Mateusz Witański

Tajemnica telekomunikacyjna a możliwość ujawnienia danych billingowych

Bezpieczeństwo : teoria i praktyka : czasopismo Krakowskiej Szkoły Wyższej im. Andrzeja Frycza Modrzewskiego 7/2, 49-62

2013

BEZPIECZEŃSTWO 2013 nr 2 (XI)
TEORIA I PRAKTYKA

Mateusz Witański*

Tajemnica telekomunikacyjna a możliwość ujawnienia danych billingowych

Wprowadzenie

W ciągu kilku ostatnich lat byliśmy świadkami sytuacji, w których billing rozmów z telefonu komórkowego stał się podstawą oskarżenia o działanie niezgodne z prawem. Społeczeństwo dowiadywało się, że politycy kontaktowali się z biznesmenami, często oskarżanymi o „podejrzane interesy", z czego wyciągano wnioski o uleganiu przez polityków korupcji bądź nieczystemu lobbingowi. Być może oskarżenia były słuszne, ale nie to jest przedmiotem niniejszej pracy. Ważnym elementem całego procesu dowodowego był billing z rozmów telefonicznych, na podstawie którego wiązano ze sobą poszczególne osoby oraz szukano poszlak. Billing tych rozmów został następnie ujawniany publicznie, często przed skierowaniem sprawy do sądu lub wydaniem wyroku. W takiej sytuacji powstaje pytanie, czy nie zostało złamane polskie prawo, w szczególności prawo telekomunikacyjne oraz Ustawa o ochronie danych osobowych?

Powyższy przykład jest przypadkiem rodzącym wątpliwości dotyczące niezgodnego z przepisami prawa telekomunikacyjnego. Drugim przykładem, mniej spektakularnym i w konsekwencji mniej rozpoznanym, wydaje się rozliczanie billingów wewnętrznych firmy, kiedy to w billingach central abonenckich zawarte są informacje o numerach abonentów zarówno wewnętrznych, jak i zewnętrznych. Czy także w tym przypadku nie są łamane przepisy prawa telekomunikacyjnego i Ustawy o ochronie danych osobowych?

* Mgr, doktorant na Wydziale Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego, biegły sądowy o specjalności telekomunikacja w zakresie analizy danych telekomunikacyjnych, przez wiele lat pracował w branży teleinformatycznej przy tworzeniu systemów billingowych.

Podstawa prawna – prawo telekomunikacyjne

Ze wstąpieniem Polski 1 maja 2004 r. do Unii Europejskiej wiązała się m.in. konieczność dostosowania prawa polskiego do wymogów dyrektyw unijnych, które kształtowały prawo wspólnotowe. W zakresie telekomunikacji są to przede wszystkim dyrektywy:

1) dyrektywa 2002/21/WE z dnia 7 marca 2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej,
2) dyrektywa 2002/20/WE z dnia 7 marca 2002 r. w sprawie zezwolenia na udostępnienie sieci i usługi łączności elektronicznej,
3) dyrektywa 2002/19/WE z dnia 7 marca 2002 r. w sprawie dostępu do sieci łączności elektronicznej i urządzeń towarzyszących oraz ich łączenia,
4) dyrektywa 2002/22/WE z dnia 7 marca 2002 r. w sprawie usługi powszechnej i praw użytkowników odnoszących się do sieci i usług łączności elektronicznej,
5) dyrektywa 2002/58/WE z dnia 12 lipca 2002 r. w sprawie przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej,
6) dyrektywa 2002/77/WE z dnia 16 września 2002 r. w sprawie konkurencji na rynkach sieci i usług łączności elektronicznej,
7) dyrektywa 2006/24/WE z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności,
8) dyrektywa 2009/136/WE z dnia 25 listopada 2009 r. zmieniająca dyrektywę 2002/22/WE oraz dyrektywę 2002/58/WE, a także rozporządzenie (WE) nr 2006/2004 w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów,
9) dyrektywa 1999/5/WE z dnia 9 marca 1999 r. w sprawie urządzeń radiokomunikacyjnych i telekomunikacyjnych urządzeń końcowych oraz wzajemnego uznawania ich zgodności.

Powyższe akty prawne są powszechnie zaliczane do tzw. nowego pakietu regulacyjnego i zastąpiły ponad 20 dyrektyw, którymi od lat 80. demonopolizowano i liberalizowano unijne rynki telekomunikacyjne. Pakiet regulacyjny jest konsekwentnym krokiem do rozwoju społeczeństwa informacyjnego i ma służyć procesowi przejścia do gospodarki cyfrowej opartej na wiedzy. Twierdzi się, że świat wkroczył w fazę rewolucji telematycznej, polegającej na sprzężeniu telekomunikacji i informatyki. Obecnie postęp w dziedzinie teleinformatyki kładzie główny nacisk na zwielokrotnienie masy przesyłowej (tzn. telematyki), a wielkie firmy informatyczne wchodzą w fuzje z przedsiębiorstwami telekomunikacyjnymi. Niezwykle dynamicznie rozwijający się rynek telekomunikacyjny wymaga więc zupełnie nowego podejścia politycznego, ekonomicznego i prawnego. Nowe podejście do rozwiązań prawnych ma na celu przede wszystkim promowanie zachodzących na rynku zmian poprzez usuwanie różnego typu barier. Dlatego legislacja w tym zakresie zmierza do stworzenia ram regulacji prawnej dla sieci i usług komunikacji elektronicznej. Pamiętać należy także, że obecne zmiany legislacyjne nie wydają się ostatecznymi ani trwałymi rozwiązaniami regulacyjnymi komunikacji elektronicznej. Docelowym rozwiązaniem jest bowiem sytuacja,

w której rynek telekomunikacyjny będzie regulowany jedynie na podstawie ogólnego prawa konkurencji[1].

