Szymon Wesołowski[*]

Przechwytywanie przekazów telekomunikacyjnych na podstawie Konwencji z 2000 r. o wzajemnej pomocy w sprawach karnych między państwami członkowskimi Unii Europejskiej

Rewolucja informacyjna

Ostatnie lata XX wieku upłynęły pod znakiem niezwykłego postępu technologii służących przetwarzaniu informacji oraz ich przesyłaniu, który wywarł bardzo głęboki wpływ na społeczeństwa praktycznie wszystkich państw świata. Ludzkość uzyskała bowiem możliwość niemal nieograniczonego komunikowania się oraz dostęp do ogromnej ilości informacji. Zmiany objęły wszystkie sfery aktywności człowieka – coraz bardziej uzasadnione jest już dziś twierdzenie o narodzinach globalnego „społeczeństwa informacyjnego" (*information society*).[1]

Szybki rozwój technologii informacyjno-komunikacyjnych, poza niewątpliwymi korzyściami w sferze społecznej czy gospodarczej, przynosi jednak również zagrożenia związane z wykorzystywaniem nowych technologii w celu popełniania przestępstw. Zagrożenia te należy postrzegać w dwóch aspektach: po pierwsze – nowe technologie mogą posłużyć popełnianiu dobrze znanych rodzajów przestępstw (ułatwiając m.in. ich planowanie, przygotowanie, koordynację), po drugie – mogą one być wykorzystane dla popełniania zupełnie nowej

[*] Mgr **Szymon Wesołowski –** absolwent Wydziału Prawa Uniwersytetu Gdańskiego; pracownik Urzędu Komitetu Integracji Europejskiej.

[1] Nowy typ społeczeństwa, kształtujący się w krajach postindustrialnych, w których rozwój technologii osiągnął najwyższe tempo, a zarządzanie informacją, jej jakość oraz szybkość przepływu są zasadniczymi czynnikami konkurencyjności, zarówno w przemyśle, jak i usługach - za: A.Bógdał-Brzezińska, M.F.Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003, s.336.

kategorii przestępstw, tzw. przestępstw komputerowych (jak np. nielegalne przechwytywanie danych czy naruszenie integralności systemu informatycznego), w których przypadku przestępcza aktywność koncentruje się zasadniczo w cyberprzestrzeni.

Nowe zagrożenia wymagają adekwatnej reakcji ze strony organów ścigania, która jednak, z wielu powodów, jest poważnie utrudniona. Przede wszystkim należy zwrócić uwagę na to, że w przypadku przestępczości wykorzystującej zaawansowane technologie duża część materiału dowodowego ma postać elektroniczną – przy przestępstwach *stricte* „komputerowych" są to często jedyne możliwe do uzyskania dowody. Z uwagi na to, że dane informatyczne mają charakter niematerialny (o ile nie utrwalono ich w postaci wydruku) i wyjątkowo nietrwały (w znakomitej większości wypadków łatwo i w bardzo krótkim czasie można je zmodyfikować bądź też bezpowrotnie usunąć), zebranie takiego materiału dowodowego nastręcza istotnych trudności i wymaga zastosowania szczególnych czynności dowodowych, wśród których bardzo istotną rolę odgrywa przechwytywanie przekazów telekomunikacyjnych.[2] Podkreślić też należy, że działania w skali jednego państwa będą w wielu sytuacjach niewystarczające, z uwagi na fakt, iż zaawansowana technologicznie przestępczość ma dziś w ogromnej liczbie przypadków wymiar wykraczający poza granice państwa. Jedynym rozwiązaniem pozostaje zatem współpraca międzynarodowa, którą w państwach członkowskich Unii Europejskiej regulują zarówno przepisy prawa unijnego, jak i ogólnego prawa międzynarodowego. Dużą rolę odgrywa tu również Rada Europy oraz – w mniejszym zakresie – inne organizacje międzynarodowe (m.in. OECD, G-8).

Pojęcie przechwytywania przekazów telekomunikacyjnych i jego znaczenie

Przechwytywanie przekazów telekomunikacyjnych (*interception of telecommunications*) jest jednym z najważniejszych środków walki z nowymi formami przestępczości. Pierwotnie przybierało ono postać podsłuchu (*wiretapping*), czyli kontroli – opcjonalnie również utrwalania – rozmów telefonicznych określonego podmiotu, utrzymywanej przed nim w tajemnicy. W miarę jednak rozwoju technologicznego, który umożliwił przekazywanie nie tylko dźwięku ale i tekstu, obrazu czy też wiadomości łączących wszystkie te elementy (wiadomości mul-

[2] *Explanatory Memorandum to Council of Europe Recommendation Rec (1995) 13 on problems of criminal procedural law connected with information technology.*

timedialnych), zakres przedmiotowy dobrze znanej czynności dowodowej rozszerzano na nowe formy przekazu. Zmiana tego zakresu uzasadnia tłumaczenie terminu *interception of telecommunications* jako „przechwytywanie przekazów telekomunikacyjnych". Przyjęte w polskiej procedurze karnej pojęcia „*kontroli i utrwalania rozmów*" bądź „*kontroli i utrwalania treści innych przekazów informacji*" (rozdział 26 k.p.k.) nie najlepiej oddają znaczenie tego terminu. Pierwsze z nich wydaje się bowiem mieć zakres zbyt wąski, drugie dla odmiany – zbyt szeroki, obejmujący również i te przekazy informacji, które nie są dokonywane za pomocą technologii informacyjno-komunikacyjnych.

Za przedmiot przechwytywania należy zatem uznać wszelkie dane przesyłane lub odbierane przez podmiot przechwytywania za pośrednictwem łączy przewodowych bądź systemów łączności bezprzewodowej (telefonia komórkowa lub satelitarna), a określane zbiorczo jako przekazy telekomunikacyjne. Warto tutaj wyjaśnić, że przyjmowane w niektórych aktach prawnych rozróżnienie między „przekazami telekomunikacyjnymi" (*telecommunications*) a „przekazami danych informatycznych" (*computer communications*)[3] nie ma szczególnego uzasadnienia i wydaje się sztuczne. Jak wspomniano, obecnie bardzo trudno jest zakreślić wyraźną granicę między danymi transmitowanymi w obrębie systemu telekomunikacyjnego (jak np. rozmowa telefoniczna) a przekazami danych między komputerami (poczta elektroniczna), ze względu na postępującą konwergencję technologii telekomunikacyjnych i informatycznych. Poprawniejsze wydaje się zatem przyjęcie jednolitej terminologii. Można wprawdzie argumentować, że w celu zapewnienia należytego stopnia ogólności należałoby mówić raczej o przechwytywaniu „danych" niż „przekazów telekomunikacyjnych", jednak wydaje się, że ten ostatni termin jest bardziej właściwy – podkreśla bowiem wyraźnie, że chodzi o przechwytywanie danych transmitowanych za pomocą środków technicznych (odpowiedniej infrastruktury telekomunikacyjnej). Rozwiewa to tym samym pojawiające się czasem wątpliwości co do tego, czy zakres omawianej tutaj czynności dowodowej obejmuje przechwytywanie danych informatycznych w drodze analizy fal elektromagnetycznych emitowanych przez monitor komputera lub fal akustycznych drukarki (również w ten sposób możliwe jest bowiem uzyskanie dostępu do przetwarzanych danych).[4]

[3] Terminem tym posługuje się Konwencja Rady Europy z 23.11.2001 r. o cyberprzestępczości.

[4] K.J.Jakubski, *Przestępczość komputerowa – zarys problematyki*, „Prokuratura i Prawo", nr 12/1996, s.42.

