Katarzyna T. Boratyńska

PODSŁUCH KOMPUTEROWY – ZAGADNIENIA WYBRANE

1. Wprowadzenie

Na przestrzeni ostatniego dziesięciolecia dokonała się światowa rewolucja w dziedzinie telekomunikacji, której wpływy spowodowały w Polsce szybką komputeryzację prawie wszystkich dziedzin życia. Intensywny rozwój łączności satelitarnej oraz sieci internetowej, stworzył zupełnie nową jakość życia (możliwość utrzymywania stałego kontaktu pomiędzy ludźmi, zakupy w sieci, dokonywanie przelewów bankowych za pośrednictwem Internetu). Jednakże w związku z szerokimi możliwościami sieci informatycznych, pojawiły się mankamenty polegające na wykorzystywaniu sieci informatycznych przez przestępców działających najczęściej w strefie przestępczości gospodarczej, gdyż w sieciach gromadzi się i przetwarza miliony danych.[1] W ramach tego typu przestępczości komputery służą przede wszystkim do organizowania i kierowania działalnością grup przestępczych, komunikowania się podczas działań niezgodnych z prawem, tworzenia baz danych i wspomagania finansowego. Zdaniem W. Paula przy pomocy sieci teleinformatycznych można dokonywać klasycznych czynów karalnych tj. handel narkotykami, przestępstwa przeciwko środowisku, handel bronią.[2] Powyższe fakty stawiają, więc przed Policją i wymiarem sprawiedliwości nowe wyzwania szczególnie związane z uzyskiwaniem i zabezpie-

1 J. Hajdukiewicz, E-przestępczość, zagrożenia dla gospodarki, Niepublikowane materiały z konferencji pt. „Przestępczość w cyberprzestrzeni", Warszawa, 15.10.2001 r.

2 W. Paul, Eine andere Betrachtungsweise der Computer Kriminalität 1991, Strafrecht 1991, s. 233.

czaniem dowodów zawartych w sieciach teleinformatycznych, dotyczących zarówno przestępstw „klasycznych" jak i przestępczości w cyberprzestrzeni. Działania ustawodawcy i organów wymiaru sprawiedliwości mają tu istotne znaczenie, gdyż jak stwierdza A. Adamski prawo jest istotnym czynnikiem kształtowania kultury informatycznej i na obecnym etapie rozwoju komputeryzacji ma do odegrania rolę, która polega na wyznaczaniu standardów „dobra" i „zła" w całkowicie nowym, pozbawionym innych odniesień normatywnych obszarze aktywności człowieka, jakim jest automatyczne przetwarzanie informacji.[3]

Nie sposób dokonać rzetelnej analizy problemów prawnych dotyczących podsłuchu komputerowego bez przynajmniej krótkiego studium zagadnień technicznych, dlatego też kolejny punkt opracowania ma na celu przybliżenie wybranych elementów problematyki stricte teleinformatycznej.

2. Podsłuch komputerowy w ujęciu technicznym

Jak wcześniej wspomniano dzisiejsze sposoby na uzyskiwanie informacji zawartych w systemach informatycznych są silnie powiązane z techniką komputerową i stanowią niezwykle poważne niebezpieczeństwo dla sieci informatycznych. W literaturze[4] podkreśla się, że podsłuch komputerowy realizowany jest najczęściej przez służby specjalne, ponieważ jedynie tego typu instytucje mają środki finansowe wystarczające na zakup szczególnego rodzaju sprzętu.[5] Niemniej jednak, mimo wysokich kosztów, coraz częściej można się spotkać z używaniem tej techniki przez konkurencyjne przedsiębiorstwa, a także zorganizowaną przestępczość, posługującą się tzw. *info–brookerami*

3 A. Adamski, Prawo karne komputerowe, Toruń 1999, s. 169 i nast.

4 B. Fischer, Przestępstwa komputerowe i ochrona informacji. Aspekty prawno–kryminalistyczne. Zakamycze 2000, s. 66; Zob. także K. J. Jakubski, Przestępczość komputerowa – zarys problematyki, Prok. i Pr. 1996, Nr 12, s. 42 i nast., K. Dudka, Podsłuch komputerowy w polskim procesie karnym – wybrane zagadnienia praktyczne, Prok. i Pr. 1999, Nr 1, s. 69 i nast.

5 Na podstawowe oprzyrządowanie składają się specjalistyczne anteny, odbiorniki pomiarowe, analizatory cyfrowe i analogowe, demodulatory.

(pośrednikami informatycznymi). Również polska Policja nie jest pozbawiona tego rodzaju środków technicznych, gdyż jak wynika z treści informacji umieszczonej na stronie internetowej serwisu IPSEC.PL, który zajmuje się bezpieczeństwem systemów komputerowych, w lutym 2001 r. Policja zakupiła urządzenia umożliwiające np. podglądanie zawartości poczty elektronicznej. Wcześniej, a mianowicie w grudniu 2000 r. Ministerstwo Spraw Wewnętrznych, planowało już sprawdzanie treści wiadomości przesyłanych siecią.[6]

Dane komputerowe można przejmować zarówno z transmisji teleinformatycznych jak i w wyniku analizy fal elektromagnetycznych emitowanych przez sprzęt komputerowy (komputery, monitory, przewody) oraz fal akustycznych generowanych przez drukarki. Działania tego rodzaju mogą być zdalne i nie pozostawiają jakichkolwiek śladów.[7]

