BEZPIECZEŃSTWO 2009 nr 3-4 TEORIA I PRAKTYKA

Piotr Kosmaty

E-podsłuch. Zarys problematyki[1]

W otaczającym nas świecie brak jest dziedziny życia społecznego, gospodarczego czy państwowego, w której nie funkcjonowałyby komputery. Z równym powodzeniem komputeryzacja wkroczyła w sferę przestępczości oraz terroryzmu.

Sieć komputerowa stała się miejscem do popełniania cyberprzestępstw, ale również bardzo popularnym medium do wymiany informacji pomiędzy przestępcami. Dla organów ścigania, a zwłaszcza organów wymiaru sprawiedliwości, sieć stanowi potencjalne źródło uzyskiwania cyberdowodów, a nawet skuteczne narzędzie do przeciwdziałania popełnianiu przestępstw.

Celem poniższych rozważań będzie próba zakreślenia problemu przechwytywania transmisji teleinformatycznych jako źródła uzyskiwania środków dowodowych. Postaram się również przybliżyć regulacje prawne dotyczące podsłuchu komputerowego.

Pojęcie podsłuchu komputerowego nie zostało zdefiniowane w obowiązujących przepisach. Zatem zadanie to zostało pozostawione doktrynie. Zdaniem K. Dudki, podsłuch komputerowy to kontrola informacji komputerowych[2]. Pomimo generalnej słuszności takiego poglądu należy go uściślić. Podsłuchem komputerowym będzie zatem działalność organów państwowych, takich jak Policja lub Prokuratura, polegająca na przechwytywaniu wszystkich danych, które mogą być wysyłane lub odbierane za pomocą komputera.

W teorii istnieje możliwość przechwytywania całości transmisji teleinformatycznych prowadzonych pomiędzy różnymi komputerami. Celowo zostało użyte słowo w teorii, gdyż jak zostanie wykazane w dalszej części artykułu, mogą być przesyłane przez sieć takie dane, których w praktyce organy ścigania nie będą zdolne przechwycić.

---

[1] Pierwotna wersja artykułu pt. *Podsłuch komputerowy – zarys problematyki* ukazała się w kwartalniku „Prokurator" 2008, nr 4.

[2] K. Dudka, *Podsłuch komputerowy w polskim procesie karnym – wybrane zagadnienia praktyczne*, „Prokuratura i Prawo" 1999, nr 1, s. 70.

Świat wirtualny, o którym mówimy, funkcjonuje dzięki infrastrukturze czyli sieci. W Polsce największymi właścicielami sieci internetowych są: Telekomunikacja Polska SA, Polskie Koleje Państwowe oraz Polskie Sieci Energetyczne. Oprócz nich funkcjonują mniejsze firmy posiadające sieć, takie jak: GHnet, ASTER czy VERANET. Sieć następnie wykorzystywana jest przez firmy świadczące usługi internetowe, takie jak: ONET.PL, WIRTUALNA POLSKA czy INTERIA.

Korzystanie z sieci nie jest anonimowe, bowiem każde urządzenie podpięte do Internetu posiada unikalny w danej chwili adres, zwany numerem IP (Internet Protocol).

Gdy użytkownik komputera chce dokonać łącza z internetem, musi skorzystać z usług firm będących dostarczycielami połączeń internetowych (ISP – Internet Service Provider). W Polsce takimi providerami są np. TP SA, GHnet czy ERA GSM.

Na tym etapie pojawia się pierwsza możliwość przejęcia danych przesyłanych przez sieć. Internet podobny w swej istocie do pajęczyny przesyła dane do kolejnych elementów sieci. Na styku poszczególnych elementów sieci znajdują się tzw. routery, których zadaniem jest przesyłanie informacji do innego elementu, tak aby finalnie trafiła do adresata. Router działa na tej samej zasadzie co centrala telefoniczna, której zadaniem jest właściwe przekierowanie rozmowy. Dostęp do routera otwiera dla organów ścigania możliwość przechwytywania danych wysyłanych z konkretnego IP (komputera).

Kolejna możliwość przejęcia wysłanych danych komputerowych pojawia się na etapie działania firm świadczących usługi internetowe. Wysłana informacja przechodzi przez serwer usługodawcy, aby następnie trafić do adresata. Dostęp do danych znajdujących się na serwerze, np. portalu ONET.PL czy podmiotów świadczących usługi w zakresie Skype, Gadu-Gadu, umożliwia zatem przejęcie i zaznajomienie się z interesującymi organy ścigania transmisjami teleinformatycznymi.

Jak wynika z powyższego, organy ścigania lub wymiaru sprawiedliwości w zakresie podsłuchu komputerowego muszą współdziałać z właścicielami infrastruktury internetowej (router) bądź z firmami świadczącymi usługi w sieci.