Rozważania nad zakresem przedmiotowym przechwytywania przekazów telekomunikacyjnych należy uzupełnić o kwestię tzw. danych użytkowych, czyli danych związanych z transmisją określonego przekazu telekomunikacyjnego. Dane takie w dużej mierze pozostają w stosunku do „właściwego" przekazu telekomunikacyjnego w podobnej relacji, jak adres odbiorcy do treści listu. Obejmują one np. numer połączenia wychodzącego lub przychodzącego czy też adres IP[5] miejsca przeznaczenia pakietu danych transmitowanych za pośrednictwem Internetu. Określają też czas trwania i datę połączenia oraz lokalizację użytkownika telefonu komórkowego. Dane te stanowią immanentny składnik przechwyconych przekazów telekomunikacyjnych. Można zatem uznać, że będą one również wchodzić w zakres analizowanej czynności (przy założeniu, że będą gromadzone w czasie rzeczywistym). Rozwiązanie takie przyjmuje większość instrumentów prawa międzynarodowego, które podejmują problem przechwytywania. Przyjmowany jest też pogląd, że dane takie mogą stanowić samoistny przedmiot przechwytywania przekazów telekomunikacyjnych – środek taki ma bowiem niejednokrotnie duże znaczenie dla określonego postępowania, a nie narusza prywatności podmiotu inwigilacji w takim stopniu, w jakim czyni to „klasyczne" przechwytywanie całych przekazów. Wydaje się on uzasadniony, jako że dopuszczalność gromadzenia przesyłanych przez kogoś informacji implikuje – *a maiori ad minus* – możliwość przechwytywania również danych użytkowych, związanych z tymi informacjami.

Niezwykle istotnym atrybutem przechwytywania jest orientacja na pozyskiwanie wyłącznie danych „dynamicznych", poddawanych transmisji, przy czym pozyskiwanie to zachodzić ma w czasie rzeczywistym. Ta właśnie cecha przechwytywania stanowi o jego charakterze, wyodrębniając go spośród innych, pokrewnych czynności dowodowych, przede wszystkim zaś odróżniając go od przeszukania i zatrzymania (*search and seizure)*, które również jest skutecznym środkiem zwalczania nowych, zaawansowanych technologicznie form przestępczości.

Przechwytywanie przekazów telekomunikacyjnych doskonale sprawdza się przy zbieraniu materiału dowodowego w systemach teleinformatycznych; środek ten zorientowany jest bowiem na gromadzenie danych transmitowanych w czasie rzeczywistym i „efemeryczność"

[5] Unikalny numer przyporządkowany urządzeniom sieciowym, wykorzystywany do komunikacji między nimi w Internecie oraz w sieciach lokalnych. Maszyny posługują się adresem (numerem) IP w celu wymiany między sobą informacji w protokole TCP/IP.

danych informatycznych nie stanowi przeszkody dla jego skuteczności. Istotnym walorem jest także łatwość utrzymania jego zastosowania w tajemnicy; „przechwycenie" danych oznacza zwykle rejestrację podczas ich transmisji, która nie wpływa na sam przekaz danych – przepływające bity są po prostu „kopiowane" i dostarczane organom ścigania.

W odniesieniu do zwalczania niektórych rodzajów przestępstw komputerowych – jak np. rozpowszechniania wirusów[6] i „robaków" internetowych (*worms*)[7] czy nielegalnego dostępu do systemu informatycznego – przechwytywanie przekazów telekomunikacyjnych jest środkiem niezastąpionym. Bardzo trudno jest bowiem w inny sposób wykryć źródło ataku na system informatyczny albo udowodnić rozsyłanie szkodliwych programów komputerowych.

Prawne uwarunkowania międzynarodowej współpracy w zakresie przechwytywania przekazów telekomunikacyjnych

Do niedawna jedyną podstawą prawną międzynarodowej współpracy na obszarze Unii Europejskiej w zakresie przechwytywania przekazów telekomunikacyjnych pozostawał art. 1, ust. 1 Europejskiej Konwencji o pomocy prawnej w sprawach karnych z 20 kwietnia 1959 r.[8] Zgodnie z tym przepisem, strony Konwencji zobowiązują się wzajemnie do udzielania sobie „*możliwie najszerszej pomocy prawnej w sprawach o przestępstwa, których ściganie należy, w chwili wystąpienia*
z wnioskiem, do właściwości organów sądowych Strony wzywającej". Jak podaje oficjalny komentarz do Konwencji,[9] przepis ten należy interpretować szeroko, jako dotyczący nie tylko form pomocy prawnej w niej przewidzianych, ale i wszelkich innych form takiej pomocy. Skuteczność tej regulacji była jednak ograniczona, niektóre państwa

[6] Samoreprodukujący się kod, który uszkadza dane lub programy, zmieniając sposób działania sprzętu – por.: A.Bógdał-Brzezińska, M.F.Gawrycki, *Cyberterroryzm...*, op.cit., s.338.

[7] Program, którego podstawowym zadaniem jest rozprzestrzenianie się w sieci komputerowej. Po zagnieżdżeniu się w nowym systemie może zachowywać się jak wirus czy „koń trojański" (ibidem, s.334).

[8] Europejska Konwencja o pomocy prawnej w sprawach karnych (Dz. U. nr 76/1999, poz. 854).

[9] *Explanatory report on the European Convention on mutual assistance in criminal matters*, CETS, no. 030.

wychodziły bowiem z założenia, że przechwytywanie przekazów telekomunikacyjnych nie może stanowić jednej z form pomocy prawnej w myśl Konwencji.

Problem dostrzegła Rada Europy, przyjmując 28 czerwca 1985 r. zalecenie R(85)10 dotyczące praktycznego zastosowania Europejskiej Konwencji o pomocy prawnej w sprawach karnych w odniesieniu do wniosków o przechwytywanie przekazów telekomunikacyjnych.[10] Postanowienia tego aktu wprowadzały rekomendowany model współpracy w zakresie międzynarodowego przechwytywania przekazów telekomunikacyjnych, oparty na Konwencji z 1959 r. Zalecenia Rady Europy nie są jednak wiążące, w związku z czym zagadnienie szerokiej interpretacji art. 1, ust. 1 wspomnianej Konwencji pozostało otwarte.

Dotychczasowy system pomocy prawnej w sprawach karnych nie odpowiadał potrzebom Unii Europejskiej, która z racji wysokiego stopnia integracji politycznej i ekonomicznej wymaga dziś zupełnie nowych rozwiązań w dziedzinie współpracy sądowej w sprawach karnych, zapewniających należytą szybkość działania i odformalizowanych, a przy tym uwzględniających rosnące znaczenie zwalczania zaawansowanej technologicznie przestępczości. Remedium na słabości europejskiego systemu pomocy prawnej stanowić ma nowa Konwencja z dnia 29 maja 2000 r. o wzajemnej pomocy w sprawach karnych między państwami członkowskimi Unii Europejskiej (dalej – Konwencja z 2000 r.).[11]

Nowa Konwencja o wzajemnej pomocy w sprawach karnych

Konwencję z 2000 r. zaprojektowano jako uaktualnienie obowiązującego obecnie w Unii Europejskiej systemu pomocy prawnej w sprawach karnych, opartego przede wszystkim na Konwencji Rady Europy z 1959 r. Zamierzeniem autorów nowego instrumentu – czemu dali wyraz w preambule – było wzmocnienie międzynarodowej współpracy w sprawach karnych, poprzez usprawnienie i przyśpieszenie udzielania pomocy prawnej przy jednoczesnym poszanowaniu praw i wolno-

[10] *Council of Europe Recommendation No. R (85) 10 of the committee of ministers to member states concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications*.

