Kamila Majchrzak
Piotr Misztal

CHARAKTER DOWODOWY RETENCJI DANYCH TELEKOMUNIKACYJNYCH W POLSKIM POSTĘPOWANIU KARNYM

I. Wstęp

Powszechna dostępność przenośnych aparatów telefonicznych i kart typu pre-paid umożliwiła zwiększenie aktywności przestępców. Szybkość porozumiewania się i przekazywania informacji, ale także w dużej mierze anonimowość utrudniło znacznie wykrywanie przestępstw i ich sprawców. Na tak zmieniającą się rzeczywistość, obojętnie nie mogły pozostać organy ścigania. Zmiana metod pracy Policji polegała w pierwszej kolejności na zastosowaniu tzw. analizy kryminalnej, czyli sposobu zbierania danych teleinformatycznych oraz dokonywania ich weryfikacji dla celów procesowych. W komendach wojewódzkich powołano wydziały specjalizujące się w interpretacji tego rodzaju informacji. Na domiar tego powołano Biuro Ekspertyz Sądowych, którego zasadniczym zadaniem jest sporządzanie opinii specjalistycznych, które później stanowią dowód w procesie karnym. Biuro Ekspertyz Sądowych zatrudnia wysoko wyspecjalizowanych biegłych posiadających stosowną wiedzą oraz wieloletnie doświadczenie zawodowe. Opinie z zakresu technik telekomunikacyjnych i teleinformatycznych obejmują badanie zasięgu stacji BTS, przemieszczanie się abonentów w czasie rzeczywistym, kryminalistyczną analizę faktów i związków między nimi[1]. Pozyskanie tych informacji nie byłoby możliwe bez retencji danych, tj. rejestrowania przez operatorów telekomunikacyjnych bilingów oraz innych informacji teleinformatycznych, które są konieczne do ustalenia, kto z kim, kiedy i gdzie się kontaktował lub próbował kontaktować za pomocą sieci GSM.[2]

II. Stacje BTS i pojęcie bilingu telefonicznego

Komunikowanie się i przesyłanie danych zakodowanych cyfrowo jest możliwe dzięki istnieniu sieci anten naziemnych BTS (Base Transceiver Station). Są to podstawowe jednostki, dzięki którym telefon komórkowy łączy się z siecią GSM. Zasięg jednej stacji bazowej określany jest mianem „komórki". Zakres działania anten dla skutecznego i wydajnego funkcjonowania sieci na danym obszarze pokrywa się. Zasięg pojedynczej stacji bazowej jest zależny od wielu czynników, w tym od rodzaju sieci GSM, ukształtowania terenu, a także od ilości abonentów logujących się do niej w danym czasie. Na obszarach słabo zaludnionych wynosi około 30 kilo metrów. W większych skupiskach miejskich operatorzy korzystają z wyższych standardów, takich jak 1800 GSM lub 1900 GSM. Zasięg jest wówczas znacznie mniejszy i nie przekracza 6-8 kilometrów. Stacje BTS połączone są ze sobą za pomocą tzw. kontrolerów stacji bazowych (Base Station Controler), których zasadniczym zadaniem jest przesyłanie i odbieranie zakodowanego cyfrowo sygnału pomiędzy stacjami BTS a cyfrową centralą telefoniczną - MSC (Mobile Switching Centre)[3]. Terminal telefoniczny loguje się do najbliższej stacji bazowej, która następnie przesyła dane do kontrolera stacji bazowej. Zadaniem BSC jest przełączanie sygnału podczas zmiany pozycji telefonu na obszarze sieci i przesyłanie go dalej do cyfrowej centrali telefonicznej[4].

Ustalenie lokalizacji następuje metodą triangulacji. Jednakże na szczególną uwagę zasługuje fakt, iż aby namierzenie było zakończone pomyślnie, telefon musi znaleźć się na obszarze co najmniej trzech stacji bazowych. Na terenach miejskich, gdzie skupisko stacji bazowych jest duże, ustalenie lokalizacji abonenta możliwe jest z dokładnością do 50 metrów. Natomiast na otwartych przestrzeniach, od 300 metrów wzwyż, w zależności jak daleko od siebie położone są poszczególne stacje bazowe BTS[5].

1 Biuro Ekspertyz Sądowych, Ekspertyzy z zakresu technik telekomunikacyjnych i teleinformatycznych [online], dostęp: 26.03.2015, http://www.ekspertyzy.net.pl/techniki-telekomunikacyjne-i-teleinformatyczne-ekspertyzy-kryminalistyczne.