Przejmowanie danych z transmisji teleinformatycznej jest w wysokim stopniu zbliżone do tradycyjnego podsłuchiwania rozmów telefonicznych, inaczej w literaturze nazywane jest szpiegostwem komputerowym.[8] Istnieje wiele metod podsłuchu transmisji teleinformatycznych.[9] Niektóre wymagają fizycznego dostępu do sieci, inne umożliwiają przechwytywanie informacji na odległość. Do pierwszej grupy można zaliczyć działanie polegające na stosowaniu systemów „pajęczarskich", czyli na podłączaniu, wnikaniu do central telefonicznych operatorów, oraz wykorzystywaniu łącz transmisji danych, a także na przechwytywaniu wiązki mikrofal łączności satelitarnej.[10] Z kolei przechwytywanie danych na odległość może dotyczyć haseł dostępu, osobistych numerów identyfikacyjnych (PIN) lub adresów IP (*Internet Pro-*

---

6 Prawo i Internet, www.vagla.pl.

7 Współczesne metody detekcji skrajnie słabych sygnałów obarczonych szumami i zakłóceniami o dużej intensywności umożliwiają wykrycie sygnałów o poziomach mniejszych o ponad 40 dB od poziomu szumów cieplnych w obwodach elektrycznych. B. Fischer, op. cit., s. 66. Zob. także K.J. Jakubski, op. cit., s. 42.

8 Zob. U. Sieber, Przestępczość komputerowa a prawo karne informatyczne w międzynarodowym społeczeństwie informacji i ryzyka, Przegląd Policyjny 1995, Nr 3, s.14.

9 Zob. S. Garfinkel, G. Spofford, Bezpieczeństwo w Unixie i Internecie, Warszawa 1997, s. 359 i nast.

10 R. Czechowski, P. Sienkiewicz, Przestępcze oblicza komputerów, Warszawa 1993, s. 58–59.

tocol)[11] komputerów włączonych do sieci, których znajomość warunkuje dostęp do właściwych zasobów informacyjnych systemu.[12] Obecnie zarówno Policja jak i ABW i AW mają możliwość uzyskiwania danych, przesyłanych przez sieć, za pomocą specjalnego oprogramowania m.in. przez sniffery.

Analiza fal elektromagnetycznych jest ściśle związana z prawami fizyki. W technikach komputerowych dominują wysokie częstotliwości, w zakresie których emitowane są fale elektromagnetyczne[13] (nadawać je może np. obudowa komputera). Z pomiarów zaburzeń pola elektromagnetycznego można określić następującą gradację:

- układ grafiki,
- drukarka,
- klawiatura,
- aparatura odczytu i zapisu na taśmie magnetycznej,
- inne seryjne złącza standardowe.[14]

Korzystając z metody analizy fal elektromagnetycznych bezpośrednie działania podsłuchowe można prowadzić z bezpiecznej, nawet kilkusetmetrowej odległości sposobem analogowym. Odtworzenie następuje wizualnie sposobem analogowym lub cyfrowym; bezpośrednio (*on–line*) w miejscu podsłuchu lub rozłącznie (*off–line*) np. w pracowni.[15]

---

11 Numer (adres) IP składa się z czterech członów. Każdy z nich może przybierać wartość od 0 do 255 np. 191.123.240.255. Ustalenie numeru IP pozwala na identyfikację komputera w sieci, gdyż każdy człon adresu oznacza, co innego. Pierwszy oznacza sieć na danym kontynencie, kolejny sieć w danym kraju, następny sieć w danym mieście, a ostatni konkretny komputer w tej sieci. Zob. także M. Kliś, A. Stella–Sawicki, Identyfikacja użytkownika komputera na podstawie vogów cyfrowych, Prok. i Pr. 2001, nr 78, s. 52.

12 A. Adamski, op. cit., s. 58.

13 Fala elektromagnetyczna jest to zaburzenie pola elektromagnetycznego polegające na okresowych zmianach pola elektrycznego i magnetycznego, rozchodzące się w przestrzeni z prędkością 30 000 km/s, H. Chmielewski, I. Baran, S. Skupiński, Ilustrowany słownik techniczny, Warszawa 1978, s. 90.

14 H.G. Wolf, Zagrożenie bezpieczeństwa wynikające z kłopotliwego promieniowania – wprowadzenie przedsięwzięć ochronnych (w:) Materiały seminarium trzeciego Forum Teleinformatyki, Legionowo 22–23 października 1997 r., s. 47.

15 Ibidem, s. 49.

Kolejnym wymagającym krótkiego komentarza jest używanie Internetu. Korzystając z Internetu nie każdy z użytkowników zdaje sobie sprawę z tego, że komunikowanie się za pomocą sieci komputerowych oraz przesyłanie wiadomości (*e–mail*) pocztą elektroniczną stwarza wysokie ryzyko naruszania poufności[16] wysyłanych informacji, gdyż z sieci może jednocześnie korzystać wielu użytkowników.[17]

Jak daleko może sięgać inwigilacja internautów można było przekonać się na podstawie sytuacji zaistniałej w Stanach Zjednoczonych po ataku terrorystycznym na WTC (*World Trade Center*), mającym miejsce 11 września 2001 r. Agenci FBI zwrócili się do największych dostawców usług internetowych (*Internet Service Providers–ISP*) o uzyskanie dostępu do danych zgromadzonych na serwerach. Sprawdzano również bazy Hotmail, ze szczególnym uwzględnieniem konkretnych, podejrzanych adresów. FBI zażądała również od ISP zainstalowania na ich komputerach specjalnego systemu – Carnivore (Mięsożerca)[18], którego głównym zadaniem jest monitorowanie przepływających przez sieci danych (w ten sposób można np. kontrolować wysyłane e–maile).[19]

