Marek Chrabkowski

Wyższa Szkoła Administracji i Biznesu, Gdynia

m.chrabkowski@wsaib.pl; ORCID:0000-0003-4857-2174

Dostęp do treści korespondencji SMS-owej w telefonie zabezpieczonym na potrzeby sprawy karnej

<http://dx.doi.org/10.12775/SIT.2018.003>

1. Wstęp

Ustalenie prawdy materialnej w sprawie karnej niejednokrotnie wiąże się z koniecznością ingerencji w prawa i wolności obywateli. Jednym z prawnie chronionych dóbr, które cierpi na skutek ingerencji organów państwa, jest prywatność. Naruszenie prywatności następuje podczas różnych czynności podejmowanych przez uprawnione podmioty. Ma miejsce podczas przesłuchania, przeszukania, oględzin, a także zbierania informacji, które z uwagi na swój charakter są prawnie chronione różnego rodzaju tajemnicami. Należą do nich m.in. dane objęte tajemnicami: lekarską, bankową, skarbową czy telekomunikacyjną. Ta ostatnia kategoria informacji wydaje się szczególnie atrakcyjna dla organów postępowania karnego. Na ich podstawie można ustalić np.:

- dane osób wchodzących w zakres kręgu towarzyskiego posiadacza telefonu;
- miejsca odwiedzane przez posiadacza telefonu;
- nazwy sieci systemu *wi-fi*, z których korzystał posiadacz telefonu;

- częstotliwość prowadzenia rozmów i utrzymywania innych form kontaktu z określonymi osobami;
- treść korespondencji, np. na podstawie zapisanych wiadomości tekstowych przekazywanych w systemie SMS.

Część z tych danych jest przechowywana przez przedsiębiorcę telekomunikacyjnego, ale są też takie, które zapisują się wyłącznie w pamięci aparatu telefonicznego. Do takich danych zaliczają się m.in. wiadomości SMS. Dotarcie do korespondencji SMS wymaga sięgnięcia do pamięci aparatu telefonicznego nadawcy lub odbiorcy informacji tekstowej przekazanej w tym systemie, ponieważ przedsiębiorca telekomunikacyjny nie może treści tej korespondencji bez żądania sądu zapisywać na swoich serwerach.

Celem badań, których wyniki zostały przedstawione w niniejszej publikacji, było udzielenie odpowiedzi na następujące pytanie badawcze: czy przepisy prawa karnego procesowego przewidują odpowiedni poziom ochrony treści korespondencji w postaci wiadomości SMS zapisanej w pamięci aparatu telefonicznego, który został zabezpieczony na potrzeby prowadzonej sprawy karnej? W związku z postawionym pytaniem badawczym przyjęto hipotezę, że poziom ochrony treści takiej korespondencji jest wysoki, ponieważ wymaga tego charakter tych danych.

Przyjęta hipoteza badawcza zdeterminowała strukturę publikacji. W artykule przedstawiono w odrębnych częściach zagadnienia dotyczące:

- wiadomości SMS jako informacji chronionych tajemnicą telekomunikacyjną;
- możliwości pozyskania treści wiadomości SMS od przedsiębiorcy telekomunikacyjnego;
- zasad dostępu do danych chronionych tajemnicą telekomunikacyjną znajdujących się w pamięci urządzeń końcowych.

Badania przeprowadzono metodą monograficzną z wykorzystaniem podstawowych metod badawczych w postaci: krytycznej analizy literatury, badania prawa i analizy orzecznictwa sądowego. Wnioski z przeprowadzonych badań zostały zawarte w zakończeniu.

2. Wiadomość SMS jako informacja chroniona tajemnicą telekomunikacyjną

W Ustawie z 16 lipca 2004 r. Prawo telekomunikacyjne¹, zwanej dalej Prawem telekomunikacyjnym (pr.tel.) nie zawarto definicji legalnej tajemnicy telekomunikacyjnej². Jej zakres został określony katalogiem danych wymienionych w art. 159 ust. 1 pr.tel. obejmującym:

- dane dotyczące użytkownika;
- treść indywidualnych komunikatów;
- dane transmisyjne, które oznaczają dane przetwarzane dla celów przekazywania komunikatów w sieciach telekomunikacyjnych lub naliczania opłat za usługi telekomunikacyjne, w tym dane lokalizacyjne, czyli wszelkie dane przetwarzane w sieci telekomunikacyjnej lub w ramach usług telekomunikacyjnych wskazujące położenie geograficzne urządzenia końcowego użytkownika publicznie dostępnych usług telekomunikacyjnych;
- dane o lokalizacji, które oznaczają dane lokalizacyjne wykraczające poza dane niezbędne do transmisji komunikatu lub wystawienia rachunku;
- dane o próbach uzyskania połączenia między zakończeniami sieci, w tym dane o nieudanych próbach połączeń, oznaczających połączenia między telekomunikacyjnymi urządzeniami końcowymi lub zakończeniami sieci, które zostały zestawione i nie zostały odebrane przez użytkownika końcowego lub nastąpiło przerwanie zestawianych połączeń.