Spośród wyżej wymienionych aktów prawnych, najważniejszym aktem regulującym tajemnicę telekomunikacyjną jest dyrektywa 2002/58/WE w sprawie przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej. Wspomniana dyrektywa jest *lex specialis* względem dyrektywy 1995/46/WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, dlatego w wielu przypadkach konieczne będzie łączne stosowanie obydwu dyrektyw. Dyrektywa 2002/58/WE ma na celu zapewnienie równego poziomu ochrony podstawowych praw i swobód, w tym prawa do prywatności. Równocześnie jej celem jest zapewnienie swobodnego przepływu danych osobowych w ramach Unii Europejskiej. Zgodnie z zapisami dyrektywy, przedsiębiorca telekomunikacyjny ma za zadanie zapewnić bezpieczeństwo usług, a czasami i sieci, zapewnić poufność przekazów i związanych z nimi danych transmisyjnych, zapewnić, iż bez wiedzy użytkownika końcowego nie zostaną gromadzone informacje z urządzenia końcowego[2].

16 lipca 2004 r. w Polsce została uchwalona ustawa Prawo telekomunikacyjne, która weszła w życie w dniu 3 września 2004 r. Później ustawa była wielokrotnie nowelizowana, ostatnio – 21 stycznia 2013 r. Ustawa Prawo telekomunikacyjne ustala przede wszystkim:

- zasady wykonywania i kontroli działalności telekomunikacyjnej,
- warunki regulowania rynków telekomunikacyjnych,
- warunki gospodarowania częstotliwościami oraz numeracją,
- prawa i obowiązki przedsiębiorców telekomunikacyjnych,
- warunki świadczenia usługi powszechnej,
- prawa i obowiązki przedsiębiorstw wobec użytkowników usług, w tym dotyczące tajemnicy telekomunikacyjnej,
- zadania i obowiązki przedsiębiorców telekomunikacyjnych na rzecz obronności, bezpieczeństwa państwa oraz porządku publicznego.

Jak wynika z powyższego zestawienia, Prawo telekomunikacyjne reguluje działalność przedsiębiorców telekomunikacyjnych, rynki, na których działają, oraz definiuje prawa i obowiązki przedsiębiorców. Warto przytoczyć w tym miejscu definicję przedsiębiorcy telekomunikacyjnego. Zgodnie z art. 2 ust. 27 ustawy:

„przedsiębiorca telekomunikacyjny – przedsiębiorcę lub inny podmiot uprawniony do wykonywania działalności gospodarczej na podstawie odrębnych przepisów, który wykonuje działalność gospodarczą polegającą na dostarczeniu sieci telekomunikacyjnych, udogodnień towarzyszących lub świadczeniu usług telekomunikacyjnych, przy czym przedsiębiorca telekomunikacyjny, uprawniony do:

a) świadczenia usług telekomunikacyjnych, zwany jest »dostawcą usług«,
b) dostarczania publicznych sieci telekomunikacyjnych lub udogodnień towarzyszących, zwany jest »operatorem«"[3].

---

[1] W. Gromski, J. Kolasa, A. Kozłowski, K. Wójtowicz, *Europejskie i polskie prawo telekomunikacyjne*, Wydawnictwo Prawnicze LexisNexis, Warszawa 2004, s. 14–16, 30.

[2] I. Kawka, *Telekomunikacyjne organy regulacyjne w Unii Europejskiej*, Kantor Wydawniczy Zakamycze, Kraków 2006, s. 138.

[3] http://www.uke.gov.pl/_gAllery/34/35/34353/I_Rozdzial_1.pdf, dostęp 10.06.2011.

W przytoczonej definicji przedsiębiorcą telekomunikacyjnym jest każdy podmiot, który uzyska status przedsiębiorcy telekomunikacyjnego, jest uprawniony do wykonywania działalności polegającej na dostarczaniu sieci telekomunikacyjnej lub udogodnień towarzyszących (podmiot zwany operatorem) oraz świadczeniu usług telekomunikacyjnych (podmiot zwany dostawcą usług). Wykładnia funkcjonalna w tym zakresie mówi także, że przedsiębiorcą telekomunikacyjnym zostaje się zaraz po wpisie do rejestru przedsiębiorców telekomunikacyjnych lub uzyskaniu uprawnień do prowadzenia działalności telekomunikacyjnej, nie zaś w momencie rozpoczęcia wykonywania czynności mieszczących się w działalności telekomunikacyjnej[4].

Dla dalszych rozważań najistotniejszym elementem ustawy będzie obowiązek przedsiębiorcy w zakresie zachowania tajemnicy telekomunikacyjnej. Aby w pełni zrozumieć istotę tego obowiązku, trzeba rozpatrzyć podstawy prawne dla zastosowania takiego rozwiązania. Przepisy prawa telekomunikacyjnego dotyczące tajemnicy telekomunikacyjnej obligują do jej zachowania jedynie podmioty prowadzące działalność telekomunikacyjną w sieciach publicznych, nie obejmują zatem podmiotów eksploatujących niepubliczne sieci telekomunikacyjne oraz dostawców usług w takich sieciach. Za publiczną sieć telekomunikacyjną ustawa przyjmuje sieć wykorzystywaną głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych. Przez sieć niepubliczną rozumie się więc sieć wykorzystywaną przez podmiot wyłącznie do własnych potrzeb. Choć przytoczony wcześniej art. 2 ust. 27 nie ogranicza pojęcia dostawcy usług do przedsiębiorców świadczących usługi w sieciach publicznych, art. 160 ust. 1 nie obejmuje dostawców usług w sieciach niepublicznych. Do tych ostatnich stosują się przepisy prawa cywilnego i karnego[5].

Tajemnica telekomunikacyjna

Obowiązująca obecnie Ustawa Prawo telekomunikacyjne wprowadza do polskiego prawa pojęcie tajemnicy telekomunikacyjnej. Zgodnie z art. 159 ust. 1 wspomnianej ustawy:

„Tajemnica komunikowania się w sieciach telekomunikacyjnych, zwana dalej »tajemnicą telekomunikacyjną«, obejmuje:

1) dane dotyczące użytkownika;
2) treść indywidualnych komunikatów;
3) dane transmisyjne, które oznaczają 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 wskazujące położenie geograficzne urządzenia końcowego użytkownika publicznie dostępnych usług telekomunikacyjnych;
4) dane o lokalizacji, które oznaczają dane lokalizacyjne wykraczające poza dane niezbędne do transmisji komunikatu lub wystawienia rachunku;
5) dane o próbach uzyskania połączenia między zakończeniami sieci, w tym dane o nieudanych próbach połączeń, oznaczających połączenia między komunikacyjnymi

[4] S. Piątek, *Prawo telekomunikacyjne. Komentarz*, Wydawnictwo C.H. Beck, Warszawa 2005, s. 80–83.

