UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

UMA PROPOSTA DE MODELO PARA TRANSMISSÃO DE DADOS INTERCEPTADOS NA INTERNET BRASILEIRA

FÁBIO CAÚS SÍCOLI

ORIENTADOR: ANDERSON CLAYTON ALVES NASCIMENTO

DISSERTAÇÃO DE MESTRADO EM ENGENHARIA ELÉTRICA
ÁREA DE CONCENTRAÇÃO INFORMÁTICA FORENSE E SEGURANÇA DA INFORMAÇÃO

PUBLICAÇÃO: PPGENE.DM – 092/12
BRASÍLIA / DF: FEVEREIRO/2012

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

UMA PROPOSTA DE MODELO PARA TRANSMISSÃO DE DADOS INTERCEPTADOS NA INTERNET BRASILEIRA

FÁBIO CAÚS SÍCOLI

DISSERTAÇÃO DE MESTRADO SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA, COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE PROFISSIONAL EM INFORMÁTICA FORENSE E SEGURANÇA DA INFORMAÇÃO.

APROVADA POR:

Anderson Clayton Alves Nascimento, Doutor, ENE/UnB
(Orientador)

Flávio Elias Gomes de Deus, Doutor, ENE/UnB
(Examinador Interno)

Robson de Oliveira Albuquerque, Doutor, ENE/UnB
(Examinador Externo)

DATA: BRASÍLIA/DF, 15 DE FEVEREIRO DE 2012.

FICHA CATALOGRÁFICA

SICOLI, FABIO CAUS
Uma Proposta de Modelo para Transmissão de Dados Interceptados na Internet Brasileira [Distrito Federal] 2012.
xvi, 98p, 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2012). Dissertação de Mestrado – Universidade de Brasília, Faculdade de Tecnologia. Departamento de Engenharia Elétrica.

1. Interceptação
2. Internet
3. Provedor
4. Sigilo
I. ENE/FT/UnB.
II. Título (Série)

REFERÊNCIA BIBLIOGRÁFICA

SICOLI, FABIO C. (2012). Uma Proposta de Modelo para Transmissão de Dados Interceptados na Internet Brasileira. Dissertação de Mestrado em Engenharia Elétrica, Publicação PPGENE.DM – 092/12, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 98p.

CESSÃO DE DIREITOS

NOME DO AUTOR: Fábio Caús Sícoli
TÍTULO DA DISSERTAÇÃO: Uma Proposta de Modelo para Transmissão de Dados Interceptados na Internet Brasileira.

GRAU: Mestre ANO: 2012

Fábio Caús Sícoli
Universidade de Brasília – Faculdade de Tecnologia – Dep. de Engenharia Elétrica
CEP 70.910-900 – Cx Postal 04591 – Brasília – DF – Brasil

Dedico este trabalho a todos que trabalham pelo progresso da ciência e pela difusão do conhecimento.

AGRADECIMENTOS

O presente trabalho foi realizado com o apoio do Departamento Polícia Federal – DPF, com recursos do Programa Nacional de Segurança Pública com Cidadania – PRONASCI, do Ministério da Justiça.

Agradeço ao Professor Dr. Anderson Clayton pela motivação, direcionamento e busca incessante pela melhoria da qualidade do trabalho.

Agradeço ao Professor MSc. João Gondim por compartilhar seu vasto conhecimento, levantar pontos importantes a serem discutidos e apoiar o desenvolvimento dessa dissertação.

A toda equipe de Coordenação do Programa de Mestrado, Professores e demais funcionários do Departamento de Engenharia Elétrica da UnB, que não pouparam esforços para fazer dessa iniciativa pioneira um grande exemplo de qualidade e competência a ser seguido por outras instituições acadêmicas.

Aos colegas de trabalho e Professores Dr. Helvio Ferreira Peixoto e MSc. Cris Amon Caminha da Rocha que foram essenciais para a realização deste Mestrado, mostrando-se sempre disponíveis para apoiar todas as atividades.

Aos meus colegas no Departamento de Polícia Federal por entenderem a importância da qualificação dos servidores e permitirem que eu dedicasse parte do tempo no ambiente de trabalho aos estudos.

À minha família, que sempre me apoiou na minha vida acadêmica e pela paciência e tolerância nas minhas ausências.

Ao colega de trabalho e amigo MSc. André Morum de Lima Simão, pelo exemplo de comprometimento, seriedade e determinação, tanto nas atividades acadêmicas quanto no trabalho ao longo dos anos. Da mesma forma, agradeço ao MSc. Paulo César Herrmann Wanner e MSc. Sergei Kalupniek que contribuíram imensamente com a revisão do trabalho realizado.

A todos, os meus sinceros agradecimentos.

RESUMO

UMA PROPOSTA DE MODELO PARA TRANSMISSÃO DE DADOS INTERCEPTADOS NA INTERNET BRASILEIRA

Autor: Fábio Caús Sícoli
Orientador: Anderson Clayton Alves Nascimento
Programa de Pós-graduação em Engenharia Elétrica
Brasília, fevereiro de 2012

O acesso ao teor das comunicações é uma ferramenta de grande importância para o conhecimento de ações desempenhadas por investigados, relações entre pessoas, seus hábitos, dentre outras informações relevantes a uma investigação criminal.

No entanto, os órgãos de segurança pública têm grandes dificuldades em acessar os dados capturados por meio de uma quebra de sigilo telemático. Dentre as razões, estão a falta de padronização nos métodos utilizados pelas operadoras de telecomunicação para enviar dados aos investigadores e a variedade de formatos de arquivos de dados capturados. Assim, prejudica-se a automatização de tarefas, deixando-as mais ineficientes e suscetíveis a erros humanos. Além disso, as rotinas atualmente utilizadas não oferecem uma cadeia de custódia confiável ou garantias de autenticidade e integridade do tráfego interceptado.

Existem leis, normas e resoluções que obrigam as operadoras de telecomunicação a fornecerem meios para que dados trafegados sejam interceptados quando da suspensão de seu sigilo. Entretanto, não há uma definição de como esses dados devem ser entregues.

Esse trabalho apresenta um modelo de como as operadoras de serviços de telecomunicação deveriam encaminhar os dados de Internet interceptados aos órgãos de segurança pública e outras entidades envolvidas. O modelo foi criado tendo em vista a legislação vigente sobre o tema, normas e resoluções da Agência Nacional de Telecomunicações, do Poder Judiciário e do Ministério Público, e ainda baseado em características técnicas das operadoras. Ademais, métodos e padrões utilizados em outros países foram examinados e usados como referência para o modelo.

O modelo proposto foi avaliado por meio da criação de um protótipo com o uso de ferramentas de software livre e programas especialmente desenvolvidos. O protótipo foi utilizado no relacionamento com provedores de serviço de comunicação das tecnologias ADSL, cabo e 3G. O modelo proposto foi considerado adequado.

ABSTRACT

A PROPOSAL OF A MODEL FOR TRANSMITTING INTERCEPTED DATA IN THE BRAZILIAN INTERNET

Author: Fábio Caús Sícoli
Supervisor: Anderson Clayton Alves Nascimento
Electrical Engineering Post-graduate Program
Brasilia, February of 2012

Accessing communication content is a very important tool for getting to know actions carried out by suspects, connections between people, their habits, as well as other relevant information to criminal investigations.

However, law enforcement agencies have great difficulty in accessing data captured from lawful interceptions. This is largely caused by the lack of standards on how these data should be delivered to investigators and the variety of traffic data file formats. This impairs the automation of tasks, making them more inefficient and prone to human error. Moreover, procedures currently used do not provide a proper chain of custody or guarantees of authenticity and integrity to intercepted traffic that will be presented in court.

In Brazil, there is legislation that requires Internet Service Providers (ISPs) to provide means of delivering data to law enforcement agencies when demanded by a court order. Nevertheless, there is no definition on how these data should be delivered.

This document presents a model for how ISPs should send captured data to law enforcement agencies and other involved entities. The model was created compliant with national legislation on the subject, rules and resolutions of the National Telecommunications Agency (ANATEL), judiciary and public prosecution, moreover based on technical characteristics of Brazilian ISPs and telecom carriers, which are key players in providing Internet access. Furthermore, methods used for the same purpose in other countries have been examined and used as reference to improve the model.

Finally, the model was evaluated using a prototype that was built with pieces of open source software and programs that were specially developed for the purpose of this work. The prototype was then used to successfully receive data from ISPs that used ADSL, cable and 3G technologies. The proposed model was considered satisfactory.

SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

LISTA DE SÍMBOLOS, NOMENCLATURA E ABREVIAÇÕES

3GPP – *Third Generation Partnership Program*

ADSL – *Asymmetric Digital Subscriber Line*

AES – *Advanced Encryption Standard*

ANATEL – Agência Nacional de Telecomunicações

ANSI – *American National Standards Institute*

ATIS – *Alliance for Telecommunications Industry Solutions*

ATM – *Asynchronous Transfer Mode*

BG – *Border Gateway*

BPX – *Broadband Packet Exchange*

BRAS – *Broadband Remote Access Server*

CALEA – *Communications Assistance for Law Enforcement Act*

CATV – *Community Antenna Television*

CC – *Content of Communication*

CCC – *Call Content Channel*

CDC – *Call Data Channel*

CF – Constituição Federal

CMTS – *Cable Modem Termination System*

CNJ – Conselho Nacional de Justiça

CNMP – Conselho Nacional do Ministério Público

CPE – *Customer Premises Equipment*

DCS – *Digital Cellular Service*

DF – *Delivery Function*

DHCP – *Dynamic Host Configuration Protocol*

DNS – *Domain Name Server*

DOCSIS – *Data over Cable Service Interface Specification*

DSLAM – *Digital Subscriber Line Access Multiplexer*

DPF – Departamento de Polícia Federal

EBGP – *External Border Gateway Protocol*

EESPT – Entidade Exploradora de Serviços Públicos de Telecomunicações

E-MTA – *Embedded Multimedia Terminal Adapter*

EQAM – *Edge Quadrature Amplitude Modulator*

ETSI – *European Telecommunications Standards Institute*

FBI – *Federal Bureau of Investigation*

FISA – *Foreign Intelligence Surveillance Act*

GGSN – *Gateway GPRS Support Node*

GPRS – *General Packet Radio Service*

GRE – *Generic Routing Encapsulation*

GSM – *Global System for Mobile Communications*

GTP – *GPRS Tunneling Protocol*

HFC – *Hybrid Fiber-Coaxial*

HI – *Handover Interface*

HSPA – *High Speed Packet Access*

HSPA+ – *Evolved High Speed Packet Access*

I-CMTS – *Integrated Cable Modem Termination System*

IAP – *Intercept Access Point*

IN – *Intelligent Network*

IRI – *Intercept Related Information*

IP – *Internet Protocol*

ISDN – *Integrated Services Digital Network*

ISP – *Internet Service Provider*

ITU – *International Telecommunications Union*

ITU-T – *International Telecommunications Union Telecommunications Standardization Sector*

kbit/s – Quilobits por segundo

KDC – *Key Distribution Center*

LAESP – *Lawfully Authorized Electronic Surveillance Protocol*

LEA – *Law Enforcement Agency*

LEMF – *Law Enforcement Monitoring Facility*

LIID – *Lawful Interception Identifier*

LGT – Lei Geral das Telecomunicações

M-CMTS – *Modular Cable Modem Termination System*

Mbit/s – Megabits por segundo

MP – Ministério Público

MPLS – *Multiprotocol Label Switching*

MSRP – *Message Session Relay Protocol*

NAS – *Network Access Server*

NSL – *National Security Letter*

OSPII – Órgão de Segurança Pública, Investigação e Inteligência

PDIAP – *Packet Data Intercept Access Point*

PLMN – *Public Land Mobile Network*

PMP – Ponto-a-multiponto

POS – *Packet over SONET*

PPP – Ponto-a-ponto

PPPoE – *Point-to-Point Protocol over Ethernet*

PSCI – Provedor de Serviço de Conexão à Internet

PSI – Provedor de Serviço de Informações

PSTN – *Public Switched Telephone Network*

RADIUS – *Remote Authentication Dial In User Service*

RAS – *Remote Access Server*

RDSI – Rede Digital de Serviços Integrados

RTP – *Real Time Transport Protocol*

SABA – *Servidor del Acceso Banda Ancha*

SCI – Serviço de Conexão à Internet

SCM – Serviço de Comunicação Multimídia

SDH – *Synchronous Digital Hierarchy*

SFTP – *SSH File Transfer Protocol*

SGSN – *Serving GPRS Support Node*

SHA-1 – *Secure Hash Algorithm-1*

SIP – *Session Initiation Protocol*

SLE – Serviço Limitado Especializado

SM – Salário Mínimo

SMP – Serviço Móvel Pessoal

SRTT – Serviços de Rede de Transporte de Telecomunicações

SSH – *Secure Shell*

STFC – Serviço Telefônico Fixo Comutado

SVA – Serviço de Valor Adicionado

TCP – *Transfer Control Protocol*

TD-SCDMA – *Time Division Synchronous Code Division Multiple Access*

TETRA – *Terrestrial Trunked Radio*

TFTS – *Terrestrial Flight Telephone System*

TIA – *Telecommunications Industry Association*

TFTP – *Trivial File Transfer Protocol*

TIIT – *Transport of Intercepted IP Traffic*

TLS – *Transport Layer Security*

TOD – *Time of Day*

UDP – *User Datagram Protocol*

UMTS – *Universal Mobile Telecommunication System*

UMTS-CS – *Circuit Switched Universal Mobile Telecommunication System*

UMTS-PS – *Packet Switched Universal Mobile Telecommunication System*

VCI – *Virtual Channel Identifier*

VLAN – *Virtual Local Area Network*

VPI – *Virtual Path Identifier*

VPN – *Virtual Private Network*

WCDMA – *Wide-band Code Division Multiple Access*

WiMAX – *Worldwide Interoperability for Microwave Access*

WMAN – *Wireless Metropolitan Area Network*

1. INTRODUÇÃO

Uma das formas de se obter informações sobre um investigado é mediante o acesso às suas comunicações (BRANCH, 2003). Por esse meio, é possível conhecer seus hábitos, ações desempenhadas, relações entre pessoas e até sua localização (COSTA, 2007).

O acesso às comunicações pode ser obtido por meio de sua interceptação legal. A interceptação pode ser definida como o processo de inspecionar a comunicação entre sujeitos de interesse de maneira legal e sem que os entes interceptados estejam cientes (BRANCH; PAVLICIC; ARMITAGE, 2004). Esse procedimento normalmente é conduzido por órgãos de segurança pública e agências de inteligência (BRANCH, 2003).

Quanto à interceptação de telefonia, tanto fixa como móvel, os órgãos de segurança chegaram a um nível de grande maturidade (LEITE, 2005). A principal ferramenta que existe hoje no País para este fim é o sistema Guardião, da empresa Dígitro Tecnologia LTDA. Ele é usado em vários órgãos, como a Policia Federal, Polícia Rodoviária Federal e algumas polícias civis (TOGNOLLI, 2007). O Guardião permite que sejam interceptados alvos simultâneos, em investigações independentes, sem que um órgão tome ciência dos investigados do outro (PALUDO; LIMA; ARAS, 2011). Além disso, há um grande número de agentes da lei treinados nesse sistema, que pode ser acessado por terminais distribuídos em todo o País. Outro ponto é que, dentro das operadoras de telefonia, já há um procedimento definido e automatizado de como direcionar as ligações dos investigados para serem capturadas e registradas por uma central de monitoramento desse sistema (AQSACOM, 2010b). Assim, o Guardião funciona com intervenções mínimas por parte das operadoras de telefonia fixa e celular.

No entanto, ter acesso às comunicações telefônicas não é o suficiente nos tempos atuais (BRANCH, 2003). Há uma grande desconfiança das pessoas em relação ao telefone, fazendo com que evitem ter conversas comprometedoras por esse meio (THOROGOOD; BROOKSON, 2007). Além disso, com o barateamento e universalização do acesso à Internet (AGÊNCIA ESTADO, 2011; CETIC.BR, 2010), grande parte das pessoas tem conexão permanente em casa ou no trabalho (BITENCOURT, 2011; TELEBRASIL, 2010).

Assim, está havendo uma migração das formas de comunicação tradicionais para a rede de dados, o que faz com que ferramentas de comunicação disponíveis na Internet sejam cada vez mais utilizadas (MARCHETTI, 2008). Algumas delas são: serviços de correio eletrônico, comunicadores instantâneos, mensagens em redes sociais e *blogs* (CETIC.BR, 2010; PINGDOM, 2011). Uma pesquisa feita em agosto de 2011 constatou que 42,4% da população brasileira tinha acesso à Internet em casa ou no trabalho. Desses, 60,1% acessavam a grande rede diariamente, 64,5% tinham perfil na rede social Orkut e 37,4% no Facebook (CNT; SENSUS, 2011).

Ao longo desse trabalho, será utilizada a sigla OSPII (órgão de segurança pública, investigação e inteligência) para denominar de maneira geral as forças policiais, agências de inteligência, o Ministério Público (quando exercendo seu poder de investigação) e outras entidades do Estado que possam exercer legalmente tais funções. A sigla será utilizada também como tradução do termo em inglês *law enforcement agency* (LEA).

1.1. DEFINIÇÃO DO PROBLEMA

Há um grande reconhecimento da importância do acesso às informações trafegadas por meio da grande rede (POLCAK et al., 2011). Entretanto, os OSPIIs não detêm o mesmo domínio da tecnologia para interceptar os dados provenientes de tráfego de Internet que possuem para interceptar chamadas telefônicas (UTIMACO, 2009). Além disso, no âmbito dos OSPIIs, há uma grande carência de conhecimento, ferramentas e métodos que garantam a agilidade da execução da interceptação, a integridade dos dados capturados e a facilidade de operação por parte dos agentes da lei (MARCHETTI, 2008; BROADWAY; TURNBULL; SLAY, 2008). As principais dificuldades enfrentadas são (PERON; DEUS; SOUSA JUNIOR, 2011):

- Inexistência de padronização no relacionamento com os provedores de acesso à Internet;
- Frequente necessidade de adaptação dos mecanismos de interceptação em razão de mudanças nos equipamentos ou nas configurações dos provedores;
- Heterogeneidade de formatos de dados utilizados pelos provedores.