Kontrowersyjnym systemem jest także projekt Echelon, o którym pierwsze informacje można było usłyszeć w 1988 r.[20] Ciekawostką jest,

---

16 Poufność (ang. confidentiality), oznacza wyłączny dostęp osób uprawnionych do określonych informacji i ochronę danych przed ich odczytaniem lub kopiowaniem przez osoby do tego nieupoważnione. Według Wytycznych OECD z 1992 roku poufność charakteryzuje „właściwość danych i informacji, polegającą na ujawnianiu ich wyłącznie uprawnionym podmiotom i na potrzeby określonych procedur, w dozwolonych przypadkach i w dozwolony sposób.

17 A. Adamski, op. cit., s. 57.

18 Carnivore wykorzystuje oprogramowanie typu sniffing (dosł. wąchać), które umożliwia przechwytywanie pakietów danych, hostów oraz innych ważnych informacji przekazywanych miedzy użytkownikami. Sniffery posługują się różnymi technikami dla zdobycia informacji np. keystroke sniffer przechwytuje i zapisuje sygnały klawiatury, www.wired.com/news/politics/.

19 P. Kępiński: Internetowa prywatność a uprawnienia organów ochrony państwa, www.vagla.pl.

20 W początkach 1988 roku Margaret Newsham, zatrudniona wcześniej w należącej do NSA bazie Menwith Hill, położonej w pobliżu Harrogate na północy Anglii (hrabstwo Yorkshire), zdecydowała się złożyć w Kongresie skargę na szereg nadużyć, jakie jej zdaniem miały miejsce w tajnych amerykańskich projektach wywiadowczych. Przy tej okazji wyszło na jaw, że w bazie owej podsłuchiwano rozmowy telefoniczne jednego z amerykańskich senatorów, podczas gdy prawo amerykańskie wyraźnie zabrania agencjom wywiadowczym tego państwa szpiegowania swoich własnych obywateli. J. Rafa, Złowrogi Echelon, PCkurier 2000, Nr 10, www.pckurier.pl.

że dotychczas władze amerykańskie nie potwierdziły oficjalnie istnienia tego sytemu. Pierwotna wersja systemu Echelon służyła analizowaniu danych przechwyconych przez dwie stacje nasłuchowe, zbudowane w celu podsłuchiwania transmisji przesyłanych przez system satelitów telekomunikacyjnych Intelsat – jedna z tych stacji znajdowała się w miejscowości Morwenstow w Anglii, druga w Yakima na północnym zachodzie USA. Skuteczność systemu w wyławianiu interesujących NSA informacji okazała się większa, niż się spodziewano: zdecydowano zatem o rozbudowie systemu. Echelon rozrósł się o nowe urządzenia nasłuchowe i nowe ośrodki komputerowe, analizujące przechwycone dane; i rozwój ten trwa do dnia dzisiejszego. Przypuszcza się, że obecnie system ten jest zdolny do przechwytywania i analizowania większości (według niektórych nawet 90%) połączeń telefonicznych, teleksowych, faksowych i internetowych w ruchu międzynarodowym, a być może w niektórych państwach także połączeń krajowych.[21] Echelon stał się również przedmiotem zainteresowania ze strony Parlamentu Europejskiego. Na zlecenie Parlamentu przygotowano raport o metodach i środkach technicznych, używanych do podsłuchu różnego rodzaju kanałów łączności w ramach projektu Echelon, jak również różnych innych tajnych projektów rozmaitych agencji wywiadowczych.[22]

21 J. Rafa, op. cit., www.pckurier.pl.

22 Raport Interception Capabilities 2000 przygotowany przez Duncana Campbella, Raporty, a jest ich pięć ujawniają fakty wykorzystywania tego systemu np. do szpiegowania działalności organizacji pacyfistycznych i charytatywnych takich jak chociażby Amnesty International, znanych osobistości jak np. księżna Diana, czy europejskich firm biorących udział w przetargach na duże kontrakty zagraniczne (istnieje podejrzenie, że informacje uzyskane z podsłuchu mogły być następnie przez przedstawicieli agencji rządowych USA przekazywane firmom amerykańskim, które dzięki temu zyskiwały przewagę w negocjacjach). Nic też dziwnego, że im więcej wiadomości na temat Echelona przenika do opinii publicznej, tym silniejsze stają się protesty przeciwko temu systemowi. W szczególności niezadowolone z ich szpiegowania są kraje europejskie, a ich niezadowolenie zwraca się głównie przeciwko Wielkiej Brytanii, która będąc członkiem UE równocześnie uczestniczy w Echelonie. Już kilka razy Echelon był przedmiotem debaty Parlamentu Europejskiego (po raz pierwszy w 1998 r., a ostatnio w lutym 2000 r.). Sporządzono na ten temat pięć raportów, które dostępne są m.in. na internetowej stronie Parlamentu Europejskiego. Komisja Europejska odrzuciła jednak żądania Parlamentu podjęcia działań w tej sprawie, uzasadniając odmowę tym, iż nie ma dowodów rzeczywistego poniesienia strat finansowych przez jakąkolwiek firmę europejską na skutek działalności Echelona. „To tylko pogłoski, a my się nie zajmujemy pogłoskami, lecz faktami" – odpowiedział komisarz Frits Bolkestein. Ostrożne stanowisko Komisji tłumaczy być może częściowo fakt, że – jak ujawniła brytyjska organizacja Statewatch – już od roku 1991 prowadzone są tajne rozmowy między państwami Unii Europejskiej w sprawie utworzenia podobnego systemu w Europie, J. Rafa, op. cit., www.pckurier.pl.