[5] *Ibidem*, s. 869.

urządzeniami końcowymi lub zakończeniami sieci, które zostały zestawione i nie zostały odebrane przez użytkownika końcowego lub nastąpiło zerwanie zestawianych połączeń"[6].

Tak więc zgodnie z Ustawą Prawo telekomunikacyjne tajemnica telekomunikacyjna obejmuje zarówno podmioty realizujące dane połączenie, jak i samo połączenie między tymi podmiotami. Równocześnie przedmiotem tajemnicy jest z jednej strony treść komunikatu przesyłanego przy pomocy danego połączenia, z drugiej zaś parametry techniczne danego połączenia.

Drugim istotnym zapisem wspomnianej ustawy jest art. 159 ust. 3, który brzmi następująco:

„Z wyjątkiem przypadków określonych ustawą, ujawnianie lub przetwarzanie treści albo danych objętych tajemnicą telekomunikacyjną narusza obowiązek zachowania tajemnicy telekomunikacyjnej"[7].

Zapis art. 159 ust. 2 wymienionej ustawy dodatkowo precyzuje kwestię dostępu do danych:

„Zakazane jest zapoznawanie się, utrwalanie, przechowywanie, przekazywanie lub inne wykorzystanie treści lub danych objętych tajemnicą telekomunikacyjną przez osoby inne niż nadawca i odbiorca komunikatu, chyba że:

1) będzie to przedmiotem usługi lub będzie to niezbędne do jej wykonania;
2) nastąpi za zgodą nadawcy lub odbiorcy, których dane te dotyczą;
3) 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;
4) będzie to konieczne z innych powodów przewidzianych ustawą lub przepisami odrębnymi"[8].

W tych trzech ustępach art. 159 Ustawy Prawo telekomunikacyjne zawiera się najważniejsza część tajemnicy telekomunikacyjnej. Pozostałe przepisy uzupełniają lub precyzują pewne elementy, które zawarte są w art. 159. Przepis ten definiuje tajemnicę telekomunikacyjną jako tajemnicę komunikowania się. Obejmuje ona informacje przekazywane w sieciach telekomunikacyjnych, dane dotyczące użytkowników oraz dane dotyczące faktu, okoliczności i rodzaju połączenia, prób uzyskania połączenia między określonymi zakończeniami sieci, a także identyfikacji bądź lokalizacji zakończeń sieci, pomiędzy którymi wykonano połączenie. Zakres przedmiotowy tajemnicy powinien być rozpatrywany w kontekście definicji usługi telekomunikacyjnej, gdyż w tym zakresie przewiduje ochronę objętą tajemnicą telekomunikacyjną. W zakres ochrony wchodzą także informacje identyfikujące użytkownika końcowego, a zawarte w umowie o świadczenie usług. Ochroną tajemnicy objęte są również treści indywidualnych komunikatów, czyli każdej informacji wymienianej lub przekazywanej między określonymi użytkownikami za pośrednictwem publicznie dostępnej sieci telekomunikacyjnej[9].

---

[6] http://www.uke.gov.pl/_gAllery/34/37/34371/VII_Dzial.pdf, dostęp 10.06.2011.

[7] *Ibidem*.

[8] *Ibidem*.

[9] A. Krasuski, *Prawo telekomunikacyjne. Komentarz*, Wydawnictwo Prawnicze LexisNexis, Warszawa 2010, s. 596–601.

Warto także wspomnieć o dwóch aktach prawnych, które w zasadniczy sposób kształtują pojęcie tajemnicy telekomunikacyjnej. Pierwszym z nich jest Konstytucja RP, która definiuje tajemnicę komunikowania się. Tajemnica telekomunikacyjna jest jej elementem, gdyż art. 49 Konstytucji RP nie precyzuje, co należy rozumieć przez komunikowanie się, także ochroną tajemnicy komunikowania się obejmuje się wszelkie sposoby porozumiewania się. Choć ustawa zasadnicza nie wprowadza bezwzględnej tajemnicy komunikowania się, ograniczenie tego dobra osobistego może nastąpić jedynie na podstawie ustawy, która musi precyzować przypadki tego ograniczenia oraz sposób jego realizacji[10]. Drugim aktem prawnym jest Ustawa o ochronie danych osobowych, która definiuje przede wszystkim dane osobowe i zakres ich ochrony. Ustawa ta ma kompleksowy charakter, gdyż stara się pogodzić z pozoru sprzeczne interesy. Z jednej strony jej celem jest ochrona osób, których dane są przetwarzane, z drugiej zaś próbuje rozwiązać kwestię wolności informacji, udostępniania danych instytucjom i obywatelom w celu wykorzystania tych danych. Ustawa wprowadza organ administratora danych, któremu nadano uprawnienia w zakresie określania celu i środków przetwarzania danych osobowych. Trzeba też zauważyć, że w ustawie zostało wprowadzone pojęcie danych ogólnie (powszechnie) dostępnych, które nie podlegają ochronie i mogą być swobodnie przetwarzane[11].

Powyżej zostały wymienione najważniejsze akty prawne regulujące tajemnicę telekomunikacyjną. Nie są to wszystkie regulacje, poniżej został przedstawiony pełen zakres aktów prawnych, które wpływają na stosowanie tajemnicy telekomunikacyjnej. Zgodnie ze stanem prawnym na dzień 1 grudnia 2009 r. są to także:

- Kodeks postępowania karnego;
- Ustawa o świadczeniu usług drogą elektroniczną;
- Ustawa o rachunkowości;
- Ustawa o kontroli skarbowej;
- Rozporządzenie Ministra Sprawiedliwości w sprawie sposobu technicznego przygotowania systemów i sieci służących do przekazywania informacji – gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczenia danych informatycznych;
- Ustawy szczególne o Policji, Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, Centralnym Biurze Antykorupcyjnym, Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, Straży Granicznej, Żandarmerii Wojskowej i Wojskowych Organach Porządkowych[12].