Esse cenário faz com que sejam utilizadas para interceptação soluções improvisadas e de difícil implantação, causando retrabalho, ineficiência e redução da capacidade de capturas simultâneas.

Além disso, por falta de uma cadeia de custódia confiável e de garantias de autenticidade e integridade do tráfego interceptado (MONTENEGRO; BUENO; NUSDEO, 2007), frequentemente ocorre anulação e desconsideração dessas informações como prova no processo criminal pelo Judiciário e Ministério Público, frustrando o trabalho de investigação dos órgãos policiais e promovendo a impunidade (RONCAGLIA, 2008).

Internacionalmente, há países que exigem a adoção de requisitos e padrões técnicos na forma que a interceptação telemática deve ser realizada pelos provedores de serviços de telecomunicação e OSPIIs. Na Europa, são majoritariamente seguidos os padrões definidos pelo *European Telecommunications Standards Institute* (ETSI), havendo regulamentações nacionais específicas em países como Alemanha, Holanda e Reino Unido. Por sua vez, nos Estados Unidos segue-se o padrão ANSI J-STD-025-B (ANSI, 2006), baseado no *Communications Assistance for Law Enforcement Act* (CALEA) (EUA, 1994).

Em nosso País, a Constituição Federal (BRASIL, 1988), a Lei nº 9.296 de 24 de julho de 1996 (BRASIL, 1996) e a Lei nº 9.472 de 16 de julho de 1997 (BRASIL, 1997) tratam da interceptação telemática. Além disso, o tema ainda é tratado em normas e resoluções da Agência Nacional de Telecomunicações (ANATEL), pelo Poder Judiciário e Ministério Público. No entanto, até a conclusão deste trabalho, não há no País regulamentação da forma em que os dados interceptados devem ser disponibilizados pelos provedores de serviço de telecomunicação.

1.2. OBJETIVO DA DISSERTAÇÃO

O objetivo deste trabalho é desenvolver um modelo para transmissão de dados interceptados na Internet brasileira de provedores de serviços de telecomunicação para OSPIIs, baseado nas peculiaridades técnicas e legais do País e nas experiências e normativos de outros países.

Além disso, pretende-se demonstrar a adequação do modelo por meio da criação de um protótipo, instalado e em funcionamento na Polícia Federal para comunicação com provedores de três tecnologias de acesso à Internet.

1.3. HIPÓTESE DE PESQUISA

Para garantir integridade, confidencialidade, disponibilidade e autenticidade dos conteúdos ligados à interceptação telemática, estar consonante com a legislação vigente e possibilitar o uso dos dados interceptados como prova no processo penal, deve-se propor um modelo para transmissão de dados interceptados na Internet. Ele deve ser baseado nas peculiaridades técnicas e legais do Brasil e definir a forma com que os provedores de telecomunicação devam se relacionar com os OSPIIs.

Há uma grande heterogeneidade de métodos e formatos que os dados interceptados são fornecidos pelos provedores de Internet aos OSPIIs. Além disso, com frequência é necessário adaptar mecanismos de interceptação, de acordo com a aquisição de novos equipamentos pelos provedores ou mudanças em suas configurações. Ademais, os padrões existentes internacionalmente para transmissão de dados interceptados não atendem a requisitos legais e técnicos brasileiros.

Por meio da adoção de um modelo, será possível definir um padrão de interação entre essas entidades, o que possibilitará o aperfeiçoamento das soluções para interceptação, gerará ganhos em eficiência, segurança, escala, além de permitir a introdução de outras características desejáveis.

1.4. MÉTODO

Para a realização desse trabalho, primeiramente foi feita uma pesquisa da literatura sobre a interceptação de dados telemáticos. Em especial, foram estudados os artigos publicados em periódicos científicos e conferências, padrões de diferentes entidades e grupos da indústria, além de especificações técnicas sobre o tema.

Em seguida, foram pesquisadas as leis e normativos sobre a interceptação de dados telemáticos em nosso País. Em decorrência dessa pesquisa, foi definido o arcabouço legal sobre o qual a solução deveria ser baseada.

Posteriormente, foram avaliadas as soluções adotadas internacionalmente, para que fossem aplicadas diretamente ou servissem de referência para a criação de um novo modelo para o propósito almejado.

O próximo passo tomado foi a criação de um modelo de entrega de dados de comunicações interceptadas que estivesse de acordo com a legislação e normas vigentes, que levasse em consideração as melhores práticas adotadas em outros países e que fosse compatível com a estrutura tecnológica das entidades que proveem o acesso à Internet no Brasil.

Como resultado, com base nesse modelo, foi construído um protótipo para enviar dados interceptados que utilizasse mecanismos específicos compatíveis com três das tecnologias mais utilizadas por provedores: ADSL, cabo e 3G.

Finalmente, o protótipo baseado no mecanismo proposto foi aplicado em um ambiente de testes, seus resultados foram analisados e discutidos a fim de validar a proposta.

1.5. ESTRUTURA DA DISSERTAÇÃO

Esta dissertação foi dividida em sete capítulos. Este capítulo contém uma introdução do trabalho. Nele, é apresentada a importância do acesso às comunicações, o cenário atual de interceptação telemática por órgãos de segurança pública, o problema a ser resolvido e os objetivos do trabalho.

O capítulo 2 apresenta o contexto legal e normativo da interceptação de dados telemáticos no Brasil. O terceiro capítulo descreve o panorama da interceptação de dados em outros países, com suas características legais, normativas, padrões e especificações técnicas.

Por sua vez, o capítulo 4 apresenta em linhas gerais a estrutura e características técnicas das principais tecnologias para provimento de acesso à Internet no Brasil, citando alguns exemplos reais de empresas que prestam esse serviço.

O quinto capítulo apresenta limitações de modelos existentes, introduz o modelo de interceptação de dados proposto, indicando requisitos e premissas utilizadas para seu desenvolvimento, suas características gerais e o escopo de sua aplicação.

No capítulo 6, é apresentado o protótipo que foi criado para aplicar o modelo proposto. Ele foi avaliado em três cenários distintos: provedores por linha telefônica (ADSL), por rede de TV a cabo e via rede celular 3G. O capítulo ainda apresenta e discute os resultados obtidos com a utilização do protótipo.

Finalmente, o capítulo 7 contém conclusões do trabalho, apresentando uma síntese dos resultados obtidos por meio do teste do modelo proposto e descrevendo sua relevância. São discutidas as principais contribuições do trabalho, as principais dificuldades encontradas para seu desenvolvimento e são propostos trabalhos futuros, com o objetivo de expandir e aperfeiçoar a pesquisa desenvolvida.

2. ASPECTOS LEGAIS E NORMATIVOS

No Brasil, é garantido aos cidadãos o direito ao sigilo das telecomunicações. Nesse sentido, existem diversos documentos legais que tratam desse sigilo e de seu eventual afastamento, desde a Constituição Federal, passando por leis, normas e resoluções da Agência Nacional de Telecomunicações (ANATEL), Poder Judiciário e Ministério Público (MP).

2.1. CONSTITUIÇÃO FEDERAL

Primeiramente, a Constituição da República Federativa do Brasil de 1988, que lista os direitos e garantias fundamentais dos cidadãos, em seu artigo 5º, inciso XII, define que é inviolável o sigilo das correspondências e das comunicações telegráficas, de dados e das comunicações telefônicas (BRASIL, 1988).

A Constituição permite o afastamento do sigilo das comunicações somente para fins de investigação criminal ou instrução processual penal por meio de ordem judicial (BANDEIRA, 2002).

2.2. LEI DAS INTERCEPTAÇÕES TELEFÔNICAS E DE DADOS

A Lei nº 9.296, de 24 de julho de 1996, regulamenta o previsto na Constituição (BRASIL, 1996). Essa lei é conhecida como "Lei das Interceptações Telefônicas" e trata do procedimento de interceptação de comunicações telefônicas e de sistemas de informática e telemática.

O parágrafo único do artigo 1º afirma que tudo o que está indicado no referido diploma legal referente à interceptação de comunicações telefônicas também se aplica à interceptação do fluxo de comunicações em sistemas de informática e telemática.

Essa lei indica que a interceptação das telecomunicações é um meio de prova excepcional, que deve ser utilizado somente quando não existem outros recursos probatórios e, ainda assim, mediante o cumprimento de uma série de requisitos legais. Assim, é necessário que haja indícios do cometimento de um crime que tenha pena de detenção e que a interceptação seja direcionada a algum suspeito específico, mediante um inquérito policial já instaurado ou uma investigação em curso. Desta forma, não se pode fazer uso de mecanismos que

monitorem constantemente as redes de comunicação em busca de indícios de práticas delituosas em geral.

No terceiro artigo, foi estabelecido que o pedido de interceptação pode ser feito pela autoridade policial ou representante do Ministério Público. No pedido, devem ser indicados os meios a serem empregados para a execução da interceptação. Além disso, o juiz pode determiná-la de ofício.

