złoży w tej kwestii stosowne oświadczenie.

II. Podśluch procesowy

Podśluchem jest uzyskiwanie, a w konsekwencji także i utrwalanie w sposób niejawny, treści rozmów telefonicznych jak i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych, w szczególności dotyczy to korespondencji przesyłanej pocztą elektroniczną. Podstawą prawną do zastosowania podśluchu procesowego jest rozdział 26 k.p.k., znowelizowany ustawą z dnia 4 lutego 2011 roku (dalej ustawa lutowa)¹⁷, dotyczący kontroli i utrwalania rozmów. Zgodnie z art. 237 § 1 k.p.k., zastosowanie przez sąd, na wniosek prokuratora, podśluchu procesowego, dopuszczalne jest jedynie w celu wykrycia i uzyskania dowodów dla toczącego się postępowania lub zapobieżenia popełnieniu nowego przestępstwa. Katalog przestępstw, dla wykrycia których dopuszcza się zastosowanie podśluchu procesowego określa § 3 art. 237 k.p.k. Do zbioru tego należą najpoważniejsze przestępstwa opisane

¹⁶ Uchwałą NRA z dnia 12.12.1993 r., „Palestra” 1994, Nr 1–2, s. 143. Zobacz także Z. Krzemiński, *Prawo o adwokaturze Komentarz*, Warszawa 1998.

¹⁷ Ustawa z dnia 4 lutego 2011 r., Dz.U. 2011.53.273 z dnia 10.03.2011r., o zmianie ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw.

w kodeksie karnym, jak i w innych ustawach¹⁸. W wypadkach nie cierpiących zwłoki kontrolę i utrwalenie treści rozmów telefonicznych może zarządzić prokurator (§ 2 art. 237 k.p.k.). Jednak zobowiązany jest on, w terminie 3 dni od wydania postanowienia w tym zakresie, zwrócić się do sądu z wnioskiem o zatwierdzenie swojego postanowienia. Sąd w terminie 5 dni, na posiedzeniu bez udziału stron, wydaje postanowienie w przedmiocie wniosku prokuratora. W wypadku niezatwierdzenia postanowienia prokuratora, sąd w postanowieniu wydanym w przedmiocie wniosku, zarządza zniszczenie wszystkich utrwalonych zapisów. Jednak prokurator może zaskarżyć przedmiotowe postanowienie, co wstrzymuje jego wykonanie. Tym samym nie wyklucza to prowadzenia kontroli, bez zgody sądu, w dalszym ciągu. Z uwagi na niejawność tej czynności, osoba najbardziej zainteresowana, czyli podsłuchiwany nie może uczestniczyć w posiedzeniu, a tym samym nie może złożyć podobnego zażalenia na pierwszym etapie postępowania. W myśl bowiem art. 239 § 1 k.p.k., w nowym brzmieniu, ogłoszenie postanowienia o kontroli i utrwalaniu rozmów telefonicznych osobie, której ono dotyczy, może być odroczone na czas niezbędny ze względu na dobro sprawy. Przy czym, w postępowaniu przygotowawczym ogłoszenie to może być odroczone, nie później niż do czasu zakończenia tego postępowania (§ 2 art. 239 k.p.k.). Dopiero po zakończeniu tego etapu postępowania, osoba podsłuchiwana może złożyć stosowne zażalenie, domagając się zbadania zasadności oraz legalności kontroli i utrwalania rozmów telefonicznych, jak i innych przekazów informacji w szczególności, korespondencji przesyłanej drogą elektroniczną (art. 241 w zw. 240 k.p.k.). Kontrola i utrwalanie rozmów telefonicznych, ale również na mocy art. 241 k.p.k., innych rozmów lub przekazów informacji, w tym korespondencji przesyłanej pocztą elektroniczną, mogą być wprowadzone najwyżej na okres trzech miesięcy, z możliwością przedłużenia, w szczególnie uzasadnionym wypadku, na okres najwyżej dalszych trzech miesięcy (art. 238 § 1 k.p.k.). Przy czym, należy zauważyć, iż bez zaistnienia „szczególnie uzasadnionego wypadku”, o którym mowa w art. 238 § 1 k.p.k., a który każdorazowo należy wykazać, przedłużenie kontroli i utrwalania rozmów telefonicznych na okres „najwyżej dalszych 3 miesięcy” jest niedopuszczalny¹⁹. Kontrola powinna być zakończona niezwłocznie po ustaniu przyczyn wymienionych w art. 237 § 1–3 k.p.k., najpóźniej jednak z upływem okresu, na który została wprowadzona (art. 238 § 2 k.p.k.). Uzasadnione wątpliwości natury konstytucyjnej, a więc prawnej

¹⁸ Ustawa z dnia 29 lipca 2005 r., o przeciwdziałaniu narkomanii – Dz.U. 2005.179.1485 z późn. zm.