Mając na uwadze powyższe rozważania, trzeba stwierdzić, że prawo telekomunikacyjne jest bardzo restrykcyjne w zakresie konieczności zachowania tajemnicy telekomunikacyjnej. Faktem jest jednak, że zachowanie tajemnicy dotyczy jedynie przedsiębiorców telekomunikacyjnych działających w publicznych sieciach telekomunikacyjnych. A dane transmisyjne generują, gromadzą i przetwarzają także firmy działające w sieciach niepublicznych oraz przedsiębiorstwa nietrudniące się działalnością telekomunikacyjną. Obecnie standardowym wyposażeniem każdej firmy jest centrala telefoniczna, która z założenia generuje dane transmisyjne. Centrale abonenckie coraz

[10] K. Kawałek, M. Rogalski, *Prawo telekomunikacyjne. Komentarz*, Wolters Kluwer Polska, Warszawa 2010, s. 857.

[11] J. Barta, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Kantor Wydawniczy Zakamycze, Kraków 2001, s. 89–92.

[12] A. Krasuski, *Prawo telekomunikacyjne..., op. cit.,* s. 607.

częściej pojawiają się także w prywatnych domach, gdzie poza funkcją telekomunikacyjną pełnią także funkcję np. domofonu. Tak więc powstaje luka prawna związana z tymi urządzeniami, które nie są w gestii działających w publicznych sieciach przedsiębiorstw telekomunikacyjnych. Także w prawie unijnym nie ma jednoznacznego rozwiązania, gdyż Rekomendacja o ochronie danych osobowych w dziedzinie usług telekomunikacyjnych ze szczególnym uwzględnieniem usług telefonicznych, przyjęta przez Komitet Ministrów Rady Europy 7 lutego 1995 r., w stosunku do central PABX wykorzystywanych w miejscu pracy odsyła do przepisów dotyczących zatrudnienia, a w stosunku do central abonenckich udostępnianych w instytucjach użyteczności publicznej do przepisów dotyczących dostawców usług[13].

Problemu nie byłoby, gdyby nie praktyka wykorzystania billingów tworzonych na podstawie wygenerowanych danych transmisyjnych oraz sposobu ich wykorzystania wewnątrz firm i instytucji. Praktyka jest bowiem taka, że każdy korzystając z telefonu firmowego, niejako domyślnie wyraża zgodę na kontrolę jego połączeń telefonicznych, na pewno w zakresie danych transmisyjnych. Danych tych nie chroni bowiem prawo telekomunikacyjne, gdyż ustawa dotyczy przedsiębiorstw telekomunikacyjnych, a nie każdego użytkownika centrali telefonicznej, czy to miejskiej, czy abonenckiej. Wydaje się, że jest to dosyć duże niedopatrzenie przy współczesnych rozwiązaniach telekomunikacyjnych, jakie są oferowane odbiorcom. Nie jest przypadkiem odosobnionym, że w biurowcu, który obsługiwany jest przez jedną firmę, zazwyczaj właściciela, dystrybuowane są różne media, w tym także media teleinformatyczne. Firmy te nie zarabiają na samych usługach telekomunikacyjnych, nie mają więc statusu przedsiębiorcy telekomunikacyjnego. Jednak, aby nie stracić, muszą refakturować koszty wygenerowanych przez użytkownika końcowego połączeń telefonicznych. Do kontroli tych połączeń wykorzystują systemy billingowe współpracujące z centralami abonenckimi.

Przykłady wykorzystania systemów billingowych współpracujących z centralami abonenckimi, których nie chronią zapisy prawa telekomunikacyjnego, można mnożyć i przytaczać mnóstwo. Nie jest przedmiotem niniejszej pracy rozstrzyganie, czy takie wykorzystanie billingów jest zgodne z prawem pracy lub innymi przepisami prawa. Niemniej rodzi to lukę prawną w dwóch przytoczonych wyżej aspektach. W obydwu sytuacjach, w świetle obowiązującego prawa, trudno jednoznacznie ocenić, czy została złamana tajemnica telekomunikacyjna. Z jednej strony billingi od operatora, z pełną informacją o połączeniu, dostaje rzeczywisty podmiot uczestniczący w połączeniu realizowanym przez przedsiębiorcę telekomunikacyjnego. Przedsiębiorca telekomunikacyjny nie może więc odpowiadać za to, co dzieje się z połączeniem poza urządzeniem, do którego jest podłączony. Z drugiej strony obsługujący centralę abonencką ma dostęp do danych transmisyjnych, na podstawie których może ustalić dane abonenta, zarówno dzwoniącego, jak i odbierającego. Może on także, na podstawie danych transmisyjnych centrali abonenckiej, mieć dostęp do chronionych tajemnicą telekomunikacyjną danych dotyczących jej użytkowników.

Ustawa Prawo telekomunikacyjne nakłada także pewne zadania i obowiązki na przedsiębiorców telekomunikacyjnych na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, co wiąże się bezpośrednio z obowiązkiem

[13] P. Fajgielski, *Ochrona danych osobowych w telekomunikacji – aspekty prawne*, Lubelskie Towarzystwo Naukowe, Lublin 2003, s. 127.

ujawniania danych transmisyjnych i danych lokalizacyjnych, a tym samym z uchyleniem tajemnicy telekomunikacyjnej. Art. 179 ust. 3 ustawy brzmi następująco:

„Przedsiębiorca telekomunikacyjny (...) jest obowiązany do:

1) zapewnienia warunków technicznych i organizacyjnych dostępu i utrwalania, zwanych dalej »warunkami dostępu i utrwalania«, umożliwiających jednoczesne i wzajemnie niezależne:
   a) uzyskiwanie przez Policję, Straż Graniczną, Agencję Bezpieczeństwa Wewnętrznego, Służbę Kontrwywiadu Wojskowego, Żandarmerię Wojskową, Centralne Biuro Antykorupcyjne i wywiad skarbowy, zwane dalej »uprawnionymi podmiotami«, w sposób określony w ust. 4b, dostępu do:
   – przekazów telekomunikacyjnych, nadawanych lub odbieranych przez użytkownika końcowego lub telekomunikacyjne urządzenie końcowe,
   – posiadanych przez przedsiębiorcę danych związanych z przekazami telekomunikacyjnymi, o których mowa w ust. 9, art. 159 ust. 1 i pkt 3–5,
   b) uzyskiwanie przez uprawnione podmioty danych związanych ze świadczoną usługą telekomunikacyjną i danych, o których mowa w art. 161,
   c) utrwalanie przez uprawnione podmioty przekazów telekomunikacyjnych i danych, o których mowa w pkt 1 lit. a i b.
2) utrwalenia na rzecz sądu i prokuratora przekazów telekomunikacyjnych i danych, o których mowa w pkt 1 lit. a i b”[14].