No Art. 5°, é definido que a decisão do juiz pela interceptação deverá indicar "a forma de execução da diligência". Assim, fica a cargo do juiz a decisão de aceitar ou redefinir os meios a serem empregados para a execução da interceptação, como recursos tecnológicos e humanos, com a indicação dos papéis a serem desempenhados pelos agentes da lei e empresas de telecomunicação envolvidas. Outro ponto definido nesse mesmo artigo é que a interceptação poderá ser realizada por um período de até 15 dias, que pode ser renovado por outros períodos de até 15 dias, mediante novas autorizações judiciais.

No artigo seguinte, fica estabelecido que os procedimentos de interceptação devem ser conduzidos pelas forças policiais. O MP será informado do procedimento e poderá acompanhar a sua realização. Outra exigência do mesmo artigo é que a transcrição do conteúdo da comunicação deve ser realizada quando possível. Além disso, o resultado da interceptação deverá ser encaminhado ao juiz para sua ciência, com um resumo das ações realizadas.

Para realizar os procedimentos de interceptação, a autoridade policial poderá requisitar às concessionárias de serviços de telecomunicação serviços e profissionais especializados, conforme o Art. 7°. Ademais, é obrigação da concessionária atender a essa requisição, podendo ser responsabilizada criminalmente pelo seu não cumprimento.

Outra questão abordada na Lei refere-se à inutilização das gravações que não forem relevantes para a apuração dos fatos. O Art. 9° define que esse procedimento poderá ser determinado por decisão judicial, mediante requerimento do MP ou da parte interessada, deverá ser assistido pelo MP e poderá ocorrer durante a fase do inquérito, da instrução penal ou até após esta. Para tanto, pode ser realizada a incineração das mídias que armazenam o conteúdo gravado.

2.3. LEI GERAL DAS TELECOMUNICAÇÕES

Outra lei que dispõe sobre a interceptação das telecomunicações é a de nº 9.472, de 16 de julho de 1997, mais conhecida como Lei Geral das Telecomunicações (LGT) (BRASIL, 1997). Ela trata da organização dos serviços de telecomunicações e define papéis e o funcionamento do órgão regulador, a Agência Nacional de Telecomunicações (ANATEL). A Agência tem a missão de organizar a exploração dos serviços de telecomunicações.

Esse diploma legal contém algumas definições importantes, que vão determinar o estabelecimento de responsabilidades, obrigações e atribuições dos entes envolvidos em uma telecomunicação.

Em seu Art. 60, § 1º, é definido o conceito de telecomunicação como sendo a transmissão, emissão ou recepção de símbolos, caracteres, sinais ou informações de qualquer natureza por um meio ou processo eletromagnético. No *caput* do mesmo artigo, os serviços de telecomunicação são definidos como um conjunto de atividades que viabilizam a oferta de telecomunicação.

Outra definição que estabelece serviços relacionados ao provimento de Internet é o de Serviços de Valor Adicionado (SVA), descrito a seguir.

2.3.1. Serviço de Valor Adicionado (SVA)

No Art. 61 da LGT, os serviços de valor adicionado são definidos como atividades que agregam novas utilidades relacionadas ao acesso, movimentação, apresentação, armazenamento ou recuperação de informações a um serviço de telecomunicação. Esses serviços em si não são considerados serviços de telecomunicação, conforme está escrito explicitamente no § 1º desse mesmo artigo. Os provedores de SVA são classificados como usuários do serviço de telecomunicações que lhes dá suporte, possuindo deveres e direitos inerentes a essa condição.

Alguns exemplos de SVAs seriam o UOL, Terra, Google, Yahoo, Youtube, Facebook, CorreioWeb, iG, Locaweb e Dropbox, além de outros provedores de conteúdo, webmail, serviços de conexão à Internet e armazenamento remoto de arquivos.

No § 2º do Art. 61, é indicado que cabe à ANATEL regular as condições e o relacionamento entre os interessados no uso das redes de serviços de telecomunicações para prestação de SVA e as prestadoras de serviço de telecomunicações.

2.4. RESOLUÇÃO Nº 59, DE 09 DE SETEMBRO DE 2008 DO CNJ

O Conselho Nacional de Justiça (CNJ) publicou a Resolução nº 59, de 09 de setembro de 2008 (CNJ, 2008), visando disciplinar e uniformizar os procedimentos do Poder Judiciário relativos à interceptação de comunicações telefônicas e de sistemas de informática e telemática.

Os artigos iniciais da resolução contêm medidas que objetivam evitar o vazamento de informações dentro dos órgãos judiciários (CNJ, 2008). Por exemplo, os pedidos de interceptação devem vir em envelopes lacrados, cuja face não deve conter a informação de que se trata de um pedido de interceptação de comunicações ou ainda o nome do investigado. Essas informações devem estar disponíveis somente ao magistrado que for efetivamente decidir sobre a concessão da quebra de sigilo.

O Art. 10 define que, quando deferido o pedido, o juiz deve incluir em sua decisão: o prazo da interceptação; o nome da autoridade que requereu o procedimento; a indicação do titular do número, linha ou terminal interceptado; o nome das autoridades policiais responsáveis pela investigação e que terão acesso às informações; a indicação de que é vedada a interceptação de outros números, linhas e terminais não listados na decisão.

De acordo com o Art. 11, devem ser expedidos ofícios às operadoras para que deem cumprimento à decisão judicial de suspensão de sigilo das telecomunicações. Esses ofícios devem conter as informações estritamente necessárias para que as operadoras possam cumprir a decisão judicial, como o número do procedimento investigativo, tipo de ação, identificação dos terminais que tiveram a interceptação ou quebra de dados deferida, além da expressa vedação de interceptação de outros terminais não discriminados na decisão.

As obrigações das operadoras de serviços de comunicação estão definidas no Art. 12. Essas devem informar ao Judiciário da data da efetivação da interceptação, de forma que seja controlado o prazo das medidas. Além disso, devem ser informados semestralmente à Corregedoria Nacional de Justiça os nomes dos funcionários que têm conhecimento sobre as

medidas de interceptações deferidas e os dos que as operacionalizam (conforme atualização contida na Resolução nº 84 de 6 de julho de 2009 do CNJ).

Para os pedidos de prorrogação de prazo das interceptações, o Art. 14 estabelece que a autoridade competente deve apresentar em mídias óticas o inteiro teor das comunicações interceptadas, as transcrições das conversas relevantes e o relatório das investigações com seus resultados. Ademais, sempre que possível, os dados contidos nessas mídias devem ser cifrados utilizando-se chaves e cifras definidas pelo magistrado condutor do processo criminal.

Finalmente, o Art. 20 estabelece que o CNJ em conjunto com a ANATEL desenvolverá estudos para estabelecer rotinas e procedimentos totalmente informatizados, que assegurem o sigilo e a segurança dos sistemas tanto no âmbito do Poder Judiciário quanto nas operadoras. Até a conclusão desta dissertação, não foram encontrados registros do desenvolvimento de estudos acerca do tema por tais órgãos.

2.5. RESOLUÇÃO Nº 20, DE 28 DE MAIO DE 2007 DO CNMP

O Conselho Nacional do Ministério Público (CNMP) publicou a Resolução nº 20, de 28 de maio de 2007 (CNMP, 2007), visando disciplinar o controle externo da atividade policial no âmbito do Ministério Público (MP).

O controle externo da atividade policial realizado pelo MP já estava determinado pela Constituição Federal, na Lei Complementar nº 75, de 20 de maio de 1993, e na Lei nº 8.625, de 12 de fevereiro de 1993 (MISSIUNAS, 2009).

Nos artigos 4º e 5º da Resolução nº 20 (CNMP, 2007), são definidas as principais incumbências do MP para o controle da atividade policial, destacando-se:

- Ter acesso a quaisquer documentos, sejam eles informatizados ou não, relativos à atividade-fim policial, em especial aos registros de autorizações judiciais para quebra de sigilo de comunicações;
- Fiscalizar o cumprimento de medidas de quebra de sigilo de comunicações, na forma da lei, até mesmo por meio do órgão responsável pela execução da medida.

Desta forma, infere-se que o MP pode ter acesso às informações quanto às ordens judiciais para quebra de sigilo telemático que foram determinadas e ainda fiscalizar o cumprimento de

diligências dessa natureza junto aos órgãos policiais e provedores de serviço de telecomunicação.

2.6. NORMAS E RESOLUÇÕES DA ANATEL

A ANATEL publicou alguns documentos oficiais que disciplinam questões relativas ao provimento de serviços de Internet. Eles estabelecem os serviços que podem ser oferecidos, critérios para outorga de concessões, obrigações para os prestadores de serviços, dentre outras definições.

2.6.1. Norma 004/95

A Norma 004/95 regula a utilização de meios da rede pública de telecomunicações para provimento e utilização de Serviços de Conexão a Internet (SCI) (ANATEL, 1995). Ela contém diversas definições, dentre elas a de Serviço de Valor Adicionado (SVA), que é semelhante à da LGT. Além disso, ela define Serviço de Conexão à Internet como um SVA que possibilita o acesso à Internet a usuários e Provedores de Serviços de Informações (PSI). Os PSI são definidos como entidades que possuem informação de interesse. Por sua vez, os Provedores de Serviço de Conexão à Internet (PSCI) são definidos como as organizações que prestam os serviços de conexão à Internet, ou seja, são os provedores de acesso à Internet. Alguns exemplos de PSCI são POP, Terra, UOL, BrTurbo e iG.