Systematyzując rodzaje objętych tajemnicą telekomunikacyjną danych, które wymienione zostały we wskazanym katalogu, można dokonać ich podziału na:

¹ Tekst jednolity: Dz.U. z 2017 r. poz. 1907 ze zm.

² S. Hoc, *Ochrona informacji niejawnych i innych tajemnic ustawowo chronionych*, Opole 2006, s. 265.

- dane dotyczące treści przekazu telekomunikacyjnego;
- dane towarzyszące przekazowi telekomunikacyjnemu:
 - dane transmisyjne;
 - dane o próbach uzyskania połączenia;
 - dane lokalizacyjne;
- dane o abonencie.

Zaproponowany podział wynika ze stopnia wrażliwości poszczególnych danych na nieuprawnioną ingerencję ze strony podmiotów zainteresowanych tymi informacjami. Największym zagrożeniem dla integralności informacyjnej osoby jest ingerencja w treść przekazu telekomunikacyjnego, czyli wszelkiego rodzaju podsłuchy rozmów, przechwytywanie korespondencji e-mailowej czy sygnału wizyjnego. Do danych dotyczących treści przekazu telekomunikacyjnego zalicza się również treści wiadomości SMS. Z tych też względów stopień ochrony tych danych przed ingerencją, również ze strony organów państwa, powinien być najwyższy.

3. Możliwości pozyskania treści wiadomości SMS od przedsiębiorcy telekomunikacyjnego

Ingerencja w dane zapisane w telefonie nie byłaby konieczna, gdyby operator telekomunikacyjny przechowywał wszystkie te dane na swoich serwerach. Na takie działanie nie pozwala jednak Prawo telekomunikacyjne, w którym zakazano zapoznawania się, utrwalania, przechowywania, przekazywania lub innego wykorzystywania treści lub danych objętych tajemnicą telekomunikacyjną przez osoby inne niż nadawca i odbiorca komunikatu, chyba że³:

- będzie to przedmiotem usługi lub będzie to niezbędne do jej wykonania;
- nastąpi za zgodą nadawcy lub odbiorcy, których dane te dotyczą;

³ Art. 178 ust. 2 pr.tel.

- dokonanie tych czynności jest niezbędne w celu rejestrowania komunikatów i związanych z nimi danych transmisyjnych, stosowanego w zgodnej z prawem praktyce handlowej dla celów zapewnienia dowodów transakcji handlowej lub celów łączności w działalności handlowej;
- będzie to konieczne z innych powodów przewidzianych ustawą lub przepisami odrębnymi.

Przepis ten, poza wskazanymi w nim wyjątkami, zabrania przedsiębiorcy telekomunikacyjnemu utrwalania, przechowywania, przekazywania lub innego wykorzystywania treści wiadomości SMS. Nie mogą tego robić również podmioty działające w imieniu przedsiębiorcy telekomunikacyjnego, ponieważ ponosi on odpowiedzialność za naruszenie tajemnicy telekomunikacyjnej przez te podmioty⁴. Przedsiębiorca telekomunikacyjny nie dysponuje treściami wiadomości SMS, a przynajmniej nie powinien nimi dysponować, więc żadna instytucja nie może tych danych pozyskać od niego.

Organy postępowania karnego mogą zobowiązać przedsiębiorcę telekomunikacyjnego, aby uruchomił procedurę utrwalania i przechowywania treści korespondencji SMS, a następnie przekazywania tych danych na potrzeby prowadzonej sprawy karnej. To uprawnienie wynika z art. 179 ust. 3b pr.tel. Zgodnie z tym przepisem w przypadku działań na rzecz sądu lub prokuratora przedsiębiorca telekomunikacyjny jest zobligowany do zapewnienia utrwalania przekazów i danych telekomunikacyjnych⁵. Dostawca publicznie dostępnych usług telekomunikacyjnych może więc utrzymywać i przekazywać treści wiadomości SMS wyłącznie na zlecenie sądu lub prokuratora. Szczegółowe zasady kontroli i utrwalania rozmów i innych form korespondencji telekomunikacyjnej w ramach sprawy karnej są określone w rozdziale 26 pt. „Kontrola i utrwalanie rozmów” Ustawy z 6 czerwca 1997 r. – Kodeks postępowania karnego⁶ (k.p.k.). Zgodnie z art. 237 § 1 k.p.k. do utrwalania treści korespondencji SMS może zobowiązać przedsiębiorcę telekomunikacyjnego sąd na wniosek prokuratora. W wypadkach niecierpiących zwłoki

⁴ Art. 162 ust. 1 pr.tel.