2 M. Domagalski, Adwokaci chcą ograniczyć zbieranie billingów [online], „Rzeczpospolita", dostęp: 26.03.2015, http://prawo.rp.pl/artykul/661107.html.

3 Zasada działania telefonu komórkowego [online], dostęp: 26.03.2015, http://inwigilacja24.com/telefonia/50.

4 W. Klicki, A. Obem, K. Szymielewicz, Telefoniczna kopalnia informacji. Przewodnik [online], dostęp: 26.03.2015, https://telefoniczna-kopalnia.panoptykon.org/?ver=dv.

5 Lokalizowanie telefonu komórkowego [online], dostęp: 26.03.2015, http://inwigilacja24.com/telefonia/namierzanie-telefonu-komorkowego; P. Jagóra, Lokalizacja w Orange [online], dostęp: 26.03.2015, http://blog.orange.pl/technologiczny/entry/lokalizacja-w-orange/.

Warto nadmienić, że lokalizacja telefonu komórkowego może nastąpić także za pomocą systemu GPS (Global Positioning System). Geolokalizacja za pomocą analizy logowań terminalu do stacji BTS nie jest tak skuteczna jak lokalizacja przy pomocy systemu GPS. Ma to znaczenie w szczególności w miejscach otwartych przestrzeni, gdzie stacje bazowe są od siebie znacznie oddalone. Korzystanie z systemu GPS umożliwia ustalenie aktualnego miejsca, w którym znajduje się telefon z dokładnością do kilku metrów. Z optyki niniejszych rozważań nie może zejść jednak fakt, że korzystanie z ustalenia lokalizacji następuje bez wiedzy abonenta oraz bez konieczności jakiejkolwiek ingerencji w oprogramowanie telefonu, którego miejsce ustalamy, co ma szczególne znaczenia dla prowadzenia czynności operacyjno – rozpoznawczych na przedpolu procesu karnego.

W polskim prawie brak jest legalnej definicji bilingów[6]. Jak wynika z lektury art. 80 Prawa telekomunikacyjnego, dostawca publicznie dostępnych usług telefonicznych dostarcza abonentowi nieodpłatnie z każdą fakturą podstawowy wykaz wykonywanych usług telekomunikacyjnych zawierający informację o zrealizowanych płatnych połączeniach z podaniem, dla każdego typu połączeń liczby jednostek rozliczeniowych odpowiadającej wartości zrealizowanych przez abonenta połączeń.

Z punktu widzenia niniejszych rozważań przez biling należy rozumieć wykaz połączeń telefonicznych (przychodzących i wychodzących), jak i innych transmisji telekomunikacyjnych np. sms, mms, video, voice.

W demokratycznym państwie prawa pojawił się problem weryfikacji dostępnych danych telekomunikacyjnych oraz ewentualnych powiązań między nimi a czynami przestępnymi. Zasadniczym problemem jest bowiem ilość tych danych, co z kolei może prowadzić do łatwych omyłek. Dzięki stosowaniu analizy kryminalnej wspomaganej odpowiednim oprogramowaniem, które umożliwia typowanie, weryfikowanie danych na podstawie bilingów telefonicznych, analizy logowania się telefonu do stacji BTS możliwe jest ustalanie związku przyczynowo - skutkowego pomiędzy określonymi zdarzeniami mogącymi mieć znaczenie dla konkretnego postępowania karnego. W związku z powyższym, szczególne znaczenie dla postępu w polskiej kryminalistyce stanowi obecność Polskiej Platformy Bezpieczeństwa Wewnętrznego, która ma na celu „stworzenie zintegrowanych narzędzi technologicznych i informatycznych, wspomagających działania na rzecz bezpieczeństwa publicznego”[7]. Na szczególną aprobatę zasługuje stworzenie programu AFIZ. Analizator Faktów i Związków, Moduł analiza bilingów wersja 1.0 to narzędzie technologiczne, które służy funkcjonariuszom Policji z wydziałów kryminalnych do analizy bilingów. AFIZ automatycznie dokonuje weryfikacji treści bilingów, a następnie sporządza wyniki tak dokonanej analizy.

III. Regulacje prawne dotyczące retencji danych telekomunikacyjnych

Problematyka retencji danych telekomunikacyjnych stanowi przedmiotem regulacji prawa europejskiego. Przyczynkiem do podjętych w 2006 roku przez Parlament Europejski i Radę prac w tym zakresie były ataki terrorystyczne w Madrycie i Londynie.

