Marcin Czosnek[1]
Grzegorz Piaskowski[2]

Tajemnica telekomunikacyjna Analiza NAT jako narzędzie do identyfikacji sprawców

Przedmiotem artykułu są dwa zagadnienia istotne z punktu widzenia organów ścigania, z którymi przychodzi im mierzyć się w trakcie praktyki stosowania prawa. W toku prowadzenia postępowań przygotowawczych często spotykaną praktyką przedsiębiorstw świadczących usługi drogą elektroniczną jest warunkowanie przekazania danych od uzyskania postanowienia prokuratora o zwolnieniu z obowiązku zachowania tajemnicy telekomunikacyjnej. W związku z tym publikacja wyjaśnia, czy dane udostępniane przez podmioty świadczące usługi drogą elektroniczną objęte są tajemnicą telekomunikacyjną. W toku realizowanych przez organy ścigania czynności o charakterze procesowym i pozaprocesowym zdarza się, że odpowiedź operatora telekomunikacyjnego nie zawiera informacji na temat sprawcy, z uwagi na niemożliwość identyfikacji użytkownika końcowego, bez podania numeru portu źródłowego. Jest to druga kwestia poruszana w artykule, który tłumaczy, czy podmioty świadczące usługi drogą elektroniczną zobowiązane są do przechowywania numeru portu źródłowego oraz czy bez numeru portu źródłowego możliwa jest identyfikacja użytkownika sieci Internet.

Na wstępie konieczne jest scharakteryzowanie tajemnicy telekomunikacyjnej. Tajemnica komunikowania stanowi naczelną gwarancję konstytucyjną wynikającą z art. 49 ustawy zasadniczej[3], której ograniczenie możliwe jest jedynie aktem prawnym rangi ustawy. Wymieniony artykuł swoim zakresem obejmuje, poza tajemnicą korespondencji, również wszelkie inne kontakty międzyosobowe[4]. W kontekście tajemnicy telekomunikacyjnej

[1] Sierż. sztab. Marcin Czosnek — asystent Instytutu Służby Kryminalnej Wydziału Bezpieczeństwa Wewnętrznego Wyższej Szkoła Policji w Szczytnie.

Adres do korespondencji: <m.czosnek@wspol.edu.pl>.

[2] Asp. szt. Grzegorz Piaskowski — specjalista Wydziału do Walki z Cyberprzestępczością Komendy Wojewódzkiej Policji w Katowicach.

Adres do korespondencji: <grzegorz.piaskowski@ka.policja.gov.pl>.

[3] Konstytucja Rzeczypospolitej Polskiej z 2 kwietnia 1997 r. (DzU nr 78, poz. 483).

[4] S. Piątek, *Prawo telekomunikacyjne. Komentarz 2013 r.*, System Informacji Prawnej Legalis.

trzeba wspomnieć, że nie tyle rodzaj danych stanowi o tym, że są one objęte tajemnicą telekomunikacyjną, ale podmiot, którego te dane dotyczą i związane z tym uregulowania zawarte w przepisach. Mając dane w postaci numeru IP — służącego do zindywidualizowania podmiotów korzystających z sieci lub usług świadczonych drogą elektroniczną, nadużyciem byłoby przypuszczenie, że każdy taki numer IP objęty jest tajemnicą telekomunikacyjną, a do wyjaśnienia tej materii konieczne jest odwołanie się do dwóch aktów prawnych, tj. do ustawy — Prawo telekomunikacyjne[5] oraz do ustawy o świadczeniu usług drogą elektroniczną[6].

Artykuł 159 ust. 1 pr. tel. enumeratywnie wylicza, jakiego rodzaju dane mieszczą się w zakresie tajemnicy telekomunikacyjnej obowiązującej w sieciach telekomunikacyjnych, służących do komunikowania się.

Sieci telekomunikacyjne zgodnie z definicją wyszczególnioną w przedmiotowej ustawie są to między innymi wszelkie systemy transmisyjne oraz inne zasoby umożliwiające transmisję sygnałów[7]. Należy podkreślić, że ochronie podlegają nie tylko dane związane z przesyłanymi komunikatami, ale wszelkie inne zdarzenia towarzyszące tym transmisjom. Obowiązywanie tajemnicy telekomunikacyjnej w sieciach niepublicznych podlega pewnym ograniczeniom w relacji z uregulowaniami tej materii w sieciach publicznych. Zgodnie z przywołanym przepisem, tajemnica telekomunikacyjna obejmuje swoim zakresem, między innymi, dane dotyczące podmiotu, a także dane o podmiocie korzystającym z publicznie dostępnej usługi telekomunikacyjnej lub żądającym świadczenia takiej usługi[8]. Podmiotem tym jest użytkownik, który jest faktycznym świadczeniobiorcą usług, jednocześnie będącym, lub nie, stroną kontraktu, którego przedmiotem jest świadczenie usług telekomunikacyjnych. Poza kryterium podmiotowym tajemnica telekomunikacyjna determinowana jest również przedmiotowo. W jej zakresie mieszczą się dane osobowe oraz inne dane o użytkownikach, choćby nie miały przymiotu osobowego i nie identyfikowały podmiotu jako określonej imiennie osoby i zawierały indywidualne informacje o użytkowniku uzyskane w związku z zawarciem umowy lub świadczeniem usługi. Ponadto, tajemnicą objęte są dane transmisyjne, dane lokalizacyjne, dane o lokalizacji, dane o próbie uzyskania połączenia oraz nieudanej próbie uzyskania połączenia. Dane transmisyjne ustawa definiuje jako dane przetwarzane dla celów przekazywania komunikatów w sieciach telekomunikacyjnych lub naliczania opłat za usługi telekomunikacyjne, w tym dane lokalizacyjne, które oznaczają wszelkie dane przetwarzane w sieci telekomunikacyjnej lub w ramach usług telekomunikacyjnych, wskazujące położenie geograficzne urządzenia końcowego użytkownika publicznie dostępnych usług telekomunikacyjnych[9]. Są to dane

[5] Ustawa z 16 lipca 2004 r. — Prawo telekomunikacyjne (DzU z 2004 r., nr 171, poz. 1800 z późn. zm.); dalej jako pr. tel.

[6] Ustawa z 18 lipca 2002 r. — o świadczeniu usług drogą elektroniczną (DzU z 2002 r., nr 144, poz. 1204 z późn. zm.).

[7] Art. 2 pkt 35 pr. tel.

[8] Art. 2 pkt 49 pr. tel.