[11] Konwencja z dnia 29.05.2000 r. o wzajemnej pomocy w sprawach karnych między państwami członkowskimi Unii Europejskiej (O.J., C 197, 12.07.2000).

ści jednostki. Konwencja została przyjęta w ramach III filaru Unii Europejskiej, na podstawie art. 34, ust. 2, pkt (d) Traktatu o Unii Europejskiej.

Przedmiotem regulacji Konwencji z 2000 r. jest pomoc prawna w sprawach karnych udzielana – co należy podkreślić – w ramach współpracy sądowej. Jej postanowienia mają zatem zastosowanie w sprawach, w których zostało już wszczęte postępowanie karne. Może to budzić pewne kontrowersje w odniesieniu do przewidzianych w Konwencji szczególnych form pomocy prawnej, które mogą przyjmować również charakter operacyjny – jak właśnie przechwytywanie przekazów telekomunikacyjnych. Za zawężeniem przedmiotu regulacji Konwencji przemawia jednak cel tego aktu, którym jest wzmocnienie i rozwój współpracy sądowej w sprawach karnych. Wskazują na to również postanowienia preambuły oraz fakt, że akt Rady ustanawiający Konwencję[12] odwołuje się do art. 31, pkt (a) Traktatu o Unii Europejskiej, który dotyczy wspólnego działania w dziedzinie współpracy sądowej w sprawach karnych. Tym samym należy przyjąć, że uregulowania Konwencji w zakresie przechwytywania przekazów telekomunikacyjnych służyć mają jedynie toczącemu się już postępowaniu karnemu i nie stanowią podstawy dla operacyjnej współpracy odpowiednich organów w tym zakresie.[13]

Konwencja z 2000 r. ma za zadanie – zgodnie z jej art. 1, ust. 1 – jedynie uzupełnić oraz ułatwić stosowanie postanowień obowiązujących już aktów, konstruujących system pomocy prawnej w sprawach karnych (system ten tworzą akty unijne – jak np. Konwencja wykonawcza Schengen – oraz akty Rady Europy, z fundamentalną Konwencją z 1959 r. na czele). Konwencja z 2000 r. powinna być zatem traktowana jedynie jako swoista „nadbudowa" tego systemu, nie zaś jako samodzielny instrument w omawianym obszarze prawa. W związku z tym należy przyjąć, że państwo nie może złożyć wniosku o pomoc prawną opierając się wyłącznie na jej postanowieniach. Z drugiej jednak strony, w razie sprzeczności między jej uregulowaniami a normami wyżej wymienionych traktatów, zastosowanie mają

[12] Akt Rady z dnia 29.05.2000 ustanawiający, zgodnie z art. 34 Traktatu o Unii Europejskiej, Konwencję o wzajemnej pomocy w sprawach karnych pomiędzy państwami członkowskimi Unii Europejskiej (O.J., C 197, 12.07.2000).

[13] M.Płachta, *Wzajemna pomoc prawna w Unii Europejskiej na podstawie Konwencji z 2000 roku,* „Studia Europejskie", nr 2/2003, s.91-106.

te pierwsze.[14] Ponadto warto zwrócić uwagę na fakt, iż w zakresie zagadnień nie unormowanych w tamtych traktatach – jak właśnie w przypadku przechwytywania przekazów telekomunikacyjnych – przepisy Konwencji znajdują pełne i niczym nie ograniczone zastosowanie.

Wniosek o przechwytywanie – zagadnienia ogólne

Przechwytywanie przekazów telekomunikacyjnych stanowi – w myśl Konwencji – jedną ze szczególnych form pomocy prawnej, jednak o tak dużym, wręcz przełomowym znaczeniu, że zostało ono wyodrębnione od innych takich form i uregulowane w osobnym Tytule III. Dla pełnego opisu funkcjonowania wewnątrzunijnej współpracy w tym zakresie należałoby jednak odwołać się nie tylko do postanowień tego Tytułu, ale i do innych uregulowań prawnych. Przepisy Tytułu III Konwencji stanowią bowiem *lex specialis* w stosunku do ogólnych rozwiązań tego aktu prawnego, które same są jednocześnie przepisami szczególnymi w stosunku do aktów tworzących dotychczasowy system pomocy prawnej w sprawach karnych w Unii Europejskiej. Celem niniejszego opracowania nie jest jednak szczegółowa analiza umiejscowienia przechwytywania przekazów telekomunikacyjnych w tym systemie, ale raczej przegląd najważniejszych w tym zakresie rozwiązań przyjętych w Konwencji z 2000 r. Mimo to, warto zwrócić uwagę na niektóre ogólne postanowienia nowej Konwencji, stanowiące faktyczne urzeczywistnienie postulatów, jakie były wielokrotnie formułowane w związku z koniecznością dostosowania systemów pomocy prawnej do zwalczania zaawansowanej technologicznie przestępczości.[15]

Artykuł 4 Konwencji reguluje sposób, w jaki wniosek o pomoc prawną jest wykonywany. Przełamuje przy tym dotychczas obowiązującą regułę, wedle której wniosek wykonywany jest zgodnie z prawem państwa wezwanego. Obecnie, w myśl uregulowań art. 4, ust. 1 wniosek taki wykonuje się – co do zasady – przy zachowaniu wymogów formalnych i procedur wyraźnie wskazanych przez państwo wzywające, dzięki czemu wzrosnąć ma skuteczność pomocy prawnej. Działania podjęte przez państwo wezwane w wykonaniu wniosku o pomoc

[14] Oficjalny komentarz do Konwencji z dnia 29.05.2000 o wzajemnej pomocy w sprawach karnych pomiędzy Państwami Członkowskimi Unii Europejskiej (O.J., C 379, 29.12.2000, s.9).

[15] Jako przykład można tu wskazać niektóre postanowienia dokumentu przyjętego przez państwa grupy G-8 w grudniu 1997 r.: *Principles and Action Plan to Combat High-Tech Crime*.

prawną mają bowiem przynieść taki sam efekt, jak gdyby zostały podjęte przez stronę wzywającą.

Konwencja kładzie również nacisk na szybkość działania, wymagając (art. 4, ust. 2), by wniosek został wykonany w najkrótszym możliwym terminie, przy jak najszerszym uwzględnieniu terminów określonych przez państwo wzywające (państwo takie jest obowiązane uzasadnić wskazywane terminy). Szybkość działania ma zaś pierwszorzędne znaczenie przy ściganiu przestępczości korzystającej z nowych technologii, szczególnie przestępczości komputerowej.

Istotnym ułatwieniem w ściganiu tych właśnie form przestępczości jest także nowe rozwiązanie w przedmiocie formy wniosku o pomoc prawną. O ile dotychczas wnioski przekazywano na piśmie, Konwencja dopuszcza użycie w tym celu jakiegokolwiek środka zdatnego do pozostawienia pisemnego zapisu – pod warunkiem, że nastąpi to w sposób umożliwiający państwu wezwanemu stwierdzenie autentyczności przesłanego dokumentu (art. 6, ust. 1). Oznacza to, między innymi, możliwość korzystania z faksu czy też poczty elektronicznej. Co więcej, sformułowania omawianego przepisu teoretycznie pozwalają państwom członkowskim na zawieranie między sobą porozumień, na mocy których mogłyby przyjmować ustne wnioski o pomoc prawną, szczególnie w nagłych wypadkach i przy założeniu, że wniosek taki byłby następnie potwierdzany na piśmie (albo w inny, ekwiwalentny w myśl art. 6, ust. 1 sposób).[16] Warto zaznaczyć, że powyższe rozwiązanie było proponowane w przyjętych przez grupę G-8 w grudniu 1997 r. zasadach,[17] który to fakt dobitnie potwierdza jego znaczenie dla skutecznego wykorzystywania przechwytywania w ściganiu nowych form przestępczości.