Jak wynika z powyższych zapisów, przedsiębiorca telekomunikacyjny zobowiązany jest do współpracy z organami państwowymi w zakresie zapewnienia bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego. Tym samym zobligowany jest m.in. do stworzenia warunków dla udostępniania takich informacji, jak treść przekazów telekomunikacyjnych, a także danych związanych z przekazem telekomunikacyjnym, takich jak wykaz abonentów, dane dotyczące użytkowników, dane transmisyjne, dane o lokalizacji oraz dane o próbach uzyskania połączenia. Zapewnienie tych warunków dostępowych powinno być tak zorganizowane, aby proces mógł odbywać się bez udziału pracowników przedsiębiorcy telekomunikacyjnego. Jedynie w indywidualnych przypadkach mogą oni brać udział w tym działaniu. Przedstawione rozwiązanie jest uzasadnione z punktu widzenia organów ścigania i instytucji wymiaru sprawiedliwości, gdyż przy pomocy usług telekomunikacyjnych dokonywana jest coraz większa liczba przestępstw, z drugiej strony rodzi to niebezpieczeństwo naruszania danych osobowych użytkowników tych usług. Aby wyeliminować możliwie najwięcej naruszeń danych osobowych, dostęp poszczególnych podmiotów uprawnionych został uregulowany w ustawach dotyczących działalności poszczególnych służb należących do grupy podmiotów uprawnionych[15].

W kontekście obowiązków przedsiębiorcy telekomunikacyjnego na rzecz bezpieczeństwa publicznego został ujawniony billing w przywołanym we wprowadzeniu przykładzie. Jednak rodzi się pytanie, o jakim billingu w tym momencie jest mowa – czy o billingu operatorskim, który pozwala na zarejestrowanie połączenia między dwoma abonentami miejskimi, czy może billingu z centrali abonenckiej jednego z interesujących wymiar sprawiedliwości abonentów? Dla osób postronnych może to nie

[14] http://www.uke.gov.pl/_gAllery/34/37/34372/VIII_Dzial.pdf, dostęp 10.06.2011.

[15] K. Kawałek, M. Rogalski, *Prawo telekomunikacyjne. Komentarz*, *op. cit.*, s. 919–922.

mieć znaczenia. Jednak aby naświetlić problem, warto przytoczyć rzeczywistą sytuację sprzed kilku lat. Prokuratura poszukiwała świadków oszustwa, jakiego dopuszczono się za pomocą sieci telekomunikacyjnej. Była w posiadaniu billingów oszusta, z których zidentyfikowała numery osób, które do tego oszusta dzwoniły. Wśród numerów znalazły się także numery jednej z instytucji, której pracownik dzwonił do podejrzanego. Instytucja miała centralę abonencką obsługującą ponad 1500 numerów wewnętrznych, nie mając więc systemu billingowego dla swojej centrali nie byłaby w stanie zidentyfikować osoby rzeczywiście dzwoniącej. W tej sytuacji instytucja korzystała z systemu billingowego, więc osoba dzwoniąca została zidentyfikowana i świadczyła przeciw podejrzanemu. Sytuacja byłaby zupełnie inna, gdyby w tej instytucji nie było systemu billingowego lub byłby traktowany zupełnie inaczej (np. dane nie byłyby na bieżąco przetwarzane lub nie byłyby archiwizowane itp.).

Przytoczony przykład obrazuje kolejną lukę w prawie telekomunikacyjnym. Nakłada ono bowiem obowiązki na przedsiębiorców telekomunikacyjnych w sprawie utrwalania danych objętych tajemnicą telekomunikacyjną, nie obejmując nimi innych podmiotów korzystających z central PABX. Szybki rozwój technologii i łączenie różnego typu usług w jednym urządzeniu powoduje, że dane transmisyjne posiadane przez przedsiębiorców telekomunikacyjnych w wielu przypadkach nie są wystarczające do prawidłowej identyfikacji użytkowników uczestniczących w połączeniu. Natomiast dokładniejsze dane, generowane przez centrale abonenckie, są w większości przypadków poza jurysdykcją prawa.

Kolejna luka prawna w zakresie tajemnicy telekomunikacyjnej oraz zapewnienia bezpieczeństwa publicznego dotyczy abonenckich central telefonicznych i świadczonych przez nie usług, które nie są w gestii przedsiębiorców telekomunikacyjnych. Sytuacja taka rodzi dwa niebezpieczeństwa. Z jednej strony dane te nie są chronione i dostęp do nich mają nieuprawnione osoby, z drugiej strony dane źródłowe z tych central nie podlegają obowiązkowi utrwalania i poddania anonimizacji.

Billing – potencjalne źródło ujawnienia chronionych danych

Warto przeanalizować znaczenie używanego wyżej pojęcia billingu. Billing to rachunek szczegółowy, zestawienie wszystkich opłat za połączenia i usługi dodane, jakie abonent przeprowadził w danym okresie rozliczeniowym. Umożliwia szczegółową kontrolę dokonanych transakcji. Może być sporządzany także tzw. minibilling, który zawiera usługi i połączenia pogrupowane zgodnie z kierunkiem przeprowadzonych rozmów[16]. Przytoczona definicja billingu ogranicza się do aspektu finansowego wykorzystania danych transmisyjnych. Unijne dyrektywy wyraźnie rozróżniają dane billingowe i transmisyjne, ograniczając dane billingowe do tych, które są niezbędne do rozliczenia rozmów. Często billing utożsamia się zarówno z zestawieniem kosztowym, jak i zestawieniem informacyjnym. Zgodnie bowiem z wytycznymi tworzenia systemu sterującego centralami, jedną z ważnych funkcji tego oprogramowania jest generowanie danych transmisyjnych w celach rozliczeniowych oraz kontrolnych i informacyjnych[17].

[16] P. Fajgielski, *Ochrona danych osobowych w telekomunikacji..., op. cit.*, s. 101.