[9] Art. 159 ust. 1 pkt 3 pr. tel.

identyfikujące zakończenie sieci, czyli stanowiące fizyczny punkt dostępu dla abonenta do publicznej sieci telekomunikacyjnej bądź adres sieciowy, popularnie znany jako adres IP[10]. Na marginesie wspomnieć należy, że jeśli dany podmiot, w ramach świadczonych usług, dysponuje numerem IP, przydzielonym użytkownikowi końcowemu, będzie miał również dostęp do innych danych identyfikujących osobę[11], wówczas nawet dynamiczne adresy IP można uznać za dane osobowe, które sytuuje się w granicach tajemnicy telekomunikacyjnej. Poza adresem IP, jako dane transmisyjne, można wymienić również numer IMEI urządzenia końcowego, czas rozpoczęcia, zakończenia i trwania połączenia oraz objętość przekazywanych danych, numer MSISDN (numer telefonu abonenta), IMSI (numer karty SIM), numer portu sieciowego lub sprzętowy adres karty sieciowej MAC (unikalny numer nadawany przez producenta karty). Komunikat to z kolei każda informacja, która jest przedmiotem wymiany lub przekazu, pomiędzy poszczególnymi użytkownikami, za pomocą publicznie dostępnych usług telekomunikacyjnych[12]. Zakres danych objętych tajemnicą telekomunikacyjną należy uzupełnić o dane wyszczególnione w art. 179 ust. 9 pr. tel., stanowiące wykaz abonentów, użytkowników lub zakończeń sieci, zawierający dane uzyskane — przy zawarciu umowy. W praktyce będą to wszelkie dane abonentów podane przez nich przy zawarciu umowy, w tym również dane o przypisanym tym abonentom numerze usługi.

Katalog podmiotów zobowiązanych do zachowania tajemnicy telekomunikacyjnej został, w obowiązującej ustawie — Prawo telekomunikacyjnie, wyznaczony szeroko i jednocześnie nieprecyzyjnie. Prawo jednostki, chroniące tajemnicę komunikowania się, w obowiązujących przepisach ma również szeroki wymiar, materializując się nie tylko w relacjach z państwem, ale również z podmiotami obsługującymi proces komunikowania z innymi uczestnikami. Z jednej strony zobowiązane podmioty zostały konkretnie wyszczególnione w art. 160 pr. tel., gdzie w ust. 3 jako obowiązanych do zachowania tajemnicy telekomunikacyjnej wskazano użytkowników sieci, którzy zapoznali się z komunikatem dla nich nieprzeznaczonym. Tytułem przykładu można wskazać, że użytkownik sieci telekomunikacyjnej, który pomyłkowo otrzymał wiadomość e-mail, przeznaczoną dla innej osoby, zobowiązany jest nie ujawniać informacji, które zapisane zostały w treści wiadomości. Poza wyżej wymienionymi podmiotami zobowiązane do zachowania tajemnicy telekomunikacyjnej są podmioty uczestniczące w wykonywaniu działalności telekomunikacyjnej w sieciach publicznych oraz podmioty z nimi współpracujące[13]. Są to przedsiębiorcy

[10] Art. 2 pkt 52 pr. tel.

[11] Wyrok Trybunału (druga izba) z 19 października 2016 r. w sprawie C582/14 — Patrick Breyer przeciwko Bundesrepublik Deutschland, <http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30d5d509ef1a4da141e49ef 5df35fec86024.e34KaxiLc3qMb40Rch0SaxyKax50?text=&docid=184668&pageIndex=0&doclang=PL&mode=lst&dir=&occ=first&part=1&cid=1171287>, 29 stycznia 2018 r.

[12] Art. 2 pkt 17 pr. tel.

[13] Art. 160 ust. 1 pr. tel.

telekomunikacyjni oraz inne podmioty — w zakresie łączącego je stosunku związanego z działalnością telekomunikacyjną w sieci publicznej niezależnie od obszaru i realizowanych podczas współpracy zadań.

Z kolei art. 159 w ust. 2 i 3 pr. tel. niejednoznacznie poszerza katalog podmiotów zobowiązanych do zachowania tajemnicy telekomunikacyjnej poprzez określenie, że z wyjątkiem przypadków określonych ustawą, ujawnianie lub przetwarzanie treści albo danych objętych tajemnicą telekomunikacyjną narusza obowiązek zachowania tajemnicy telekomunikacyjnej. Jednocześnie, ustawa wskazuje, kto i w jakich sytuacjach może zapoznawać się z danymi objętymi tajemnicą telekomunikacyjną poprzez zakaz zapoznawania się, utrwalania, przechowywania, przekazywania lub innego wykorzystywania treści lub danych objętych tajemnicą telekomunikacyjną przez osoby inne niż nadawca i odbiorca komunikatu, z pewnymi wyjątkami. Jak już wyjaśniono, komunikatem jest każda informacja, która jest przedmiotem wymiany lub przekazu pomiędzy poszczególnymi użytkownikami realizowanego za pomocą publicznie dostępnych usług telekomunikacyjnych. Chodzi więc o informacje, które w jakimś sensie identyfikują osobę będącą stroną zawartej umowy. Zgodnie z art. 2 pkt 49 pr. tel. użytkownikiem jest, jak to przywołano powyżej, podmiot korzystający z publicznie dostępnej usługi telekomunikacyjnej lub żądający świadczenia takiej usługi. W związku z tym tylko odbiorca i nadawca komunikatu, a także wyjątkowo inne podmioty, uprawnione są do zapoznawania się, utrwalania, przechowywania, przekazywania lub innego wykorzystywania treści komunikatów i danych, wyszczególnionych w art. 159 ust. 1 pr. tel. jako objętych tajemnicą telekomunikacyjną. Kluczowe znaczenie w tej konstrukcji mają wspomniane wyjątki. Dotyczą one możliwości zapoznawania się, utrwalania, przechowywania, przekazywania lub innego wykorzystywania treści komunikatów i danych wyszczególnionych w art. 159 ust. 1 pr. tel. za zgodą nadawcy i odbiorcy, których dane dotyczą, a także — jeżeli wyszczególnione powyżej czynności będą niezbędne do wykonaniu usługi lub są jej przedmiotem oraz w celu łączności podejmowanej w ramach działalności handlowej. W związku z tym ustawa dopuszcza, aby podmioty uczestniczące w wykonywaniu działalności telekomunikacyjnej w sieciach publicznych oraz podmioty z nimi współpracujące mogły korzystać z danych objętych tajemnicą telekomunikacyjną w celu wykonaniu usługi lub jeśli takie dane są przedmiotem usługi oraz w celu łączności podejmowanej w ramach działalności handlowej.