W odróżnieniu od Carnivore, Echelon ma bardziej światowy charakter. W projekt ten zaangażowane są następujące kraje: Stany Zjednoczone, Wielka Brytania, Australia i Nowa Zelandia. Przedsięwzięcie to opiera się na pracy 120 satelitów, które mają możliwość przechwytywania i rejestrowania każdej formy elektronicznej komunikacji, a w szczególności rozmów telefonicznych, faksów, telefaksów, e–maili. Uzyskane w ten sposób informacje są przekazywane do komputerów wyposażonych w bardzo pojemne dyski i wysoką moc obliczeniową, które dzięki specjalnemu oprogramowaniu – „Dictionary" (dosł. słownik) poddawane są wstępnej analizie. Głównym elementem oprogramowania są specjalne wyszukiwarki internetowe, które reagują na konkretne słowa np. ibn Laden, wąglik, bomba, terroryzm, etc.[23] Uzyskane informacje cechujące się wysokim prawdopodobieństwem są przekazywane do dalszej analizy dokonywanej przez specjalistów elektronicznego wywiadu. W praktyce każdego dnia analitycy są „zasypywani" ogromnymi ilościami danych.[24]

Największą różnicą między systemem Carnivore a Echelon jest rozmiar zasięgu, który w przypadku Carnivore ma charakter bardziej „lokalny" – dotyczy w większym stopniu społeczności amerykańskiej. Jednakże biorąc pod uwagę fakt polegający na tym, że Internet jest siecią międzynarodową, Carnivore może także wykraczać poza granice Stanów Zjednoczonych. Z kolei Echelon jest systemem globalnym, który potrafi wychwycić informację z najodleglejszych zakątków kuli ziemskiej, a szczególnie niebezpieczny jest dla europejskich przedsiębiorstw. [25]

Pomimo różnic oba systemy nie potrafią uporać się z informacjami zakodowanymi. Jedyną, zatem możliwością zachowania tajemnicy informacji jest używanie kryptografii.

---

23 W ostatnim okresie FBI prowadzi próby nad zastosowaniem komputerowego podsłuchu reagującego na konkretne słowa–hasła. J. Kenny, H. More, Principles of Investigation, New York 1994, s. 261.

24 Por. także Nick Hager, Secret Power, New Zealand's Role in the International Spy Network 1996, www.fas.org/irp/eprint/sp.

25 Podejrzewa się, ze przez elektroniczny podsłuch europejskie firmy straciły na rzecz konkurencji zza oceanu kilka dochodowych kontraktów (np. Airbus przegrał z Boeningiem zamówienia na samolot do Arabii Saudyjskiej. W związku z tym Komisja Europejska zwróciła się oficjalnie do władz w Londynie i Waszyngtonie z żądaniem wyjaśnień. J. Bielecki, Ameryka śledzi, Rzeczpospolita 2000, Nr 46, www.rzeczpospolita.pl.

3. Podsłuch komputerowy – zagadnienia prawne

Jak dotąd polskie ustawodawstwo nie uregulowało w odrębny, kompleksowy sposób dowodów generowanych komputerowo. Podstawę prawną podsłuchu komputerowego można jednakże wywieść z treść art. 241 kpk., zgodnie z którym przepisy zawarte w rozdziale 26 kpk. stosuje się odpowiednio do kontroli oraz utrwalania, przy użyciu środków technicznych treści przekazów informacji innych niż rozmowy telefoniczne. Wniosek z tego, że art. 241 kpk. stosować się będzie odpowiednio do Internetu i tzw. podsłuchu elektronicznego dotyczącego przede wszystkim poczty elektronicznej oraz IRC, ICQ itp. Jednakże przypadki, w których można przeprowadzić kontrolę i utrwalanie rozmów zawarto w katalogu zamkniętym (art. 237 § 3 kpk.), pozostawiając poza nim większość przestępstw, których można dokonać za pomocą techniki komputerowej, co automatycznie wyłączyło w odniesieniu do tych przestępstw zastosowanie podsłuchu komputerowego.

Trafnie zauważa W. Daszkiewicz[26], że w ramach art. 241 kpk. będzie można przejmować dane komputerowe za pomocą transmisji teleinformatycznych czy analizy fal elektromagnetycznych emitowanych przez sprzęt komputerowy oraz fal akustycznych emitowanych przez drukarki, ponieważ pozwalają one – przy użyciu odpowiedniej aparatury na przejęcie i utrwalenie informacji, oczywiście same fale nie mają w żadnym wypadku charakteru treści przekazu informacji.[27] Podkreślić należy, że pogląd ten znalazł swoje potwierdzenie w nowelizacji kpk. z 10 stycznia 2003 r. skutkiem tego art. 241 kpk. w obecnym brzmieniu daje podstawę do stosowania kontroli i utrwalania rozmów nie tylko telefonicznych lub innych prowadzonych wyłącznie za pośrednictwem połączeń sieciowych, ale także innych rozmów lub przekazów informacji, w tym korespondencji przesyłanej drogą telefoniczną.