[17] W. Kabaciński, M. Żal, *Sieci telekomunikacyjne*, Wydawnictwo Komunikacji i Łączności, Warszawa 2008, s. 465–466.

Niewiele osób rozróżnia zawartość billingów kosztowych oraz zestawień informacyjnych. Przyczyna leży głównie w dostępie jedynie do billingów operatora, nie zaś do źródłowych danych transmisyjnych.

Zawartość standardowego billingu operatorskiego, jaki generowany jest dla użytkownika końcowego, jest oparta na danych billingowych i ograniczona do numeru dzwoniącego, numeru odbierającego, czasu rozpoczęcia rozmowy oraz czasu trwania rozmowy. W prawie brak jest definicji danych billingowych, przyjmuje się, że są to te dane, które niezbędne są do wystawienia rachunku[18]. Dlatego czasami informacja poszerzona jest o istotne dla rozliczenia szczegóły, takie jak typ usługi (np. rozmowa, SMS, MMS) czy strefa (rozmowa z Katowicami, Warszawą czy Krakowem). Na ile dane te mogą zwiększyć wiedzę o połączeniach, każdy może ocenić sam. Niemniej, oglądając przypadkowy billing, niewiele będzie można powiedzieć o samej rozmowie – przede wszystkim nie będzie można zidentyfikować odbiorców kryjących się za numerami. Aby poznać więcej szczegółów, należałoby odnieść się do danych transmisyjnych, które poza danymi billingowymi zawierają także m.in. informację o fakcie nawiązania połączenia, rodzaj połączenia, dane dotyczące kierowania, daty lub objętości przekazu, zastosowanego protokołu przesyłu, lokalizacji urządzenia końcowego nadawcy lub odbiorcy, a także wykorzystywanej sieci[19]. Katalog tych danych nie został ściśle określony i jest zbiorem otwartym.

Trochę inaczej wygląda sprawa z systemami billingowymi współpracującymi z centralami abonenckimi. W przypadku billingów generowanych przez te systemy użytkownik ma większe pole manewru, jeżeli chodzi o dobór informacji zawartych w zestawieniu. Nie oznacza to bynajmniej obligatoryjnie większej zawartości informacyjnej zestawienia billingowego. Daje to jedynie większe możliwości dostosowania zestawienia do własnych potrzeb w ramach dostarczanych danych. Nie można powiedzieć, że zawsze będzie zwiększona ilość danych ponad dane billingowe, gdyż nie każda centrala telefoniczna zrzuca większy od podstawowego zakres danych. Właśnie różnice w rekordach taryfikacyjnych zawierających dane transmisyjne wpływają na fakt, że producenci systemów billingowych dla central abonenckich dają tak duże możliwości konfiguracyjne. Billingi wygenerowane przez systemy dedykowane dla central abonenckich można więc traktować także jako zestawienia informacyjne. W zależności od centrali, w billingu mogą być zawarte takie informacje, jak nazwy abonentów (dzwoniącego i odbierającego), liczba osób lub urządzeń uczestniczących w połączeniu (np. w sytuacji przełączania rozmowy lub rozmowy konferencyjnej), kierunek połączenia (wychodzące, przychodzące), informacja o operatorze realizującym połączenie (istotne w przypadku korzystania z operatorów alternatywnych), powód rozłączenia (zawieszenie połączenia, przerwanie połączenia), skutek rozmowy (odebrana, nieodebrana). Przedstawione informacje są najczęściej wykorzystywanymi, przykładowymi danymi. Możliwości jest o wiele więcej – centrale IP mogą przekazywać w rekordzie taryfikacyjnym ponad 100 różnych danych[20].

Powracając do tajemnicy telekomunikacyjnej, trzeba odpowiedzieć na pytanie, jak powyższe rozważania wpływają na jej zachowanie. Abstrahując w tym miejscu od

[18] A. Krasuski, *Prawo telekomunikacyjne..., op. cit.*, s. 632.

[19] P. Fajgielski, *Ochrona danych osobowych w telekomunikacji..., op. cit.*, s. 139–141.

[20] http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/service/7_0_1/cdr-defs/cdradmin.html, dostęp 10.06.2011.

rozwiązań prawnych, wejście w posiadanie billingu operatora mówi niewiele o połączeniach. Dopiero konfrontacja tych danych z powszechnie dostępnymi danymi, takimi jak spisy abonentów, może przybliżyć jego zawartość. Wejście w posiadanie billingu wygenerowanego przez system współpracujący z centralą abonencką może z większym prawdopodobieństwem prowadzić do złamania tajemnicy telekomunikacyjnej. Przede wszystkim billing taki może zawierać dużo więcej danych objętych ochroną, oraz więcej, bardziej szczegółowych informacji technicznych o przebiegu połączenia.

Warto też przeanalizować zawartość billingów abonenckich pod kątem zadań na rzecz bezpieczeństwa publicznego. Niewątpliwie billingi takie są uzupełnieniem informacyjnym dla billingów operatorskich. Zawierają informacje o tym, co działo się po drugiej stronie centrali abonenckiej. W wielu przypadkach informacje te są kluczowe dla sprawy, dla której są gromadzone i analizowane. Z drugiej strony nie można ich przeceniać, gdyż wymagają bardzo dużej wiedzy i umiejętności analitycznych, aby je wykorzystać w sposób prawidłowy. Różnorodność w zakresie danych, ich zawartości, formatu i znaczenia jest tak wielka i znacząca dla ostatecznego kształtu billingu, że wykracza poza zakres zawartych tutaj rozważań[21].

Możliwość ujawnienia danych billingowych

Dotychczasowe rozważania dotyczące tajemnicy telekomunikacyjnej prowadzą do wniosku, że mimo bardzo restrykcyjnych przepisów prawa możliwości ujawnienia chronionych prawnie danych transmisyjnych jest wiele. Problem ten należy rozpatrywać w dwóch aspektach. Pierwszym aspektem będą uregulowania prawne, które chronią dane billingowe oraz określają zakres, w jakim te dane mogą być ujawniane. Drugim aspektem jest kontekst techniczny, który warunkuje możliwości poszczególnych podmiotów w zakresie generowania i przetwarzania, w tym ujawniania, danych billingowych.