¹⁹ Postanowienie SN z 19 stycznia 2011 r., WZ 53/10, OSNKW nr 3/2011.

dopuszczalności ingerencji w tajemnicę komunikacji pomiędzy adwokatem, a klientem, a która zawiera jednocześnie tajemnicę zawodową, budzi regulacja § 4 art. 237 k.p.k. W myśl bowiem tej regulacji, kontrola i utrwalanie treści rozmów telefonicznych są dopuszczalne w stosunku do osoby podejrzanej, oskarżonego oraz w stosunku do pokrzywdzonego lub innej osoby, z którą może się kontaktować oskarżony, albo która może mieć związek ze sprawcą lub grożącym przestępstwem. Bezspornym jest, że takim zapisem ustawa tworzy otwarty katalog osób wobec których może być stosowany podsłuch, a więc kontrola i zapis treści rozmów telefonicznych. Jak z tego wynika, również wobec adwokata, udzielającego porady prawnej lub prowadzącego już obronę klienta. Brak jest bowiem w ustawie wyłączenia obrońcy, jako podmiotu, wobec którego istniał by formalny zakaz stosowania podsłuchu procesowego. Zasadne jest więc pytanie, mimo wszystko, o dopuszczalność zastosowania, a w konsekwencji procesowego wykorzystania, zapisów takiej kontroli, mającej na celu niejawnie utrwalenie czynności zawodowych adwokata, posługującego się w kontaktach z klientem telefonem lub komputerem. Szczególnie jest to istotne, wobec istniejących w procedurze karnej, ale i ustawie Prawo o adwokaturze, zakazów dowodowych, i braku jakiegokolwiek odniesienia się do tej materii w przepisach rozdziału 26 k.p.k. Wydaje się, iż próba udzielenia odpowiedzi na tak sformułowane pytanie, niekoniecznie będzie prosta. Celem nadrzędnym w tym przypadku, jak i w przypadku czynności operacyjnych nieprocesowych jest bowiem zebranie materiału, który będzie mógł stanowić pełnowartościowy materiał dowodowy w postępowaniu karnym. A tym samym, uzyskanie takiego materiału, który będzie mógł być wykorzystany w procesie, w sprawie o przestępstwo lub przestępstwo skarbowe, w stosunku do którego jest możliwe zarządzenie takiej kontroli (art. 237 § 8 k.p.k.). Przy czym, odnośnie podsłuchu procesowego, wykorzystanie takiego materiału w postępowaniu karnym, możliwe będzie w oparciu o dyspozycję art. 393 § 1 k.p.k. Co jednak zrobić w sytuacji, w której uzyskany materiał dotyczy adwokata, udzielającego porady lub pełniącego rolę obrońcy. Wydaje się iż w takim przypadku, należy jednoznacznie stanąć na stanowisku, iż wówczas zastosowanie mieć będą zakazy dowodowe, o których mowa była powyżej, a tym samym, wystąpi negatywna przesłanka procesowa, wykorzystania w jakikolwiek sposób, tak pozyskanego materiału dowodowego w procesie. W tym miejscu powstaje jednak kolejna wątpliwość, co należy zrobić z tak zabezpieczonym materiałem. W obowiązujących regulacjach rozdziału 26 k.p.k., w kontekście prawa do obrony, jak i zachowania tajemnicy obrończej, dość swobodnie traktuje się konieczność zniszczenia utrwalonych materiałów, które nie mają znaczenia dla

postępowania karnego, a które zawierają informacje będące w zakresie tajemnicy zawodowej adwokata. Dość powiedzieć, iż regulacje te w ogóle nie różnią takiej tajemnicy i cechują się zbyt dużą dozą uznaniowości. W myśl tych regulacji, prokurator, po zakończeniu kontroli, wnosi o zarządzenie zniszczenia wszystkich utrwalonych zapisów, jeżeli w całości nie mają one znaczenia dla postępowania karnego. Sąd orzeka o tym niezwłocznie. Po zakończeniu postępowania przygotowawczego prokurator wnosi o zarządzenie zniszczenia utrwalonych zapisów w części, w jakiej nie mają znaczenia dla postępowania karnego, w którym zarządzono kontrolę i utrwalanie rozmów telefonicznych, oraz nie stanowią dowodu, o którym mowa w art. 237 a k.p.k. Sąd w przedmiocie wniosku orzeka na posiedzeniu, w którym mogą wziąć udział strony (art. 328 § 4 k.p.k.). Z wnioskiem o zarządzenie zniszczenia utrwalonych zapisów, nie wcześniej niż po zakończeniu postępowania przygotowawczego, może wystąpić także osoba wymieniona w art. 237 § 4 k.p.k. (inna osoba). Sąd orzeka w przedmiocie wniosku na posiedzeniu, w którym udział mogą wziąć strony oraz wnioskodawca (art. 238 § 5 k.p.k.).

Kolejnym ważnym zagadnieniem, z punktu widzenia gwarancji prawa do obrony, jest również możliwość wykorzystania utrwalonego podczas kontroli materiału dowodowego, stanowiącego dowód popełnienia przestępstwa wymienionego w art. 237 § 3 k.p.k., którego dopuściła się osoba, wobec której kontrola była stosowana, ale innego niż objęte zarządzeniem kontroli, albo popełnionego przez inną osobę. W takim bowiem przypadku prokurator, w czasie trwania kontroli albo nie później niż w ciągu 2 miesięcy od dnia jej zakończenia może wystąpić do sądu z wnioskiem o wyrażenie zgody na jego wykorzystanie w postępowaniu karnym. Sąd wydaje postanowienie w przedmiocie wniosku w terminie 14 dni na posiedzeniu bez udziału stron (art. 237a k.p.k.). Z powyższych regulacji wynika, iż ustawa dopuszcza tak zwaną zgodę następczą sądu, na wykorzystywanie dowodów pochodzących z kontroli procesowej, ale które wykaczały poza zakres postanowienia sądu, pierwotnie zarządzającego taką kontrolę.