Możliwa jest jeszcze jedna, wielce skuteczna metoda „przechwytywania" i utrwalania dla celów dowodowych wszelkich danych wysyłanych bądź otrzymywanych z konkretnego komputera. Dzięki tej metodzie możliwe jest skontrolowanie danych komputerowych, zanim zostaną wysłane do sieci. Ma to kolosalne znaczenie w kontekście faktu, że przestępcy lub terroryści mogą szyfrować informacje przed ich wysłaniem. Organy ścigania mają możliwość zaznajomienia się z informacją przed jej zaszyfrowaniem. Metoda ta polega na wprowadzeniu do komputera osoby, której dane chce się kontrolować, ukrytego programu pozwalającego na nieograniczoną kontrolę jej działalności.

Oczywiście, program ten wprowadza się podstępnie bez wiedzy użytkownika komputera. Można go zainstalować poprzez: a) fizyczny dostęp do urządzenia b) poprzez wykorzystanie luk w oprogramowaniu c) za pomocą przesłanego pocztą elektroniczną SPAMU. Jak łatwo zauważyć, taki podsłuch oparty jest na zasadzie programu zwanego „koniem trojańskim". W praktyce „konie trojańskie" wykorzystywane są przez hackerów, aby włamać się do komputera innej osoby. Metoda ta, jakkolwiek bardzo skuteczna, bo dająca pełną kontrolę nad komputerem określonej osoby, może rodzić

pytania o jej legalność. Organ ścigania, chcąc prowadzić taki podsłuch, musi wcześniej dokonać „włamania" do czyjegoś komputera.

Jak już wspomniano na wstępie, można przejmować wszelkie dane, które są wysyłane lub odbierane za pośrednictwem komputera. Najczęściej podsłuch komputerowy prowadzony jest w stosunku do: poczty elektronicznej (e-mail), komunikatorów internetowych (np. Gadu-Gadu, Tlen), telefonii komputerowej (Skype), przesyłania głosu z obrazem, transmisji głosowej przez Internet (*voice over* IP). Dotyczy to ponadto zbierania informacji, z jakiego IP odwiedzano konkretne strony internetowe lub przechwytywania transmisji plików. Mając na uwadze błyskawiczny rozwój technologii komputerowej, należy liczyć się ze wzrostem nowych form transmisji teleinformatycznych, w stosunku do których będzie prowadzony podsłuch komputerowy.

Sytuacja skomplikuje się, gdy z podsłuchiwanego komputera będą wysyłane informacje zaszyfrowane. Rozróżniamy dwa rodzaje szyfrowania transmisji teleinformatycznych: symetryczne i asymetryczne. Przy pierwszych zarówno nadawca, jak i odbiorca przekazu informacji muszą znać klucz do ich rozszyfrowania. Przy drugich klucz do odszyfrowania zna tylko odbiorca informacji, stąd ta grupa szyfrów zwana jest „szyfrowaniem z kluczem publicznym". Jeżeli organ ścigania w trakcie prowadzonego podsłuchu napotka kryptogram (zaszyfrowaną wiadomość), powinien podjąć próbę jego odszyfrowania. W tym celu musi wykorzystać algorytm i klucz. W przypadku szyfrów symetrycznych odszyfrowanie następuje na podstawie cech transmisji. Jest bowiem wiele mechanizmów szyfrowania używanych na co dzień (ustandaryzowanych). Przy szyfrach asymetrycznych do ustalenia klucza niezbędne będzie przeprowadzenie działań operacyjnych, jak np. włamanie do komputera czy podsłuch lub podgląd pomieszczeń.

Na koniec tej części rozważań chciałbym wskazać, iż istnieje możliwość ukrycia prawdziwego znaczenia przekazu teleinformatycznego. Określa się to pojęciem steganografia[3], czyli przesyłanie informacji tak, aby osoby postronne, np. organy ścigania, nie podejrzewały jej istnienia. Jest to bardzo niebezpieczna „broń" w rękach wysoko wyspecjalizowanych grup przestępczych, a nawet terrorystów. W przypadku prowadzenia podsłuchu komputerowego organ ścigania, przejmując określoną informację, nie ma w ogóle świadomości, że jest ona zaszyfrowana. W przypadku kryptografii organ wie, że przejął informację zaszyfrowaną i musi podjąć próbę ustalenia jej znaczenia. Obrazowo można by to wytłumaczyć w następujący sposób: osoba „X" za pomocą poczty elektronicznej przesyła osobie „Y" widok morza z wyspą. Wyłącznie te dwie osoby wiedzą, co w tym przekazie oznacza „morze", a co „wyspa". Pamiętać należy, że jest to przykład bardzo uproszczony, gdyż świat wirtualny jest dalece odmienny od świata realnego. Jak widać, przy steganografii przestępcy potrafią ukryć fakt przesłania określonych informacji. W praktyce spowoduje to, że policja lub inne służby specjalne nie będą zdolne do prowadzenia skutecznego podsłuchu komputerowego. Stąd zatem można wnosić, że tylko w teorii istnieje możliwość przejęcia wszystkich transmisji teleinformatycznych.

Obecnie wydaje się, że jedyną dostępną formą walki ze zjawiskiem steganografii są działania operacyjne zainteresowanych organów. Jedynie w ich toku będzie można ustalić, czy doszło do przesłania informacji i jaka jest jej treść.

---

[3] Wikipedia, http://pl.wikipedia.org (dostęp: 25.10.2008).