Zgodnie z art. 1 dyrektywy 2006/24/WE, celem aktu było zbliżenie przepisów państw członkowskich w zakresie obowiązków dostawców ogólnie dostępnych usług łączności elektronicznej lub publicznych sieci łączności w zakresie zatrzymywania pewnych danych przez nie generowanych lub przetwarzanych, aby zapewnić dostępność przedmiotowych danych do celu dochodzenia, wykrywania i ścigania poważnych przestępstw, określonych w ustawodawstwie każdego państwa członkowskiego. Dyrektywa odnosi się do danych o ruchu i lokalizacji oraz do powiązanych z nimi danych niezbędnych do identyfikacji abonenta lub zarejestrowanego użytkownika, z wyłączeniem jednak samej treści komunikatów elektronicznych, w tym informacji uzyskiwanych przy użyciu sieci łączności elektronicznej. Zatrzymane dane winny być udostępniane jedynie właściwym organom krajowym, w szczególnych przypadkach i zgodnie z krajowym ustawodawstwem oraz zgodnie z zasadą konieczności i proporcjonalności. W przypadku telefonii komórkowej zatrzymaniu podlegają następujące kategorie danych:

- numer nadawcy połączenia oraz nazwisko i adres abonenta lub zarejestrowanego użytkownika;
- wybierany numer/-y odbiorcy/-ów połączenia (w tym numery, na które połączenie jest przekierowywane/przełączane) oraz nazwisko/-a i adres/-y abonenta/-ów lub zarejestrowanego/-ych użytkownika/-ów;
- data i dokładny czas rozpoczęcia i zakończenia połączenia;
- rodzaj połączenia - wykorzystana usługa telefoniczna;
- narzędzie komunikacji lub tego, co może służyć za narzędzie komunikacji - numery nadawcy i odbiorcy połączenia, międzynarodowy numer tożsamości telefonicznej abonenta mobilnego (IMSI) nadawcy połączenia, międzynarodowy numer fabryczny mobilnego aparatu telefonicznego (IMEI) nadawcy połączenia, IMSI i IMEI odbiorcy połączenia;

6 A. Staszak, Prawne podstawy dopuszczalności żądania bilingów, „Przegląd Bezpieczeństwa Wewnętrznego” 2011, nr 4, s. 75.

7 Polska Platforma Bezpieczeństwa Wewnętrznego [online], dostęp: 26.03.2015, http://www.ppbw.pl/glowna_o_ppbw.php.

- w przypadku anonimowych usług opłaconych z góry (pre-paid) data i dokładny czas początkowej aktywacji usługi oraz etykieta lokalizacji (identyfikator komórki), z której dokonano aktywacji;

- etykieta lokalizacji (identyfikator komórki) na początku połączenia oraz dane pozwalające ustalić położenie geograficzne komórek przez odniesienie się do ich etykiet lokalizacji (identyfikatorów komórki) w czasie, przez który zatrzymywane są dane odnośnie połączenia.

Wskazane wyżej dane mają być zatrzymywane na okresy nie krótsze niż 6 miesięcy oraz nie dłuższe niż dwa lata od daty połączenia. Wszystkie dane, z wyjątkiem tych, które zostaną udostępnione i zachowane, podlegają zniszczeniu pod koniec okresu zatrzymania.

W tym miejscu należy wskazać, że 8 kwietnia 2014 roku Trybunał Sprawiedliwości Unii Europejskiej orzekł, iż dyrektywa ta jest nieważna[8]. Trybunał uznał, że dyrektywa ingeruje w prawa podstawowe do poszanowania życia prywatnego i do ochrony danych osobowych, jednakże nie narusza zasadniczej treści praw podstawowych, bowiem nie pozwala na zapoznawanie się z treścią komunikatów. Podkreślono, że choć retencja danych odpowiada celowi w postaci interesu ogólnego, jakim jest zwalczanie poważnej przestępczości, to prawodawca Unii przekroczył granice, które wyznacza zasada proporcjonalności.

Europejska dyrektywa retencyjna została wdrożona do polskiego porządku prawnego ustawą z dnia 24 kwietnia 2009 r. o zmianie ustawy - Prawo telekomunikacyjne oraz niektórych innych ustaw. Na operatorów publicznej sieci telekomunikacyjnej oraz dostawców publicznie dostępnych usług telekomunikacyjnych został nałoży obowiązek zatrzymywania i przechowywania, na własny koszt, przez okres 24 miesięcy danych niezbędnych do:

- ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego: inicjującego połączenie oraz do którego kierowane jest połączenie;
- określenia daty i godziny połączenia oraz czasu jego trwania, rodzaju połączenia, lokalizacji telekomunikacyjnego urządzenia końcowego.

Po upływie ww. okresu dane te winny być niszczone, z wyjątkiem tych, które zostały zabezpieczone, zgodnie z przepisami odrębnymi.