⁵ Art. 179 ust. 3b pr.tel.

⁶ Tekst jednolity: Dz.U. z 2017 r. poz. 1904.

kontrolę i utrwalanie treści rozmów telefonicznych może zarządzić prokurator, który jest obowiązany zwrócić się w terminie 3 dni do sądu z wnioskiem o zatwierdzenie postanowienia⁷. Sąd wydaje postanowienie w przedmiocie wniosku w terminie 5 dni na posiedzeniu bez udziału stron. W wypadku niezatwierdzenia postanowienia prokuratora sąd w postanowieniu wydanym w przedmiocie wniosku zarządza zniszczenie wszystkich utrwalonych zapisów. Zaskarżenie postanowienia wstrzymuje jego wykonanie. Kontrola i utrwalanie treści korespondencji SMS są dopuszczalne tylko wtedy, gdy toczące się postępowanie lub uzasadniona obawa popełnienia nowego przestępstwa dotyczy przynajmniej jednego z typów przestępstw wymienionych w ustawowym katalogu zawartym w art. 237 § 3 k.p.k.⁸ Nie są to więc wszystkie przestępstwa i przestępstwa skarbowe, ale wyłącznie przestępstwa poważne o znacznym ciężarze gatunkowym albo charakteryzujące się niską skutecznością wykrywczą przy wykorzystaniu konwencjonalnych środków dowodowych, np. łapownictwo, przy którym żadna ze stron nie jest zainteresowana ujawnieniem procederu korupcyjnego. Ustawodawca wymienił w tym katalogu około 50 typów przestępstw na szacowaną liczbę około 1000 ustanowionych w polskim prawie karnym, co stanowi ok. 0,5% ogółu typów przestępstw obowiązujących w naszym kraju. Regulacja ta świadczy o wyjątkowości tego rozwiązania, które pozwala na ingerencję w tajemnicę telekomunikacyjną w zakresie treści przekazu tylko w nielicznych sprawach karnych.

O wzmożonej ochronie utrwalonej treści korespondencji świadczy również dyspozycja art. 237 § 6 k.p.k. Przepisem tym ograniczono krąg podmiotów uprawnionych do zapoznawania się z utrwaloną na potrzeby sprawy karnej treścią korespondencji wyłącznie do sądu i prokuratora. Jedynie w przypadkach niecierpiących zwłoki za zgodą sądu lub prokuratora z treścią korespondencji SMS może zapoznać się funkcjonariusz organu ścigania prowadzący lub wykonujący czynności w postępowaniu przygotowawczym.

⁷ Art. 237 § 1 k.p.k.

⁸ Art. 241 k.p.k. w zw. z art. 237 § 1 k.p.k.

4. Zasady dostępu do danych chronionych tajemnicą telekomunikacyjną znajdujących się w pamięci urządzeń końcowych

Najpopularniejszym miejscem deponowania danych chronionych tajemnicą telekomunikacyjną poza zbiorami danych przedsiębiorców telekomunikacyjnych jest pamięć urządzeń końcowych. Aparaty telefoniczne i inne urządzenia mobilne zachowują na potrzeby użytkownika dane chronione tajemnicą telekomunikacyjną. W telefonie mogą znajdować się zapisane treści przekazów telekomunikacyjnych w postaci informacji tekstowych SMS czy też nagranych rozmów telefonicznych. W pamięci telefonu odnotowywane są również dane towarzyszące przekazowi telekomunikacyjnemu w postaci wykazu połączeń czy danych lokalizacyjnych. Nie wszystkie te dane są rejestrowane na serwerach operatorów telekomunikacyjnych, więc niektóre z nich można uzyskać wyłącznie z pamięci aparatu telefonicznego. O znaczeniu dowodów tam zapisanych świadczy chociażby determinacja Federalnego Biura Śledczego (FBI) w działaniach zmierzających do pozyskania danych z aparatu telefonicznego firmy Apple. W jednej z nagłośnionych medialnie spraw w Stanach Zjednoczonych powstał spór pomiędzy FBI a Apple'em w sprawie dostępu do danych zapisanych w urządzeniu stworzonym przez tego producenta. W dniu 2 grudnia 2015 r. pochodzący z Pakistanu Amerykanin Syed Rizwan Farook i jego żona Tashfeen Malik otworzyli ogień do osób przybyłych na świąteczne przyjęcie w ośrodku pomocy niepełnosprawnym Inland Regional Center w kalifornijskim mieście San Bernardino. W wyniku ataku zginęło 14 osób, a 21 zostało rannych. Oboje terroryści zginęli w obławie. Istniało uzasadnione podejrzenie, że zamachowcy z San Bernardino nie działali sami, więc FBI postanowiło odczytać informacje zapisane w telefonie zamachowca. Dane w należącym do terrorysty iPhone były fabrycznie tak skutecznie zabezpieczone, że bez znajomości hasła nie można było tego telefonu odblokować, a po 10 nieudanych próbach wpisania hasła telefon automatycznie uruchamia funkcję kasowania zapisanych w nim informacji. FBI po uzyskaniu nakazu