Ważniejszy z punktu widzenia użytkownika jest aspekt prawny. Prawo bowiem reguluje, jakie dane i w jakim zakresie będą chronione, w jakim przypadku i komu będą one udostępniane, a także jakie grożą konsekwencje przy nieuprawnionym przetwarzaniu danych. Odpowiednie uregulowania prawne mają zapewnić użytkownika sieci telekomunikacyjnej, że jest bezpieczny podczas korzystania z usług telekomunikacyjnych. W tym wypadku prawo daje wiele możliwości obejścia przepisów, w szczególności gdy korzystamy z sieci niepublicznych. W tej sytuacji abonent praktycznie nie jest chroniony przepisami prawa, gdyż prawo telekomunikacyjne nie obejmuje koniecznością zachowania tajemnicy telekomunikacyjnej usług w sieciach niepublicznych, a Ustawa o ochronie danych osobowych nie wspomina wprost o danych transmisyjnych i billingowych. W wielu przypadkach dane transmisyjne mogą nie zostać objęte ochroną Ustawy o ochronie danych osobowych także ze względu na sposób przetwarzania, gdy uniemożliwia to skorelowanie danych z konkretnymi osobami[22]. Tak więc posługiwanie się tymi danymi bywa niemal bezkarne.

---

[21] M. Witański, *Analiza rekordu taryfikacyjnego centrali telefonicznej*, „Przegląd Telekomunikacyjny. Wiadomości Telekomunikacyjne" 2011, nr 12.

[22] P. Fajgielski, *Ochrona danych osobowych w telekomunikacji..., op. cit.*, s. 223.

Prawo telekomunikacyjne oraz Ustawa o ochronie danych osobowych dają także możliwość swobodnego przetwarzania danych ogólnie dostępnych, co w przypadku usług telekomunikacyjnych odnosić się będzie głównie do powszechnie dostępnych spisów abonentów. Dla zachowania anonimowości abonent może wyrazić brak zgody na umieszczenie w spisie abonentów, może także nie zgodzić się na prezentację numeru wywołującego podczas realizacji połączenia. Kroki te ograniczą możliwości identyfikacji użytkownika końcowego, korzystającego z konkretnego numeru telefonu.

Unijne dyrektywy duży nacisk kładą także na dane przetwarzane dla celów naliczania opłat za usługi, zweryfikowania płatności oraz realizacji rozliczeń międzyoperatorskich. W prawodawstwie unijnym pojawiają się sugestie dotyczące zastosowania w poszczególnych krajach takich sposobów rozliczeń oraz takich metod generowania rachunków, aby nie było konieczności (możliwości) zobaczenia danych abonenta. Zauważa się bowiem, że rachunki szczegółowe umożliwiają rozpoznanie kręgu znajomych abonenta i częstotliwości kontaktów z poszczególnymi numerami. Rachunki szczegółowe ułatwiają kontrolę prawidłowości naliczania opłat, co z kolei przemawia za jak największą ich szczegółowością. Postuluje się także, żeby za przetwarzanie danych w celach księgowych odpowiadała jedna osoba, najlepiej pracownik dostawcy usług, a w zakres jego obowiązków wchodziły tylko zadania konieczne do wykonania tego rodzaju działalności[23].

Prawo telekomunikacyjne reguluje także kwestie dostępu do danych transmisyjnych, w tym billingowych. Daje szerokie uprawnienia organom ścigania oraz instytucjom wymiaru sprawiedliwości w zakresie dostępu do danych, narzucając przedsiębiorcom telekomunikacyjnym konieczność zapewnienia na własny koszt tego dostępu, wyłączając jednak z pracy operacyjnej pracowników przedsiębiorcy. Sytuacja permanentnego dostępu do danych billingowych, niespotykana w innych krajach europejskich[24], może rodzić niebezpieczeństwo naruszenia dóbr osobistych użytkowników końcowych poprzez realizację zadań wynikających z obowiązków na rzecz obronności i bezpieczeństwa[25]. Wątpliwości wobec ciągłego dostępu do danych transmisyjnych stacjonarnych sieci publicznych budzi także fakt, że wśród istotnych przestępstw dokonanych za pomocą telefonii stacjonarnej, na szkodę obywatela lub przedsiębiorcy telekomunikacyjnego, jest wymieniane jedynie przestępstwo nadużycia telefonu stacjonarnego, które polega na podpięciu się do cudzego telefonu stacjonarnego i korzystaniu z usług telefonicznych na szkodę jego właściciela[26]. Stały dostęp do danych transmisyjnych tego przestępstwa nie wykryje. Należy mieć nadzieję, że przepisy zawarte w ustawach dotyczących działalności poszczególnych służb w sposób odpowiedni zapewniają zachowanie tajemnicy telekomunikacyjnej.

Możliwość ujawnienia danych billingowych w aspekcie technicznym łączy się z trzema kwestiami. Najistotniejszy dla ujawniania danych jest podział na dwa źródła danych billingowych. Do powszechnie znanego źródła danych, jakim jest dostawca usług w sieci publicznej, trzeba dołożyć dostawcę usług w sieci niepublicznej. Różnice między billingami poszczególnych dostawców, a także uwarunkowania prawne

[23] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Wolters Kluwer Polska, Kraków 2007, s. 269–270.

[24] http://wyborcza.pl/1,76842,8634123,Nasze_billingi_i_internet_pod_lupa_sluzb.html, dostęp 10.06.2011.

[25] K. Kawałek, M. Rogalski, *Prawo telekomunikacyjne. Komentarz*, *op. cit.*, s. 919.

[26] M. Rogalski, *Przestępstwa telekomunikacyjne*, Kantor Wydawniczy Zakamycze, Kraków 2006, s. 95.

związane z dwoma typami sieci telekomunikacyjnej zostały wcześniej zarysowane. Brak ochrony prawnej dla billingów sieci niepublicznej rodzi dużą możliwość wycieku niezamierzonego, jak i zamierzonego tych danych. Biorąc pod uwagę fakt, że billingi dostawców niepublicznych zawierają dużo więcej danych identyfikujących podmiotowy i przedmiotowy zakres połączenia, ujawnienie takich danych może okazać się dużo groźniejsze niż ujawnienie billingów dostawcy publicznego.