26 W. Daszkiewicz, Prawo karne procesowe. Zagadnienia ogólne, Poznań 2001, s. 155.

27 Odmienny pogląd dotyczący przejmowania danych komputerowych przy pomocy transmisji teleinformatycznych etc. przedstawia K. Dudka, która uznaje, że tego rodzaju czynności dozwolone są podczas podsłuchu pozaprocesowego. Zob K. Dudka, Kontrola korespondencji i podsłuch w polskim procesie karnym, Lublin 1998, s. 69 i nast.

Trzeba podkreślić, że specyfika podsłuchu komputerowego polega w szczególności na tym, że dokonuje się go wyłącznie w sieci komputerowej, a więc dotyczy informacji znajdujących się w danym momencie, w sieci teleinformatycznej. Nieodmiennie wobec tego, wiąże się z tym pojęcie danych ruchowych (*traffic data*), które zostało zdefiniowane w projekcie Dyrektywy Parlamentu i Komisji Europejskiej dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze komunikacji elektronicznej, jako „wszelkie dane przetwarzane podczas lub w celu transmisji przekazu informacji za pośrednictwem sieci teleinformatycznej."[28] Ponadto określenie danych ruchowych formułuje w art. 1d Konwencja Rady Europy dotycząca cyberprzestępczości, zgodnie z którą „dane dotyczące ruchu" oznaczają dowolne dane informatyczne odnoszące się do komunikowania się za pomocą systemu informatycznego, wygenerowane przez system informatyczny, który utworzył część w łańcuchu komunikacyjnym wskazując swoje pochodzenie, przeznaczenie, ścieżkę, czas, rozmiar, czas trwania lub rodzaj danej usługi.[29]

Dane ruchowe mogą występować zarówno w formie dynamicznej (faza transmisji), jak i w postaci statycznej (przechowywanie) i w zależności od tego mogą podlegać odmiennemu reżimowi czynności procesowych.[30] Wykorzystanie danych ruchowych w formie dynamicznej (podsłuch transmisji z filtrowaniem pakietów IP np. według kryterium adresu) może posłużyć do ustalenia sprawców ataków typu Denial of Service.[31] Biorąc pod uwagę to, że w przypadku poczty elektronicznej, dane ruchowe stanowią integralny element przekazu informacji, ich przechwytywanie będzie wymagało uzyskania zgody sądu.

---

28 Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector of 12 July 2000 COM (2000), Document 500PC0385.

29 Convention on Cyber–Crime. European Committee on Crime Problems (CDPC). Committee of Experts on Crime in Cyber–Crime, Strasbourg 11 May 2001k, Article 1d.

30 Zob. A. Adamski, op. cit., s. 192 i nast.

31 Atak polegający na uniemożliwieniu świadczenia usług przez zaatakowany komputer poprzez obciążenie jego krytycznych zasobów (czas procesora, pomięć operacyjna, pasmo transmisyjne w sieci). A. Adamski, M. Koziński, Dane ruchowe – elektroniczny trop cyberprzestępcy: aspekty techniczne i prawne, Materiały z konferencji pt. „Techniczne aspekty przestępczości teleinformatycznej." WSPol Szczytno 2001, s. 34–35.

Przejęcie danych poprzez wejście do sieci i zastosowanie urządzeń podsłuchowych nie sprawia większych trudności, o ile nie jest szyfrowane, gdyż najczęściej przekaz dokonywany jest za pomocą linii telefonicznych. Trzeba podkreślić, że uzyskiwanie i rejestrowanie informacji odbywa się w czasie rzeczywistym podczas przesyłania siecią telekomunikacyjną. Stąd też, jak słusznie uważa K. Dudka, jeżeli za rozmowę telefoniczną uznamy wszelki przekaz informacji przy użyciu sieci telekomunikacyjnej, to musimy uznać, że jest to łączność niezależna od rodzaju użytego odbiornika (telefon, komputer), a tym samym nadać podsłuchowi komputerowemu walor podsłuchu telefonicznego ze wszystkimi wynikającymi z tego implikacjami. Dopiero w sytuacji, gdy łącza sieci komputerowej nie będą wykorzystywały linii telefonicznych do przekazywania informacji pomiędzy serwerami można będzie mówić o podsłuchu *stricte* komputerowym. [32]

Ponadto w przypadku podsłuchu komputerowego pojawia się problem ustalenia danych osobowych osób wykorzystujących sieci teleinformatyczne do porozumiewania się. Trudność polega na tym, że samo wejście do Internetu i przesłanie wiadomości nie daje podstaw do zidentyfikowania osoby, która dokonała tychże czynności. Nawet w przypadku, gdy pod wiadomością widnieje imię i nazwisko, nie przesądza to o pochodzeniu danej wiadomości z tego źródła, gdyż informację taką mogła przesłać zupełnie inna osoba, posługując się cudzym nazwiskiem.[33] Problem ten zwiększa się jeszcze w sytuacji, gdy wiadomość jest zakodowana. Pomimo przełamania szyfru i poznania treści wiadomości praktycznie nie ma żadnych szans na indywidualizację osoby, która przesłała daną wiadomość.[34] Co najwyżej, w przypadku zamontowania urządzenia podsłuchowego przy wyjściu (na linii) konkretnego komputera będziemy mogli ustalić numer konkretnego

32 K. Dudka, op. cit., s. 71.

33 S. Ziółkowski, Nowoczesne technologie przetwarzania informacji, a projektowane zmiany procedury karnej, (w:) Prawne aspekty nadużyć popełnianych z wykorzystaniem nowoczesnych technologii przetwarzania informacji. Przestępczość komputerowa. Materiały z międzynarodowej konferencji naukowej, (red.) A. Adamski, Poznań 1994, s. 186.