sądowego zażądało od firmy Apple odblokowania telefonu terrorysty, a ta odmówiła. W uzasadnieniu swojej decyzji Apple oskarżył rząd USA o bezprecedensowe działania uderzające w bezpieczeństwo jej klientów⁹. Pomimo braku współdziałania ze strony producenta specjalistom FBI udało się przełamać zabezpieczenia iPhone'a i dostać się do pamięci tego urządzenia¹⁰.

W Polsce dostęp funkcjonariuszy organów ścigania do danych zapisanych w pamięci urządzenia końcowego na etapie toczącej się sprawy karnej nie jest szczególnie limitowany. Na podstawie art. 236a k.p.k. przepisy dotyczące zatrzymania rzeczy i przeszukania stosuje się odpowiednio do dysponenta i użytkownika urządzenia zawierającego dane informatyczne lub systemu informatycznego, w zakresie danych przechowywanych w tym urządzeniu lub systemie albo na nośniku znajdującym się w jego dyspozycji lub użytkowaniu, w tym korespondencji przesyłanej pocztą elektroniczną. Jak wynika z tych przepisów, zatrzymanie rzeczy i przeszukanie jest dozwolone co do zasady na żądanie sądu lub prokuratora¹¹. W sytuacjach niecierpiących zwłoki przeszukanie może być przeprowadzone na podstawie nakazu kierownika jednostki Policji lub legitymacji służbowej policjanta¹². W takim przypadku czynność ta wymaga zatwierdzenia przez sąd lub prokuratora w ramach tzw. kontroli aposteriorycznej¹³. Jeżeli kierownik instytucji państwowej lub samorządowej albo też osoba, u której dokonano zatrzymania rzeczy lub u której przeprowadza się przeszukanie, oświadczy, że wydane lub znalezione przy przeszukaniu pismo lub inny dokument zawiera informacje niejawne lub wiadomości objęte tajemnicą zawodową

⁹ O. Szewczyk, *FBI żąda odblokowania iPhone'a islamisty, Apple odmawia*, „Polityka” z dnia 18.02.2016, <http://www.polityka.pl/tygodnikpolityka/swiat/1651420,1,fb-i-zada-odblokowania-iphonea-islamisty-apple-odmawia-kto-ma-racje.read> (dostęp: 26.01.2017 r.).

¹⁰ D. Kosiński, *Koniec kłopotów FBI i początek naszych – zabezpieczenia iPhone'a zostały właśnie złamane*, „Spider'sWeb” z dnia 29.03.2016, <http://www.spidersweb.pl/2016/03/fbi-zabezpieczenia-iphone-zlamane.html> (dostęp: 26.01.2017 r.).

¹¹ Art. 217 § 1 k.p.k. i art. 220 § 1 k.p.k.

¹² Art. 220 § 3 k.p.k.

¹³ Art. 220 § 3 zd. 2 k.p.k.

lub inną tajemnicą prawnie chronioną albo ma charakter osobisty, organ przeprowadzający czynność przekazuje niezwłocznie pismo lub inny dokument bez jego odczytania prokuratorowi lub sądowi w opieczętowanym opakowaniu¹⁴. Przepisy art. 225 § 1 i 2 k.p.k. określają specjalny tryb postępowania z pismami i dokumentami zawierającymi informacje zawodowe, osobiste, niejawne lub inne prawnie chronione. Jak podkreślają przedstawiciele doktryny, jego funkcją jest ograniczenie dostępu funkcjonariuszy, którzy przeprowadzają przeszukanie, do treści dokumentów zawierających taką tajemnicę¹⁵. Organ przeprowadzający przeszukanie nie może sprawdzać, czy oświadczenie kierownika instytucji państwowej lub samorządowej albo też osoby, u której dokonano zatrzymania rzeczy lub u której przeprowadza się przeszukanie, jest prawdziwe, ponieważ musiałoby się to wiązać z zapoznaniem się z treścią pism lub dokumentów, a więc właśnie z tym, czego przepis zakazuje¹⁶. Tryb ten nie obowiązuje w stosunku do pism lub innych dokumentów, które zawierają informacje niejawne o klauzuli „zastrzeżone” lub „poufne” albo dotyczą tajemnicy zawodowej lub innej tajemnicy prawnie chronionej, jeżeli ich posiadaczem jest osoba podejrzana o popełnienie przestępstwa¹⁷.