A norma também estabelece que para prover e usar os SCIs, a utilização de meios da rede pública de telecomunicações se faz por meio de serviços de telecomunicação oferecidos pelas Entidades Exploradoras de Serviços Públicos de Telecomunicações (EESPT). Ademais, o PSCI pode utilizar quaisquer dos Serviços de Telecomunicações prestados pelas EESPT para se conectar à Internet. Finalmente, fica garantido que os meios da rede pública de telecomunicações podem ser utilizados para conectar SCIs à Internet, no exterior, e interconectar SCIs de provedores diversos.

Os PSCIs possuem razoável autonomia em relação às EESPTs, em decorrência de a norma garantir que os últimos não podem definir características técnicas e funcionais, itens de hardware e software a serem utilizados pelos PSCIs ou ainda os pontos de conexão entre os PSCIs. Tampouco podem estabelecer as facilidades e as características do serviço de conexão ofertado.

2.6.2. Resolução nº 73, de 25 de Novembro de 1998

A Resolução nº 73, de 25 de novembro de 1998, aprovou o Regulamento dos Serviços de Telecomunicações. No inciso V do Art. 9º do anexo da resolução (ANATEL, 1998), são assegurados aos usuários dos serviços de telecomunicações a inviolabilidade e o segredo de sua comunicação, a não ser quando ocorrer alguma das hipóteses ou condições previstas em leis e na Constituição.

No Art. 26, é indicado que a prestadora de serviço de telecomunicações deverá zelar pelo sigilo inerente aos serviços de telecomunicações e pela confidencialidade dos dados e informações trafegadas pelos seus usuários. Para tanto, a prestadora deve empregar todos os meios e tecnologias necessários.

O parágrafo único do mesmo artigo ainda estabelece que a prestadora deve disponibilizar todos os recursos tecnológicos necessários a suspender o sigilo de telecomunicações, quando determinado por autoridade judiciária ou outra legalmente investida desses poderes. Além disso, a prestadora deve manter um controle permanente de todos os casos, deverá acompanhar a efetivação das determinações judiciais e zelar para que elas sejam cumpridas estritamente dentro dos limites autorizados. Dessa forma, é também obrigação da operadora garantir que somente o tráfego dos assinantes autorizados seja interceptado e que o prazo da quebra do sigilo não ultrapasse o determinado na ordem judicial.

No Art. 46 da referida resolução, novamente é indicado como dever da prestadora que seu serviço seja prestado com segurança. No parágrafo 3º, a segurança é definida como o sigilo dos dados referentes ao uso do serviço pelos usuários, assim como a preservação da confidencialidade das informações transmitidas para a prestação do serviço.

2.6.3. Resolução nº 272, de 9 de Agosto de 2001

A Resolução nº 272, de 9 de agosto de 2001, aprovou o Regulamento do Serviço de Comunicação Multimídia (SCM). Além disso, essa resolução (ANATEL, 2001) determinou que, a partir de sua publicação, não deveriam mais ser expedidas autorizações de exploração dos Serviços Limitados Especializados (SLE) de redes e circuitos. As autorizações para prestação desses serviços poderiam ser adaptadas ao regime regulatório do SCM, mediante o atendimento das condições estabelecidas nessa resolução, conforme o Art. 68. O SCM é considerado o substituto e o agregador dos SLE e SRTT (Serviços de Rede de Transporte de Telecomunicações), e foi criado para atender a convergência tecnológica (ANATEL, 2008a),

unificando os serviços e dando operatividade à Lei Geral das Telecomunicações (LGT). Desta forma, pelo fato de esses serviços estarem em vias de extinção, eles não serão abordados nessa dissertação.

2.6.3.1. Serviço de Comunicação Multimídia (SCM)

O Serviço de Comunicação Multimídia é definido no Art. 3º do anexo da referida resolução como um serviço de telecomunicações fixo, de interesse coletivo, no regime privado, que permite o oferecimento de capacidade de transmissão, emissão e recepção de sinais de dados, áudio, vídeo, imagens, textos ou outras informações de qualquer natureza, não importando o meio utilizado, para prestar o serviço a assinantes de uma determinada área.

No parágrafo único do mesmo artigo, ainda é definido que o SCM se distingue do Serviço Telefônico Fixo Comutado (STFC) e dos serviços de comunicação eletrônica de massa, como por exemplo, o Serviço de TV a Cabo, o Serviço de Radiodifusão, o Serviço de Distribuição de Sinais de Televisão e de Áudio por Assinatura via Satélite (DTH) e o Serviço de Distribuição de Sinais Multiponto Multicanal (MMDS).

Algumas das principais operadoras do SCM no Brasil são a Oi, Net, Telefônica, GVT, Embratel, CTBC, Sercomtel, Intelig, Telmex, Global Crossing, Eletronet, Eletropaulo e Light (ANATEL, 2008b; TELECO, 2011b).

No inciso VIII do Art. 4º, os SVAs são definidos de maneira semelhante ao já estabelecido na LGT e na Norma 004/95 da Anatel. Para o provimento de SVA, é assegurado o uso das redes de suporte do SCM, de acordo com o Art. 7º. Ainda é definido que a ANATEL é quem estabelece as regras de relacionamento entre os provedores de SVA e as prestadoras do SCM.

O Art. 57 da Resolução nº 272 contém um texto semelhante ao do Art. 26 da Resolução nº 73 da ANATEL, de 25 de novembro de 1998, referente aos deveres das prestadoras quanto ao sigilo dos Serviços de Telecomunicações. No Art. 57, é definido que a prestadora do SCM deverá cuidar do sigilo inerente aos serviços de telecomunicações e da confidencialidade dos dados e informações dos seus assinantes. Para assegurar esse direito de seus assinantes, a prestadora deverá empregar todos os meios e tecnologias necessárias.

No parágrafo único do mesmo artigo, é estabelecido que, mediante determinação judicial para quebra do sigilo de telecomunicações dos seus assinantes, a prestadora deve disponibilizar os

dados de telecomunicações requeridos à autoridade judiciária ou outra legalmente investida desses poderes que determinou tal diligência.

No Art. 59 da referida resolução, é indicado como direito do assinante do SCM a inviolabilidade e segredo de suas comunicações, ressalvadas as hipóteses e condições legais e condicionais da suspensão do sigilo das telecomunicações.

2.7. DIFERENÇAS ENTRE SCM E SCI

O Serviço de Comunicação Multimídia (SCM) é um exemplo de serviço de telecomunicações e é prestado normalmente por empresas que detêm infraestrutura de telecomunicação, como as empresas de telefonia. Serviço de telecomunicações é definido como o conjunto de atividades e meios que possibilitam a emissão, transmissão ou recepção de informações de qualquer natureza, conforme o Art. 60 da LGT (BRASIL, 1997). Desta forma, ele é um meio que torna viável a capacidade de emissão, transmissão ou recepção, por diversos processos, dos variados tipos de informação, não importando o conteúdo transportado.

Por sua vez, o Serviço de Conexão à Internet (SCI) é um subtipo de Serviço de Valor Adicionado (SVA) que viabiliza o acesso à Internet a usuários e provedores de serviços de informações, conforme a Norma 004/95 (ANATEL, 1995).

Nesse mesmo contexto, um Provedor de Serviço de Conexão à Internet (PSCI), também conhecido popularmente como "provedor de acesso à Internet", é um prestador de Serviço de Valor Adicionado. Para prestar o SCI, o provedor deve utilizar a rede de telecomunicações de uma empresa que detenha concessão de serviço de telecomunicações (VALENTE, 2007). Assim, o PSCI é considerado um usuário do serviço de telecomunicações o qual lhe dá suporte e um intermediário entre o assinante e um concessionário do serviço de telecomunicações, conforme mostrado na Figura 2.1. O PSCI é constituído dos seguintes itens: equipamentos necessários para realizar o roteamento, encaminhamento e armazenamento de informações; software e hardware necessários para implementar os protocolos de Internet, rotinas para autenticação e administração de usuários, conexões, correio eletrônico, acessos remotos, armazenamento de arquivos, controle de segurança, dentre outros.