34 Np. mechanizmy protokołu TCP/IP pozwalają na fałszowanie adresu IP nadawcy pakietu, komputer, do którego adresy te docierają (urządzenie podsłuchowe), interpretuje je jako wysłane przez inny komputer, niż to miało miejsce w rzeczywistości. Zob. B. Fischer, op. cit., s. 113.

komputera, z którego nadana została wiadomość, ale nadal bez potwierdzenia tożsamości osoby.

Przy każdorazowym połączeniu z Internetem za pomocą modemu, operator sieci przydziela użytkownikowi konkretny numer IP. Trzeba podkreślić, ze nie jest to numer stały, a przydzielany jest tylko na czas bytności w sieci. Dlatego też, aby określić, jaki komputer korzystał z danego IP bardzo istotnym jest czas wejścia i wyjścia z sieci użytkownika. Należy, więc przyporządkować datę i godzinę, korzystającemu z takiego IP, na podstawie billingu wskazującego, jaki numer i kiedy łączył się z danym numerem (umożliwiającym wejście do Internetu).[35] Odczytanie konkretnego adresu IP odbywa się z wykorzystaniem logów cyfrowych, które są niczym innym, jak informacjami mającymi swoje źródło na serwerze. Na ich podstawie można zorientować się, że np. komputer o adresie IP 231.127.46.89 przebywał w sieci od godz. 11.30 do 12.00, na stronie oraz dokonał operacji polegającej na skopiowaniu artykułu dotyczącego bezpieczeństwa w Internecie. Odpowiednia analiza logów cyfrowych pozwala czasem na zidentyfikowanie sprawcy np. hackingu (włamanie do systemu), ale nie zawsze logi będą miały wartość dowodową. Jak trafnie stwierdzają M. Kliś i A. Stella–Sawicki, logi jako dane cyfrowe przechowywane na nośnikach wielokrotnego zapisu – mogą być za pomocą odpowiednich narzędzi modyfikowane i preparowane bez żadnych ograniczeń.[36] Dlatego też najważniejszą kwestią jest stworzenie jednoznacznej procedury uzyskiwania i zabezpieczania logów cyfrowych, od niej zależy bowiem prawdziwość informacji zawartych w logach. Wydaje się, że najbardziej funkcjonalnym rozwiązaniem byłoby użycie specjalnych urządzeń do zapisu, np. płyt optycznych jednorazowego użytku, na których niemożliwa jest modyfikacja raz zapisanych danych cyfrowych lub też wydzielenie specjalnego serwera, który zajmowałby się magazynowaniem danych przesyłanych do niego szyfrowanymi łączami. Przedstawione metody mają na celu przede wszystkim odizolowanie administratora jako osoby, która jest najbliżej tych danych, od możliwości ingerencji.

35 M. Kliś, A. Stella–Sawicki, op. cit., s. 53.

36 Idem, s. 53.

Problematyka zabezpieczenia niejednokrotnie była tematem obrad Rady Europy. W załączniku do Zalecenia Komitetu Ministrów Rady Europy nr R(95)13 pkt 13 z 1995 r. znajduje się stwierdzenie, że „ogólna potrzeba zbierania i okazywania dowodów elektronicznych w sposób, który najlepiej zapewni i wykaże ich integralność i autentyczność, zarówno w celu wewnętrznego oskarżania, jak i współpracy międzynarodowej, winna być zauważona…" W zaleceniach Rady Europy podkreśla się, że dane zapisane na nośniku komputerowym nie są rzeczą i nie spełniają cech przypisanych przedmiotom, dlatego też nie ma podstaw prawnych stosowania do nich przepisów dotyczących przeszukania bądź zatrzymania rzeczy.[37] Jednakże stwierdzenia te nie przemawiają zbytnio do wyobraźni wymiaru sprawiedliwości. Największym problemem jak słusznie podkreśla P. Krawczyk[38] jest przyzwyczajenie organów ścigania do materialności materiału dowodowego. Złudne, bo faktycznym dowodem może być informacja zapisana na twardym dysku, a nie sam dysk, który jest tylko „kawałkiem elektroniki". Podobnie, jak dowodem jest raczej odcisk palca skopiowany na odpowiedni nośnik, a nie na przykład całe drzwi z klamką, na której ten odcisk znaleziono. Jednakże z przykrością należy stwierdzić, że ustawodawca przy tworzeniu nowej procedury karnej nie wziął pod uwagę rekomendacji zawartych w zaleceniach. Brak uregulowań w tej materii wypełniła ustawa z 10 stycznia 2003 r. nowelizująca kpk., dodano bowiem art. 236a kpk., zgodnie z którym przepisy o zatrzymaniu i przeszukaniu stosowane są odpowiednio do dysponenta i użytkownika systemu informatycznego w zakresie danych przechowywanych w tym systemie lub nośniku znajdującym się w jego dyspozycji lub użytkowaniu, w tym korespondencji już przesyłanej pocztą elektroniczną.