Odnosząc zakresy omawianych regulacji do przykładu telefonu komórkowego zabezpieczanego podczas przeszukania, dochodzi się do wniosku, że zakaz zapoznania się z zawartością pamięci tego urządzenia przez funkcjonariuszy organów ścigania dokonujących zatrzymania rzeczy lub przeszukania obowiązuje tylko w wyjątkowych sytuacjach, a mianowicie, gdy wydawany jest przez inną osobę niż osoba podejrzana, a dodatkowo osoba wydająca urządzenie złoży oświadczenie, że w telefonie zapisane są dane chronione tajemnicą telekomunikacyjną. Przepis wymaga złożenia oświadczenia na okoliczność oczywistą, że w każdym użytkowanym telefonie znajdują się dane prawnie chronione. Kuriozalność tego rozwiązania

¹⁴ Art. 225 § 1 k.p.k.

¹⁵ P. Hofmański, E. Sadzik, K. Zgryzek, w: *Kodeks postępowania karnego. Komentarz*, red. P. Hofmański, Warszawa 2011, Art. 225, Nb. 2.

¹⁶ Ibidem.

¹⁷ Art. 225 § 2 k.p.k.

polega na tym, że brak oświadczenia na temat kwestii oczywistej otwiera funkcjonariuszom organów ścigania nieograniczony dostęp do danych zapisanych w pamięci aparatu telefonicznego, w tym do treści korespondencji w postaci zapisanych w nim wiadomości SMS. Jak wynika z przytoczonych przepisów, ochrona dostępu do treści korespondencji SMS nie istnieje, gdy do zabezpieczenia aparatu telefonicznego dochodzi u osoby podejrzanej. Nie ma wtedy żadnych ograniczeń dostępowych do treści korespondencji SMS zapisanej w pamięci telefonu, ponieważ szczególny tryb postępowania nie obowiązuje w stosunku do pism i dokumentów, które dotyczą tajemnicy informacji niejawnych o klauzuli tajności „poufne” lub „zastrzeżone”, zawodowej lub innej chronionej ustawą, jeśli ich posiadaczem jest uczestnik postępowania o tym statusie¹⁸. Nadmienić należy, że status osoby podejrzanej nie jest wynikiem podjęcia określonej decyzji procesowej w sprawie karnej, lecz jest rezultatem kierunku prowadzenia tej sprawy, więc ma charakter konkludentny. Jeżeli czynności podejmowane w postępowaniu karnym zmierzają do ustalenia albo wykluczenia udziału określonej osoby w popełnieniu przestępstwa, to staje się ona osobą podejrzaną. Status ten ma charakter przejściowy i nie przesądza kwestii przedstawienia w określonej perspektywie czasowej zarzutów osobie podejrzanej. Taka osoba równie dobrze może wystąpić w sprawie karnej wyłącznie w charakterze świadka. Skoro można bez ograniczeń ingerować w dane zapisane w telefonie komórkowym osoby podejrzanej, to zgodnie z *argumentum a maiori ad minus* zasady te stosuje się również w odniesieniu do informacji zapisanych w telefonach podejrzanego i oskarżonego¹⁹. Nadmienić jeszcze należy, że wskazane przepisy dotyczą zasad postępowania w sprawach karnych dotyczących wszystkich typów przestępstw. Z korespondencją SMS zapisaną w telefonie komórkowym organy ścigania mogą się zapoznać nawet w sprawach tak błahych występków jak kradzież z włamaniem do piwnicy, z której wyniesiono przetwory owocowo-warzywne, czy usiłowanie oszustwa polegającego na zamianie w supermarkecie opakowań towarów na te z niższą ceną.

¹⁸ *Kodeks postępowania karnego. Komentarz*, art. 225.

¹⁹ *Ibidem*.

Tego typu sytuacje są ewidentnymi przykładami naruszenia zasady proporcjonalności.