Konkludując powyższe uwagi w zakresie kontroli procesowej, zgodzić się należy z poglądem, iż pomimo faktu, że przepisy rozdziału 26 k.p.k. nie zawierają wprost zakazu stosowania podsłuchu procesowego wobec obrońcy, a tym samym nie chronią tajemnicy adwokackiej, to jednak z uwagi na treść przepisów: art. 178 k.p.k., art. 225 § 3 k.p.k., art. 73 § 1 k.p.k., oraz art. 6 ustawy – Prawo o adwokaturze, proces karny zawiera skuteczne gwarancje prawa do obrony, także w zakresie niedopuszczalności podsłuchu procesowego. Kontrola zaś treści rozmów podejrzanego z obrońcą, poza przypadkami opisanymi

w art. 73 § 2 i 3 k.p.k. – a więc ewentualnego zastrzeżenia przez prokuratora, w terminie do 14 dni, obecności prokuratora bądź osoby przez niego wskazanej, podczas porozumiewania się obrońcy z klientem, jest niedopuszczalna i nielegalna²⁰. Jednocześnie, na marginesie niniejszych rozważań, *de lege ferenda*, należałoby wskazać, iż uprawnienia prokuratora, o którym mowa w art. 73 § 2 i 3 k.p.k., w sposób zasadniczy ingerują, a tym samym ograniczają prawo do obrony i powinny ulec wykreśleniu z polskiej procedury karnej²¹.

III. Podśłuch pozaprocessowy

Podstawy prowadzenia czynności operacyjnych określają przepisy stosownych ustaw regulujących materialnoprawne podstawy funkcjonowanie poszczególnych służb specjalnych. Działania operacyjne w Polsce mogą prowadzić następujące służby:

- Policja – na podstawie art. 19 ustawy²²;
- Agencja Bezpieczeństwa Wewnętrznego – na podstawie art. 27 ustawy²³;
- Służba Kontrwywiadu Wojskowego – na podstawie art. 31 ustawy²⁴;
- Centralne Biuro Antykorupcyjne – na podstawie art. 17 ustawy²⁵;
- Straż Graniczna – na podstawie art. 9e ustawy²⁶;
- Wywiad Skarbowy – na podstawie art. 36c ustawy²⁷;
- Żandarmeria Wojskowa – na podstawie art. 31 ustawy²⁸;

²⁰ P. Kardas, op.cyt., s. 21 oraz z przywołanym tamże uzasadnieniem postanowienia SN z 26 X 2011 r., I KZP 12/11, w którym SN stwierdził, że „obrońca jest też oczywiście poza kręgiem osób, wobec których dopuszcza się kontrolę i utrwalanie rozmów (art. 237 § 4 k.p.k.)”.

²¹ Odmienne w tym zakresie wypowiedział się TK w wyroku z 17 lutego 2004 r., SK 39/02, OTK-A 2004, nr 2, poz. 7.

²² Ustawa z dnia 6 kwietnia 1990 r., o policji, Dz.U. 2011.287.1687, tekst jednolity.

²³ Ustawa z dnia 24 maja 2002 r., o Agencji Bezpieczeństwa Wewnętrznego, Dz.U. Nr 74, poz. 676 z późn. zm.

²⁴ Ustawa z dnia 9 czerwca 2006 r., o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, Dz.U. 2006.104.709, z późn. zm.

²⁵ Ustawa z dnia 9 czerwca 2006 r., o Centralnym Biurze Antykorupcyjnym, Dz.U. 2006.104.708, z późn. zm.

²⁶ Ustawa z dnia 12 października 1990 r., o Straży Granicznej, Dz.U. 2005.234.1997, z późn. zm.

²⁷ Ustawa z dnia 28 września 1991 r., o kontroli skarbowej, Dz.U. 2004.8.65., z późn. zm.

²⁸ Ustawa z dnia 24 sierpnia 2001 r., o Żandarmerii Wojskowej i wojskowych organach porządkowych, Dz.U. 2001.123.1353., z późn. zm.

- Służba Kontrwywiadu Wojskowego i Wywiadu Wojskowego – na podstawie art. 31 ustawy²⁹.

Z punktu widzenia niniejszego opracowania, w sposób szczegółowy omawiane są działania operacyjno-rozpoznawcze Policji, jako organu, który najczęściej korzysta ze swoich uprawnień w tym zakresie. Jednocześnie należy wskazać, iż po nowelizacji lutowej w zasadniczy sposób ujednolicono zasady przeprowadzanie tych czynności oraz sądowej kontroli nad ich zasadnością i przebiegiem, w stosunku do wszystkich służb specjalnych.