Warto jeszcze rozpatrzyć przechowywanie, przetwarzanie czy też utrwalanie danych z logów cyfrowych mając na względzie ochronę prawa do prywatności. Czy czynności dokonywane w odniesieniu do logów cyfrowych stanowią naruszenie tego prawa. Wydaje się, że na to

37 A. Adamski, Komputer w paragrafach, Rzeczpospolita 1996, Nr 254, s. 16, także B. Fischer, Odpowiedzialność karna, PiŻ 1997, Nr 50, s. 11.

38 P. Krawczyk, Zdrowy rozsądek, a zabezpieczanie sprzętu komputerowego, www.hedera.linuxnews.pl/news/2001/06/19/long/419.html.

pytanie należy odpowiedzieć przecząco, ponieważ brak tu czynnika osobowego, jak również nie można mówić o kontroli komunikacji w ujęciu treści. Oczywiście polemikę może wywołać kwestia szczegółowości tych danych, które są przechowywane na serwerze w postaci cyfrowej, ale przyjętym standardem jest zapisywanie tylko tego, jaki IP połączył się z innym IP oraz data numeru portu, na którym prowadzona była komunikacja. Ażeby naruszyć art. 47 Konstytucji RP niezbędne jest powiązanie konkretnego adresu IP ze zindywidualizowaną osobą, a takie dane w logu cyfrowym się nie znajdują. Oczywiście informacje takie można uzyskać poprzez zwrócenie się do dostawcy usług internetowych o podanie danych osobowych użytkownika konkretnego numeru IP, z tym, że może to nastąpić w określonych przypadkach, gdyż dane te są chronione przez ustawę o ochronie danych osobowych.[39]

Trzeba także odpowiedzieć na pytanie czy rejestracja danych zawartych w logach cyfrowych stanowi podsłuch w rozumieniu przepisów kpk. Wydaje się, że treść art. 241 kpk. odnosi się wprost do art. 237 kpk., który mówi bezpośrednio o utrwalaniu treści oraz o kontroli rozmów. Należy, więc stwierdzić, że gromadzenie danych w postaci informacji odnoszącej się jedynie, co do samej formy przekazu nie jest podsłuchem. Brakuje tu ustawowych znamion podsłuchu, jakimi są utrwalanic i kontrola przekazu.

Zagadnieniem, którego nie sposób pominąć przy rozważaniu problematyki podsłuchu komputerowego jest kwestia monitorowania Internetu. W ustawodawstwach krajów zachodnich pojawiły się unormowania pozwalające na podsłuchiwanie sieci Internetowych, a ich powstanie nie jest czymś wyjątkowym. Nakaz zainstalowania systemu do selektywnego podsłuchiwania informacji przesyłanych Internetem uchwalił parlament brytyjski. Przepisy zawarte w Regulations of Investigators Powers Act nakazują instalację u wszystkich brytyjskich providerów, systemu GTAC. System ten ma umożliwiać służbom specjalnym selektywne podsłuchiwanie informacji przesyłanych Internetem.[40]

---

39 Ustawa o ochronie danych osobowych, Dz.U. Nr 133, poz. 883, z 1997 r. z późn. zm.

40 Regulation of Investigators Powers Act 2000, www.homso.gov.uk/acts2000/20000023.htm.

Również w Rosji operatorzy telekomunikacyjni mają obowiązek instalowania na własny koszt urządzeń do podsłuchu dowolnych połączeń jest to system SROM-2.[41]

Jeśli zaś chodzi o ustawodawstwo polskie to sytuacja przedstawia się następująco. W dniu 24 stycznia 2003 r. zostało wydane rozporządzenie w sprawie wykonywania przez operatorów zadań na rzecz obronności bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.[42] Podstawą wydania tego rozporządzenia jest art. 40 ustawy o prawie telekomunikacyjnym, który nakłada na operatorów obowiązek świadczenia takich zadań, a szczegółowe regulacje pozostawia decyzji ministra właściwego do spraw łączności po dokonaniu przez niego konsultacji z Ministrem Obrony Narodowej, Ministrem Sprawiedliwości, ministrem właściwym do spraw wewnętrznych, ministrem właściwym do spraw finansów publicznych, po zasięgnięciu opinii Szefa Urzędu Ochrony Państwa (obecnie Szefa Agencji Bezpieczeństwa Wewnętrznego).

Rozporządzenie wymaga, aby wszyscy krajowi operatorzy telekomunikacyjni oraz operatorzy Internetu zainstalowali na własny koszt urządzenia oraz niezbędne łącza, pozwalające służbom śledczym na monitorowanie w dowolnym momencie całego ruchu przechodzącego przez danego operatora, który miał na dodatek obowiązek archiwizować przechwycone dane na użytek uprawnionych organów.[43] Zebrane dane podczas monitorowania sieci mają być dostępne dla uprawnionych organów – Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Żandarmerii Wojskowej, Policja i wywiadowi skarbowemu – w przeciągu całej doby przez okres 12 miesięcy (§ 5 pkt 7 rozporządzenia).

Obowiązujące rozporządzenie jeszcze w fazie projektu[44] zostało jednogłośnie skrytykowane przez obradujące w dniu 13 stycznia 2001 r.

41 Koszt spełnienia tych wymagań sięga niekiedy 30 tys. dolarów, a zainstalowanie podsłuchu jest jednym z warunków otrzymania koncesji na usługi telekomunikacyjne, www.arek.ispec.pl/snews/171.html.

42 Rozporządzenie Ministra Infrastruktury w sprawie wykonywania przez operatorów zadań na rzecz obronności bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, Dz.U. Nr 19, poz. 166 z 2003 r.