Praktyka policyjna idzie jeszcze dalej, przyjmując, że dostęp do danych informatycznych zawartych w urzędzeniu (lub na nośniku) jest możliwy w drodze nie tylko przeszukania, ale także oględzin. Autorzy publikacji w uzasadnieniu swojego stanowiska stwierdzili, że oględziny są również czynnością procesową przeprowadzaną wyłącznie przez organ procesowy, więc nie ma powodów, aby wykluczać taką ewentualność²⁰. Nie można jednak zgodzić się z tym poglądem. Należy podkreślić, że w przypadku oględzin czynność ta nie jest poddana kontroli sądowej ani prokuratorskiej, a w rozdziale 23 k.p.k. dotyczącym oględzin, otwarcia zwłok i eksperymentu procesowego nie ma żadnego odniesienia do trybu postępowania w przypadku ujawnienia danych chronionych tajemnicą telekomunikacyjną. Przepisy regulujące oględziny rzeczy nie dochowują standardów konstytucyjnych w zakresie dostatecznej określoności regulacji prawnej ingerującej w prawa i wolności człowieka. Leszek Bosek zwraca uwagę, że zawarty w art. 31 ust. 3 Konstytucji RP²¹ wymóg ustanawiania ograniczeń konstytucyjnych wolności i praw „tylko w ustawie” oznacza nie tylko wyłączność ustawy w omawianym zakresie, z zastrzeżeniem dopuszczalności wyjątkowego normowania pewnych mniej istotnych kwestii techniczno-wykonawczych w aktach normatywnych podustawowych²². Autor ten podkreślił, że wymóg „tylko w ustawie” jest jednocześnie równoznaczny z wymogiem dostatecznej określoności regulacji prawnej²³. Trybunał Konstytucyjny, odnosząc się do art. 31 ust. 3 Konstytucji RP, stwierdził, że uzależnienie dopuszczalności ograniczeń praw i wolności od ich ustanowienia tylko w ustawie jest czymś więcej niż tylko przypomnieniem ogólnej zasady wyłączności ustawy dla normowania sytuacji prawnej jednostek, stanowiącej klasyczny element idei państwa prawnego.

²⁰ K. Wiciak, J. Kosiński, *Oglądamy czy przeszukujemy?*, „Policja 997” z dnia 25.06.2017 r., <http://www.gazeta.policja.pl/997/informacje/144955,Ogladamy-czy-przeszukujemy.html> (dostęp 12.01.2018 r.).

²¹ Dz.U. z 1997 r. Nr 78, poz. 483 ze zm.

²² L. Bosek, w: Konstytucja RP. Tom. I. *Komentarz do art. 1–86*, red. M. Safjan, L. Bosek, Warszawa 2016, Art. 31, Nb. 85.

²³ Ibidem.

Jest to także sformułowanie wymogu odpowiedniej szczegółowości unormowania ustawowego²⁴. Ustawodawca nie przewidział procedury poddawania rzeczy oględzinom, które prowadzą do ingerencji w tajemnicę prawnie chronioną. Ingerencja taka może być czyniona wyłącznie na podstawie przepisów, w których *expressis verbis* takie uprawnienie przewidziano. W przypadku danych zapisanych w pamięci telefonu przepisy te są zawarte w rozdziale 25 k.p.k. dotyczącym zatrzymania rzeczy i przeszukania, więc ingerencja w dane zapisane w pamięci telefonu wyłącznie na podstawie przepisów rozdziału 23 k.p.k. regulującego oględziny jest niedopuszczalna.

5. Podsumowanie

Pozyskiwanie chronionych tajemnicą telekomunikacyjną danych, które pozostają w dyspozycji przedsiębiorcy telekomunikacyjnego, jest silnie reglamentowane. W zależności od rodzaju danych występują różne systemy ochrony dostępu. Mocniejszy – w odniesieniu do treści przekazu telekomunikacyjnego, i słabszy – w odniesieniu do danych towarzyszących przekazowi telekomunikacyjnemu i danych o abonencie. W przypadku sięgania po treści przekazów telekomunikacyjnych, w tym korespondencji SMS, nadzór sądowy ma charakter aprioryczny. Operator telekomunikacyjny nie może utrzymywać wiadomości SMS bez stosowanego postanawiania sądu karnego, a z utrwalonymi treściami może się zapoznać co do zasady sąd i prokurator. W przepisach regulujących dostęp do chronionych tajemnicą telekomunikacyjną danych, które pozostają poza zbiorami przedsiębiorców telekomunikacyjnych, ustawodawca nie zastrzegł potrzeby reglamentowania dostępu do nich w sposób aż tak restrykcyjny. Ochrona dostępu do tych danych ma charakter znacznie słabszy niż w przypadku pozyskiwania danych od przedsiębiorców telekomunikacyjnych. W trakcie czynności podejmowanych na podstawie przepisów Kodeksu postępowania karnego funkcjo-