Jako możliwie najprostszy, jednocześnie najbardziej prawdopodobny, przykład naruszenia obowiązku zachowania tajemnicy telekomunikacyjnej wskazać można przedsiębiorcę telekomunikacyjnego, który ujawnia bez zachowania trybów, wynikających z ustaw szczególnych personalia i adres abonenta korzystającego — w charakterze kupującego lub sprzedającego — z platformy handlowej, któremu został przydzielony przez przedsiębiorcę, świadczącego usługę dostępu do publicznej sieci telekomunikacyjnej, określony numer IP.

Na marginesie wspomnieć należy, że ustawa — Prawo telekomunikacyjne nie zawiera przepisów skutkujących odpowiedzialnością

za przestępstwo w przypadku naruszenia obowiązku dochowania tajemnicy telekomunikacyjnej. Niemniej bezprawne ujawnienie danych telekomunikacyjnych może skutkować nałożeniem na sprawcę finansowej sankcji administracyjnej określonej w art. 209 ust. 1 pkt 24 pr. tel. Sprawca naruszenia obowiązku dochowania tajemnicy telekomunikacyjnej odpowie za przestępstwo określone w art. 266 § 1 k.k.[14] Dobrem chronionym w tym przepisie jest m.in. tajemnica zawodowa. Tajemnica telekomunikacyjna ma niewątpliwie charakter tajemnicy zawodowej. Przedmiotem ochrony jest bezpośrednio prawidłowe wykonywanie określonej działalności, w której doniosłe znaczenie odgrywa relacja oparta na zaufaniu[15]. Niewątpliwie fundamentem działalności przedsiębiorcy telekomunikacyjnego i innych profesjonalistów świadczących usługi drogą elektroniczną jest zaufanie klienta, że treść komunikatów, dane objęte tajemnicą, w tym dane dotyczące użytkownika, nie zostaną ujawnione przez depozytariusza informacji. Przestępstwo z art. 266 § 1 k.k. ma charakter czynu indywidualnie właściwego, tzn. — że może być popełnione wyłącznie przez osobę, która ze względu na pełnione funkcje lub wykonywany zawód zobowiązana jest do zachowania określonej tajemnicy. Występek może być popełniony wyłącznie po zapoznaniu się z określoną informacją przez osobę, która dobrowolnie przyjęła na siebie obowiązek utrzymania informacji w tajemnicy lub — jak ma to miejsce w przypadku tajemnicy telekomunikacyjnej — została do jej zachowania zobligowana przez przepisy ustawy. Depozytariusz informacji pełni rolę szczególnego gwaranta dochowania tajemnicy w związku z powstałym stosunkiem zaufania, który łączy go z dysponentem informacji. Relacja zaufania rodzi się przede wszystkim w związku z faktem, że samo przekazanie informacji realizowane jest przez dysponenta dobrowolnie, co nie wymaga od depozytariusza podejmowania jakichkolwiek dodatkowych czynności do jej uzyskania, gdyż wystarczającym do tego jest sam fakt pełnienia określonej funkcji lub wykonywanego zawodu. Innymi słowy — przedsiębiorca telekomunikacyjny lub podmiot świadczący usługi drogą elektroniczną, a także osoby działające w ich imieniu, jako że mają ułatwiony sposób dostępu do informacji w związku z dobrowolnym podaniem ich przez użytkownika, są szczególnymi gwarantami dochowania tajemnicy telekomunikacyjnej, a ujawnienie, może skutkować przypisaniem sprawcy odpowiedzialności karnej za opisane przestępstwo, które zagrożone jest karą grzywny, karą ograniczenia wolności albo pozbawienia wolności do lat 2. Wskazane przestępstwo można popełnić tylko umyślnie w zamiarze bezpośrednim i ewentualnym[16].

Z tajemnicą telekomunikacyjną wiąże się obowiązek retencji danych telekomunikacyjnych, do którego zobowiązany jest wyłącznie operator

[14] Ustawa z 6 czerwca 1997 r. — Kodeks karny (DzU z 1997 r., nr 88, poz. 553 z późn. zm.); dalej jako k.k.

[15] A. Zoll, *Kodeks karny. Komentarz do art. 117–277 k.k. Tom II,* Warszawa 2013, s. 1480–1481.

[16] A. Sakowicz, Art. 266 k.k. [w:] M. Królikowski, R. Zawłocki, *Kodeks karny. Część szczególna. Tom II. Komentarz do artykułów 222–316*, System Informacji Prawnej Legalis 2017.

publicznej sieci telekomunikacyjnej oraz dostawca publicznie dostępnych usług telekomunikacyjnych. Wspólnym mianownikiem dla wymienionych podmiotów jest zdefiniowane w art. 2 pkt 27 pr. tel. pojęcie przedsiębiorcy telekomunikacyjnego, przez którego rozumie się podmiot, który w ramach prowadzonej działalności gospodarczej, realizowanej na podstawie przepisów, upoważniony jest do dostarczania sieci telekomunikacyjnych oraz świadczenia usług towarzyszących i świadczenia usług telekomunikacyjnych. Świadczenie usług telekomunikacyjnych polega na realizowaniu usług za pomocą wykorzystywanej sieci, a także na odpłatnym zbywaniu we własnym imieniu i na własny rachunek usługi telekomunikacyjnej, wykonywanej przez innego dostawcę usług.

Przykładem publicznie dostępnej usługi telekomunikacyjnej jest usługa przedpłacona, świadczona w sieci komórkowej, tzw. prepaid, lub abonament telefoniczny w sieci stacjonarnej. Usługi towarzyszące związane są z siecią lub usługami telekomunikacyjnymi. Stwarzają one możliwość samego świadczenia lub mogą także stanowić wsparcie w wykonywaniu usług realizowanych w ramach sieci. Przykładem takiej usługi może być dostarczenie systemu dostępu warunkowego lub elektroniczny przewodnik po programach. Z kolei dostarczanie sieci telekomunikacyjnej polega na zapewnieniu sieci telekomunikacyjnej, w ramach której możliwe jest m.in. świadczenie usług. Retencji podlegają dane generowane w sieci telekomunikacyjnej przez okres dwunastu miesięcy od dnia połączenia lub nieudanej próby połączenia. Okres ten został skrócony nowelizacją z 16 listopada 2012 r. ustawy — Prawo telekomunikacyjne z dwudziestu czterech do dwunastu miesięcy. Skrócenie okresu retencji danych było odpowiedzią na postulaty środowisk forsujących poglądy poszerzania obywatelskich swobód konstytucyjnych oraz organów odpowiedzialnych za ochronę praw obywateli. Z punktu widzenia organów ścigania skrócenie okresu retencji danych jest niekorzystne, z uwagi na niemożność poczynienia ustaleń w zakresie danych objętych tajemnicą telekomunikacyjną, po upływie relatywnie krótkiego okresu dwunastu miesięcy. W przypadku gdy prowadzone postępowanie przygotowawcze lub realizowane czynności pozaprocesowe dotyczą zdarzenia historycznego, które miało miejsce dawniej, aniżeli dwunastomiesięczny okres retencyjny, wówczas nie ma możliwości uzyskania danych objętych tajemnicą telekomunikacyjną w związku z tym, że zgodnie z art. 180a ust. 1 pkt 1 pr. tel., z dniem upływu tego czasu, z zastrzeżeniem wyjątków określonych w przepisach odrębnych, dane takie winny zostać zniszczone. Dane zniszczone zostają w momencie ich stałego, nieodwracalnego usunięcia z zasobów przedsiębiorcy telekomunikacyjnego, tak aby przedsiębiorca był niezdolny do ich odtworzenia przy wykorzystaniu normlanych środków technicznych służących do prowadzenia działalności telekomunikacyjnej[17]. W zakresie rodzaju danych, objętych dwunastomiesięcznym okresem retencji, trzeba wskazać, że są to dane objęte tajemnicą telekomunikacyjną, co do których uwagi