Katarzyna Dudka w 1999 r. stwierdziła: „dowody uzyskane w toku podsłuchu komputerowego będą miały znaczenie przede wszystkim w fazie *in rem* postępowania przygotowawczego, gdy zadaniem procesu karnego jest ustalenie faktu popełnienia przestępstwa i wyjaśnienie jego okoliczności, natomiast przydatność podsłuchu komputerowego w fazie *in personam* odgrywać będzie rolę ograniczoną"[4]. Wraz z postępem technicznym pogląd taki jakkolwiek słuszny traci na znaczeniu. Obecnie coraz więcej komputerów wyposażonych jest w mikrofony lub minikamery. Daje to organom ścigania możliwość takiego prowadzenia podsłuchu komputerowego, aby poza przechwytywaniem danych można było ustalić, kto w danej chwili je wysyła lub odbiera. Indywidualizacja osoby, która przesyła wiadomość, staje się coraz bardziej realna, gdyż można ją obserwować.

Na gruncie polskiego ustawodawstwa podsłuch komputerowy może być prowadzony zarówno w procesie karnym, jak i poza nim w ramach czynności operacyjno-rozpoznawczych prowadzonych przez uprawnione organy. Przechwytywanie danych komputerowych w procesie odbywa się na podstawie rozdziału 26 kpk zatytułowanego „Kontrola i utrwalanie rozmów". Jakkolwiek w art. 237 § 1 kpk mowa jest o kontroli i utrwalaniu treści rozmów telefonicznych, to mocą art. 241 kpk rozdział ten ma zastosowanie również do podsłuchu komputerowego. Zgodnie z tym ostatnim przepisem, regulacje dotyczące kontroli i utrwalania rozmów telefonicznych stosuje się odpowiednio do kontroli z użyciem środków technicznych treści innych rozmów lub przekazów informacji, w tym korespondencji przesyłanej pocztą elektroniczną. Zdaniem T. Grzegorczyka, zakres kontroli i utrwalania, o jakich mowa w art. 237 kpk obejmuje:

a) treści rozmów innych niż telefoniczne, a więc wszelkie rozmowy, bez względu na to jak i gdzie są prowadzone (w domu, w parku, na ulicy, w biurze itd.),
b) treści przekazów informacji innych niż telefoniczne, a wśród nich także korespondencję przesyłaną pocztą elektroniczną[5].

W pierwszym przypadku chodzi o rozmowę między dwiema lub więcej osobami, prowadzoną bez przekaźnika technicznego. W drugim o przekazy informacji z wykorzystaniem urządzeń technicznych (innych niż telefon).

Problem w tym aspekcie budził kontrowersję do noweli z 10 stycznia 2003 r., mocą której zmieniono treść omawianego przepisu. W swoim poprzednim brzmieniu stanowił, iż regulacje z rozdziału 26 stosuje się odpowiednio do kontroli oraz do utrwalania z użyciem środków technicznych treści przekazów informacji innych niż rozmowy telefoniczne. Z uwagi na problemy interpretacyjne tego zapisu Sąd Najwyższy w uchwale z 21 marca 2000 r.[6] Przyjął, iż: „przekazywanie informacji innych niż rozmowy telefoniczne oznacza niemające charakteru rozmowy telefonicznej: przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej, przez przewody, systemy radiowe, optyczne lub jakiekolwiek inne urządzenia wykorzystujące energię elektromagnetyczną". Uzasadnieniem takiego stanowiska miało być respektowanie konstytucyjnego prawa do ochrony tajemnicy komunikowania się. Stąd ta zawężająca interpretacja cytowanego przepisu. Art. 241 kpk w obecnym kształcie wyeliminował

[4] *Ibidem*, s. 71.

[5] T. Grzegorczyk, *Kodeks Postępowania Karnego wraz z komentarzem do Ustawy o świadku koronnym*, Kraków 2003, s. 620.

[6] I. KZP 60/99, OSNKW 3-4/2000, poz. 26.

wszelkie wątpliwości co do zakresu jego stosowania, tym samym straciło na znaczeniu omawiane stanowisko Sądu Najwyższego. Zatem należy w pełni zgodzić się ze stanowiskiem T. Grzegorczyka, zgodnie z którym w procesie karnym można stosować podsłuch do rozmów telefonicznych, rozmów innych niż telefoniczne (w pomieszczeniu, na otwartej przestrzeni) oraz do wszelkich przekazów informacji z wykorzystaniem urządzeń technicznych. Oczywiste jest więc, że w procesie karnym można prowadzić podsłuch komputerowy bez ograniczeń.