Kolejnym nowatorskim rozwiązaniem Konwencji jest niemal całkowita eliminacja z postępowania w sprawie pomocy prawnej centralnych organów administracji państwowej. O ile dotychczas pomoc prawna w sprawach karnych pozostawała niemalże w całości w gestii resortów sprawiedliwości, to w myśl art. 6, ust. 1 Konwencji zasadą jest już bezpośredni kontakt oraz przekazywanie wniosków między organami sądowymi obu zainteresowanych państw, właściwymi rzeczowo i miejscowo do ich wykonania. W sprawach wiążących się z przechwytywaniem przekazów telekomunikacyjnych za właściwy organ należy uznać, zgodnie z art. 17 Konwencji, organ sądowy, a jeżeli nie jest on w danym państwie właściwy w zakresie przechwyty-

[16] Ibidem, s.13.
[17] Ibidem.

wania, inny, równorzędny organ, wskazany przez państwo członkowskie na podstawie art. 24, ust. 1, pkt (e) Konwencji, działający w ramach śledztwa bądź dochodzenia.

Przedstawione powyżej najważniejsze, ogólne rozwiązania Konwencji stanowią istotny przyczynek do realizacji postulatów przyśpieszenia, ułatwienia i zwiększenia skuteczności pomocy prawnej w sprawach karnych. Szczególnego znaczenia nabierają zaś w odniesieniu do tej formy pomocy prawnej, jaką jest przechwytywanie przekazów telekomunikacyjnych. Środek ten, jak już podkreślano, jest bardzo skuteczną bronią w zwalczaniu zaawansowanej technologicznie przestępczości – jednak warunkiem jego skuteczności jest właśnie szybkość zastosowania. W erze niepodzielnego panowania technologii cyfrowych, w której o uzyskaniu dowodów rozstrzygają minuty i sekundy, tradycyjny system pomocy prawnej okazuje się bowiem anachronizmem.

Przechwytywanie przekazów telekomunikacyjnych

Konwencja z 2000 r. zawiera wiele nowatorskich rozwiązań prawnych, jednak o jej wyjątkowości w stosunku do innych, tworzących dotychczasowy system pomocy prawnej w sprawach karnych, aktów stanowi przede wszystkim rozszerzenie wachlarza jej regulacji na współpracę w zakresie przechwytywania przekazów telekomunikacyjnych. Konwencja jest bowiem pierwszym wiążącym unijnym aktem prawnym, który normuje kwestie przechwytywania informacji.

Warto zwrócić uwagę na bardzo szeroki zakres przedmiotowy regulacji Konwencji w tej dziedzinie. Nie definiuje ona wprawdzie pojęcia przekazu telekomunikacyjnego (*telecommunications*), jednak jego zakres wyznacza oficjalny komentarz do tego aktu. Zgodnie z nim, pojęcie to „*powinno być rozumiane w najszerszym znaczeniu tego słowa*", czyli obejmować „*wszelkie formy przekazu informacji, które mogą być przedmiotem przekazu za pomocą obecnych jak i przyszłych technologii*". Podkreślono również, że państwo wezwane powinno dostarczyć przechwycone dane techniczne, jak numery wybrane, czas i długość trwania połączenia oraz, w miarę możliwości, lokalizację podmiotu przechwytywania.[18]

Stosowanie przepisów Tytułu III Konwencji do przechwytywania „nowych i przyszłych technologii" jest możliwe ze względu na fakt, że jej unormowania, abstrahując całkowicie od kwestii technicznych,

[18] Oficjalny komentarz do Konwencji z dnia 29.05.2000…, op.cit., s.22.

skupiają się jedynie na wyodrębnieniu sytuacji, w których przechwytywanie informacji nabiera kontekstu międzynarodowego określając przy tym formy, jakie przybiera wówczas współpraca państw członkowskich Unii (postanowienia są tym samym „technologicznie neutralne").[19]

Tytuł III Konwencji reguluje trzy typy sytuacji, w których dochodzi do zgodnego z prawem, „umiędzynarodowionego" przechwytywania przekazów telekomunikacyjnych. Jednak tylko jedna z nich (ujęta w art. 18) wpisuje się w ramy klasycznej koncepcji pomocy prawnej, opartej na schemacie: państwo A występuje do państwa B z wnioskiem o dokonanie czynności procesowej C. W odniesieniu natomiast do dwóch pozostałych kategorii sytuacji trudno jest mówić o jakiejkolwiek formie pomocy prawnej. Obie, choć diametralnie różne, są rezultatem postępu technicznego. Państwa posiadły dziś bowiem, w odniesieniu do niektórych technologii informacyjno-komunikacyjnych, możliwość samodzielnego przechwytywania przekazów telekomunikacyjnych podmiotów znajdujących się na obcym terytorium. Z kolei wprowadzenie na rynek innych technologii prowadzi do utraty przez te państwa zdolności do inwigilacji nawet podmiotów znajdujących się na ich własnym terytorium.

Przed twórcami Konwencji z 2000 r. stanął tym samym problem zarówno odpowiedniej regulacji „samodzielnego", transgranicznego przechwytywania (kontrowersyjny art. 20 Konwencji), jak i zapewnienia państwom możliwości prowadzenia przechwytywania na ich własnym terytorium (art. 19). W obu przypadkach współpraca między państwami jest znikoma bądź całkowicie wyłączona – na umieszczeniu ich regulacji w Konwencji o pomocy prawnej zaważyły względy polityczne. Rada Unii Europejskiej uznała bowiem, że przedstawione sytuacje powinny, w związku z ich rosnącą aktualnością, zostać uregulowane w prawie międzynarodowym. Ma to być kolejny krok w budowie Unii Europejskiej jako „obszaru wolności, bezpieczeństwa i sprawiedliwości".[20]

[19] *Communication from the Commission: Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*, COM (2000) 890.

[20] Oficjalny komentarz do Konwencji z dnia 29.05.2000 …, op.cit., s.21.

Wniosek o przechwycenie na podstawie art. 18 Konwencji

Jak wspomniano, artykuł 18 Konwencji wpisuje przechwytywanie przekazów telekomunikacyjnych w klasyczny schemat pomocy prawnej. Reguluje on sytuacje, w których państwo członkowskie wzywane jest przez inne państwo do wykonania przechwytywania.

Właściwy organ państwa wzywającego może złożyć wniosek wyłącznie wtedy, gdy przechwytywanie ma służyć celom prowadzonego śledztwa lub dochodzenia i tylko przy zachowaniu wymogów przewidzianych prawem wewnętrznym państwa wzywającego. Sam wniosek może mieć dwojaki charakter, wzywając do:

- przechwycenia i niezwłocznej transmisji przekazu telekomunikacyjnego do państwa wzywającego albo
- przechwycenia, rejestracji oraz późniejszej transmisji zarejestrowanego przekazu do państwa wzywającego.

W myśl postanowień Konwencji zasadą mają być wnioski o przechwycenie i niezwłoczną transmisję (innymi słowy o przekazanie przechwytywanych danych w czasie rzeczywistym), wyjątkiem natomiast o rejestrację przechwyconego materiału. Takie ujęcie stanowi odwrócenie dotychczasowej praktyki w tej dziedzinie, gdzie dominowały wnioski drugiego typu. Można doszukiwać się w nowym podejściu wpływów rezolucji Rady UE z dnia 17 stycznia 1995 r. dotyczącej prawnie dozwolonego przechwytywania przekazów telekomunikacyjnych,[21] która postulowała, by wszelkie przechwytywane dane były udostępniane w czasie rzeczywistym (pkt. 2 załącznika do rezolucji).