Kontrolę operacyjną w interesującym nas zakresie, a więc w formie niejawnego kontrolowania treści korespondencji, uzyskiwanie w sposób niejawni informacji i dowodów oraz ich utrwalanie, w szczególności treści rozmów telefonicznych lub innych informacji przekazywanych za pomocą sieci telekomunikacyjnych, zarządza w drodze postanowienia sąd okręgowy, na pisemny wniosek Komendanta Głównego Policji, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego. Kontrola operacyjna może być zarządzona także przez sąd okręgowy, na pisemny wniosek komendanta wojewódzkiego Policji, złożony po uzyskaniu pisemnej zgody prokuratora okręgowego właściwego ze względu na siedzibę składającego wniosek organu Policji. Warunkiem zasadności przedmiotowego wniosku, a co za tym idzie jego ewentualnego uwzględnienia przez sąd, musi być respektowanie przez organ występujący, zasady subsydiarności, określonej w art. 19 ust. 1 ustawy o Policji. Tym samym, wniosek taki będzie zasadny, gdy inne środki na drodze do wykrycia przestępstwa okazały się niewystarczające, a więc bezskuteczne albo nieprzydatne. Przedmiotowy wniosek należy przedstawić sądowi wraz z materiałami uzasadniającymi potrzebę zastosowania kontroli operacyjnej. Wniosek taki dla swej legalności musi więc określać podmiot i przedmiot kontroli, przestępstwo w związku z popełnieniem bądź obawą popełnienia dla którego kontrolę zarządził, oraz sposób jej przeprowadzenia. Dotyczyć to może kontroli jakiegokolwiek nośnika informacji, w tym połączeń telefonicznych, zapisów poczty elektronicznej, czy też wykazu bilingów. Określenie elementarnych składników postanowienia wynika wprost z dyspozycji art. 94 § 1 k.p.k., który w pkt 3 określa, iż postanowienie powinno zawierać również wskazanie sprawy oraz kwestii, której postanowienie dotyczy. W przypadkach niecierpiących zwłoki, a jeżeli mogłoby to spowodować utratę informacji lub zatarcie albo zniszczenie dowodów przestępstwa, Komendant Główny Policji lub komendant wojewódzki Policji może zarządzić, po uzyskaniu pisemnej zgody

²⁹ Ustawa z dnia 9 czerwca 2006 r., o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, Dz.U. 2006.104.709 z późn. zm.

właściwego prokuratora (Generalnego lub okręgowego), kontrole operacyjną, zwracając się jednocześnie do właściwego miejscowo sądu okręgowego z wnioskiem o wydanie postanowienia w tej sprawie. Sąd okręgowy w terminie 5 dni od dnia zarządzenia kontroli operacyjnej (podśluch) wydaje ewentualną zgodę (następczą) albo odmawia jej udzielenia (ust. 3 art. 19 ustawy o Policji). Na postanowienie sądu w przedmiocie kontroli operacyjnej organowi Policji, który złożył wniosek o wydanie postanowienia w tym zakresie, przysługuje zażalenie. Osoba podsłuchiwana, wobec tajności przeprowadzanych czynności, nie ma takiego uprawnienia. Tym samym na tym etapie postępowania, a w zasadzie czynności przedprocesowych, jej interes nie jest w jakikolwiek sposób reprezentowany. W przypadku nieudzielenia zgody w powyższym terminie, organ zarządzający wstrzymuje kontrolę operacyjną oraz dokonuje protokolarnego, komisyjnego zniszczenia materiałów zgromadzonych podczas jej stosowania. Kontrolę operacyjną zarządza się na okres nie dłuższy niż 3 miesiące (art. 19 ust. 8 ustawy o Policji). W przypadkach, w których jest to uzasadnione koniecznością, sąd okręgowy, na pisemny wniosek Komendanta Głównego Policji lub komendanta wojewódzkiego Policji, po uzyskaniu pisemnej zgody właściwego prokuratora okręgowego, może przedłużyć, jednorazowo, stosowania kontroli operacyjnej na okres nie dłuższy niż kolejne trzy miesiące. Łącznie, wskazany okres podstawowy, w którym zarządzenia przeprowadzenia kontroli operacyjnej w postaci podśluchu może mieć miejsce, wynosić może 6 miesięcy. Nie oznacza to jednak, iż jest to okres maksymalny, na jaki możliwe będzie zastosowanie podśluchu pozaprocesowego. W ust. 9 art. 19 ustawy o Policji przewidziano bowiem szczególny tryb przedłużenia przedmiotowej kontroli, na dalszy czas oznaczony, w przypadkach, gdy podczas dotychczasowej kontroli operacyjnej pojawią się nowe okoliczności, istotne dla zapobieżenia lub wykrycia przestępstwa albo ustalenia sprawców i uzyskania dowodów przestępstwa. Jak wynika z powyższego zapisu, brak jest w nim określenia maksymalnego czasu, na jaki zastosowanie podśluchu byłoby możliwe. Nie wskazanie ograniczenia czasowego, nie służy zapewnieniu przestrzegania, przez stosowne służby, praw i wolności obywatelskich i może prowadzić do nadużyć, w szczególności w sytuacjach dość „pobieżnego” rozpatrywania przez sądy okręgowe przedkładanych przez służby wniosków. Ponadto, pomimo, iż ustawa zobowiązuje służby specjalne do przedkładania sądowi materiałów zgromadzonych w toku zarządzanych kontroli operacyjnych, trudno będzie sędziemu ocenić, czy przedłożony materiał jest zupełny, a nie poddany przez wnioskodawcę (służby), wstępnej wybiórczej selekcji. O ile w toku rozpoznawania wniosku o zastosowanie podśluchu, czy innej formy przeprowadzanie

czynności operacyjnych, sąd bada raczej spełnienie tylko warunków formalnych wniosku, to przy rozpoznawaniu wniosku o przedłużenie, powinien już rozważać również jego celowość w oparciu o zebrany i zabezpieczony materiał dowodowy. Wątpliwości natury konstytucyjnej budzi ponadto brak w ustawie o Policji, jak i w innych regulacjach organizacyjnych każdej ze służb, wskazania określonego kręgu osób, wobec których nie byłoby możliwe zastosowanie podsłuchu operacyjnego. Tym samym do kręgu podmiotów mogących być w zainteresowaniu służb specjalnych, stosując posiłkowo art. 237 § 4 k.p.k., może należeć każdy, w tym i adwokat. A co za tym idzie, wobec braku zapisu gwarancji procesowych, tak w ustawie o Policji, jak i pozostałych regulacjach dotyczących pozostałych służb, np. w postaci zakazów dowodowych, podobnych, czy też tożsamy z tymi w kpk, podmiotem wobec którego można prowadzić czynności operacyjnej w postaci podsłuchu pozaprocesowego, może stać się również adwokat wykonujący obronę klienta. Trudno nie ulec wrażeniu, iż w przedmiotowej sytuacji może dojść do naruszenia praw i wolności obywatelskich, w tym przede wszystkim, prawa do obrony, czego ustawodawca zdaje się nie zauważać.