[17] S. Piątek, *Prawo telekomunikacyjne. Komentarz 2013 r.*, System Informacji Prawnej Legalis.

wyszczególnione zostały powyżej. Ustawodawca szczegółowy wykaz danych objętych retencją delegował do przepisów wykonawczych.

Na uwagę zasługuje fakt, że ustawa dopuszcza wyjątki od dwunasto-miesięcznego okresu retencji niektórych danych w przypadku istnienia odrębnej do tego podstawy prawnej. Taka podstawa prawna zawarta jest w art. 164 pr. tel., wedle którego dane użytkowników końcowych mogą być przetwarzane w okresie obowiązywania umowy, a po jej zakończeniu, w okresie dochodzenia roszczeń lub wykonywania innych zadań przewidzianych w ustawie lub przepisach odrębnych. Ponadto art. 165 pr. tel. przewiduje, że przetwarzanie danych transmisyjnych, niezbędnych dla celów naliczania opłat abonenta i opłat z tytułu rozliczeń operatorskich jest dozwolone, ale tylko do końca okresu obowiązywania umowy, a po jej zakończeniu — w okresie dochodzenia roszczeń lub wykonywania innych zadań przewidzianych w ustawie lub przepisach odrębnych. Uzasadnienie dłuższego okresu retencji danych zawiera również art. 168 pr. tel., w którym zapisano, że dostawca publicznie dostępnych usług telekomunikacyjnych przechowuje dane o wykonanych usługach telekomunikacyjnych w zakresie umożliwiającym ustalenie należności za wykonanie tych usług oraz rozpatrzenie reklamacji, co najmniej przez okres dwunastu-miesięcy, a w przypadku wniesienia reklamacji — przez okres niezbędny do rozstrzygnięcia sporu. Podstawa wydłużenia okresu retencji danych zawarta została również w art. 52 pr. tel., który określa, że przedsiębiorca telekomunikacyjny przechowuje dokumentację związaną z prowadzeniem rachunkowości regulacyjnej lub kalkulacji kosztów, stosując odpowiednio przepisy rozdziału 8 ustawy z 29 września 1994 r. o rachunkowości[18]. Przepisy ustawy o rachunkowości w art. 74 wyznaczają pięcioletni termin na przechowywanie ksiąg rachunkowych, który wydaje się właściwy do zastosowania w przypadku dokumentacji związanej z prowadzeniem rachunkowości regulacyjnej lub kalkulacji kosztów przedsiębiorcy telekomunikacyjnego[19]. Ponadto art. 188 pr. tel. wskazuje, że w zakresie nieuregulowanym w ustawie do opłat, o których mowa w art. 183–185 — artykuły te dotyczą kwestii uiszczania przez przedsiębiorcę telekomunikacyjnego opłaty telekomunikacyjnej[20] oraz opłaty za częstotliwość i numerację — stosuje się odpowiednio przepisy rozdziałów 5–9 działu III ustawy z 29 sierpnia 1997 r. — Ordynacja podatkowa[21]. Uprawnienia organów podatkowych, określone w tych przepisach, przysługują prezesowi Urzędu

[18] Ustawa z 29 września 1994 r. o rachunkowości (DzU z 1994 r., nr 121, poz. 591 z późn. zm.).

[19] S. Piątek, *Prawo telekomunikacyjne*..., wyd. cyt.

[20] Opłaty wyszczególnione w art. 183–185 pr. tel. stanowią formę pozyskiwania środków przeznaczanych na sfinansowanie określonych zadań wynikających z działalności administracji telekomunikacyjnej. Opłaty stanowią dochód publiczny w rozumieniu ustawy z 27 sierpnia 2009 r. o finansach publicznych. Opłaty wnoszone są przez przedsiębiorcę telekomunikacyjnego na konto Urzędu Komunikacji Elektronicznej.

[21] Ustawa z 29 sierpnia 1997 r. — Ordynacja podatkowa (DzU z 1997 r., nr 137, poz. 926); dalej jako Ordynacja podatkowa.

Komunikacji Elektronicznej. W art. 70 zawartym w rozdziale 8 działu III Ordynacji podatkowej przewidziany został pięcioletni okres przedawnienia zobowiązań podatkowych. Wobec powyższego faktem jest, że operator telekomunikacyjny zobowiązany jest przechowywać wybrane dane telekomunikacyjne przez okres dłuższy aniżeli dwanaście miesięcy. W zależności od podstawy prawnej i polityki przyjętej przez operatora zakres tych danych może być różny. Co do zasady pozyskanie tych danych, w trybie przewidzianym dla organów ścigania, na potrzeby prowadzonych postępowań przygotowawczych lub realizowanych czynności o charakterze pozaprocesowym jest niemożliwe. Jednakże nie można wykluczyć, że w prowadzonym postępowaniu w stosunku do operatora telekomunikacyjnego przez prezesa Urzędu Komunikacji Elektronicznej, w związku z opłatą telekomunikacyjną, opłatą za częstotliwość, czy opłatą za numerację, bądź też w prowadzonym przez organy Krajowej Administracji Skarbowej wobec operatora telekomunikacyjnego postępowaniu pozyskane i włączone do materiału dowodowego zostaną dane telekomunikacyjne obejmujące swoim zakresem ponad dwunastomiesięczny okres retencji danych w zakresie określonego abonenta. Nie ma przeciwwskazań do tego, by prokurator uzyskał i wykorzystał na potrzeby prowadzonego postępowania przygotowawczego z akt postępowań prezesa UKE lub organów Krajowej Administracji Skarbowej takie informacje, w szczególności, jeśli miałoby się to przyczynić do ustalenia sprawcy przestępstwa o znacznym ciężarze gatunkowym.