Ustawą z dnia 16 listopada 2012 roku o zmianie ustawy - Prawo telekomunikacyjne oraz niektórych innych ustaw, wobec licznych głosów sprzeciwu ze strony opinii publicznej, skrócono okres, przez który operatorzy obowiązani są przechowywać zatrzymane dane telekomunikacyjne, z 24 do 12 miesięcy.

Zatrzymywanie i udostępnianie danych retencyjnych następuje nieodpłatnie, na koszt operatora, co nie jest zjawiskiem powszechnym w Europie (odpłatność wprowadzono m. in. w Belgii, Danii, Francji, Holandii, Wielkiej Brytanii). Zasadę nieodpłatnego udostępniania danych retencyjnych potwierdził Sąd Najwyższy: „Przepis art. 180a ust. 1 pkt 2 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne nakłada na operatorów publicznej sieci telekomunikacyjnej oraz dostawców ogólnie dostępnych usług telekomunikacyjnych obowiązek udostępniania, to jest wyszukiwania, tworzenia stosownych zestawień i przesyłania za pomocą sieci telekomunikacyjnej uprawnionym podmiotom, w tym sądowi i prokuratorowi danych, o których mowa w art. 180c ust. 1 ustawy. Tak rozumiane koszty udostępniania tych danych obciążają operatora lub dostawcę i nie mogą wchodzić w skład kosztów sądowych, a zatem nie stanowią wydatków, o których mowa w art. 618 k.p.k.”[9].

Podmiotami uprawnionymi do pozyskania danych telekomunikacyjnych są Policja (art. 20c ustawy o Policji), Straż Graniczna (art. 10b ustawy o SG), Agencja Bezpieczeństwa Wewnętrznego oraz Agencja Wywiadu (art. 28 ustawy o ABW oraz AW), Centralne Biuro Antykorupcyjne (art. 18 ustawy o CBA) i organy kontroli skarbowej (art. 36b ustawy o kontroli skarbowej). Udostępnienie danych telekomunikacyjnych może nastąpić w celu realizacji zadań przypisanych danemu organowi (CBA, ABW/AW) bądź zapobieżenia lub wykrycia przestępstw (Policja, SG, organy kontroli skarbowej), ale ustawodawca w żaden sposób nie odnosi się do ich rodzaju (nie kataloguje, jak w przypadku kontroli operacyjnej). Możliwe jest zatem żądanie wydania danych w każdej kategorii spraw, bez względu na jej wagę. Brak jest jedynie możliwości występowania z tego typu żądaniem w sprawach o wykroczenia[10].

Operatorzy, co do zasady, udostępniają przedmiotowe dane na pisemny wniosek organu centralnego (np. w przypadku Policji - Komendanta Głównego Policji) i organu szczebla wojewódzkiego (np. komendanta wojewódzkiego Policji) oraz osobom upoważnionym przez ww. organy, jak również na ustne żądanie funkcjonariusza posiadającego pisemne upoważnienie ww. osób bądź za pośrednictwem sieci telekomunikacyjnej funkcjonariuszowi posiadającemu pisemne upoważnienie ww. osób. W ostatnim przypadku udostępnianie danych telekomunikacyjnych odbywa się bez udziału pracowników podmiotu prowadzącego działalność telekomunikacyjną lub przy niezbędnym ich udziale, jeżeli możliwość taka jest przewidziana w porozumieniu zawartym pomiędzy organem centralnym a tym podmiotem. Marek

8 Wyrok TSUE z dn. 8 kwietnia 2014 r., C-293/12 i C-594/12, Dz.U.UE.C.2014.175.6/2.

9 Postanowienie SN z dn. 25 marca 2010 r., I KZP 37/09, OSNKW 2010/5/43.

10 A. Staszek, Prawne podstawy dopuszczalności żądania bilingów, „Przegląd Bezpieczeństwa Wewnętrznego” 2011, nr 4, s. 72-86.

Dyjasz, dyrektor Biura Kryminalnego KGP, ujawnił, że w polskiej policji 327 funkcjonariuszy może w każdej chwili podłączyć się komputerowym interfejsem do każdego z operatorów sieci komórkowych i sprawdzić połączenia, a także miejsca logowania w stacjach bazowych (BTS) każdego numeru komórkowego, jaki uznają za stosowne[11].