²⁴ Wyrok TK z dnia 12 stycznia 2000 r., P 11/98, OTK 2000, nr 1, poz. 3; Wyrok TK z dnia 28 czerwca 2005 r., SK 56/04, OTK-A 2005, nr 6, poz. 67; Wyrok TK z dnia 5 maja 2004 r., P 2/03, OTK-A 2004, nr 5, poz. 39.

nariusze organów ścigania mogą bez problemu uzyskać dostęp do danych zapisanych w pamięci aparatu telefonicznego, a tylko wyjątkowo przepisy prawne im tego zabraniają. Zakaz dotyczy czynności przeszukania lub zatrzymania rzeczy przeprowadzanych pod nieobecność osoby podejrzanej (podejrzanego, oskarżonego) i tylko wtedy, gdy wydający oświadczy, że w telefonie znajdują się dane chronione tajemnicą telekomunikacyjną. W pozostałych przypadkach, których w praktyce jest przeważająca większość, funkcjonariusze organów ścigania nie mają żadnych ograniczeń w dostępie do informacji chronionych tajemnicą korespondencji a zawartych w pamięci aparatu telefonicznego, bez względu na to, czy dotyczy ona treści przekazu telekomunikacyjnego (np. treść informacji przesyłanych w systemie SMS), czy tylko danych towarzyszących przekazowi telekomunikacyjnemu (np. wykaz połączeń albo dane zawarte w książce adresowej). Praktyka policyjna idzie jeszcze dalej i uzasadnia możliwość zapoznawania się z treścią korespondencji SMS nawet podczas oględzin telefonu, która to czynność wyłączona jest spod apriorycznej kontroli prokuratorskiej i sądowej.

Regulacje przewidziane w Kodeksie postępowania karnego charakteryzują się rażącą dysproporcją w poziomie ochrony tajemnicy telekomunikacyjnej z uwagi na miejsce zdeponowania chronionych danych. W przypadku pozyskiwania tych danych ze źródeł innych niż zbiory przedsiębiorcy telekomunikacyjnego krąg podmiotów uprawnionych do zapoznawania się z wiadomościami SMS zapisanymi w pamięci urządzenia końcowego nie został ograniczony. Brak zewnętrznej kontroli nad czynnościami procesowymi ingerującymi w tajemnicę telekomunikacyjną łącznie z treściami przekazów wymaga interwencji ustawodawcy. Trybunał Konstytucyjny trafnie zwrócił uwagę, że pozyskiwanie informacji o życiu prywatnym jednostek przez organy władzy publicznej musi być ograniczone do koniecznych sytuacji, dopuszczalnych w demokratycznym państwie wyłącznie dla ochrony konstytucyjnie uznanych wartości i zgodnie z zasadą proporcjonalności²⁵. Dlatego też warunki gromadzenia i przetwarzania tych danych przez władze publiczne muszą być unormowane w ustawie w sposób jak najbardziej przejrzysty, wy-

²⁵ Wyrok TK z dnia z 30 lipca 2014 r., K 23/11, Dz.U. z 2014 r. poz. 1055.

kluczający arbitralność i dowolność ich stosowania²⁶. Tych warunków, w odniesieniu do danych wchodzących w zakres tajemnicy telekomunikacyjnej, nie spełniają przepisy Kodeksu postępowania karnego regulujące zatrzymanie rzeczy i przeszukanie, a całkowicie niedostosowane są przepisy dotyczące oględziny rzeczy. Poczynione ustalenia zaprzeczyły przyjętej hipotezie, że poziom ochrony treści korespondencji w postaci wiadomości SMS, zapisanej w pamięci aparatu telefonicznego, który został zabezpieczony na potrzeby prowadzonej sprawy karnej jest wysoki. Mimo znaczącej wrażliwości danych w postaci wiadomości SMS zapisanych w urządzeniu końcowym ustawodawca nie dostrzegł potrzeby ich wzmożonej ochrony, a przepisy Kodeksu postępowania karnego dotyczące tych kwestii nie spełniają standardu określoności regulacji prawnej.

Formułując wnioski *de lege ferenda*, należy zaznaczyć, że w przypadku ingerencji przez organy procesowe w dane chronione tajemnicą telekomunikacyjną, które zostały zapisane w pamięci urządzenia końcowego, w szczególności w zakresie treści korespondencji (w tym wiadomości SMS) zasadne byłoby wprowadzenie przez ustawodawcę:

- apriorycznej kontroli sądowej zezwalającej na taką ingerencję;
- katalogu przestępstw, których popełnienie uzasadniałoby ingerencję;
- ograniczonego kręgu podmiotów uprawnionych do zapoznania się z treściami przekazów zapisanych w urządzeniu końcowym;
- szczególnego trybu postępowania w stosunku do wszystkich urządzeń końcowych z zapisanymi danymi bez względu na podmiot, u którego zabezpieczono dowodowe urządzenie.