Natomiast wydaje się, że w trakcie procesu karnego nie będzie można wykorzystywać takich form inwigilacji, jak przejmowanie danych komputerowych za pomocą analizy tzw. ulotu elektromagnetycznego. Polega on na analizowaniu fal elektromagnetycznych emitowanych przez sprzęt komputerowy (komputery, przewody, myszki, monitory), czy fal akustycznych emitowanych przez drukarki[7]. W tych przypadkach bowiem nie mamy do czynienia z rozmową, a tym bardziej z przekazem informacji. Właśnie z tych względów uważam, że w procesie będzie można stosować podsłuch wykorzystujący szyby okienne jako membrany, z których informacja „zbierana" jest wiązką lasera. Nie zgadzam się z A. Kiedrowicz, jakoby w procesie nie można było stosować inwigilacji za pomocą oprogramowania szpiegowskiego[8]. Swoje twierdzenie opiera ona na założeniu, że Kodeks Postępowania Karnego zezwala na kontrolę przekazów informacji jedynie w ramach sieci telekomunikacyjnych, co w przypadku np. telefonii internetowej nastręcza zazwyczaj poważnych trudności natury technicznej. Zdaniem tej autorki, można to ominąć poprzez odwołanie się do instytucji kontroli operacyjnej. Przepis art. 241 kpk daje pełne podstawy do stosowania podsłuchu, także poza siecią telekomunikacyjną. Mówi on bowiem o kontroli i utrwalaniu przy użyciu środków technicznych treści innych rozmów niż telefoniczne. Chodzi zatem o takie, które są prowadzone zarówno za pośrednictwem sieci telekomunikacyjnej, jak i poza nią.

Podsłuch komputerowy zarządzany jest w procesie w celu wykrycia i uzyskania dowodów dla toczącego się postępowania lub zapobieżenia w popełnieniu nowego przestępstwa. Może go zarządzić tylko sąd na wniosek prokuratora. W wypadku niecierpiącym zwłoki może to zrobić prokurator, który musi w ciągu trzech dni wystąpić do sądu o zatwierdzenie wydanego przez siebie postanowienia. Sąd w ciągu kolejnych pięciu dni rozstrzyga na posiedzeniu o zatwierdzeniu prokuratorskiej decyzji. Podsłuch komputerowy może być zastosowany tylko wtedy, gdy postępowanie dotyczy któregoś z enumeratywnie wymienionych w § 3 art. 237 kpk przestępstw, czyli:

1) zabójstwa,
2) narażenia na niebezpieczeństwo powszechne lub sprowadzenia katastrofy,
3) handlu ludźmi,
4) uprowadzenia osoby,
5) wymuszania okupu,
6) uprowadzenia statku powietrznego lub wodnego,
7) rozboju, kradzieży rozbójniczej lub wymuszenia rozbójniczego,
8) zamachu na niepodległość lub integralność państwa,

---

[7] K.J. Jakubski, *Przestępczość komputerowa. Zarys problematyki*, „Prokuratura i Prawo" 1996, nr 12, s. 42.

[8] A. Kiedrowicz, *Zagadnienie kontroli przekazów informacji w ramach telefonii internetowej*, „Prokuratura i Prawo" 2008, nr 10.

9) zamachu na konstytucyjny ustrój państwa lub jego naczelne organy albo na jednostkę Sił Zbrojnych Rzeczypospolitej Polskiej,
10) szpiegostwa lub ujawnienia tajemnicy państwowej,
11) gromadzenia broni, materiałów wybuchowych lub radioaktywnych,
12) fałszowania oraz obrotu fałszywymi pieniędzmi, środkami lub instrumentami płatniczymi albo zbywalnymi dokumentami uprawniającymi do otrzymania sumy pieniężnej, towaru, ładunku bądź wygranej rzeczowej albo zawierającymi obowiązek wpłaty kapitału, odsetek, udziału w zyskach lub stwierdzenie uczestnictwa w spółce,
13) wytwarzania, przetwarzania, obrotu i przemytu środków odurzających, prekursorów, środków zastępczych lub substancji psychotropowych,
14) zorganizowanej grupy przestępczej,
15) mienia znacznej wartości,
16) użycia przemocy lub groźby bezprawnej w związku z postępowaniem karnym,
17) łapownictwa i płatnej protekcji,
18) stręczycielstwa, kuplerstwa i sutenerstwa,
19) przestępstw określonych w rozdziale XVI Ustawy z dnia 6 czerwca 1997 r. Kodeks karny (Dz.U. Nr 88, poz. 553, z późn. zm.) oraz w art. 5–8 Rzymskiego Statutu Międzynarodowego Trybunału Karnego, sporządzonego w Rzymie dnia 17 lipca 1998 r. (Dz.U. z 2003 r. Nr 78, poz. 708), zwanego dalej „Statutem".

Zakres podmiotowy stosowania podsłuchu komputerowego określony jest bardzo szeroko. Można go zarządzić w stosunku do osoby podejrzanej, oskarżonego oraz w stosunku do pokrzywdzonego lub innej osoby, z którą może się kontaktować oskarżony, albo która może mieć związek ze sprawcą lub z grożącym przestępstwem. Takie ujęcie zakresu podmiotowego powoduje, że podsłuch komputerowy może być stosowany w praktyce wobec każdej osoby. Nietrudno bowiem wyobrazić sobie sytuacje, w których praktycznie każdy, nawet przypadkowo może mieć styczność ze sprawcą lub grożącym przestępstwem.