Uzyskane materiały, mające znaczenie dla postępowania karnego, przekazywane są właściwemu prokuratorowi. W takiej sytuacji nie ma zatem potrzeby ponownego zwracania się przez prokuratora o udostępnienie danych telekomunikacyjnych, co jednak w praktyce bardzo często ma miejsce[12]. Jakkolwiek przepisy wyraźnie tego nie regulują, żądanie ponownego pozyskiwania w postępowaniu karnym dokumentów już wcześniej zdobytych od podmiotów trzecich należałoby traktować jako nieracjonalne[13]. Wszelki pozostałe dane winny być niezwłocznie zniszczone w sposób komisyjny i protokolarny, ustawodawca jednakże nie wskazuje precyzyjnego terminu w jakim powinny one zostać usunięte. Na domiar tego, ustawy o CBA oraz ABW/AW w ogóle nie przewidują regulacji w tym zakresie.

Kodeks postępowania karnego reguluje udostępnianie danych telekomunikacyjnych sądom i prokuratorom. Zgodnie z art. 218 k.p.k. podmioty prowadzące działalność telekomunikacyjną obowiązane są wydać sądowi lub prokuratorowi, na żądanie zawarte w postanowieniu, dane telekomunikacyjne, jeżeli mają one znaczenie dla toczącego się postępowania. Postanowienie doręcza się jednocześnie abonentowi telefonu lub nadawcy, którego wykaz połączeń lub innych przekazów informacji został wydany, przy czym może ono być odroczone na czas oznaczony, niezbędny ze względu na dobro sprawy, lecz nie później niż do czasu prawomocnego zakończenia postępowania. Podobnie jak w przypadku udostępniania danych telekomunikacyjnych organom ścigania, ustawodawca nie wprowadza dalej idących ograniczeń co do kręgu lub szczególnych kwalifikacji przestępstw, w związku z którymi dane te mogą być pozyskiwane, nie wprowadza też ograniczeń co do podmiotów, wobec których mogą one zostać wykorzystane, a jedynym w zasadzie kryterium, od którego uzależnia ich użycie, jest przydatność dla toczącego się postępowania karnego[14].

Porównując zasady udostępniania danych telekomunikacyjnych sądom i prokuratorom oraz innym uprawnionym do tego podmiotom uwidacznia się brak zachowania racjonalnej proporcji w ich określeniu. Sąd/prokurator, by otrzymać ww. informacje musi wydać postanowienie oraz zawiadomić o tym zainteresowanego, a żądane dane muszą pozostawać w ścisłym związku z prowadzonym postępowaniem karnym. Z drugiej strony, organy ścigania bez podejmowania żadnej indywidualnej decyzji w sprawie, w każdej dogodnej dla siebie chwili, również przed wszczęciem postępowania na etapie czynności operacyjnych, nawet bez udziału pracownika podmiotu udostępniającego dane oraz bez wiedzy inwigilowanej jednostki może wejść w posiadanie określonych informacji. Podejmowane przez organy ścigania czynności pozostają zatem poza wszelką kontrolą zarówno sądową, jak i obywatelską. Przyjęcie takiego kształtu regulacji prawnej procesu udostępniania danych wydaje się być pozbawione jakiejkolwiek logiki i godzi w podstawowe prawa człowieka i obywatela.

W efekcie trwającej dyskusji społecznej i negatywnej oceny prac polskiego ustawodawcy nad regulacją retencji danych, Rzecznik Praw Obywatelskich i Prokurator Generalny wystąpili ze skargami do Trybunału Konstytucyjnego. W konsekwencji, dnia 30 lipca 2014 roku Trybunał Konstytucyjny orzekł, iż część przepisów regulujących retencję danych jest niezgodna z Konstytucją i straci moc z końcem stycznia 2016 roku[15]. Podobne wyroki zapadły również w innych państwach Unii Europejskiej, w szczególności w Rumunii, gdzie sąd opowiedział się kategorycznie przeciwko zasadzie prewencyjnego gromadzenia danych o obywatelach i uznał, iż retencja danych godzi w zasadę domniemania niewinności[16]. Do podobnych wniosków doszła również Najwyższa Izba Kontroli[17] stwierdzając, że obowiązujące przepisy regulujące pozyskiwanie przez uprawnione podmioty danych telekomunikacyjnych nie chronią w stopniu wystarczającym praw i wolności obywatelskich przed nadmierną ingerencją ze strony państwa. Należy bowiem pamiętać, że „z ochrony przewidzianej dla dóbr osobistych korzysta tajemnica rozmów, tożsamość uczestniczących w niej osób, ich numery telefoniczne, adresy poczty elektronicznej, a także informacje o samym fakcie prowadzenia rozmowy, czasie jej trwania, próbach połączenia oraz treści przekazu. Z tego względu tajemnica obejmuje również tzw. bilingi”[18].