Wykorzystanie dowodu uzyskanego podczas stosowania kontroli operacyjnej dopuszczalne jest wyłącznie w postępowaniu karnym w sprawie o przestępstwo lub przestępstwo skarbowe, w stosunku do którego dopuszczalne jest stosowanie takiej kontroli przez jakikolwiek uprawniony podmiot. Znamienne w tej materii jest uchwała SN³⁰, na tle art. 17 ust. 1 i 2 ustawy o CBA, w której za dowody pozwalające na wszczęcie postępowania karnego lub mające znaczenie dla toczącego się postępowania karnego, a uzyskane w wyniku kontroli operacyjnej zarządzanej postanowieniem sądu, uznano jedynie dowody dotyczące przestępstw, wskazanych w postanowieniu o zastosowanie kontroli operacyjnej lub w postanowieniu o udzieleniu tzw. zgody następczej, w tym wydanej także w toku kontroli operacyjnej, a popełnionych przez osobę, której dotyczyła zgoda pierwotna i osobę, co do której wydano zgodę następczą. Dowody zebrane w toku kontroli operacyjnej, a zarządzanej przez sąd, wobec konkretnej osoby podejrzewanej o popełnienie przestępstw należących do katalogu określonego w ustawach kompetencyjnych, należą zawsze do zasobu legalnego, a tym samym mogą być wykorzystywane procesowo³¹.

³⁰ Uchwała SN z 23 marca 2011 r., I KZP 32/10, OSNKW nr 3/2011, podobnie Postanowienie SN z 25 marca 2010 r., I KZP 2/10, Postanowienie SN z 26 kwietnia 2007 r., I KZP 6/07, D. Drajewicz: *zgoda następcza sądu na stosowanie kontroli operacyjnej*, „Państwo i Prawo” 2009, Nr 1.

³¹ Wyrok TK z 12 grudnia 2005 r., K 32/04.

Jeżeli w wyniku stosowania kontroli operacyjnej uzyskano dowód popełnienia przestępstwa lub przestępstwa skarbowego, w stosunku do którego można zarządzić kontrolę operacyjną, popełnionego przez osobę, wobec której była stosowana kontrola operacyjna, innego niż objęte zarządzeniem kontroli operacyjnej albo popełnionego przez inną osobę, o zgodzie na jego wykorzystanie w postępowaniu karnym orzeka postanowieniem sąd, który zarządził kontrolę operacyjną albo wyraził na nią zgodę w trybie określonym w ust 3 art. 19 ustawy o Policji, na wniosek prokuratora. Wniosek taki prokurator kieruje do sądu nie później niż w ciągu miesiąca od dnia otrzymania materiałów zgromadzonych podczas stosowania kontroli operacyjnej, przekazanych mu przez organ Policji niezwłocznie, nie później jednak niż w terminie 2 miesiące od dnia zakończenia tej kontroli. Sąd wydaje postanowienie w powyższym zakresie w terminie 14 dni od dnia złożenia wniosku przez prokuratora. Zgromadzone podczas stosowania kontroli operacyjnej materiały niezawierające dowodów pozwalających na wszczęcie postępowania karnego lub dowodów mających znaczenie dla toczącego się postępowania karnego podlegają niezwłocznemu, protokolarnemu i komisijnemu zniszczeniu. Przy czym faktycznego zniszczenia dokonuje organ Policji, który ma jedynie obowiązek zawiadomienia o tej czynności właściwego prokuratora okręgowego. Wydaje się *de lege ferenda*, iż w celu pełnego zapewnienia gwarancji procesowych, kontrola nad faktycznym zniszczeniem materiałów operacyjnych powinna odbywać się w obecności prokuratora i to obligatoryjnie. Osobie, wobec której zastosowano kontrolę operacyjną, nie udostępnia się materiałów zgromadzonych podczas trwania tej kontroli, a uregulowanie to nie narusza uprawnień wynikających z art. 321 k.p.k., w zakresie dotyczącym zaznajomienia podejrzanego z materiałami postępowania. Jednocześnie ustawa o Policji zobowiązuje podmioty wykonujące działalność telekomunikacyjną oraz podmioty świadczące usługi pocztowe, do zapewnienia Policji, na własny koszt, warunków technicznych i organizacyjnych umożliwiających prowadzenie kontroli operacyjnej. Prowadzi to więc do sytuacji, w której zarówno Policja jak i pozostałe służby, mogą występować do operatorów telekomunikacyjnych z nieograniczoną ilością wniosków o zabezpieczenie danych telekomunikacyjnych, nie bacząc przy tym, na jakiegokolwiek ograniczenia z tym związane, w tym również finansowe.