STRESZCZENIE

Dostęp do treści korespondencji SMS-owej
w telefonie zabezpieczonym na potrzeby sprawy karnej

Korespondencja SMS-owa zapisana w pamięci urządzeń telekomunikacyjnych może stanowić ważny dowód w sprawie karnej. Zgodnie z Prawem

²⁶ Ibidem.

telekomunikacyjnym nie może być ona utrwalana przez przedsiębiorcę telekomunikacyjnego bez nakazu sądowego. Uzyskanie zgody sądu na kontrolę i utrwalanie treści korespondencji SMS nie pozwala na uzyskanie dostępu do korespondencji wcześniejszej, ponieważ postanowienie sądowe skierowane do przedsiębiorcy telekomunikacyjnego wywołuje skutki *ex nunc*. Do wcześniejszej korespondencji można dotrzeć wyłącznie poprzez sięgnięcie do pamięci aparatu telefonicznego nadawcy lub odbiorcy informacji tekstowej przekazanej w systemie SMS. Artykuł jest podsumowaniem badań, które miały na celu ustalenie zakresu ochrony treści korespondencji SMS, objętej tajemnicą telekomunikacyjną a zapisanej w pamięci końcowego urządzenia telekomunikacyjnego zabezpieczonego na potrzeby prowadzonej sprawy karnej. W ramach badań skupiono się na zakresach ochrony tych danych, wynikających z przepisów prawnych, które uprawniają do pozyskiwania treści korespondencji przez organy państwa w związku z realizacją czynności dowodowych w sprawie karnej.

Słowa kluczowe: wiadomość SMS; telefon; tajemnica korespondencji; tajemnica komunikowania; tajemnica telekomunikacyjna; sprawa karna; postępowanie karne, dowód

SUMMARY

Access to the content of SMS correspondence in an impounded mobile phone in connection with a criminal case

SMS correspondence stored in telecommunications equipment, can provide important evidence in a criminal case. In accordance with the Telecommunications Law, it must not be recorded by a telecommunications company without a court order. Obtaining court's approval for controlling and recording SMS correspondence does not allow access to the earlier correspondence as the court order issued to the telecommunications company causes the *ex nunc* effect. Earlier correspondence may only be accessed by referring to the memory of the device that belongs to the sender or the receiver of the text message. The article summarises the study which aimed to determine the scope of protection of the SMS correspondence content stored in the memory of the terminal telecommunications equipment which was impounded for a criminal case. The research focused on the scope of data protection in connection with the legislation that allows the authorities to obtain the content of correspondence in connection with gathering evidence in a criminal case.

Keywords: secrecy of correspondence; secrecy of communication; secrecy of telecommunication; text message; SMS correspondence; telephone; criminal case; criminal proceedings

BIBLIOGRAFIA

- Bosek L., w: *Konstytucja RP. Tom I. Komentarz do art. 1–86*, red. M. Safjan, L. Bosek, Warszawa 2016.
- Hoc S., *Ochrona informacji niejawnych i innych tajemnic ustawowo chronionych*, Opole 2006.
- Kodeks postępowania karnego. Komentarz*, red. P. Hofmański, E. Sadzik, K. Zgryzek, Warszawa 2011.
- Kosiński D., *Koniec kłopotów FBI i początek naszych – zabezpieczenia iPhone'a zostały właśnie złamane*, Spider'sWeb z dnia 29.03.2016 r., <http://www.spidersweb.pl/2016/03/fbi-zabezpieczenia-iphone-zlamane.html> (dostęp: 26.01.2017 r.).
- Szewczyk O., *FBI żąda odblokowania iPhone[a] islamisty, Apple odmawia*, „Polityka” z dnia 18.02.2016 r., <http://www.polityka.pl/tygodnikpolityka/swiat/1651420,1,fbi-zada-odblokowania-iphonea-islamisty-apple-odmawia-kto-ma-racje.read> (dostęp: 26.01.2017 r.).
- Wiciak K., Kosiński J., *Oglądamy czy przeszukujemy?*, „Policja 997” z dnia 25.06.2017 r., <http://www.gazeta.policja.pl/997/informacje/144955,Ogladamy-czy-przeszukujemy.html> (dostęp: 12.01.2018 r.).