11 Ponad 300 policjantów z dostępem do naszych bilingów [online], dostęp: 26.03.2015, http://www.tvn24.pl/wiadomosci-z-kraju,3/ponad-300-policjantow-z-dostepem-do-naszych-bilingow,171897.html.

12 Tamże.

13 D. Szumiło-Kulczycka, Czynności operacyjno-rozpoznawcze i procesowe (na tle prawa polskiego i niemieckiego), „Państwo i Prawo” 2011, nr 11, s. 71-83.

14 Tamże.

15 Wyrok TK z dn. 30 lipca 2014 r., K 23/11, OTK-A 2014/7/80, Dz.U.2014/1055.

16 Wyrok Curtea Constitutionala a Romaniei z dn. 8 października 2009 r., Decizia nr.1.258, Monitorul Oficial nr.798 din 23.11.2009, [online] http://www.legi-internet.ro/fileadmin/editor_folder/pdf/Decizie_curtea_constitutionala_pastrarea_datelor_de_trafic.pdf, http://www.legi-internet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf (wersja angielskojęzyczna).

17 NIK na temat billingów [online], dostęp: 26.03.2015, http://www.nik.gov.pl/aktualnosci/nik-na-temat-billingow.html.

18 Wyrok SA w Warszawie z dn. 26 kwietnia 2013 r., I ACa 1002/12, LEX nr 1322739.

IV. Charakter dowodowy bilingów oraz analizy logowań do stacji BTS

Dowodem w procesie karnym może być wszystko co jest dopuszczalne (nie jest zabronione przez prawo), a co umożliwia realizację prawa karnego materialnego[19]. Z punktu widzenia postępowania karnego instytucja lokalizacji telefonów komórkowych za pomocą stacji BTS ma istotne znaczenie dla osiągania trafnej reakcji karnej. Zdaniem T. Grzegorczyka „trafna reakcja to nie tylko wymóg, aby niewinny nie poniósł odpowiedzialności, a winny był zawsze do niej pociągnięty, ale także to, by osoba winna poniosła odpowiedzialność nie mniejszą niż tę, na którą zasłużyła i nie większą od tej, którą ponieść powinna a więc aby była to reakcja sprawiedliwa"[20]. Sąd Najwyższy zauważył, że dowodem w procesie karnym może być wszystko to, co jest zdolne do wyrobienia przekonania sądu o winie lub niewinności oskarżonego, ale tylko wówczas, gdy przeprowadzone zostało w trybie przewidzianym przez prawo i ujawnione na przewodzie sądowym"[21]. W literaturze przedmiotu wyróżnia się[22]:

1. fakty główne - okoliczności stanowiące o przestępności czynu (bezprawność, karalność, karygodność, zawinienie),

2. fakty uboczne, czyli te okoliczności, które nie stanowią bezpośrednich elementów przestępstwa, jednakże umożliwiają wyciągniecie wniosków odnośnie faktu głównego.

W doktrynie i orzecznictwie wskazuje się, że Sąd powinien opierać się przede wszystkim na dowodach pierwotnych, określanych jako „dowód z pierwszej ręki, gdy źródło dowodowe zetknęło się bezpośrednio z udowadnianym faktem"[23]. Bazowanie na dowodach pochodnych może w istocie wpływać ujemnie na sytuację oskarżonego, co nie powinno mieć miejsca, z uwagi na represyjny charakter procesu karnego.

Telefon komórkowy może dostarczać w postępowaniu karnym wielu informacji. Przesyła on dane, które pozwalają na jego lokalizację w następujących wypadkach[24]:

- w momencie logowania się do sieci (numer abonenta zostaje przypisany do danej sesji),
- w momencie aktywności terminala (wykonywanie/odbieranie połączeń/ sms/ mms),
- w przypadku zmiany Location Area Code,
- w przypadku Location update,
- w przypadku wylogowywania się z sieci.

W wyroku Sądu Apelacyjnego w Warszawie z dnia 15 grudnia 2010 r. stwierdzono, że aktywność telefonów komórkowych w postaci wykazów połączeń (bilingów) oraz rejestracji miejsc logowań przez stacje bazowe BTS jest w pełni wartościowym materiałem dowodowym. Jednakże, aby biling telefoniczny bądź logowanie się do konkretnych stacji BTS mogło być dowodem w sprawie, konieczne jest ustalenie czy śledzony numer należał do „figuranta" czyli do osoby, która podlegała w konkretnej sprawie inwigilacji.