Każdy wniosek o przechwytywanie, niezależnie od swojego charakteru, powinien spełniać określone wymogi formalne. Art. 18, ust. 3 Konwencji określa elementy obligatoryjne takiego wniosku. Zgodnie z nim, wniosek zawiera:

- wskazanie organu składającego wniosek;
- potwierdzenie wydania prawomocnego postanowienia o przechwytywaniu w związku z postępowaniem karnym;
- informacje służące identyfikacji podmiotu przechwytywania;
- wskazanie czynu przestępczego, którego postępowanie dotyczy;
- postulowany czas trwania przechwytywania;

[21] *Council Resolution of 17 January 1995 on the lawful interception of telecommunications,* O.J., C 329, 4.11.1996.

– w miarę możliwości, odpowiednie dane techniczne, zapewniające wykonanie wniosku – w szczególności właściwy numer połączenia z siecią.

Ponadto wniosek może też zawierać dodatkowe elementy, w zależności od sytuacji, w której został wydany oraz jego charakteru. Warto zauważyć, że stosunkowo precyzyjny, indywidualny charakter wniosku faktycznie wyklucza międzynarodową współpracę w tej dziedzinie w formie przechwytywania całości ruchu sieciowego i późniejszego wyszukiwania wśród przechwyconych danych ewentualnych relewantnych informacji (tzw. *fishing expeditions*).

Artykuł 18, ust. 2 wyodrębnia trzy różne sytuacje, w zależności od tego, gdzie znajduje się podmiot przechwycenia. Wnioski o pomoc prawną można zatem składać, gdy podmiot ten będzie obecny w:

1) państwie wzywającym, które potrzebuje pomocy technicznej państwa wezwanego, aby przechwycić wysyłane i odbierane przez podmiot przekazy telekomunikacyjne (art. 18, ust. 2, pkt [a] Konwencji);
2) państwie wezwanym, a wysyłane i odbierane przez niego przekazy telekomunikacyjne mogą być przechwycone na terytorium tego państwa (art. 18, ust. 2, pkt [b] Konwencji);
3) innym („trzecim") państwie członkowskim, które zostało poinformowane o fakcie przechwytywania na podstawie art. 20, ust. 2, pkt (a), a państwo wzywające potrzebuje pomocy technicznej państwa wezwanego, aby przechwycić wysyłane i odbierane przez ten podmiot przekazy telekomunikacyjne (art. 18, ust. 2, pkt [c] Konwencji).

Wykonanie przez państwo wezwane wniosku o przechwytywanie i bezpośrednią transmisję uzależnione jest od spełnienia określonych przesłanek, przy czym znów decydującą rolę odgrywać będzie lokalizacja podmiotu przechwytywania. Jeżeli znajduje się on poza terytorium państwa wezwanego (sytuacje 1 i 3), wniosek taki wykonywany jest bez większych formalności, wymagane jest jedynie, by zawierał elementy wymienione w art. 18, ust. 3 (elementy konieczne). Jeżeli jednak podmiot znajduje się na terytorium tego państwa (sytuacja 2), wówczas udzielenie pomocy prawnej obwarowane jest dodatkowymi wymogami. Wniosek, poza elementami koniecznymi, zawierać musi zwięzły opis stanu faktycznego sprawy[22] (*summary of facts*), w związku

[22] W kwestii interpretacji tego wyrażenia oficjalny komentarz do konwencji odsyła do art. 12, ust. 2, pkt (b) Europejskiej Konwencji o ekstradycji z 13.12.1957, zgodnie z którym opis taki określać ma czyny, w związku z którymi wnioskuje się o przechwy-

z którą wnioskuje się podjęcie przechwytywania. Poza tym, wykonany może być wtedy i tylko wtedy, gdy środek taki – przechwytywanie informacji – zostałby przez państwo wezwane podjęty w podobnej sprawie krajowej, a dodatkowo jego wykonanie może być uzależnione od wszelkich warunków, jakie wchodziłyby w grę w takiej sprawie (np. poprzez zastrzeżenie, że dana osoba nie powinna być inwigilowana, w czasie gdy kontaktuje się ze swoim prawnikiem, lekarzem czy duchownym). Wymienione obostrzenia wiążą się ze specyfiką sytuacji – podejmując przechwytywanie państwo wzywane decyduje się bowiem na niezwykle głęboką ingerencję w prywatność osoby przebywającej na jej terytorium i to w interesie innego państwa.

Wskazane wyżej (w odniesieniu do sytuacji 2) przesłanki mają pełne zastosowanie również przy wykonywaniu wniosków o przechwytywanie, rejestrację oraz późniejszą transmisję przechwyconych danych i to niezależnie od tego, w którym państwie znajduje się podmiot przechwytywania. Należy przy tym podkreślić, że państwo wezwane jest obowiązane do wykonania takiego wniosku wtedy i tylko wtedy, gdy nie jest możliwa transmisja przechwyconych danych w czasie rzeczywistym (art. 18, ust. 6). Sytuacja taka może zachodzić wówczas, gdy państwo wezwane lub państwo wzywające nie są technicznie przygotowane do dokonania takiej transmisji. Postanowienie to spotkało się przy pracach nad Konwencją z krytyką Wielkiej Brytanii, z której inicjatywy wprowadzono w art. 18, ust. 7 możliwość złożenia przez państwo członkowskie deklaracji, że ust. 6 tego artykułu będzie je wiązał tylko w sytuacjach, gdy samo nie będzie w stanie zapewnić takiej transmisji. (W konsekwencji, państwo wezwane, które ma możliwość dostarczania przechwytywanych danych w czasie rzeczywistym będzie mogło zawsze odmówić wykonania wniosku o przechwytywanie i rejestrację.)[23] Oczywiście nic nie stoi na przeszkodzie, by państwo wezwane wykonało taki wniosek dobrowolnie, pomimo braku wyraźnie określonego obowiązku prawnego.

Ponadto należy dodać, że zgodnie z art. 18, ust. 8 państwo wzywające może, składając wniosek o przechwytywanie i rejestrację, wystą-

---

tywanie oraz czas i miejsce popełnienia tychże czynów – za: Oficjalny komentarz do Konwencji z dnia 29.05.2000 …, op.cit., s.21.

[23] W Wielkiej Brytanii prawo nie przewiduje rejestracji przechwytywanych informacji i przyjęcie takiego obowiązku stanowiłoby poważne obciążenie dla brytyjskich organów ścigania – por. *Letter from Kate Hoey MP to Lord Tordoff of 30 November 1998, The United Kingdom Parliament, Select Committee on European Union Twelfth Report* (http://www.parliament.the-stationery-office.co.uk/pa/ld199900/ldselect/ldeucom/93/9315.htm).

pić również o przekazanie transkryptu zarejestrowanych informacji (przepis ten ma przede wszystkim zastosowanie do utrwalonych rozmów telefonicznych).

Nie wymaga szerszego komentarza art. 18, ust. 9 Konwencji, w myśl którego państwo wezwane traktuje przekazane mu informacje jako poufne zarówno w interesie wymiaru sprawiedliwości, jak i podmiotu przechwytywania jest, aby o zastosowanym środku wiedziało jak najmniej osób.

Zagadnieniem nieodłącznie wiążącym się z problematyką pomocy prawnej jest kwestia kosztów, jakie pociąga za sobą wykonanie wniosku o taką pomoc. Nie inaczej rzecz się ma z „umiędzynarodowionym" przechwytywaniem przekazów telekomunikacyjnych. Kwestię tę reguluje art. 21 Konwencji, zgodnie z którym koszty ponoszone przez operatorów sieci lub usługodawców w związku z wykonaniem wniosku o przechwytywanie na podstawie art. 18, obciążają państwo wzywające.