IV. Bilingi, czyli wykaz połączeń telefonicznych

Pojęcie bilingu, nie mając wprawdzie materialnoprawnej definicji w żadnej z obowiązujących regulacji prawnych, potocznie rozumiane jest jako wykaz

połączeń telefonicznych danego abonenta³², otrzymany zazwyczaj w formie komputerowego wydruku. Z kolei pojęcia połączenia i połączenia telefonicznego, znajdują się w zapisach ustawy Prawo telekomunikacyjne. Przez połączenie ustawa prawo telekomunikacyjne rozumie fizyczne lub logiczne połączenie telekomunikacyjnych urządzeń końcowych pozwalające na przesłanie przekazów telekomunikacyjnych (art. 2 pkt 24). Połączenie telefoniczne zaś, to połączenie ustanowione za pomocą publicznie dostępnej usługi telefonicznej, pozwalającej na dwukierunkową łączność w czasie rzeczywistym (art. 2 pkt 26). Do ważniejszych z punktu widzenia niniejszej publikacji definicji zaliczyć można również pojęcie przekazu telekomunikacyjnego, którym wedle ustawy są treści rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych (art. 2 pkt 27a). O ile samo otrzymanie wydruku wykazu połączeń (biling), biorąc pod uwagę prawo jego otrzymania przez każdego abonenta, a więc podmiotu będącego stroną umowy o świadczenie usług telekomunikacyjnych, wraz z fakturą za dany okres rozliczeniowy (art. 80 ust. 1 prawa telekomunikacyjnego), nie ma w sobie nic nadzwyczajnego, o tyle istniejące uregulowania prawne, dające takie uprawnienia dodatkowo innym podmiotom, w tym służbom, są na tyle kontrowersyjne, iż wymagają szczególnego omówienia.

Ustawa Prawo telekomunikacyjne, w art. 180a-180d, nakłada na operatorów publicznych sieci telekomunikacyjnych oraz dostawców publicznie dostępnych usług telekomunikacyjnych, na ich koszt, obowiązek zatrzymywania i przechowywania danych niezbędnych do ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego, który inicjuje połączenie oraz do którego połączenie jest kierowane. Jednocześnie obowiązek ten dotyczy określenia daty i godziny połączenia oraz czasu jego trwania, rodzaju tego połączenia, a także lokalizacji telekomunikacyjnego urządzenia końcowego (art. 180c ust.1 prawa telekomunikacyjnego). W obowiązującym stanie prawnym obowiązek ten trwa przez okres 24 miesięcy, licząc od dnia połączenia lub nieudanej próby tego połączenia. Po upływie tego okresu operator oraz dostawca zobowiązany jest zniszczyć dane (art. 180a ust. 1 pkt 1), chyba że zostały one zabezpieczone zgodnie z odrębnymi przepisami. W tym miejscu należy wskazać, iż okres 24 miesięcy na zatrzymywanie danych, który przewiduje obowiązująca ustawa prawo telekomunikacyjne, jest najdłuższym okresem, na jaki możliwe jest zatrzymywanie danych w całej Unii Europejskiej, według zaleceń art. 6 Dyrektywy Retencyjnej z 2006 roku, przy czym okres

³² A. Staszak, *Prawne podstawy dopuszczalności żądania bilingów*, „Przegląd Bezpieczeństwa Wewnętrznego” 2011, nr 4.

minimalny według teź to 6 miesięcy, od daty połączenia. Nie sposób nie zauważyć, iż utrzymywanie w Polsce, najdłuższego z zalecanych terminów na zatrzymywanie danych telekomunikacyjnych (ich przechowywanie), nie znajduje żadnego merytorycznego uzasadnienia. W chwili obecnej trwają prace nad nowelizacją prawa telekomunikacyjnego m.in. w zakresie ograniczenia powyższego okresu do 12 miesięcy³³. Na problem retencji danych w naszym systemie prawa, zwróciła uwagę Naczelna Rada Adwokacka, organizując w maju 2011 roku konferencję pt. „Retencja danych: troska o bezpieczeństwo czy inwigilacja obywateli”, która poprzedzona była ogłoszeniem Raportu Komisji Praw Człowieka przy NRA o Retencji Danych³⁴. Autorzy Raportu wskazują, iż Polak, według danych Komisji Europejskiej, jest obywatelem najbardziej inwigilowanym w całej Unii Europejskiej, a znaczna część obowiązującego prawa w tym zakresie jest niezgodna z EKPCz, czy też z Konstytucją RP. Zakres ingerencji służb w prawa i wolności obywatelskie jest nieuzasadniony i nieproporcjonalny, jak na warunki demokratycznego państwa prawa. Do obowiązków operatorów należy również udostępnianie powyższych danych uprawnionym podmiotom, Służbie Celnej, sądowi i prokuratorowi, na zasadach i w trybie określonym w odrębnych przepisach (ust. 1 pkt 2 art. 180a). Taką odrębną regulacją jest np. art. 20 c ustawy o Policji, który upoważnia Policję do otrzymania danych telekomunikacyjnych, jeżeli jest to konieczne w celu zapobiegania lub wykrywania przestępstw. Warto zwrócić uwagę, że ustawa o Policji, praktycznie umożliwia podjęcie wszelkich działań prewencyjnych, bowiem literalne brzmienia zapisu „w celu zapobiegania”, nie oznacza nic innego jak prewencję, a więc przyzwolenie na swoistą dowolność działania w tym zakresie. Ponadto nie wprowadzono ustawowego zapisu dotyczącego specjalnego obligatoryjnego wymogu, leżącego po stronie funkcjonariuszy Policji, do posiadania każdorazowo, stosownych uprawnień do otrzymania danych telekomunikacyjnych. Z brzmienia przepisów wynika, że operator udostępnia dane na wniosek Komendanta Głównego Policji lub komendanta wojewódzkiego Policji albo osoby przez nich upoważnionej, bezpośrednio policjantowi wskazanemu we wniosku lub za pośrednictwem sieci telekomunikacyjnej. Taki zapis nie ogranicza kręgu osób mogących zapoznać się z danymi, a wprost go powiększa. Prowadzi to do możliwości wystąpienia niekontrolowanego pobierania danych, i to nie tylko w związku ze sprawami wymienionymi w katalogu art. 19 ust. 1 ustawy o Policji, ale także we wszyst-