Drugą kwestią związaną z aspektem technicznym jest sposób zabezpieczenia dostępu do tych danych. Prawo telekomunikacyjne nakłada na dostawcę usług publicznych wiele obostrzeń w zakresie zapewnienia bezpieczeństwa danych transmisyjnych. Zgodnie z ustawą dane te nie mogą być przechowywane dłużej niż 12 miesięcy zarówno dla celów bezpieczeństwa państwowego i publicznego, jak i dla rozliczeń. Nieco dłuższy, bo pięcioletni okres przechowywania dokumentów księgowych, w tym billingów telekomunikacyjnych jako podstawy naliczania kosztów, przewiduje Ustawa o rachunkowości[27]. Po tym okresie dane powinny być niszczone lub co najmniej poddane anonimizacji zgodnie z zasadami Ustawy o ochronie danych osobowych. Powyższe obostrzenia nie obowiązują przedsiębiorstw świadczących usługi w sieciach niepublicznych lub niezarejestrowanych przedsiębiorców wykorzystujących na własne potrzeby centrale abonenckie. Sposobów obchodzenia się z danymi billingowymi w tych przedsiębiorcach jest mnóstwo, od postawienia niezabezpieczonego systemu billingowego na serwerze dostępnym z zewnątrz aż po stosowanie restrykcyjnych przepisów, zgodnych z wymienionymi wcześniej ustawami. Niepokój budzi to, ile z osób mających dostęp do danych transmisyjnych centrali abonenckiej nie zdaje sobie sprawy, jak wrażliwe dane posiada. Nie jest to problem związany tylko z systemem billingowym, a ogólnie z zarządzaniem informatycznymi zasobami firmy. Czynnik ludzki w tym wypadku odgrywa kluczową rolę w zwiększeniu prawdopodobieństwa nieumyślnego ujawnienia danych billingowych w wyniku włamania lub przypadkowego wejścia w posiadanie danych transmisyjnych[28].

Trzecia kwestia techniczna dotyczy obowiązków na rzecz bezpieczeństwa państwowego oraz publicznego. Dostawcy usług publicznych mają obowiązek zapewnienia dostępu do danych, takiego obowiązku nie mają dostawcy usług niepublicznych. Powoduje to konieczność uruchomienia procedur sądowych w celu oficjalnego dotarcia do billingów pochodzących z central telefonicznych. Próby dotarcia do danych mogą okazać się nieskuteczne, gdyż operator centrali abonenckiej nie ma żadnego obowiązku związanego z przechowywaniem danych, a tym bardziej z przechowywaniem tych danych przez określony czas i w określonej formie. Dlatego przejście formalnej procedury może okazać się w sumie bezwartościowe, gdy okaże się, że w danych billingowych są braki, dane są nieczytelne lub przetworzone w taki sposób, że stają się bezużyteczne w interesującej organy ścigania sprawie. Rodzi to niebezpieczeństwo, że ujawnienie danych billingowych, nawet zgodne z prawem, będzie miało skutki zupełnie inne niż zamierzone przez organy ścigania lub instytucje wymiaru sprawiedliwości.

[27] http://www.mf.gov.pl/_files_/rachunkowosc/akty_prawne/ustawa_o_rachunkowosci.pdf, dostęp 10.06.2011.

[28] E. Schetina, K. Green, J. Carlson, *Bezpieczeństwo w sieci*, Wydawnictwo Helion, Gliwice 2002, s. 20–24.

Podsumowanie

Europejscy i polscy prawodawcy w sposób zdecydowany dążą do jak największej ochrony obywateli. Wydając odpowiednie dyrektywy, Unia Europejska chce uchronić obywateli przed powszechną inwigilacją, jakiej można się spodziewać w dobie coraz szybciej rozwijających się technologii teleinformatycznych. Dlatego kładzie duży nacisk na wprowadzanie w państwach unijnych rozwiązań, które pozwolą obywatelom na zachowanie maksimum prywatności. Idąc tą ścieżką, od początku XXI wieku polskie prawo dostosowywane jest do wytycznych zawartych w unijnych dyrektywach. Zarówno Ustawa o ochronie danych osobowych, jak i prawo telekomunikacyjne zawierają przepisy, które w sposób bardzo restrykcyjny nakazują ochronę danych osobowych osób korzystających z sieci teleinformatycznych. Zapisy te nie nadążają jednak za bardzo szybkim rozwojem telekomunikacji i informatyki.

W ustawie prawo telekomunikacyjne jest kilka przepisów, które sprawiają, że zachowanie tajemnicy telekomunikacyjnej jest zagrożone. Najważniejszą luką prawną jest odniesienie przepisów w zakresie tajemnicy telekomunikacyjnej oraz obowiązków na rzecz bezpieczeństwa jedynie do przedsiębiorstw telekomunikacyjnych prowadzących działalność w sieciach publicznych. Stwarza to niebezpieczeństwo nieprawidłowego zabezpieczenia danych transmisyjnych oraz nieodpowiedniego przetwarzania tych danych przez przedsiębiorców działających w niepublicznych sieciach telekomunikacyjnych. Drugą istotną luką prawną jest obowiązek zapewnienia stałego, niekontrolowanego dostępu do danych transmisyjnych dla uprawnionych podmiotów. W tej sytuacji możliwe jest nieuzasadnione naruszanie dóbr osobistych abonentów. Wątpliwości budzić może także traktowanie billingów jako dokumentów księgowych i konieczność ich przechowywania nawet przez 5 lat. Dla celów księgowych powinien wystarczyć rachunek lub faktura.

Aby rozważyć wszystkie aspekty zachowania tajemnicy telekomunikacyjnej, trzeba wspomnieć o czynniku ludzkim. Odpowiednie stosowanie prawa zależy od człowieka, który jest odpowiedzialny za wdrożenie w życie konkretnych przepisów. Człowiek tworzy przepisy, procedury, informatyczne narzędzia wspomagające, wreszcie człowiek stosuje te narzędzia. Wrażliwość ludzka może, mimo braku odpowiednich przepisów, zapobiec nieuprawnionemu ujawnianiu danych billingowych pochodzących z sieci niepublicznych. Z drugiej strony brak takiej wrażliwości może doprowadzić do świadomego złamania tajemnicy telekomunikacyjnej i ujawnienia danych billingowych. Tak więc wszystko zależy od człowieka.