Bilingi telefoniczne oraz logowania do sieci BTS są dowodami o charakterze pośrednim, gdyż pozostają w ścisłym logicznym związku z faktem głównym, tj. przestępstwem. Ponadto wskazać należy, że poszlaki podobnie jak dowody pośrednie świadczą o istnieniu faktów ubocznych. Sąd Apelacyjny w Warszawie skonstatował, że „poszlaki można porównać do tkania drobnymi nićmi pajęczej sieci powiązań. Misterna konstrukcja tej sieci, związana w procesie logiczną konstrukcją myślową wzajemnych powiązań, prowadzących od faktów odległych, przez bliższe, aż do głównego - pozwala na przyjęcie przestępstwa za udowodnione. Poszlakę charakteryzuje większe oddalenie od faktu głównego i silniejsza zawiłość związku poszlak z faktem głównym. Mimo to poszlaka należy do szerokiego zbioru dowodów pośrednich, ze względu na silnie akcentowaną cechę pośredniości. Poszlaka jest jednak odleglejsza od faktu głównego niż typowe dowody pośrednie, (np.: świadek ze słuchu, odciski palców), jest więc dowodem trudniejszym ale nie mniej wartościowym"[25].

Łańcuch wiążących się ze sobą poszlak uznać należy za zamknięty tylko wtedy, gdy każda z poszlak nie budzi wątpliwości, tj. uniemożliwia jakiekolwiek inne rozwiązanie. Konieczna jest więc wszechstronna analiza całokształtu okoliczności, które mogą mieć znaczenie przy orzekaniu w przedmiocie procesu karnego. Pominięcie przez sąd

19 T. Grzegorczyk, Dowody w procesie karnym, Warszawa 2006, s. 3.; R. Kmiecik, E. Skrętowicz, Proces karny część ogólna, Kraków 2006, s. 312.

20 T. Grzegorczyk, Kodeks postępowania karnego oraz ustawa o świadku koronnym. Komentarz, Warszawa 2008, s. 51.

21 Wyrok SN z dn. 7 czerwca 1978 r., I Kr 66/78, LEX nr 63485.

22 M. Cieślak, Zagadnienia dowodowe w procesie karnym, Warszawa 1955, s.44.; S. Waltoś, Proces karny. Zarys systemu, Warszawa 2009, s. 341-343.; J. Nelken, Dowód poszlakowy w procesie karnym, Warszawa 1970, s. 95, 98.

23 T. Grzegorczyk, J. Tylman, Polskie postępowanie karne, Warszawa 2011, s. 105.

24 Zalogowana Nokia Prezydenta - technikalia [online], dostęp: 26.03.2015, http://e2rdo.salon24.pl/415152,zalogowana-nokia-prezydenta-technikalia.

25 Wyrok SA w Warszawie z dn. 15 grudnia 2010 r., II AKa 356/10, „Apelacja Warszawska" 2011, nr 2, s.9.

orzekający lub niedokładne wyjaśnienie poddające chociażby tylko jedną z poszlak w wątpliwość, uniemożliwia wydania prawidłowego rozstrzygnięcia. Pełnowartościowym dowodem z poszlak będzie zespół okoliczności w rozumieniu udowodnionych faktów o charakterze ubocznym, które prowadzą do ustalenia jednej wersji zdarzenia, tj. faktu głównego, z którego wynika, że oskarżony popełnił zarzucany mu czyn przestępny. Ocena poszczególnych poszlak musi być wnikliwa, obiektywna oraz krytyczna, gdyż poszlaka ma walor dowodu jedynie, jeżeli zostanie ustalona w sposób nie budzący wątpliwości. Dowody z bilingów telefonicznych oraz logowań się do stacji BTS powinny być oceniane zgodnie z art. 7 k.p.k., tj. na podstawie wszystkich przeprowadzonych dowodów, ocenianych swobodnie z uwzględnieniem zasad prawidłowego rozumowania oraz wskazań wiedzy i doświadczenia życiowego. Ma słuszność Sąd Najwyższy stwierdzając, że „warunkiem sine qua non poprawności dowodzenia pośredniego jest wyłączenie innej wersji, czyli konkurencyjnej hipotezy, co do przebiegu zdarzenia będącego przedmiotem rozpoznania. Od tego wymagania nie można odstąpić w sferze dokonywania ustaleń faktycznych na niekorzyść oskarżonego”[26].

Mając na uwadze treść art. 5 § 2 k.p.k., w myśl którego niedające się usunąć wątpliwości rozstrzyga się na korzyść oskarżonego, brak jest jakichkolwiek podstaw do przyjęcia, że dowód z poszlak pozwala na uznanie winy oskarżonego w przypadku ustalenia możliwości zaistnienia jakichkolwiek innych wersji zdarzenia[27].