³³ Więcej informacji o projekcie zmian na stronie głównej Ministerstwa Administracji i Cyfryzacji www.mac.gov.pl.

³⁴ Raport NRA.

kich innych, bliżej nieokreślonych sprawach, na zasadzie prewencji. Nie ma bowiem w ustawie zamkniętego katalogu spraw, odnośnie których udostępnianie danych byłoby wyłączone. Jednocześnie brak jest wskazania niezależnego organu, najlepiej sądu, który dokonywałby weryfikacji, pod kątem merytorycznej zasadności żądania takich danych w każdym konkretnym przypadku. Z punktu widzenia prawa do prywatności jak i innych praw podstawowych, także nie poprawia tej sytuacji fakt, iż materiały, które zawierają informacje mające znaczenie dla postępowania karnego, Policja przekazuje właściwemu miejscowo i rzeczowo prokuratorowi (art. 20 c ust. 6). Z zapisu tego jasno wynika, iż to funkcjonariusz Policji dokonuje selekcji tego co może być ważne dla sprawy i niejako *ex post* przekazuje ten materiał prokuratorowi. Fakt, że to właśnie funkcjonariusz policji podejmuje w istocie samodzielną decyzję, należy ocenić bardzo negatywnie. Uprawnienie to pozbawione jakiegokolwiek kontroli, tak nad pobieraniem, jak i faktycznym wykorzystaniem danych, stwarza niewątpliwie pole do nadużyć. Podśłuchiwany nie jest przy tym informowany o przeprowadzeniu takiej kontroli, nawet po jej zakończeniu. Materiały, które nie zawierają informacji istotnych dla postępowania karnego, podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu (art. 20 c ust. 7). W tym zakresie z kolei wątpliwości prawne budzi brak sprecyzowania w ustawie konkretnego terminu, w którym zniszczeniu muszą ulec zabezpieczone dane. W toku czynności operacyjnych Policja pozyskuje ogromną ilość informacji, niekoniecznie potrzebnych dla toczącego się postępowania, które z kolei może wykorzystać operacyjnie w dowolny sposób. Okres zaś retencji danych transmisyjnych, który wynosi w Polsce dwa lata jest na tyle długi, iż praktycznie umożliwia służbom pełną inwigilację obywateli, przez ten czas. Ponadto, jak wspomiano to już wielokrotnie, żadna z ustaw nie przewiduje katalogu osób, które podlegałyby wyłączeniu od możliwości żądania przez służby danych retencyjnych. Nie ma więc formalnych ograniczeń, aby w sposób operacyjny kontrolować czynności telekomunikacyjne adwokata, a tym samym wkraczać w jego prawo do wolności komunikowania się, jak i zasadę obowiązującej go tajemnicy zawodowej. Podobne wątpliwości budzi obowiązująca regulacja art. 218 i 218a k.p.k., a więc uprawnień do procesowego żądania od operatorów danych telekomunikacyjnych. Na mocy tego artykułu, urzędy, instytucje i podmioty prowadzące działalność telekomunikacyjną obowiązane są wydać sądowi lub prokuratorowi, na żądanie zawarte w postanowieniu, dane o których mowa w art. 180c i 180d ustawy prawo telekomunikacyjne, jeżeli mają znaczenie dla toczącego się postępowania. Tylko sąd lub prokurator mają prawo je otwierać lub zarządzić ich otwarcie. Trudno nie