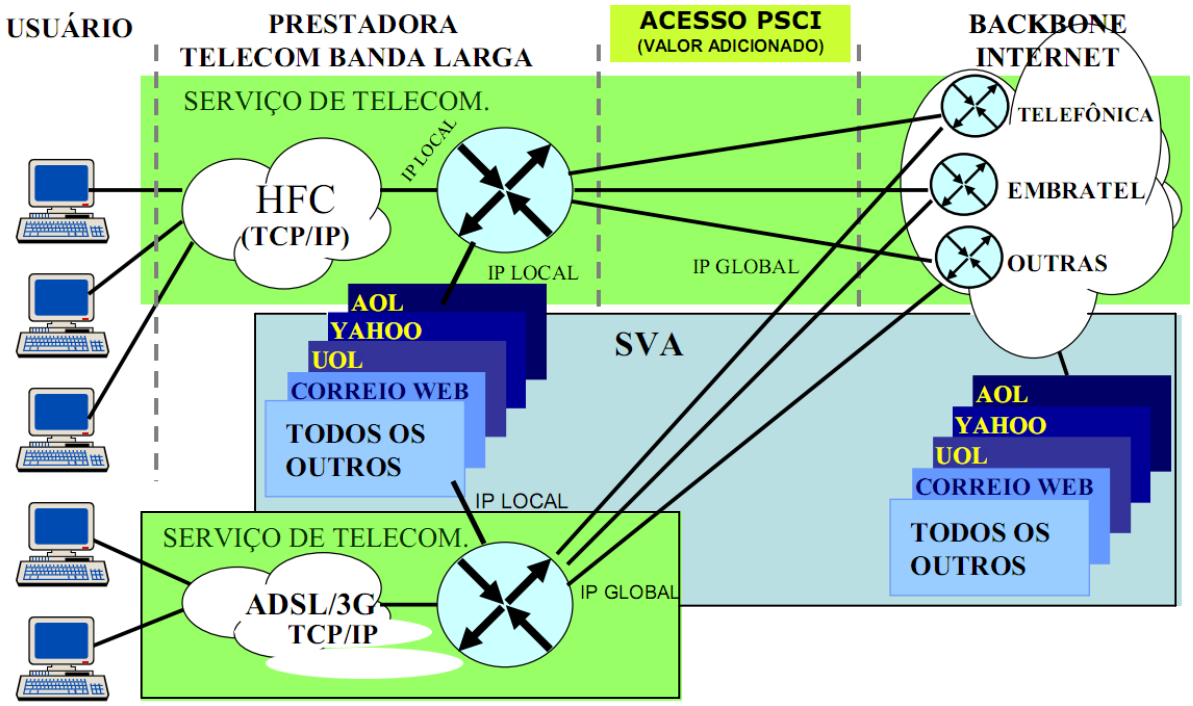


Figura 2.1 - Relação entre o Serviço de Telecom e PSCI (VALENTE, 2007).

Por outro lado, o SVA é a atividade que acrescenta a um serviço de telecomunicações novas utilidades, tais como: autenticação, acesso, armazenamento, movimentação, recuperação e apresentação de informações. O SVA dá suporte a um serviço de telecomunicações, não representando em si um serviço de telecomunicações, mas constituindo um usuário desse serviço, conforme descrito no Art. 61 da LGT.

Para um usuário (assinante) estabelecer uma conexão à Internet, algumas atividades necessitam ser realizadas. No início da conexão, o PSCI é autenticado pelo servidor de autenticação da prestadora de telecomunicações, com o objetivo de verificar se o PSCI está credenciado àquela prestadora. Posteriormente, o usuário é autenticado pelo servidor de autenticação do PSCI. Em seguida, o sistema da prestadora de telecomunicações libera o fluxo de dados do usuário para a Internet por meio do enlace contratado pelo PSCI, conectando assim o usuário à Internet.

Tendo sido realizada esta conexão ao *backbone* da Internet, os pacotes de dados podem trafegar entre o sistema do usuário e os sistemas de informações da rede mundial de computadores, conforme mostrado na Figura 2.2 (VALENTE, 2007).

Com isso, o PSCI viabiliza sua prestação de serviço mediante a utilização da infraestrutura da prestadora de telecomunicações e disponibiliza seus sistemas e equipamentos para utilizar os serviços disponíveis na grande rede.

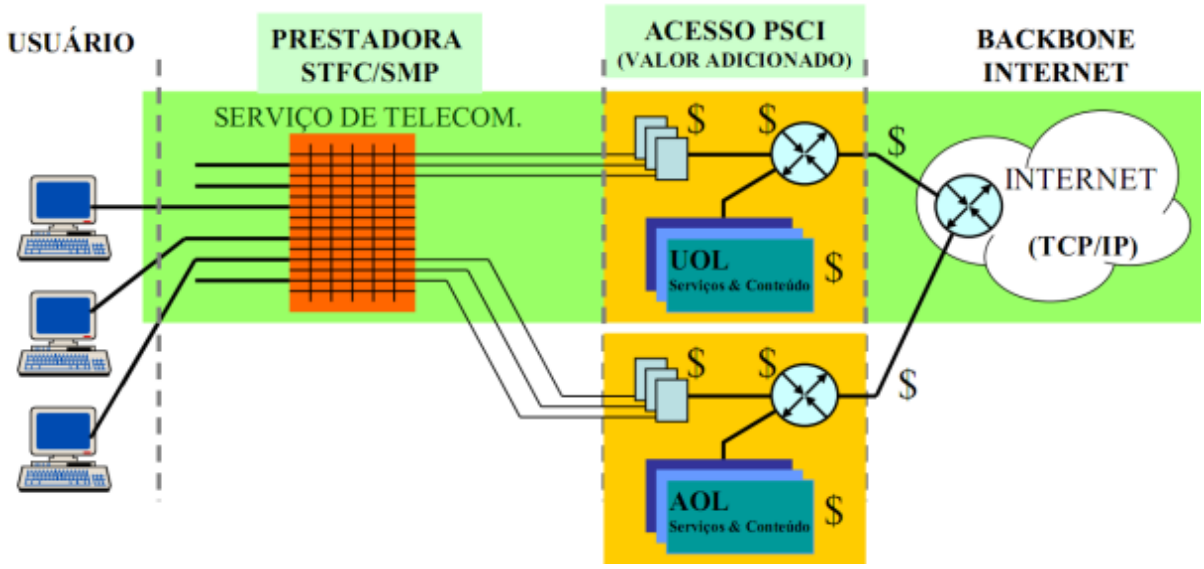


Figura 2.2 - Modelo de negócios de acesso à Internet (VALENTE, 2007).

2.8. SÍNTESE DO CAPÍTULO

Neste capítulo, foi apresentado o conjunto de leis, normas e resoluções que abordam questões relativas à interceptação telemática no Brasil. Além disso, foram apontados aspectos regulatórios em que se situam os serviços relacionados ao provimento de acesso à Internet, com a indicação de papéis desempenhados e obrigações das partes envolvidas. No capítulo a seguir, será apresentado o contexto da interceptação de dados em outros países.

3. A INTERCEPTAÇÃO TELEMÁTICA EM OUTROS PAÍSES

A elevada quantidade de tecnologias para comunicação representa um desafio para os órgãos de segurança pública e agências de segurança nacional ao redor do mundo (UTIMACO, 2009). Soma-se a isso a sofisticação das organizações criminosas em explorar canais de comunicação emergentes. Desta forma, governos de alguns países e organizações internacionais criaram regulamentos para permitir e facilitar a interceptação autorizada de dados trafegados.

Embora leis e normas que controlem a interceptação de canais tradicionais, como telefones fixos e celulares, já existam há alguns anos, muitos destes documentos legais foram ampliados para incluir comunicações via Internet (UTIMACO, 2009). São incluídos nesses documentos obrigações para empresas de telecomunicações, provedores de acesso à Internet, operadores de redes e provedores de serviço que oferecem ou mantêm infraestruturas por meio do qual a comunicação ocorre.

A seguir, são apresentados os panoramas de alguns países.

3.1. ESTADOS UNIDOS

Nos Estados Unidos, existem diferentes leis que regem a interceptação das comunicações. Em geral, a interceptação das telecomunicações de terceiros, seja telefônica ou de dados é ilegal, tanto quando feita por indivíduos quanto pelo governo, com pequenas exceções para investigação criminal. Mesmo quando permitidas, as interceptações ocorrem sob a supervisão do Poder Judiciário (SHERR et al., 2009).

As normas jurídicas referentes a assuntos domésticos estadunidenses, como no contexto de investigações criminais, são mais restritivas, enquanto que as que são aplicadas a comunicações internacionais são mais permissivas (SCHWARTZ, 2009a).

O dispositivo legal norte-americano mais antigo sobre o sigilo das comunicações é o *Wiretap Act*, que data de 1968. Ele protege a privacidade das comunicações, trata da interceptação de comunicações em andamento e define os requisitos que devem ser cumpridos para que esse tipo de procedimento seja autorizado.

Muitas formas de comunicação modernas não são abrangidas por essa lei. Os atributos de uma telecomunicação, como origem, destino e duração, são geralmente regulados pelo *Pen Register Act.* Por outro lado, o acesso à informação que esteja armazenada em um servidor é regido pelo *Stored Communications Act*.

O *Pen Register Act* é a segunda lei referente a assuntos domésticos e entrou em vigor em 1986. Ele regulou o acesso à listagem de chamadas discadas e recebidas por um determinado número de telefone. Essa lei foi emendada pelo *Patriot Act* de 2001, aprovado após o ocorrido em 11 de setembro de 2001 (AQSACOM, 2006). Foi então regulado o acesso à informação de discagem, roteamento, endereçamento e sinalização, abordando endereços IP e informações de endereços de correio eletrônico.