Podmioty prowadzące działalność w dziedzinie telekomunikacji są obowiązane umożliwić wykonanie postanowienia sądu lub prokuratora w zakresie podsłuchu komputerowego oraz zapewnić rejestrowanie faktu prowadzenia takiej kontroli. Dotyczy to wspomnianych na wstępie właścicieli infrastruktury internetowej oraz firm prowadzących działalność usługową w sieci.

Prawo do zapoznawania się z przejętymi danymi komputerowymi ma sąd lub prokurator, a w wypadkach niecierpiących zwłoki także policja.

Podsłuch komputerowy zarządzany w oparciu o przepisy kpk może rozpocząć się dopiero po wszczęciu postępowania przygotowawczego. Podzielić należy pogląd K. Marszała[9], iż brak jest formalnych przeszkód do stosowania podsłuchu komputerowego w ramach dochodzenia w niezbędnym zakresie (art. 308 kpk). Natomiast z całą stanowczością taką możliwość należy odrzucić w trakcie prowadzenia czynności sprawdzających. Bowiem czynności te w swojej istocie, nie należą do postępowania przygotowawczego i z tego powodu wykluczone jest stosowanie w ich ramach podsłuchu komputerowego.

[9] K. Marszał, *Podsłuch w polskim procesie karnym* de lege lata *i* de lege ferenda, *Problemy nauk penalnych. Prace poświęcone pani prof. Oktawii Górniok*, „Prace Naukowe Uniwersytetu Śląskiego", nr 1150, Katowice 1996, s. 350.

Kontrola i utrwalanie danych komputerowych może być zarządzona na okres 3 miesięcy z możliwością przedłużenia w szczególnie uzasadnionych wypadkach o dalsze 3 miesiące. Takie rozwiązanie nie jest prawidłowe, gdyż sztywne określenie ram czasowych często może stać w sprzeczności z dobrem postępowania, zwłaszcza w sprawach czasochłonnych i o skomplikowanym charakterze. Podobnego zdania jest K. Dudka, według której takie rozwiązanie częstokroć uniemożliwi organowi procesowemu osiągnięcie celu czynności, jakim jest zgromadzenie dowodów w sprawie[10]. Stosowanie podsłuchu komputerowego musi być zakończone niezwłocznie po ustaniu przyczyn, dla których go zarządzono, najpóźniej z upływem okresu, na który został wprowadzony.

Ogłoszenie postanowienia o kontrolowaniu przesyłanych danych teleinformatycznych osobie inwigilowanej może być odroczone na czas niezbędny ze względu na dobro sprawy, lecz nie później niż do czasu prawomocnego zakończenia postępowania. *Ratio legis* takiego zapisu jest w pełni zrozumiałe. Podsłuch może być skuteczny tylko wtedy, gdy osoba, której został założony, nie wie o tym. Odroczyć można oczywiście również postanowienie o przedłużeniu stosowania podsłuchu[11]. Uzasadnieniem dla odroczenia ogłoszenia postanowienia jest dobro sprawy. Dobro sprawy wymaga, aby informacja o stosowaniu podsłuchu nie dotarła do osoby zainteresowanej, gdyż w przeciwnym wypadku podsłuch będzie spełniać tylko funkcję środka ograniczającego swobodę komunikowania się z otoczeniem[12]. Odroczenie nie może być dłuższe niż moment prawomocnego zakończenia postępowania. W pełni należy się zgodzić z R.A. Stefańskim, który twierdzi, że chodzi tu o zamknięcie tego etapu postępowania, w którym zakończono podsłuch, a więc o zakończenie postępowania przygotowawczego lub sądowego[13]. Wprawdzie wykładnia literalna wskazuje, że chodzi o prawomocne zakończenie całego postępowania, to jednak podejrzany lub jego obrońca i tak zapoznają się z takim postanowieniem w trybie czynności zaznajamiania się z materiałami postępowania przygotowawczego. Niedołączenie takiego postanowienia do akt sprawy byłoby istotnym ograniczeniem praw oskarżonego[14].

Na postanowienie dotyczące zarządzenia podsłuchu komputerowego przysługuje zażalenie. Osoba, którą poddano inwigilacji, może domagać się zbadania zasadności oraz legalności przejmowania danych teleinformatycznych. Na postanowienie prokuratora w przedmiocie podsłuchu zażalenie rozpoznaje sąd. Zgodnie z dyspozycją art. 459 § 3 kpk zażalenie przysługuje stronom, a także osobie, której postanowienie bezpośrednio dotyczy.

Operacyjny podsłuch komputerowy mogą stosować: Policja, Agencja Bezpieczeństwa Wewnętrznego oraz Agencja Wywiadu, Centralne Biuro Antykorupcyjne, Straż Graniczna, Urzędy Kontroli Skarbowej, Służba Kontrwywiadu Wojskowego i Służba Wywiadu Wojskowego oraz Żandarmeria Wojskowa. W ustawach regulujących działalność tych służb znajdują się podstawy prawne do stosowania pozaprocesowego

[10] K. Dudka, [w:] *ibidem*, s. 76.

[11] P. Hoffmański, E. Sadzik, K. Zgryzek, *Kodeks postępowania karnego, komentarz*, t. 1, s. 866.