Regulacje w zakresie procedury uzyskiwania przez organy ścigania i wymiaru sprawiedliwości danych, objętych tajemnicą telekomunikacyjną, określone zostały w art. 180d pr. tel. Według tego przepisu uprawnione podmioty — w tym policja na podstawie art. 20c ustawy o Policji, a także prokurator i sąd — uprawnione są do uzyskiwania danych objętych tajemnicą telekomunikacyjną określonych w przepisach art. 159 ust. 1 pkt 1 i 3–5, w art. 161 oraz w art. 179 ust. 9, które omówiono wyżej, a także danych związanych ze świadczoną usługą telekomunikacyjną na zasadach i przy zachowaniu procedur określonych w przepisach odrębnych. Sąd i prokurator, aby otrzymać dane objęte tajemnicą telekomunikacyjną, zobowiązani są wystąpić do operatora telekomunikacyjnego z żądaniem udostępnienia danych, kierowanym na podstawie art. 218 k.p.k.[22] Żądanie materializuje się w formie stosownego postanowienia określającego zakres żądanych informacji.

Istotną pozycję z punktu widzenia organów ścigania stanowią dane numeru IP wraz z numerem portu. Numer IP wraz z numerem portu ma największe znaczenie w realizowanych przez organy ścigania czynnościach wykrywczych w zakresie różnego rodzaju przestępstw, których wspólny mianownik stanowią usługi świadczone drogą elektroniczną i poczty e-mail. Podmiotami, świadczącymi ww. usługi, są m.in. przedsiębiorstwa prowadzące platformy handlowe, platformy wymiany walut,

[22] Ustawa z 6 czerwca 1997 r. — Kodeks postępowania karnego (DzU z 1997 r., nr 89, poz. 555 z późn. zm.).

przedsiębiorstwa prowadzące portale informacyjne, rozrywkowe, społecznościowe, a także banki, przedsiębiorstwa świadczące usługę hostingu[23], poczty e-mail, a także ubezpieczyciele w zakresie zawierania umów ubezpieczenia i zgłaszania roszczeń drogą elektroniczną oraz władze państwowe i samorządowe udostępniające usługi elektroniczne za pośrednictwem platformy ePUAP 2 i innej.

Przepisy prawa nie obligują podmiotów, świadczących usługi drogą elektroniczną, do retencji danych, ponieważ nie przekazują one sygnałów w sieci telekomunikacyjnej, lecz przechowują dane dostarczone przez usługobiorców. Sednem usług świadczonych drogą elektroniczną jest wysyłanie i odbieranie danych za pomocą systemów teleinformatycznych, a nie za pomocą sygnałów w sieci telekomunikacyjnej[24]. Jednakże podmioty, świadczące usługi drogą elektroniczną, mają prawo przetwarzać — na podstawie art. 18 ustawy o świadczeniu usług drogą elektroniczną — dane osobowe usługobiorcy niezbędne do nawiązania, ukształtowania treści, zmiany lub rozwiązania stosunku prawnego między nimi, a także inne dane niezbędne ze względu na właściwość świadczonej usługi lub sposób jej rozliczenia oraz dane charakteryzujące sposób korzystania przez usługobiorcę z usługi świadczonej drogą elektroniczną — dane eksploatacyjne. Numer IP oraz numer portu użytkownika, korzystającego z usług, stanowią dane eksploatacyjne. Przedsiębiorstwa, świadczące usługi drogą elektroniczną, zobowiązane są zgodnie z art. 18 ust. 6 ustawy o świadczeniu usług drogą elektroniczną, nieodpłatnie udostępnić wymienione dane organom ścigania na potrzeby prowadzonych przez nie postępowań.

W kwestii pierwszego problemu omawianego w publikacji, czyli — czy dane udostępniane przez podmioty świadczące usługi drogą elektroniczną objęte są tajemnicą telekomunikacyjną, wskazać należy, że — porównując zakres danych eksploatacyjnych wyszczególniony w art. 18 ustawy o świadczeniu usług drogą elektroniczną z danymi (objętymi tajemnicą telekomunikacyjną) wskazanymi w art. 159 ust. 1 pkt 1 i art. 161 ust. 2 pr. tel. — można przyjąć, że są to dane tożsame, które identyfikują osobę będącą stroną danej umowy. Mimo że wskazane wyżej dane pokrywają się, to kluczem, rozróżniającym je jest okoliczność, że dotyczą różnych podmiotów, klasyfikowanych na podstawie odrębnych aktów prawnych, korzystających z usług telekomunikacyjnych bądź korzystających z usług świadczonych drogą elektroniczną, a są to również różne usługi. W przypadku ustawy — Prawo telekomunikacyjne, korzystającym jest „użytkownik" (w tym będący osobą fizyczną — art. 161 ust. 2 pr. tel.) w rozumieniu przepisu art. 2 pkt 49 pr. tel. (podmiot korzystający z publicznie dostępnej usługi telekomunikacyjnej lub żądający świadczenia takiej usługi), natomiast w ustawie o świadczeniu usług drogą elektroniczną korzystającym jest — „usługobiorca", a więc osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca

[23] Usługa hostingu polega na dostarczaniu/zapewnianiu m.in. określonej objętości dysku, na którym można zamieścić dane umożliwiające funkcjonowanie strony internetowej.

[24] M. Siwicki, *Retencja danych transmisyjnych na podstawie art. 180a Prawa telekomunikacyjnego,* „Prokuratura i Prawo" 2011, nr 9, s. 113.

osobowości prawnej, która korzysta z usługi świadczonej drogą elektroniczną. Dysponując samą daną, w postaci dowolnego numeru IP, nie sposób tylko na tej podstawie określić, czy jest to dana objęta tajemnicą telekomunikacyjną, albowiem rozróżnienie takie zależne jest od tego, czy dana dotyczy usługobiorcy usług, świadczonych drogą elektroniczną i informacja żądana jest od przedsiębiorcy świadczącego usługi drogą elektroniczną czy dotyczy użytkownika sieci telekomunikacyjnej i żądana jest od przedsiębiorcy telekomunikacyjnego zobowiązanego do zachowania tajemnicy telekomunikacyjnej. Aby zobrazować to na przykładzie wskazać należy, że dane logowania do konta platformy handlowej dotyczące usługobiorcy platformy nie są objęte tajemnicą telekomunikacyjną, ponieważ są to dane, które przechowuje administrator platformy dzięki dostarczeniu ich przez samych usługobiorców. Z kolei żądanie skierowane do przedsiębiorcy telekomunikacyjnego o udostępnienie danych abonenta, któremu przydzielony został numer IP logowania do platformy handlowej, przechowywany przez administratora platformy, stanowi dane objęte tajemnicą telekomunikacyjną, ponieważ dotyczą przekazywania sygnałów w sieci telekomunikacyjnej.