O *Stored Communications Act* trata das comunicações assíncronas, tais como mensagens de correio eletrônico, e do acesso a informações armazenadas em servidores. Tipicamente, uma mensagem de correio eletrônico é transmitida pelo remetente e depois armazenada por algum servidor. Assim, as forças de segurança normalmente preferem se valer dessa lei para acessar correios eletrônicos, já que os requisitos para uma quebra de sigilo por meio do *Stored Communications Act* são menos rígidos que os do *Wiretap Act* (SCHWARTZ, 2009a).

A principal norma jurídica destinada à coleta de informações dentro do território estadunidense para ações de inteligência referentes ao exterior é o *Foreign Intelligence Surveillance Act* (FISA), promulgado em 1978. O FISA está relacionado à aquisição de informações de inteligência referentes a um país estrangeiro, organizações terroristas, agentes estrangeiros ou ainda terroristas em território ianque.

Nesse mesmo sentido, existem outras leis que autorizam o FBI a obter informações sobre terceiros por meio de *National Security Letters* (NSL), não precisando de autorização judicial para isso (SCHWARTZ, 2009b). Uma NSL é uma diretiva escrita pelo FBI em assuntos relativos à segurança nacional norte-americana.

3.1.1. *Communications Assistance for Law Enforcement Act*

Em 1994, foi aprovada a lei chamada de *Communications Assistance for Law Enforcement Act* (CALEA). Um de seus propósitos é tornar claras as obrigações dos provedores de serviço de telecomunicações e fabricantes de equipamentos em cooperar com os órgãos de segurança

pública, no que refere a interceptação de comunicações mediante ordem judicial ou outra autorização legal (EUA, 1994).

De acordo com as seções 1002 e 1005 do CALEA, provedores de serviços de telecomunicação e fabricantes de equipamentos devem projetar e modificar seus dispositivos, instalações e serviços para que contenham capacidade embutida de monitoramento. Eles devem ser capazes de interceptar o conteúdo das comunicações e seus metadados em tempo real ou em um tempo considerado razoável. Ambos devem ser encaminhados às instalações dos órgãos de segurança pública, sem prejuízo do funcionamento da comunicação em andamento. Outra provisão é que se alguma forma de criptografia for oferecida pelos provedores de telecomunicações, eles serão os responsáveis por decifrar os dados antes de entregá-los.

O CALEA permitiu uma melhoria na capacidade de os órgãos de segurança realizar monitoramento eletrônico de telecomunicações, como comunicações telefônicas, Internet e VoIP (SHERR et al., 2009).

Enquanto o CALEA define claramente as responsabilidades legais dos provedores de serviços de telecomunicações, ele não estabelece as especificações técnicas e protocolos referentes às configurações de interceptação, coleta de dados e entrega de dados. Em seu lugar, a lei estabeleceu, em sua seção 1006, que deveria ser criada uma força tarefa, composta de representantes de provedores de serviços de telecomunicações e de agências federais e estaduais de segurança pública, para desenvolver um padrão da indústria (SHERR et al., 2009). Foi essa força tarefa que criou o padrão ANSI J-STD-025, cuja versão "B" está descrita a seguir.

3.1.2. O padrão ANSI J-STD-025-B

O padrão ANSI J-STD-025-B, com título *Lawfully Authorized Electronic Surveillance*, define interfaces entre provedores de serviços de telecomunicações e agências de segurança pública para proceder ao monitoramento eletrônico de telecomunicações autorizado por lei (ANSI, 2006). O monitoramento definido pelo padrão abrange o conteúdo da conexão (pacotes de dados trafegados e voz) e identificação da conexão (origem, destino e direção).

O padrão, normalmente referido como o *J-Standard*, foi definido em conjunto entre a *Telecommunications Industry Association* (TIA) e a *Alliance for Telecommunications*

Industry Solutions (ATIS). Seu desenvolvimento, conforme estabelecido no CALEA, também teve a participação de representantes de órgãos de segurança pública, investigação e inteligência (OSPIIs). Dessa forma, ele foi desenvolvido de forma a atender a interesses, às vezes conflitantes, do FBI, da indústria de telecomunicações e de outros grupos (SHERR et al., 2009).

A maioria dos provedores de serviços de telecomunicações está em conformidade com o CALEA por meio do uso de equipamentos compatíveis com as interfaces desse padrão, que são usados para transmitir dados interceptados para centrais de monitoramento dos OSPIIs (SHERR et al., 2009).

O J-STD-025-B define um modelo de interceptação dividido em cinco diferentes funções: acesso, entrega, coleta, administração do provedor de serviço e administração do órgão de segurança. Essas funções e o relacionamento entre elas podem ser vistos na Figura 3.1.

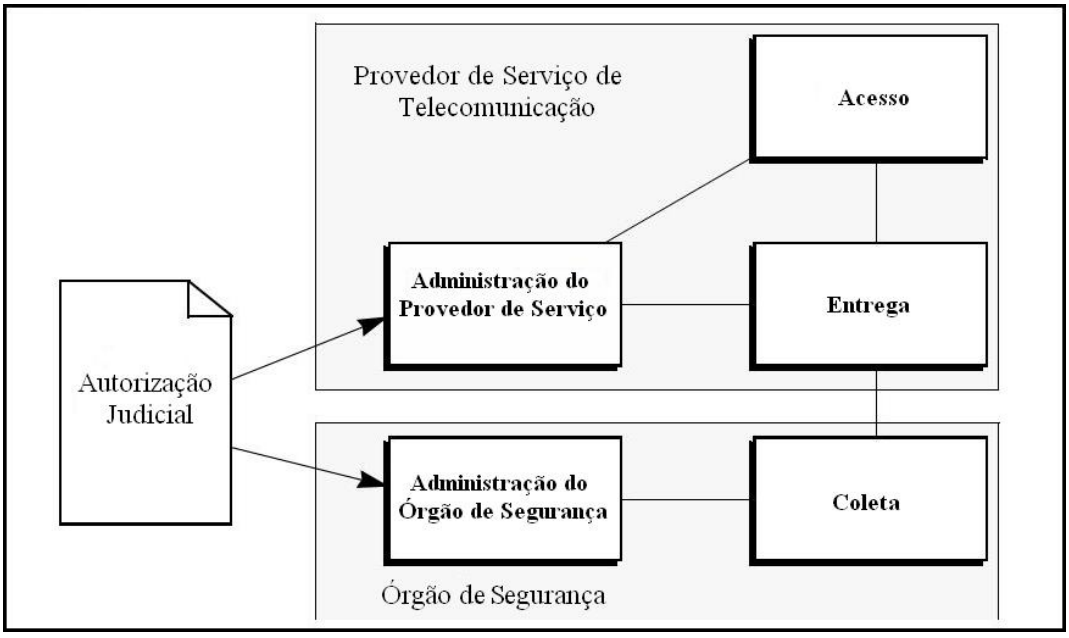


Figura 3.1 - Modelo de Monitoramento Eletrônico – adaptado de (ANSI, 2006).

A Função de Acesso, formada por um ou mais Pontos de Acesso de Interceptação (*Intercept Access Points* – IAPs), isola e provê acesso ao conteúdo da comunicação e à informação de identificação de um assinante interceptado sem que ele tome conhecimento. Os Pontos de Acesso de Interceptação podem variar de acordo com o provedor de serviço e seus equipamentos (ANSI, 2006).

A Função de Acesso deve prover os seguintes serviços (ANSI, 2006): acessar de maneira furtiva a informação de identificação de um assinante interceptado e o conteúdo de sua comunicação, a fim de disponibilizar esses dados à Função de Entrega; prevenir acesso não autorizado; manipular dados; informar as interceptações em curso.

Um ponto de acesso de interceptação de pacotes (*Packet Data Internet Access Point* – PDIAP) é o elemento que acessa os pacotes enviados ou recebidos pelo assinante quando um serviço de comunicação por pacotes é utilizado. Os pacotes devem ser enviados à Função de Coleta assim que eles forem interceptados. Isso deve ocorrer sem interpretação ou modificação, exceto quando há necessidade de reenquadramento, segmentação ou encapsulamento para transportá-lo ou ainda para remover informações cuja interceptação não tenha sido autorizada.

A Função de Entrega é responsável por entregar a comunicação interceptada a uma ou mais Funções de Coleta, sendo capaz de duplicar esses dados caso haja múltiplas investigações em curso lidando com o mesmo assinante. Com esse objetivo, deve poder receber conteúdo da comunicação e informações de conexões dos assinantes interceptados por meio de uma ou mais Funções de Acesso. Além disso, deve garantir que os dados transmitidos à Função de Coleta estejam autorizados para os devidos OSPIIs. Finalmente, a função deve prevenir o acesso não autorizado, a manipulação de dados ou a divulgação das interceptações em curso.

Para realizar a Função de Entrega, são usados dois tipos de canais distintos: Canais de Conteúdo de Chamadas (*Call Content Channels* – CCCs) e Canais de Dados de Chamadas (*Call Data Channels* – CDCs), conforme mostrado na Figura 3.2. Os primeiros conduzem o áudio ao vivo ou o fluxo de dados das linhas ativas monitoradas. Já os CDCs carregam os metadados das conexões, com informações tais como: início e fim de conexão, tempo de chamada, números discados e status da linha. As mensagens trocadas no CDC devem estar de acordo com o protocolo LAESP (*Lawfully Authorized Electronic Surveillance Protocol*), que é definido no *J-Standard*. O foco das definições contidas no padrão é a interface entre as funções de Entrega e Coleta.