Przechwytywanie przekazów telekomunikacyjnych na terytorium krajowym za pośrednictwem dostawców usług[24]

Artykuł 19 Konwencji normuje sytuację, o której trudno powiedzieć, że jest jakąkolwiek formą pomocy prawnej, nie ma tu bowiem – co do zasady – bezpośredniej współpracy państw. Artykuł ten ma w zamierzeniu umożliwić przechwytywanie przekazów telekomunikacyjnych dokonywanych drogą satelitarną (utworzono go z myślą o projektowanym systemie łączności satelitarnej Irydium) oraz za pomocą innych, podobnych technologii, jakie mogą pojawić się w przyszłości.

W systemach łączności satelitarnej możliwość pełnego monitorowania przekazów wysyłanych i odbieranych przez dany podmiot posiada jedynie państwo, na którego terytorium znajduje się stacja naziemna (*ground station*), przez którą przepływają wszelkie informacje transmitowane drogą satelitarną. Aby zatem uniknąć konieczności każdorazowego występowania do państwa, w którym taka stacja się

[24] Konwencja nie definiuje pojęcia „dostawcy usług" (*service provider*), można się tu zatem odwołać do rozumienia tego terminu, jakie przyjęto w innym wspólnotowym akcie dotyczącym przechwytywania: rezolucji Rady z 17.01.1995 r. w sprawie prawnie dozwolonego przechwytywania przekazów telekomunikacyjnych. Zgodnie z zawartą w niej definicją, dostawcą usług jest osoba fizyczna lub prawna świadcząca publicznie usługi telekomunikacyjne, które to świadczenie polega w całości albo w części na transmisji oraz przekierowywaniu przekazów danych w obrębie sieci teleinformatycznej.

znajduje, z wnioskiem o przechwycenie przekazów telekomunikacyjnych podmiotu znajdującego się w państwie wzywającym, art. 19 przewiduje odpowiednie rozwiązanie techniczne. Nakłada on bowiem na państwo, w którym stacja naziemna się znajduje, obowiązek zapewnienia innym państwom bezpośredniego dostępu do transmitowanych przez taką stację informacji za pośrednictwem wyznaczonego dostawcy usług, obecnego w danym państwie. W ten sposób inne państwa otrzymują możliwość samodzielnego przechwytywania odpowiednich informacji, bez konieczności angażowania jakichkolwiek innych państw.

Warunki, pod jakimi państwo „przechwytujące" może korzystać z zapewnionego w ten sposób dostępu do przekazów przesyłanych drogą satelitarną określa art. 19, ust. 2. Zgodnie z nim, przechwytywanie takich przekazów może być prowadzone za pośrednictwem dostawcy usług jedynie wówczas, gdy:

- ma ono na celu osiągnięcie celów śledztwa albo dochodzenia;
- odbywa się zgodnie z właściwymi przepisami prawa krajowego oraz
- podmiot przechwytywania znajduje się na terytorium państwa przechwytującego.

Jak łatwo zauważyć, przechwytywanie za pośrednictwem usługodawcy podejmowane jest na dokładnie takich samych zasadach, jak inne tego typu środki w państwie przechwytującym. Staje się ono na powrót wewnętrzną sprawą państwa przechwytującego – decyzja co do podjęcia takiego środka oraz jej wykonanie należą do wyłącznej kompetencji tego państwa, bez jakiegokolwiek angażowania państwa, na którego terytorium znajduje się stacja naziemna. Można zatem powiedzieć, że regulacja art. 19 Konwencji pozwala na przywrócenie państwom członkowskim tych ich uprawnień, jakich pozbawia je postęp technologiczny.

Pojawia się jednak pytanie, czy analizowane rozwiązanie (tj. zapewnienie zdalnego dostępu do przepływających przez stację naziemną danych) nie doprowadzi do niekontrolowanego monitorowania przekazów telekomunikacyjnych podmiotów znajdujących się na terytorium innych państw. Zgodnie z oficjalnym komentarzem do Konwencji możliwość taką można, w drodze odpowiednich zabiegów technicznych, skutecznie wyłączyć, zapewniając państwom członkowskim dostęp jedynie do informacji wysyłanych bądź odbieranych z ich tery-

toriów (państwo A będzie zatem miało dostęp wyłącznie do przekazów podmiotów znajdujących się na terytorium A).[25]

Przechwytywanie przekazów satelitarnych za pośrednictwem usługodawcy ma być prowadzone przez dane państwo zasadniczo na własny użytek. Jednak w myśl art. 19, ust. 3 Konwencji, opisany mechanizm może być zastosowany również na rzecz państwa wzywającego, które wystąpiło na podstawie art. 18, ust. 2, pkt (b) z wnioskiem o przechwytywanie przekazów telekomunikacyjnych podmiotu znajdującego się na terytorium państwa wezwanego.

Warto też zwrócić uwagę na art. 19, ust. 4, zgodnie z którym zawsze możliwe jest wystąpienie do państwa, na którego terytorium znajduje się stacja naziemna, z wnioskiem o przechwytywanie informacji na podstawie art. 18. Sformułowanie to ma dwojakie uzasadnienie. Po pierwsze, państwo wzywające może nie mieć zdalnego dostępu do danych przepływających przez stację naziemną (państwo siedziby takiej stacji obowiązane jest bowiem zapewnić dostęp tylko tym państwom członkowskim Unii, które się o to zwrócą). Wniosek na podstawie art. 18, ust. 2, pkt (a) będzie w takiej sytuacji jedynym sposobem uzyskania właściwych danych.

Po drugie, należy liczyć się z tym, że określony podmiot, przebywający w chwili rozpoczęcia przechwytywania na terytorium państwa wzywającego, będzie – podczas przechwytywania – przemieszczać się pomiędzy kilkoma państwami. W takim wypadku wystąpienie od razu z wnioskiem na podstawie art. 18 będzie najwłaściwszym – z punktu widzenia ekonomiki postępowania – rozwiązaniem. Państwo siedziby stacji ma bowiem, potencjalnie, pełny dostęp do informacji przekazywanych przez podmiot przechwytywania za pośrednictwem łączy satelitarnych. Można przy tym założyć, że wniosek, o którym mowa, musiałby mieć charakter kompleksowy, odnosząc się do wszystkich lub niektórych sytuacji, omówionych w art. 18. Przykładowo, gdyby podmiot przechwytywania poruszał się wahadłowo między państwem wzywającym A a danym państwem trzecim C, to wniosek o przechwytywanie do państwa siedziby stacji B musiałby przywoływać jako swoją podstawę zarówno art. 18, ust. 2, pkt (a), jak i pkt (c).

W debacie nad konwencyjnym uregulowaniem przechwytywania za pośrednictwem usługodawców istotnym zagadnieniem był wpływ projektowanych rozwiązań na funkcjonowanie branży telekomunikacyjnej. Podkreślano w szczególności dwie kwestie: czy zapewnienie zdalnego dostępu będzie warunkiem koniecznym uruchomienia dzia-

[25] Oficjalny komentarz do Konwencji z dnia 29.05.2000 …, op.cit., s.20.