43 Por. E. Ura, Prawo telekomunikacyjne. Komentarz, Warszawa 2001, s. 68.

44 Pierwszy projekt tego rozporządzenia otrzymała 19 grudnia 2000 r. Polska Izba Informatyki i Telekomunikacji (PIIT), www.vagla.pl/projekt-mswia.htm.

Walne Zgromadzenie Członków Stowarzyszenia ISOC Polska (Internet Society Poland). W podjętej uchwale ISOC wskazało na negatywne cechy proponowanego rozwiązania, a mianowicie na brak gwarancji poszanowania konstytucyjnego prawa do ochrony tajemnicy komunikowania się, nadto że w rozporządzeniu nakazane są rozwiązania techniczne, które uniemożliwiają sądowy nadzór nad inwigilacją (§ 7 i § 14 projektu rozporządzenia, obecnie § 5 pkt 2 oraz § 9 rozporządzenia). Jak wiadomo jedną z wolności osobistych jest wolność i ochrona tajemnicy komunikowania się. Może być ona ograniczona jedynie w przypadkach i w sposób określony w ustawie, a nie w rozporządzeniu. Zgodnie zaś z art. 31 Konstytucji RP ograniczenie wolności i swobód konstytucyjnych może nastąpić wyłącznie w sytuacjach, kiedy jest to konieczne w demokratycznym państwie prawnym dla bezpieczeństwa, porządku publicznego, ochrony środowiska, zdrowia, moralności publicznej albo też wolności i praw innych osób. Ograniczenie to nie może odnosić się, co do samej istoty wolności i prawa, a tak należy zinterpretować monitorowanie wszystkich informacji przepływających przez Internet, w tym także dane dotyczące umów zawieranych *on–line*. Omawiane rozporządzenie wyłącza wolność komunikowania się i tajemnicę w Internecie. Ponadto zdaniem ISOC proponowane rozwiązania techniczne umożliwiają masową zautomatyzowaną inwigilację obywateli w Internecie. Również uniemożliwiona zostaje sejmowa (budżetowa) kontrola nad faktycznymi rozmiarami i zakresem prowadzonej inwigilacji, ponieważ koszty związane z zakupem systemów temu służących ponosi operator telekomunikacyjny.

W uchwale ISOC podkreślała także, że informacje zgromadzone podczas inwigilacji w Internecie nie mają mocy dowodowej w postępowaniu sądowym. Nie ma, więc racjonalnych przesłanek do ich gromadzenia, gdyż w świetle prawa nie mogą być one wykorzystane zgodnie z obowiązującymi przepisami, zaś koszty budowy systemu powszechnej inwigilacji ma ponosić operator i jego klienci, czyli każdy dostawca usług internetowych musiałby na własny koszt zainstalować urządzenia umożliwiające uprawnionym organom (policji, służbom specjalnym) przechwytywanie dowolnych informacji. Twórca projektu wchodzi tym samym w kompetencje Sejmu narzucając operatorom, a w konsekwencji całemu społeczeństwu obowiązek podatkowy na „rzecz inwigilacji".

Jeżeli zaś chodzi o techniczną realizację zautomatyzowanego systemu inwigilacji to jest ona technicznie możliwa, ale nie ma możliwości kontroli sposobu i zakresu jego wykorzystania, a także wiarygodności zgromadzonych tym sposobem danych.[45] Musiałyby to być urządzenia sterowane z zewnątrz, poza jakąkolwiek obsługą operatora, który byłby zobowiązany utrzymywać dodatkowe łącze zlokalizowane w miejscu wskazanym przez służby specjalne. Urządzenia musiałyby być umieszczone w takim miejscu systemu, by mogły przechwycić informacje jeszcze przed ich zaszyfrowaniem. Stworzenie takiego systemu umożliwiłoby podsłuchiwanie 24 godziny na dobę. Podsłuch byłby niejawny; nie byłoby wiadomo, które informacje przechwyciły służby specjalne i w jakim celu to zrobiły.[46]

Oczywistym jest, że ustawodawstwo nie nadąża za rozwojem komputeryzacji, dlatego też skutecznym rozwiązaniem byłoby wprowadzenie unormowań nie tylko w formie ustaw, ale także i innych regulacji prawnych takich jak: regulaminy czy instrukcje. Dzięki temu skróciłby się czas przeznaczony w razie konieczności na nowelizację.

Ponadto przy praktycznym wykorzystywaniu informacji uzyskanych podczas podsłuchu komputerowego pojawia się również problem wynikający z rozwoju informatycznego. Chodzi tu o utrudnienia powstające w wyniku zapewniania dostępu do systemów komputerowych i zabezpieczaniu w celach dowodowych informacji zawartych w tych systemach, przeszukaniu tych systemów, czy elektroniczną obserwacją systemów. Obecnie najlepiej funkcjonuje i jest najbardziej rozpowszechniona procedura podsłuchu transmisji i nagrywania kontaktów telekomunikacyjnych w oparciu o tradycyjne rozwiązania, czyli pośrednio.[47]

45 Uchwała z dnia 13 stycznia 2001 r. Walne Zgromadzenie Członków Stowarzyszenia ISOC Polska (Internet Society Poland),

46 G. Skowron, Permanentna inwigilacja, Dziennik Polski z 22.12.00 r., Por. też, Następca RIP SROM–2, czyli podsłuch po polsku, T. Świderek, Ofensywa krasnoludków, Rzeczpospolita 2001, Nr 15.

47 Zob. także B. Fischer, op. cit., s. 185–186.