Pragmatyka postępowania organów ścigania w zakresie przestępstw określanych mianem oszustw internetowych, przejęcia konta, oszustw bankowych, oszustw na szkodę tzw. parabanków i wielu innych, w ramach których następuje wymiana korespondencji sprawcy z pokrzywdzonym drogą elektroniczną, w pierwszej kolejności wymaga wystąpienia, ze strony organów ścigania do administratora platformy handlowej, banku, dostawcy poczty e-mail, administratora komunikatora o udostępnienie danych logowania sprawcy do konta. Mimo że przedsiębiorstwo, świadczące usługi drogą elektroniczną, nie musi przechowywać danych logowania do konta, to najczęściej w celu realizacji umowy zawartej z usługobiorcą, takie dane retencjonuje. Następnie, po uzyskaniu danych logowania do konta, które w najlepszym wypadku będą stanowić numer IP oraz numer portu, organy ścigania zwracają się do przedsiębiorcy telekomunikacyjnego o udostępnienie danych abonenta, któremu przydzielony został numer IP/numer portu w czasie określonego logowania do konta.

Jak już wspomniano na wstępie, bardzo często zdarza się, że w zakresie danych logowania, przedsiębiorcy, świadczący usługi drogą elektroniczną, przechowują wyłącznie dane IP bez numerów portów. Stanowi to problem w przypadku tzw. natowanych adresów IP, gdyż przedsiębiorca telekomunikacyjny nie jest w stanie zidentyfikować danych użytkownika końcowego bez informacji w zakresie przydzielonego mu numeru portu. Brak możliwości ustaleń danych użytkownika końcowego, który logował się do konta użytego do popełnienia przestępstwa uniemożliwia w czynnościach pozaprocesowych ustalenie sprawcy, a w prowadzonym postępowaniu przygotowawczym, skutkuje najczęściej umorzeniem postępowania karnego na podstawie art. 322 § 1 k.p.k. z powodu niewykrycia sprawcy czynu. Istnieje jednak sposób ustalenia danych użytkownika końcowego na podstawie tylko numeru IP i czasu logowania do konta. Tym sposobem jest analiza NAT.

W przypadku natowanego adresu IP, gdy nie posiadamy numeru portu źródłowego, otrzymywana jest od operatora telekomunikacyjnego (Orange,

T-Mobile, Play, Plus) niejednoznaczna odpowiedź zawierającą kilka lub kilkadziesiąt numerów MSISDN zarejestrowanych na różne podmioty, przez co na tym etapie nie jest możliwe wytypowanie konkretnego sprawcy. Natomiast gdy skierowane do operatora telekomunikacyjnego zapytanie zawiera numer portu źródłowego, otrzymywana odpowiedź jest jednoznaczna. Tego rodzaju sytuacja występuje ponieważ z natowanego adresu korzysta jednocześnie wiele urządzeń. Rysunek 1 obrazuje działanie NAT. Różne urządzenia łączą się Internetem poprzez adres IP 94.254.121.5. Jak widać, bez numeru portu np. 53567 nie jest możliwe sprecyzowanie, o które urządzenie chodzi.

Rysunek 1

Działanie NAT

Źródło: opracowanie własne

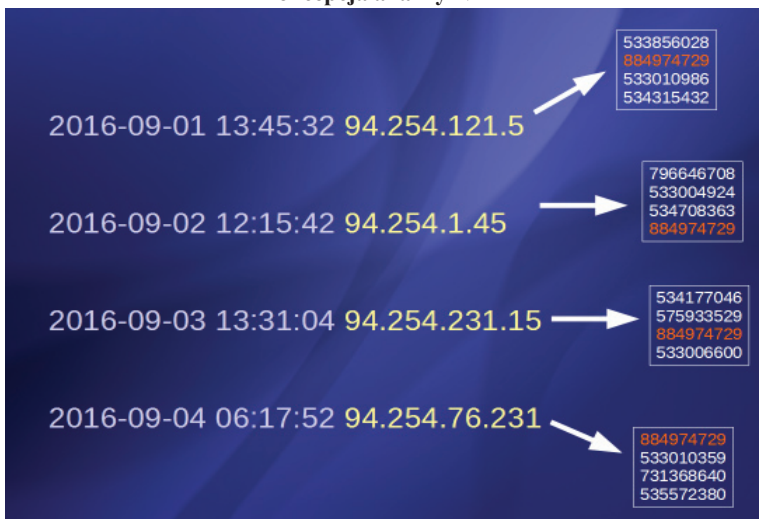
Koncepcja analizy NAT jest bardzo prosta. Na potrzeby ustaleń można założyć, że nawet jeśli osoba dokonująca połączeń internetowych często zmienia karty SIM i/lub modemy, to (dokonując kilku lub kilkunastu sprawdzeń różnych IP w kilku następujących po sobie dniach lub tygodniach) połączenia te będą wykonywane przy użyciu karty SIM o tym samym numerze abonenckim MSISDN i/lub przy użyciu tego samego urządzenia — czyli w plikach wynikowych od operatorów będzie się powtarzał sam numer MSISDN i/lub IMEI.

Analiza polega na przetworzeniu wszystkich plików uzyskanych od operatora dotyczących danego sprawdzenia. Dane należy przeszukać pod kątem występowania tych samych numerów MSISDN oraz tych samych numerów IMEI. W przypadku gdy ten sam numer MSISDN i/lub numer IMEI powtarza się wśród kilkuset innych numerów dla różnych IP w ciągu kilku lub kilkunastu dni z bardzo wysokim prawdopodobieństwem można go wytypować jako właściwy dla sprawdzanych połączeń.

Od operatora otrzymuje się o wiele więcej numerów abonenckich MSISDN niż cztery, ale celem rysunku 2 jest zobrazowanie koncepcji takiej analizy. W wyniku skierowania zapytania bez numeru portu źródłowego o cztery punkty w czasie otrzymano cztery zbiory z różnymi numerami MSISDN. Wśród nich powtarza się tylko jeden. W związku z tym jest on poszukiwanym numerem MSISDN.