łalności przez operatora telefonii satelitarnej oraz kogo obciążać będą koszty związane z odpowiednim dostosowaniem infrastruktury telekomunikacyjnej oraz jej funkcjonowaniem? O ile pierwsza z nich została szybko wyjaśniona – przyjęto, że możliwość budowy stacji naziemnej telefonii satelitarnej w Unii Europejskiej nie będzie uzależniona od zapewnienia zdalnego dostępu do przepływających przez stację danych[26] – to brak jest wyraźnych postanowień w kwestii kosztów dostosowania infrastruktury. Konsorcjum Irydium, dobrowolnie podjęło się dokonać takiego dostosowania na własny rachunek, można się zatem spodziewać, że również od przyszłych operatorów telefonii satelitarnej będzie się oczekiwało podjęcia takiego kroku. Uprawnione jest założenie, że przynajmniej niektóre państwa członkowskie Unii uzależnią przyznanie takiemu operatorowi koncesji na działalność od zapewnienia zdalnego dostępu na własny koszt.[27]

Przechwytywanie przekazów telekomunikacyjnych bez technicznej pomocy państwa zawiadomionego

Najwięcej kontrowersji wśród wszystkich uregulowań Konwencji wzbudza artykuł 20, pozwalający na przechwytywanie informacji na terenie innego państwa-strony bez konieczności składania wniosku o pomoc prawną, a jedynie informując je o tym fakcie. Parlament Europejski zdecydowanie opowiadał się za usunięciem tego artykułu z projektu Konwencji, wyrażając obawę, że może on być interpretowany jako próba regulacji działań służb specjalnych państw członkowskich Unii, którą to problematykę uznano za zbyt kontrowersyjną, by zajmować się nią na szczeblu wspólnotowym. Podkreślił on przy tym, że poddanie działań takich służb regulacji art. 20 Konwencji oznaczałoby tym samym zgodę na ingerencję w nie organów sądowniczych, co ze zrozumiałych względów byłoby nie do przyjęcia dla wielu państw Unii.[28] Ostatecznie jednak art. 20 został przez Radę Unii Europejskiej utrzymany.

---

[26] *Satellite telecommunications – the „service provider solution". The United Kingdom Parliament, Select Committee on European Union Twelfth Report* (http://www.parliament.the-stationery-office.co.uk/pa/ld199900/ldselect/ldeucom/93/9303.htm#a2).

[27] Ibidem; *Letter from Kate Hoey MP to Lord Tordoff of 3 March 1999* (http://www.parliament.the-stationery-office.co.uk/pa/ld199900/ldselect/ldeucom/93/9318.htm).

[28] *Report on the draft Council Act establishing the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union*, Euro-

Istota konstrukcji przewidzianej w art. 20 zawiera się w jego ust. 2. Stanowi on, że jeżeli dla osiągnięcia celów śledztwa albo dochodzenia właściwy organ państwa członkowskiego Unii (państwo przechwytujące – *intercepting Member State*) zarządza przechwytywanie przekazów telekomunikacyjnych podmiotu, którego adres telekomunikacyjny używany jest na terytorium innego państwa członkowskiego (państwo zawiadamiane – *notified Member State*), a techniczne wsparcie tego państwa nie jest konieczne dla wykonania przechwycenia, wówczas wystarczy je jedynie zawiadomić o prowadzonym na jego terytorium przechwytywaniu. Zawiadomienia dokonuje się:

– przed rozpoczęciem przechwytywania – jeżeli w chwili zarządzenia przechwytywania wiadomym jest, że dany podmiot znajduje się w zawiadamianym państwie; w takiej sytuacji państwo przechwytujące obowiązane jest wstrzymać się z podjęciem przechwytywania do czasu podjęcia przez państwo zawiadamiane stosownej decyzji;

– niezwłocznie po powzięciu wiadomości, że podmiot przechwytywania znajduje się na terytorium zawiadamianego państwa – w pozostałych przypadkach; przechwytywanie może być wówczas kontynuowane do czasu podjęcia decyzji przez państwo zawiadamiane.

Artykuł 20, ust. 3 precyzuje zakres informacji, jakie powinno zawierać zawiadomienie o planowanym bądź już prowadzonym przechwytywaniu. Odpowiadają one elementom koniecznym wniosku o przechwytywanie na podstawie art. 18, z tą oczywistą różnicą, że nie jest potrzebne podanie danych technicznych umożliwiających wykonanie przechwytywania (państwo zawiadamiane nie jest angażowane w najmniejszym stopniu w techniczne aspekty przechwytywania). Przekazane informacje państwo zawiadamiane traktuje jako poufne (art. 18, ust. 5), zapewniając w ten sposób zachowanie tajemnicy postępowania prowadzonego na jego terytorium przez obce państwo. Dodatkową gwarancję dochowania poufności przekazywanych informacji przewiduje art. 18, ust. 6, zgodnie z którym, jeśli powyższe informacje mają szczególny charakter, wówczas mogą być przekazane do właściwego organu państwa zawiadamianego za pośrednictwem określonego organu (jest to zatem wyjątek od ukształtowanej w art. 6, ust. 1 Konwencji zasady bezpośrednich kontaktów właściwych organów zainteresowanych państw). Dla wprowadzenia w życie tego postanowienia konieczne jest jednak zawarcie odpowiednich porozumień dwustron-

pean Parliament, Committee on Citizen's Freedoms and Rights, Justice and Home Affairs, 9636/1999 – C5-0091/1999 and SN 5060/1999 – C5-0331/1999 – 1999/0809 (CNS), s.46.

nych między zainteresowanymi państwami, konkretyzujących organy, za których pośrednictwem informacje mają być przekazywane.

Zawiadomiony w powyższym trybie właściwy organ danego państwa powinien odpowiednio zareagować. Zgodnie z postanowieniami art. 20, ust. 4 Konwencji może on, alternatywnie bądź to bezzwłocznie – najpóźniej w ciągu 96 godzin od otrzymania stosownych informacji – podjąć decyzję w przedmiocie przechwytywania planowanego albo już prowadzonego przez inne państwo, bądź też wystąpić (również w ciągu 96 godzin) o przedłużenie terminu do powzięcia decyzji, przy czym musi ona wówczas zapaść w czasie ośmiu dni od chwili zawiadomienia. Przedłużenie takie ma umożliwić przeprowadzenie przez państwo zawiadamiane wewnętrznych procedur, do których obliguje je własne ustawodawstwo. Dla zapobieżenia arbitralnemu uciekaniu się do przedłużania terminu, Konwencja przewiduje konieczność przedłożenia przez państwo zawiadamiane pisemnego uzasadnienia takiego posunięcia. Zasadą pozostaje zatem rozstrzygnięcie w przedmiocie przechwytywania w czasie nie przekraczającym czterech dni.

Podejmując rozstrzygnięcie w tej kwestii państwo zawiadamiane powinno zdecydować się na jedną z dwóch opcji. Po pierwsze, może zezwolić na podjęcie albo kontynuację trwającego już przechwytywania, przy czym może ono uzależnić swoją zgodę od spełnienia warunków, które mogłyby wchodzić w grę przy zastosowaniu takiego środka w podobnej sprawie krajowej (art. 20, ust. 4, lit. [c], pkt [i]). Po drugie, państwo zawiadamiane może odmówić zgody na podjęcie przechwytywania albo zażądać zaprzestania trwającego już przechwytywania (art. 20, ust. 4, lit. [c], pkt [ii]). Negatywna decyzja nie jest jednak pozostawiona wyłącznie jego swobodnemu uznaniu; może być podjęta wtedy, gdy w danym przypadku przechwytywanie byłoby niedopuszczalne w myśl wewnętrznego ustawodawstwa tego państwa albo też na podstawie art. 2 Europejskiej Konwencji o pomocy prawnej z 1959 r. (czyli, gdy np. przechwytywanie jest lub ma być prowadzone w sprawie o przestępstwo, które państwo zawiadamiane uważa za przestępstwo polityczne bądź skarbowe). Decyzja taka wymaga przy tym zawsze pisemnego uzasadnienia.