Dowód z analizy logowań telefonu do stacji BTS, a także wykaz połączeń przychodzących i wychodzących może być zarówno dowodem obciążającym, jak i odciążającym. Ujawnienie takich informacji w procesie karnym może być w interesie samego oskarżonego, tj. stanowić jego alibi. Słusznie zauważa K. Marszał podkreślając, że „strona uwikłana w konflikcie procesowym, jest bezpośrednio zainteresowana treścią rozstrzygnięcia i ma prawo walczyć z przeciwnikiem o to, aby było one dla niej najkorzystniejsze”[28]. Przez alibi należy rozumieć pewną okoliczność lub dowód, że oskarżony w czasie popełnienia czynu, który mu się zarzuca przebywał w innym miejscu niż tam, gdzie go w rzeczywistości popełniono[29]. Jak zasadnie podkreśla M. Kucharczyk, na alibi składają się następujące elementy: czas popełnienia przestępstwa ustalony przez organy ścigania, czas przebywania oskarżonego w innym miejscu niż locus delicti, miejsce popełnienia przestępstwa oraz miejsce, gdzie rzekomo przebywał oskarżony, a także sposób i forma popełnienia przestępstwa[30]. Sprawdzenie alibi powinno polegać na uzyskaniu wyczerpujących wyjaśnień przez oskarżonego, skrupulatnym sprawdzeniu okoliczności składających się na alibi oraz przeprowadzeniu dowodów weryfikujących alibi, czyli np. bilingów telefonicznych, logowania się telefonu oskarżonego w chwili zdarzenia do stacji BTS[31].

V. Zakończenie

Szybki postęp naukowy (w tym technologiczny) wywiera istotny wpływ na szeroko rozumiane życie społeczne, w tym przestępczość. Co za tym idzie, konieczna jest współpraca organów ścigania z naukowcami celem opracowania nowoczesnych metod ścigania. Jedną z nich stanowi możliwość wykorzystania danych telekomunikacyjnych w postępowaniu karnym. Dane te mogą posłużyć nie tylko do sprawdzenia kto, z kim i kiedy się komunikował, lecz również gdzie się znajdował. Informacje te stanowią w pełni wartościowy dowód o charakterze pośrednim, zarówno dla wykazania, iż oskarżony dopuścił się zarzucanego mu czynu zabronionego, jak również, że przestępstwa nie popełniono. Europejski Inspektor Ochrony Danych Peter Hustinx stwierdził, iż retencja danych telekomunikacyjnych stanowi „bez wątpienia najbardziej ingerujące w prywatność narzędzie, jakie zostało wdrożone w Unii Europejskiej ze względu na skalę zbierania danych oraz liczbę osób, których dotyczy”[32]. Dokonując oceny retencji danych telekomunikacyjnych i jej niewątpliwej przydatności dla procesu karnego, nie możemy zatem zapominać o konieczności zapewnienia wszystkim obywatelom odpowiedniej ochrony ich konstytucyjnych praw i wolności.

26 Wyrok SN z dn. 7 marca 2001 r., IV KKN 455/00, LEX nr 51429.

27 Wyrok SN z dn. 21 października 2002 r., V KKN 283/01, „Prokuratura i Prawo” 2003, nr 11, s. 6.; wyrok SN z dn. 28 czerwca 2001 r., II KKN 550/98, LEX nr 51674.

28 K. Marszał, Proces karny zagadnienia ogólne, Katowice 2008, s. 100.

29 M. Hauswirt, S. Popower, Encyklopedia podręczna prawa karnego, Warszawa (bez daty wyd.), s. 341.; T. Tomaszewski, Procesowe funkcje alibi (alibi a poszlaka), „Państwo i Prawo” 1992, nr 5, s. 67.

30 M. Kucharczyk, Glosa do wyroku Sądu Apelacyjnego w Lublinie z dnia 29 marca 2006 r., sygn. II AKa 291/05, „Prokuratura i Prawo” 2007, nr 1, s. 67.

31 Tamże.

32 W. Klicki, Retencyjny przegląd wydarzeń [online], dostęp: 26.03.2015, http://panoptykon.org/wiadomosc/retencyjny-przeglad-wydarzen

***

The evidential value of telecommunications data retention in Polish criminal procedure

The widespread availability of mobile telephones, cards prepaid allowed to increase the activity of criminals. The speed of communication and sharing of information, but also to a large extent anonymity significantly hindered the detection of crimes and their perpetrators. For such a changing reality, could not remain indifferent law enforcement. When evaluating telecommunications data retention and its undoubted usefulness for forensic science, we can not forget about the need for us all to adequate protection of the rights and freedoms. This information is the full value of an indirect proof, either to show that the accused committed the alleged offense, as well as the crime was not committed.