Rysunek 2

Koncepcja analizy NAT



Źródło: opracowanie własne

Przeprowadzenie analizy NAT jest możliwe w przypadku każdego operatora mobilnego (Orange, T-Mobile, Play, Plus). Należy jednak spełnić pewne warunki. Trzeba posiadać, co najmniej dwa unikalne adresy IP (im więcej unikatowych numerów, tym lepiej) dotyczące jednego sprawcy. Jest to o tyle istotne, że w przypadku posiadania tego samego adresu IP z różnymi czasami, wykonanie ustaleń nie jest możliwe.

Tabela 1

Przykład kilku unikatowych numerów IP dotyczących jednego sprawcy

data	godzina	numer IP
2018.01.01	15:54:24	188.146.25.33
2018.01.01	08:09:50	188.146.124.191
2018.02.31	15:04:02	188.146.56.61
2018.02.30	13:46:54	188.146.4.51

Źródło: opracowanie własne

Tabela 2

Przykład jednego unikatowego numeru IP dotyczącego jednego sprawcy uniemożliwiającego poczynienie ustaleń

data	godzina	numer IP
2018.01.01	03:54:24	188.146.25.33
2018.01.01	08:09:50	188.146.25.33
2018.01.01	15:04:02	188.146.25.33
2018.01.01	20:46:54	188.146.25.33

Źródło: opracowanie własne

Z długoletniej praktyki wynika, że 5–10 różnych adresów IP w zupełności wystarcza do przeprowadzenia wiarygodnej analizy i nie ma potrzeby sprawdzania większej liczby adresów IP. Natomiast dwa adresy IP mogą być niewystarczające do przeprowadzenia jednoznacznej analizy.

W przypadku natowanych adresów IP należy od operatora uzyskać listę numerów MSISDN (w przypadku Play oraz Orange otrzymuje się również numery IMEI), które „wychodziły na świat", tj. do Internetu poprzez dany adres IP.

Zapytania w formie postanowień prokuratorskich powinny zawierać żądanie wydania listy numerów MSISDN, które łączyły się przez dane IP. Błędem będzie sformułowanie żądania wskazania przez operatora danych konkretnego użytkownika. Pomimo zastosowania takiego sformułowania należy spodziewać się, że żądanie takie nie zawsze zostanie zrozumiane właściwie. Należy wtedy wyjaśnić, że dane takie są potrzebne w celu wykonania analizy NAT, operator nimi dysponuje, przez co ma możliwość ich dostarczenia.

Jest oczywiste, że powinno żądać się danych w formie elektronicznej. Podczas żądania jakichkolwiek danych telekomunikacyjnych z uwagi na łatwość przetwarzania nigdy nie powinno się sięgać po nie w formie wydruku na papierze.

W przypadku uzyskiwania danych, udostępnianych przez operatora za pośrednictwem interfejsów, ustalenia powinny być dokonane w sposób opisany poniżej.

Osoby, korzystające z interfejsu Poezja (Orange) powinny wybrać typ zapytania „POŁĄCZENIA IP" (a nie „USTALENIA DYNAMICZNE IP"). Dla przykładowego IP: 2018-03-06 21:10:15 37.47.123.8 pola w formatce należy wypełnić następująco:

Tabela 3

Przykład wypełnienia formatki w interfejsie Poezja

DATA OD	20180306
CZAS OD	211012
DATA DO	20180306
CZAS DO	211018

Źródło: opracowanie własne

Z praktyki wynika, że dobrze jest margines czasowy ustawić na ± 3 sekundy.

W przypadku interfejsu Finezja (T-Mobile) należy wybrać „20. MSISDN dla IP 01.06.2015 (kw. niestandardowa)". Podobnie jak w przypadku Orange margines czasowy ustawić można na ± 3 sekundy.

Korzystając z interfejsu Ruda (Play), należy wybrać typ zapytania „dane transmisyjne", kategoria zapytania „IP" oraz zaznaczyć opcję „Zapytanie bez numeru portu". Nie ma potrzeby ustawiania marginesu czasowego.

W przypadku sieci Plus należy zadać odpowiednio sformułowane zapytanie niestandardowe.

Analizę można przeprowadzić za pomocą aplikacji arkusz kalkulacyjny lub przy wykorzystaniu autorskich programów P4A oraz IDA.

Program P4A jest dedykowany dla plików operatora Play. Programu IDA można używać do analizy plików wszystkich operatorów, ale jego użycie jest mniej wygodne. W planach jest stworzenie automatycznego narzędzia dla wszystkich operatorów mobilnych.

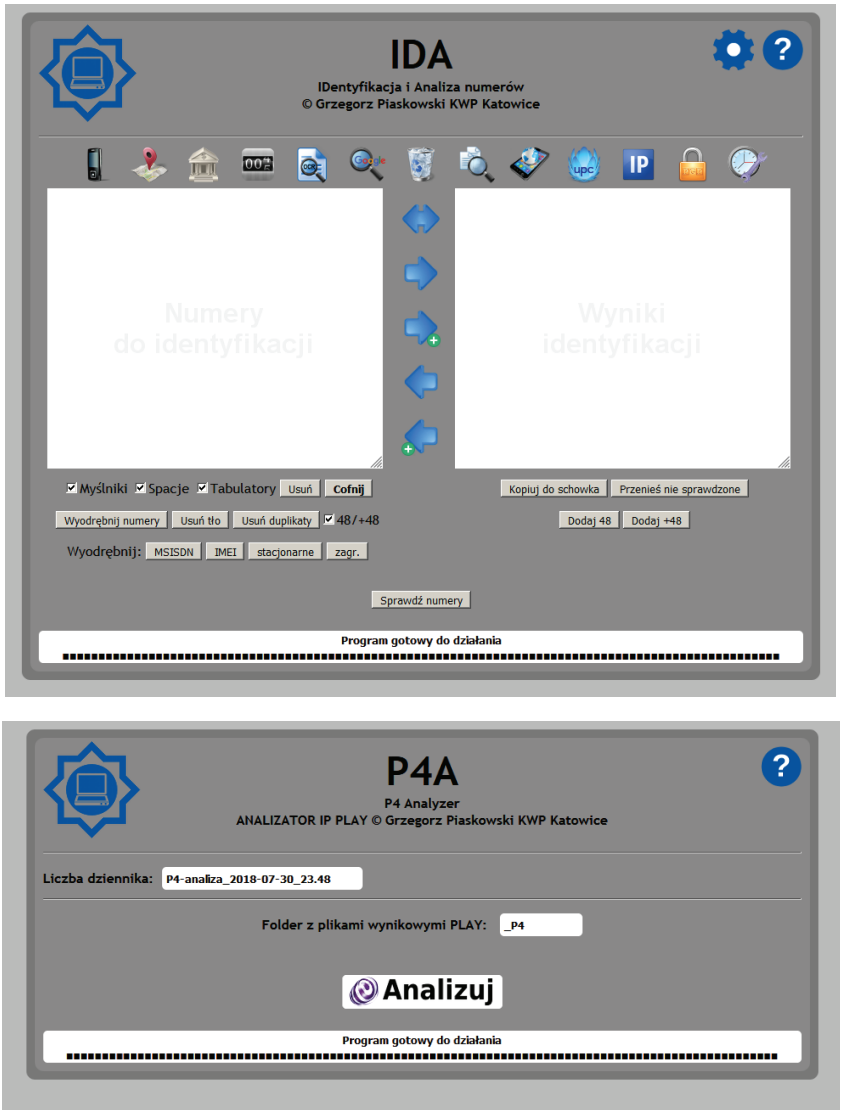
Aby uzyskać programy należy skontaktować się z asp. szt. Grzegorzem Piaskowskim z Wydziału dw. z Cyberprzestępczością w KWP w Katowicach.