[12] R. Kmiecik, *Kontrola rozmów telefonicznych jako czynność procesowa i operacyjno-rozpoznawcza*, Lublin 1986, s. 223.

[13] R.A. Stefański, *Kodeks...*, t. 1, s. 1026.

[14] K. Ponikwia, *Uwagi krytyczne w stosunku do art. 239 kpk*, „Prawo i Prokuratura" 2002, nr 10, s. 143.

przejmowania transmisji teleinformatycznych[15]. Operacyjny podsłuch komputerowy jest elementem tzw. kontroli operacyjnej prowadzonej przy wykonywaniu czynności operacyjno-rozpoznawczych, podejmowanych w celu zapobieżenia, wykrycia, ustalenia sprawców, a także uzyskania i utrwalenia dowodów umyślnych przestępstw ściganych z oskarżenia publicznego. Kontrola operacyjna prowadzona jest niejawnie i polega na:

1) kontrolowaniu treści korespondencji;
2) kontrolowaniu treści przesyłek;
3) stosowaniu środków technicznych umożliwiających uzyskanie w sposób niejawny informacji i dowodów oraz ich utrwalenie, a w szczególności treści rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych.

To właśnie ta ostatnia forma kontroli operacyjnej stanowi podstawę do prowadzenia kontroli transmisji teleinformatycznych, jak również stosowania specjalistycznych technik do zdalnego podsłuchiwania (ulot elektromagnetyczny, wiązka lasera itp.). Również przy operacyjnym przechwytywaniu danych komputerowych istnieje wymóg, aby dotyczyło to postępowań o określone enumeratywnie wymienione w ustawie przestępstwa. W przypadku Ustawy o Policji dotyczy to przestępstw:

1) przeciwko życiu, określonych w art. 148–150 kodeksu karnego,
2) określonych w art. 134, 135 § 1, 136 § 1, 156 § 1 i 3, 163 § 1 i 3, 164 § 1 i 3, 166, 167, 173 § 1 i 3, 189, 200, 204 § 4, 223, 228 § 1 i 3–5, 229 § 1 i 3–5, 230 § 1, 230a § 1, 231 § 2, 232, 245, 246, 252 § 1–3, 253, 258, 269, 280–282, 285 § 1, 286 § 1, 296 § 1–3, 296a § 1, 2 i 4, 296 b § 1 i 2, 299 § 1–6 oraz w art. 310 § 1, 2 i 4 kodeksu karnego,
3) przeciwko obrotowi gospodarczemu, określonych w art. 297–306 kodeksu karnego, powodujących szkodę majątkową lub skierowanych przeciwko mieniu, jeżeli wysokość szkody lub wartość mienia przekracza pięćdziesięciokrotną wysokość najniższego wynagrodzenia za pracę, określonego na podstawie odrębnych przepisów,
4) skarbowych, jeżeli wartość przedmiotu czynu lub uszczuplenia należności publicznoprawnej przekraczają pięćdziesięciokrotną wysokość najniższego wynagrodzenia za pracę, określonego na podstawie odrębnych przepisów,
5) nielegalnego wytwarzania, posiadania lub obrotu bronią, amunicją, materiałami wybuchowymi, środkami odurzającymi lub substancjami psychotropowymi albo prekursorami oraz materiałami jądrowymi i promieniotwórczymi,
6) określonych w art. 8 Ustawy z dnia 6 czerwca 1997 r. – przepisy wprowadzające kodeks karny (Dz.U. Nr 88, poz. 554, Nr 160, poz. 1083 oraz z 1998 r. Nr 113, poz. 715),
7) określonych w art. 43–46 Ustawy z dnia 1 lipca 2005 r. o pobieraniu, przechowywaniu i przeszczepianiu komórek, tkanek i narządów (Dz.U. Nr 169, poz. 1411),
8) ściganych na mocy umów i porozumień międzynarodowych.

[15] Art. 19 Ustawy z dnia 6 kwietnia 1990 r. o Policji, art. 27 Ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 17 Ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym, art. 9c Ustawy z dnia 12 października 1990 r. o Straży Granicznej, art. 36c Ustawy z dnia 28 września 1991 r. o kontroli skarbowej, art. 31 Ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, oraz art. 31 Ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i Wojskowych Organach Porządkowych.

Pozytywnie należy ocenić zabieg ustawodawcy polegający na stworzeniu zamkniętego katalogu przestępstw, co stanowi niewątpliwie funkcję gwarancyjną dla obywateli przed nadmierną ingerencją państwa w sferę konstytucyjnego prawa do ochrony tajemnicy komunikowania się. Rozwiązanie takie przyjęto również we wspomnianym powyżej procesowym podsłuchu komputerowym. Słusznie K. Eichstaedt dostrzegł, że w katalogu – obok przestępstw bardzo niebezpiecznych dla porządku prawnego, jakimi niewątpliwie są zbrodnia zabójstwa czy też zamach na prezydenta RP – zawiera on także przestępstwa o niezbyt dużym ciężarze gatunkowym, jak chociażby przestępstwo podłączenia się do cudzego aparatu telefonicznego (art. 285 § 1 kk), zagrożone karą do 3 lat pozbawienia wolności. Może zatem powstać tendencja do nadużywania możliwości, jakie daje policji kontrola operacyjna[16].