Odmawiając zgody na prowadzenie przechwytywania przekazów telekomunikacyjnych na swoim terytorium, państwo zawiadamiane może również wprowadzić obostrzenia co do wykorzystania informacji przechwyconych w czasie, gdy podmiot przechwytywania przebywał na jego terytorium – zgodnie z art. 20, ust. 4, lit. (c), pkt (iii) – bądź to zakazując ich wykorzystania, bądź też uzależniając ich wykorzystanie od spełnienia pewnych określonych warunków.

Do czasu podjęcia stosownej decyzji przez państwo zawiadamiane państwo przechwytujące może kontynuować trwające już przechwytywanie, z tym jednak ograniczeniem, że uzyskany w ten sposób materiał nie zostanie przez nie wykorzystany.

Ograniczenia tego nie stosuje się, jeżeli zainteresowane państwa uzgodniły inaczej bądź też, gdy wykorzystanie materiału jest konieczne dla podjęcia nagłych środków w celu zapobieżenia bezpośredniemu i poważnemu zagrożeniu dla bezpieczeństwa publicznego.

Jak łatwo zauważyć, art. 20 Konwencji kształtuje „czasowe" domniemanie zgody państwa zawiadamianego na prowadzenie przechwytywania na jego terytorium przez inne państwo członkowskie – może ono być swobodnie prowadzone aż do chwili podjęcia właściwej decyzji przez państwo zawiadamiane, a dopiero później wyłącznie za zgodą tego państwa. Kwestią otwartą pozostają natomiast konsekwencje, jakie dla prowadzonego przechwytywania pociąga za sobą przekroczenie przez państwo zawiadamiane terminu wydania decyzji w przedmiocie przechwytywania albo niepodjęcie takiej decyzji. Konwencja nie reguluje bowiem tej sytuacji. Wydaje się jednak, że domniemanie zgody państwa zawiadamianego będzie miało nadal zastosowanie. Art. 20 dopuszcza odmowną decyzję państwa zawiadamianego jedynie w uzasadnionych, jasno określonych sytuacjach, zaś zasadą powinno być zezwolenie na przechwytywanie. Gdyby więc założyć, że brak decyzji państwa zawiadamianego jest równoznaczny z odmową takiego zezwolenia, to państwo zawiadamiane uzyskałoby możliwość całkowicie arbitralnego zakazywania prowadzenia przechwytywania na jego terytorium, wbrew intencjom twórców Konwencji. Państwo przechwytujące nie powinno zatem ponosić negatywnych następstw zaniechania drugiej strony i dalej prowadzić podjęte czynności. Co więcej, można też przyjąć, że po przekroczeniu 96-godzinnego terminu państwo to będzie miało pełne prawo wykorzystania zebranych informacji – przyjęcie odmiennej koncepcji prowadziłoby bowiem do patowej sytuacji, w której sens dalszego prowadzenia przechwytywania stałby pod znakiem zapytania.

Więcej wątpliwości budzi natomiast skuteczność decyzji w przedmiocie przechwytywania wydanej przez państwo zawiadamiane z przekroczeniem konwencyjnego terminu, np. po dziesięciu dniach od chwili zawiadomienia. Nierespektowanie zakreślonych w Konwencji terminów niewątpliwie negatywnie wpływa na pewność pomocy prawnej, zmniejszając też skuteczność podejmowanych środków. (Warto przy tym raz jeszcze podkreślić jak istotną rolę odgrywa szybkość działania przy ściganiu zaawansowanej technologicznie prze-

stępczości.) Tym samym brak jest raczej podstaw do uznania „spóźnionej" decyzji za wiążącą dla państwa przechwytującego; nie można jednak wykluczyć, że w praktyce decyzje takie będą przez państwa respektowane.

Argumentem przemawiającym za przyjęciem powyższych wywodów jest również treść art. 20, ust. 4, pkt (d) Konwencji, zobowiązującego państwa członkowskie Unii do podjęcia koniecznych środków dla zapewnienia udzielenia państwu przechwytującemu odpowiedzi na zawiadomienie w terminie 96 godzin. Konwencja podkreśla zatem dodatkowo znaczenie określonych jej postanowieniami terminów. Warto przy tym zauważyć, że wskazany przepis wzywa państwa członkowskie do wyznaczenia czynnych całą dobę punktów kontaktowych, które umożliwiałyby odpowiednio szybkie interakcje zainteresowanych państw: zarówno przekazania zawiadomienia o planowanym bądź prowadzonym przechwytywaniu, jak i odpowiedzi na nie. W przepisie tym należy doszukiwać się wpływów rozwiązań kształtowanych przez państwa grupy G-8, a konkretniej zaproponowanej w cytowanym już dokumencie[29] koncepcji powołania międzynarodowej sieci czynnych całą dobę punktów kontaktowych. Transponowanie tej koncepcji do prawa unijnego poprzez postanowienia Konwencji należy ocenić jako istotny krok w zwalczaniu nowych form przestępczości, pozwala to bowiem na znaczne przyśpieszenie działań państw członkowskich Unii na tym polu.

Skuteczność przyjętych w art. 20 Konwencji rozwiązań w walce z korzystającą z wysokiego rozwoju nowych technologii przestępczością może być zwiększona na podstawie ust. 7 tego artykułu. Przepis ten umożliwia złożenie przez każde państwo członkowskie – i w każdym czasie – oświadczenia, że zawiadamianie go o prowadzonym na jego terytorium na podstawie art. 20 przechwytywaniu nie jest konieczne. Tym samym Konwencja przewiduje możliwość istotnego „zacieśnienia współpracy" w dziedzinie przechwytywania informacji.

Zakończenie

Konwencja z 2000 r. została już ratyfikowana przez dwanaście państw członkowskich Unii[30] i zgodnie z jej art. 27, ust. 3 wejdzie w życie 23 sierpnia 2005 r., po upływie 90 dni od daty notyfikowania

[29] *Principles and Action Plan* ..., op.cit.

[30] Państwa te to: Austria, Belgia, Dania, Estonia, Finlandia, Francja, Hiszpania, Holandia, Litwa, Łotwa, Portugalia, Węgry (stan na dzień 15 czerwca 2005 r.).

Sekretarzowi Generalnemu Rady Unii Europejskiej zakończenia procesu ratyfikacji przez ósme z kolei państwo, które było członkiem Unii w momencie przyjęcia aktu Rady ustanawiającego Konwencję .

Należy się spodziewać, że rozwiązania nowej Konwencji dotyczące przechwytywania przekazów telekomunikacyjnych przez długi czas pozostaną aktualne. Przedstawione powyżej uregulowania uznaje się dziś bowiem za najwyższy poziom współpracy w tym zakresie, możliwy do osiągnięcia w obecnej sytuacji politycznej w Unii. Przed dokonaniem jakichkolwiek dalej idących zmian w jej postanowieniach konieczne jest sprawdzenie, jak rozwiązania przyjęte w Konwencji funkcjonować będą w praktyce. Komisja Europejska zapowiedziała już, że wraz z państwami członkowskimi, przedstawicielami przemysłu (branży telekomunikacyjnej i informatycznej), użytkownikami nowych technologii oraz organami nadzorującymi ochronę danych osobowych będzie przyglądała się bacznie wprowadzaniu odpowiednich postanowień Konwencji w życie, aby zapewnić, że wszystkie nowe inicjatywy w zakresie przechwytywania są skuteczne, przejrzyste i właściwie uwzględniają interesy zaangażowanych w te działania stron.[31]

[31] *Communication from the Commission: Creating a Safer Information Society…,* op.cit.