Analizę NAT można również przeprowadzić dla stacjonarnych operatorów internetowych. Jest to jednak zagadnienie nieco trudniejsze. Takie analizy mają bardziej indywidualny charakter i nie da się sprowadzić do jednego uniwersalnego prostego algorytmu. Należy wystąpić do operatora o fragmenty logowań za odpowiednie okresy czasu. Następnie pliki należy przeszukać pod kątem powtarzającego się MAC adresu, docelowego adresu IP lub wewnętrznego adresu IP. Jest to zależne od kilku czynników, np. rodzaju dostawcy usług elektronicznych, od którego pochodzą logowania z adresami IP, sposobu zbierania danych przez operatora telekomunikacyjnego itp.

Na koniec należy wspomnieć o właściwej pragmatyce kierowania ze strony organów ścigania do dostawcy usług elektronicznych zapytań o dane. Nigdy nie ma pewności czy w logowaniach będą natowane adresy IP. Gdy organy ścigania zwracając się do dostawcy usług elektronicznych wskażą zbyt krótki okres czasu potencjalnej aktywności sprawcy np. jeden dzień, otrzymana próbkę adresów IP może być zbyt mała do skutecznego przeprowadzenia analizy NAT. Dlatego minimalnym analizowanym okresem powinno być co najmniej kilka dni. Logowania z okresu jednego miesiąca prawie zawsze umożliwiają przeprowadzenie analizy NAT. Niestety w wielu przypadkach można spotkać się z sytuacją, w której organy ścigania występują do dostawcy usług elektronicznych o dane wyłącznie za dzień, w którym miało miejsce przestępstwo. Jest to bardzo zła praktyka, skutkująca otrzymaniem bezwartościowych danych, a w konsekwencji umorzeniem postępowania. Na rysunku 3 przedstawiono zrzut ekranu autorskich interfejsów, umożliwiających przeprowadzenie w prosty sposób analizy NAT.

Rysunek 3

Zrzut ekranu autorskich programów IDA oraz P4



Źródło: opracowanie własne

Podsumowując, w zakresie pierwszego problemu omawianego w publikacji — czy dane udostępniane przez podmioty świadczące usługi drogą elektroniczną objęte są tajemnicą telekomunikacyjną — wskazać należy, że w związku z faktem, że podmioty świadczące usługi drogą elektroniczną, przekazują dane dotyczące korzystającego z sieci definiowanego jako „usługobiorcy" — a więc osoby fizycznej, osoby prawnej albo jednostki

organizacyjna nieposiadającej osobowości prawnej, która korzysta z usługi świadczonej drogą elektroniczną — to nie są to dane objęte tajemnicą telekomunikacyjną. Wobec tego warunkowanie przez przedsiębiorstwa świadczące usługi drogą elektroniczną przekazania danych usługobiorców od uzyskania postanowienia prokuratora o zwolnieniu z obowiązku zachowania tajemnicy telekomunikacyjnej jest nieuzasadnione. Ponadto przedsiębiorstwa, świadczące usługi drogą elektroniczną, zobowiązane są zgodnie z art. 18 ust. 6 świadczeniu usług drogą elektroniczną, nieodpłatnie udostępnić wymienione dane organom ścigania na potrzeby prowadzonych przez nie postępowań. W kontekście drugiego problemu poruszonego na wstępie artykułu — czy podmioty świadczące usługi drogą elektroniczną zobowiązane są do przechowywania numeru portu źródłowego oraz czy bez numeru portu źródłowego możliwa jest identyfikacja użytkownika sieci Internet — należy mieć na uwadze, że przepisy prawa nie obligują podmiotów świadczących usługi drogą elektroniczną do retencji danych, ponieważ nie przekazują one sygnałów w sieci telekomunikacyjnej, lecz przechowują dane dostarczone przez usługobiorców. Sednem usług, świadczonych drogą elektroniczną jest wysyłanie i odbieranie danych, za pomocą systemów teleinformatycznych, a nie za pomocą sygnałów w sieci telekomunikacyjnej. Jak zostało to wyjaśnione, za pomocą analizy NAT możliwa i nieskomplikowana jest identyfikacja użytkownika sieci Internet bez przydzielonego mu numeru portu źródłowego. Podstawową kwestią w tym zakresie jest dysponowanie co najmniej dwoma unikalnymi adresami IP (im więcej unikatowych numerów, tym lepiej), dotyczące jednego sprawcy, a następnie wytypowanie powtarzającego się w tych adresach IP numeru MSISDN.

Słowa kluczowe: tajemnica, telekomunikacja, analiza, NAT, dane, usługi, świadczenie, elektronicznie, przedsiębiorca, proces, IP

Streszczenie: Celem publikacji jest przybliżenie problematyki związanej z zakresem obowiązywania tajemnicy telekomunikacyjnej, a w tym określeniem podmiotów zobowiązanych do jej zachowania. Artykuł odpowiada ponadto na pytanie — czy podmioty świadczące usługi drogą elektroniczną zobowiązane są do przechowywania numeru portu źródłowego oraz czy bez numeru portu źródłowego możliwa jest identyfikacja użytkownika końcowego sieci Internet.

Keywords: secrecy, telecommunications, analysis, NAT, data, services, provision, electronic, entrepreneur, process, IP

Summary: The purpose of this publication is to present the issues related to the scope of telecommunications secrecy, including the definition of entities obliged to maintain it. The article also answers the question whether entities providing services by electronic means are obliged to store the source port number and whether without the source port number it is possible to identify the Internet end-user.