Organy ścigania mogą sięgać po podsłuch komputerowy tylko wówczas, gdy zostanie jednoznacznie stwierdzone, że inne środki okazały się bezskuteczne, albo zachodzi wysokie prawdopodobieństwo, że będą nieskuteczne lub nieprzydatne. Takie rozwiązanie zwane jest w doktrynie *klauzulą subsydiarności*. Wedle niej sięgnięcie po podsłuch to ostateczność, co równocześnie jest hamulcem przed nieograniczoną ingerencją w sferę praw i wolności obywatelskich. Sąd przed wydaniem postanowienia o zezwoleniu na kontrolowanie transmisji teleinformatycznych powinien dokładnie sprawdzić, czy inne środki okazały się bezskuteczne, nieprzydatne lub czy istnieje *rzeczywiście* wysokie prawdopodobieństwo, że będą nieskuteczne.

Obecny kształt procedury, na podstawie której zarządza się operacyjny podsłuch komputerowy, spełnia standardy państwa prawnego. Procedura ta respektuje zarówno postanowienia Konstytucji RP (art. 49), jak i Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności (art. 8)[17]. Postanowienie o zarządzeniu operacyjnego przejmowania danych komputerowych wydaje Sąd Okręgowy na pisemny wniosek Komendanta Głównego Policji, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, lub na pisemny wniosek Komendanta Wojewódzkiego Policji złożony po uzyskaniu pisemnej zgody właściwego miejscowo Prokuratora Okręgowego. Właściwość miejscową sądu określa siedziba organu składającego wniosek. Wniosek rozpoznawany jest przez sąd jednoosobowo na posiedzeniu niejawnym. Jak widać, decyzja o operacyjnej inwigilacji komputerowej leży w rękach niezawisłego sądu, co stanowi wystarczającą gwarancję przed nadużyciami ze strony organów państwowych. Pamiętać należy, że pod rygorem poprzednich unormowań prawnych zgodę na podsłuch komputerowy wydawał Minister Spraw Wewnętrznych i Administracji.

Ramy czasowe stosowania operacyjnego podsłuchu komputerowego uregulowane zostały nieco odmiennie niż w rozdziale 26 kpk, zgodnie z którym w procesie można go stosować maksymalnie do sześciu miesięcy. W toku czynności operacyjno-rozpoznawczych można go prowadzić przez okres nie dłuższy niż trzy miesiące. Gdyby nie ustały przyczyny jego zarządzenia sąd może jednorazowo przedłużyć ten okres o dalsze trzy miesiące. W uzasadnionych przypadkach, gdy pojawią się nowe okoliczności, Sąd Okręgowy *tylko* na wniosek Komendanta Głównego Policji może przedłużyć jego stosowanie na dalszy okres. Brak jest jednak podstaw do obawy o nadużywanie tego przepisu, gdyż decyzja należy do niezawisłego sądu. Podobnie jak przy proce-

[16] K. Eichstaedt, *Zarządzenie przez sąd kontroli operacyjnej w ujęciu procesowym*, „Prokuratura i Prawo" 2003, nr 9, s. 30.

[17] Dz.U. z 1993 r., Nr 61, poz. 284–285.

sowym podsłuchu komputerowym, tak i w jego operacyjnej odmianie istnieje możliwość jego zarządzenia przez organ policji w sytuacjach niecierpiących zwłoki, jeżeli mogłoby to spowodować utratę informacji lub zatarcie albo zniszczenie dowodów przestępstwa. Komendant Główny Policji lub Komendant Wojewódzki Policji musi posiadać jedynie zgodę właściwego prokuratora. Zarządzając przechwytywanie danych komputerowych, zobligowany jest *jednocześnie* zwrócić się do właściwego sądu o wydanie stosownego postanowienia. Sąd w ciągu pięciu dni od otrzymania wniosku udziela zgody na funkcjonowanie podsłuchu. W przypadku procesowego podsłuchu prokurator zgodę musi uzyskać w ciągu ośmiu dni od jego zarządzenia. Organy ścigania oraz wymiaru sprawiedliwości korzystające z tej ścieżki muszą pamiętać, aby nie doszło do odwrócenia zasady, że to sąd decyduje o założeniu podsłuchu. Gdy sąd nie zatwierdzi decyzji o stosowaniu podsłuchu, należy go natychmiast wstrzymać, a zgromadzone dzięki niemu materiały muszą ulec protokolarnemu, komisyjnemu zniszczeniu.