dostrzec, iż powyższa regulacja, nie uzależnia otrzymanie bilingów od jakiegokolwiek kontroli ze strony sądu, a jedynie wymaga na etapie postępowania przygotowawczego, wydania stosownego postanowienia ze strony prokuratora. Konkretny zaś operator, do którego prokuratura się zwróci jest zobowiązany udostępnić dane telekomunikacyjne. Wątpliwości budzi również brak katalogu spraw oraz osób, odnośnie których żądanie bilingów byłoby wyłączone. Kwestią otwartą pozostaje, czy w oparciu o art. 218 ust. 1 i 218a k.p.k., a w związku z art. 6, 178 i art. 180 k.p.k. w szczególności jego § 2, żądanie wydruku połączeń adwokata pełniącego funkcję obrońcy jest zgodne m.in. z konstytucyjną gwarancją prawa do obrony. Zdaniem autora niniejszego opracowania zdecydowanie nie, natomiast trzeba zwrócić uwagę, iż problemem w tej materii jest nie tylko wykorzystanie danych retencyjnych w procesie, ale praktycznie nieograniczona możliwość swobodnego dostępu do tych danych. W szczególności dotyczy to danych osób zobowiązanych do zachowania tajemnicy zawodowej, jak dziennikarz, lekarz, czy adwokat. Postanowienie, o którym mowa powyżej, doręcza się abonentowi telefonu lub nadawcy, którego wykaz połączeń lub innych przekazów informacji został wydany. Doręczenie postanowienia może być jednak odroczone na czas oznaczony, niezbędny ze względu na dobro sprawy, lecz nie później niż do czasu prawomocnego zakończenia postępowania. Jak z powyższego wynika, osoba inwigilowana, pozbawiona jest dostępu do informacji o czynnościach operacyjnych przeprowadzanych wobec niej, a co się z tym wiąże, naruszane są jej prawa, w tym prawo do prywatności, wolności komunikowania się oraz w kontekście niniejszego opracowania również realne prawo do obrony. Podmioty prowadzące działalność telekomunikacyjną obowiązane są niezwłocznie zabezpieczyć, na żądanie sądu lub prokuratora zawarte w postanowieniu, na czas określony, nieprzekraczający jednak 90 dni, dane informatyczne przechowywane w urządzeniach zawierających te dane na nośniku lub w systemie informatycznym (art. 218 a k.p.k.). Jak widać, powyższe regulacje procesowe również nie zawierają katalogu osób podlegających wyłączeniu spod możliwości zażądania bilingów połączeń, a co za tym idzie i innych danych, o których wspomniano wcześniej, jak w szczególności miejsc logowania się BTS, czy poczty elektronicznej, adwokata, jak też i jego klienta. Reasumując, trudno nie odnieść wrażenia, iż faktyczne pozyskanie danych telekomunikacyjnych w postaci bilingów, objętych z jednej strony tajemnicą komunikowania się, a z drugiej strony konstytucyjnym prawem do obrony, nie stanowi dla służb praktycznie żadnego problemu i dotyczy zarówno fazy procesowej jak i pozaprocessowej.

IV. Podsumowanie

Zaprezentowany po krótku, z uwagi na ograniczone ramy niniejszego opracowania, obraz prawnych możliwości dostępu służb specjalnych do danych telekomunikacyjnych obywateli, w tym osób zobowiązanych do zachowania tajemnicy zawodowej, w szczególności adwokatów, nie daje podstaw do zadowolenia. Bliższe zapoznanie się z obowiązującymi w tym zakresie regulacjami prawnymi wskazuje, iż w wielu miejscach zapisy ustaw są nieostre, bądź w ogóle nie odnoszą się do podstawowych kwestii regulujących sposób działania służb. Przykładem niech będzie brak ustawowego wskazania katalogu osób podlegających wyłączeniu od inwigilacji, a wobec których obowiązywałby zakaz dowodowy, związany z obowiązkiem zachowania tajemnicy zawodowej, w szczególności dziennikarskiej, lekarskiej czy adwokackiej. O ile w oparciu o przepisy Kodeksu postępowania karnego, adwokat ma większe szanse na uniknięcie takiej inwigilacji (procesowo) w zakresie kontroli swoich danych telekomunikacyjnych, o tyle w oparciu o regulacje ustaw szczególnych, może to być już dyskusyjne. Walka z przestępczością, czy terroryzmem nie może uzasadniać naruszania podstawowych praw i wolności obywatela, a jakiegokolwiek ograniczanie tych praw, bądź ingerencje w te prawa, powinny podlegać ustawowym regulacjom. Ponadto zapisy tych regulacji muszą w jasny sposób określać cel takiego naruszenia, zachować proporcjonalność użycia środków technicznych, w tym metod działania oraz wskazywać konkretny okres, na jaki prawa te mogą ulec ograniczeniu. Przede wszystkim zaś, w demokratycznym państwie prawnym, działania służb specjalnych muszą podlegać legalnej kontroli ze strony niezależnych organów, w głównej mierze niezawisłego sądu. Obywatel powinien być informowany o dokonanych, przez stosowne służby wszelkich naruszeniach jego praw i wolności. Konstytucyjna zasada prawa do obrony, oraz wynikający z niej bezwzględny zakaz dowodowy (art. 178 k.p.k.), wyklucza w sposób oczywisty możliwość wykorzystania w postępowaniu karnym materiału zebranego w toku podsłuchu procesowego, jak i pozaprocesowego, czy też za pomocą innych środków technicznych, nakierowanych na pozyskanie informacji z nośników teleinformatycznych, które bezpośrednio dotyczyłyby tajemnicy zawodowej adwokata. Obecny stan prawny nie jest jednak w tym zakresie zadawalający. Nie znajdziemy bowiem żadnej regulacji ustawowej, która w sposób jednoznaczny wykluczałaby taką możliwość. Dotyczy to zarówno przepisów rozdziału 26 k.p.k., jak i ustaw szczególnych. Tym samym ustawodawca w dalszym ciągu na uprzywilejowanej pozycji stawia or-

gany państwa, a nie prawa i wolności obywatela. Najlepszym tego przykładem jest w zasadzie powszechny dostęp do wykazu połączeń telefonicznych – billingów, które operatorzy telekomunikacyjni, zobowiązani są udostępniać stosownym instytucjom. Nie oznacza to wprawdzie formalnej możliwości wykorzystania takiego dowodu w postępowaniu karnym, ale może w zasadniczy sposób naruszać prawo obywatela do wolności komunikowania się oraz prawo do obrony, jak i stanowić naruszenie tajemnicy zawodowej adwokata.