W wyniku ostatnich nowelizacji tzw. ustaw policyjnych rozstrzygnięto niegdyś kontrowersyjny problem wykorzystania dowodowego materiałów zgromadzonych w wyniku operacyjnego przechwytywania transmisji teleinformatycznych. Warto wspomnieć, iż przeciwko takiemu rozwiązaniu kategorycznie występowała B. Nita, twierdząc, iż wyników podsłuchu operacyjnego nie można wykorzystać jako dowodu w procesie[18]. Identyczne stanowisko prezentował S. Waltoś, według którego wyniki podsłuchu operacyjnego nie są w stanie dostarczyć dowodu, który można by wykorzystać w postępowaniu przed sądem[19]. Problem ten rozstrzygnięto w art. 19 ust. 15 Ustawy o Policji, stanowiąc, iż w przypadku uzyskania dowodów pozwalających na wszczęcie postępowania karnego lub mających znaczenie dla toczącego się postępowania karnego Komendant Główny Policji lub Komendant Wojewódzki Policji przekazuje właściwemu prokuratorowi wszystkie materiały sporządzone podczas stosowania kontroli operacyjnej, w razie potrzeby z wnioskiem o wszczęcie postępowania karnego. W postępowaniu przed sądem, w odniesieniu do tych materiałów, stosuje się odpowiednio przepis art. 393 §1 zd. 1 kpk, który pozwala na odczytanie na rozprawie wyników operacyjnego przechwytywania transmisji teleinformatycznych. Uważam to rozwiązanie za słuszne i tylko szkoda, że zostało wprowadzone stosunkowo późno.

Analizując regulacje dotyczące podsłuchu operacyjnego, pamiętać należy o niezwykle istotnym postanowieniu Sądu Najwyższego z 26 kwietnia 2007 r.[20] Sąd Najwyższy określił jednoznacznie, że uzyskane dowody pozwalające na wszczęcie postępowania karnego lub mające znaczenie dla toczącego się postępowania karnego to dowody tylko i wyłącznie uzyskane na popełnienie przestępstw określonych w art. 19 ust. 1 (ściśle z zakresem przedmiotowym).

W sytuacji kiedy zostaną zgromadzone w czasie kontroli operacyjnej dowody popełnienia przestępstw określonych w art. 19 ust 1 Ustawy o Policji przez osobę inną, nieobjętą postanowieniem wydanym w trybie art. 19 ust. 2 Ustawy o Policji albo zostaną popełnione przez osobę objętą tym postanowieniem, ale z kolei będą dotyczyć przestępstw innych niż wskazane w tym postanowieniu mogą być wykorzystane w po-

[18] B. Nita, *Przedmiotowy zakres podsłuchu procesowego*, „Prokuratura i Prawo" 2002, nr 9, s. 61.

[19] S. Waltoś, *Proces karny – zarys systemu*, Warszawa 1995, s. 369.

[20] Postanowienie SN I KZP 6/07 z 26 kwietnia 2007 r.

stępowaniu przed sądem (w trybie art. 393 § 1 zd. 1 kpk), pod warunkiem że w tym zakresie zostanie wyrażona tzw. *następcza zgoda sądu* na przeprowadzenie kontroli operacyjnej w trybie niecierpiącym zwłoki (art. 19 ust. 3 Ustawy o Policji).

Kończąc rozważania dotyczące podsłuchu komputerowego, chciałbym krótko odnieść się do problemu konkurencji pomiędzy procesowym a operacyjnym podsłuchem komputerowym. W doktrynie zdania są podzielone odnośnie do dopuszczalności stosowania podsłuchu operacyjnego po wszczęciu procesu karnego. Taką możliwość wykluczają S. Pikulski[21] czy P. Tomaszewski[22]. Z kolei A. Hoc[23] czy R. Kmiecik[24] nie widzą zagrożenia wynikającego z niepotrzebnego „nakładania się" obu instytucji. Należy opowiedzieć się za słusznością zapatrywań prezentowanych przez tych ostatnich autorów.

Po pierwsze, operacyjny podsłuch komputerowy prowadzony jest w trybie ustaw szczególnych, takich jak np. Ustawa o Policji, która stanowi regulację niezależną od kodeksu postępowania karnego.

Po drugie, przestępstwa wymienione w kodeksie nie pokrywają się z katalogiem przestępstw umieszczonym w art. 19 Ustawy o Policji. Zatem podsłuch operacyjny ma szerszy zakres przedmiotowy i w związku z tym daje możliwości wykrycia przestępstw, których ujawnienie nie byłoby możliwe poprzez zastosowanie podsłuchu procesowego.

Po trzecie, decyzję o zastosowaniu podsłuchu komputerowego podejmuje sąd. Byłoby nielogiczne, aby prokurator po wszczęciu procesu zwracał się do policji, aby ta zaprzestała podsłuchu, skoro zezwolił na to sąd.

Po czwarte, brak jest przepisu zabraniającego stosowania obu podsłuchów jednocześnie. Wspólne ich stosowanie może tylko zwiększyć efektywność organów ścigania i wymiaru sprawiedliwości w zwalczaniu przestępczości.

---

[21] S. Pikulski, *Działania operacyjne policji*, WPP 1996, nr 12.

[22] P. Tomaszewski, *Uwagi do art. na temat „Refleksje na marginesie art.10 ustawy o UOP"*, WPP 1992, nr 3–4.

[23] S. Hoc, *Refleksje na marginesie art. 10 ustawy o UOP*, WPP 1992, nr 3–4.

[24] R. Kmiecik, *Kontrola rozmów telefonicznych jako czynność procesowa i operacyjno-rozpoznawcza*, Lublin 1996, s. 224.