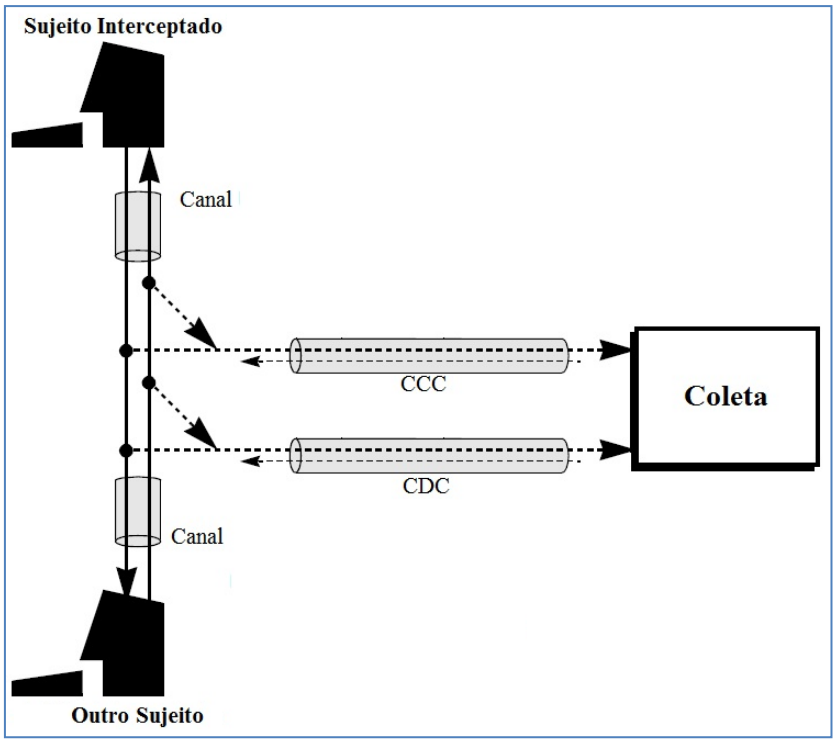


Figura 3.2 - Ponto de acesso de interceptação e canais da função de entrega – adaptado de (ANSI, 2006).

A Função de Coleta é de responsabilidade do OSPII, que se encarrega de coletar e analisar a informação de identificação de um assinante interceptado e o conteúdo de sua comunicação. Tem-se como premissa que os equipamentos de coleta do órgão de segurança mantêm informações do estado atual das associações entre os assinantes interceptados e os dados que são entregues à Função de Coleta, ou seja, sabem exatamente de que assinantes são os dados que estão coletando. Assim, os equipamentos de coleta partem do princípio que essas associações só são modificadas mediante o recebimento de uma nova mensagem LAESP indicando a mudança.

As funções de Administração dos provedores de serviço e dos OSPIIs estão fora do escopo do padrão J-STD-025-B (ANSI, 2006). A primeira é a que controla as Funções de Acesso e Entrega do provedor de serviços. Por sua vez, a Função de Administração dos órgãos de segurança é a que controla o monitoramento eletrônico por meio da Função de Coleta.

No J-STD-025-B, há menção explícita que interceptações só devem ser executadas com a devida autorização judicial ou outra previsão legal (ANSI, 2006).

3.2. CANADÁ

No Canadá, o *Criminal Code* (R.S.C., 1985, c. C-46) (CANADÁ, 1985), em seu Art. 184, estabelece que ninguém pode interceptar propositalmente uma comunicação privada, a não ser que tenha o consentimento expresso ou implícito de quem originou ou recebeu a comunicação. Outros casos permitidos são quando há autorização judicial, se a interceptação for necessária para o propósito do serviço oferecido, se for feita aleatoriamente para verificação da qualidade da transmissão ou ainda para proteger os direitos ou propriedades das pessoas relativas ao serviço, como serviços de *firewall* e filtros anti-spam.

A legislação permite também que um agente do estado intercepte uma comunicação privada se a interceptação é consentida pelo emissor ou receptor, quando se acredita que há um risco à integridade física da pessoa que consentiu. Os registros dessa comunicação devem ser destruídos imediatamente quando se verifica pela análise do tráfego interceptado que não há risco à integridade física de algum indivíduo.

Conforme o Art. 184-2, a autorização para interceptação deve ser emitida por um juiz quando existirem indícios razoáveis de que um crime foi ou está sendo cometido, quando a interceptação for consentida por alguma das partes ou quando se acreditar que informação referente ao crime poderá ser obtida por meio da interceptação.

São previstos casos excepcionais, quando a interceptação das telecomunicações é permitida sem ordem judicial. O Art. 184-4 define que um agente da lei pode proceder à interceptação se houver indícios razoáveis que a urgência da situação é tamanha que uma autorização, seguindo os trâmites normais, não poderia ser obtida em tempo hábil a fim de que permitisse evitar danos graves ao patrimônio ou a pessoas.

Não há regulamentação técnica no Canadá que contenha a descrição específica de como as interceptações telemáticas devem ser executadas no país.

3.3. CHILE

O Decreto 142 (CHILE, 2005), publicado em 2005, contém as regras sobre a interceptação e gravação de comunicações telefônicas e outras formas de telecomunicação. Assim como em outros países, é garantida a inviolabilidade de todas as comunicações privadas, permitindo sua interceptação somente nos casos e formas definidas em lei.

No Art. 2º do Decreto, é definido que para efetivar as interceptações e gravações determinadas, os prestadores de serviços de telecomunicação deverão disponibilizar aos órgãos policiais os meios necessários para realizar as diligências, a fim de que se alcance todos os serviços que o assinante investigado acesse e cuja interceptação tiver sido autorizada. Os prestadores têm a obrigação de não permitir a interceptação do tráfego de assinantes não listados na autorização judicial.

Outra definição, contida no Art. 5º, é de que os prestadores não poderão manter ou incorporar em suas redes equipamentos ou tecnologias que dificultem ou impeçam a interceptação ou gravação das comunicações.

O Art. 6º determina que os provedores de acesso à Internet devem manter, de forma reservada, à disposição do Ministério Público e órgãos de segurança, uma lista atualizada com sua faixa de endereços IPs e um registro de pelo menos seis meses dos endereços IPs e dados de conexão de seus assinantes.

O Decreto ainda define que a *Subsecretaría de Telecomunicaciones*, que regula as telecomunicações no Chile, expedirá uma norma técnica para disciplinar os requisitos técnicos para interceptações e gravações. Até a conclusão dessa dissertação, nenhuma norma nesse sentido foi publicada.

3.4. EUROPA

No velho continente, a interceptação legal de dados telemáticos é abordada por leis nacionais, resoluções e tratados do Conselho da Europa e do Parlamento Europeu. Além disso, existem normas e especificações técnicas do *European Telecommunications Standards Institute* (ETSI) sobre o tema. Alguns desses documentos serão discutidos a seguir.

3.4.1. Resolução relativa à intercepção legal de telecomunicações

Em 1995, o Conselho da Europa adotou uma resolução relativa à intercepção legal de telecomunicações (CONSELHO DA EUROPA, 1995). O documento contém uma lista de necessidades dos órgãos responsáveis pela aplicação da lei, no que tange a execução técnica de intercepções de telecomunicações. Algumas delas são:

- Acesso à totalidade das telecomunicações transmitidas a partir de um identificador do serviço utilizado pelo assinante sujeito à intercepção, com exclusão das outras comunicações que não tenham relação com o referido na ordem de judicial;
- Poder interceptar as comunicações de assinantes que se desloquem temporária ou permanentemente no âmbito de um sistema de telecomunicações;
- Acessar informações sobre a localização geográfica dos assinantes;
- Poder interceptar transmissões de telecomunicações simultâneas, em tempo real e em tempo integral;
- Receber os dados que forem interceptados por múltiplas interfaces, providas pelos provedores de serviços, para um centro de monitoramento dos órgãos policiais de maneira segura;
- Receber os dados interceptados em um formato conhecido. Além disso, os dados devem ser encaminhados decifrados, decodificados e descompactados, quando os provedores procederem aos serviços de criptografia, codificação ou compactação;
- O assinante que tem seu tráfego interceptado ou qualquer outra pessoa não autorizada não pode ser capaz de detectar a interceptação;
- Os prestadores de serviços de telecomunicação devem garantir que as comunicações interceptadas sejam transmitidas somente aos serviços de monitoramento especificados na ordem de intercepção.

3.4.2. Tratado nº 185

A partir de 2001, alguns países se tornaram signatários do Tratado nº 185 do Conselho da Europa, que é uma convenção sobre crimes cibernéticos (CONSELHO DA EUROPA, 2011). Este foi o primeiro tratado internacional sobre crimes cometidos via Internet e em outras redes computacionais, lidando com crimes de direitos autorais, fraudes computacionais, pornografia infantil e ataques a redes (CONSELHO DA EUROPA, 2001).

Dentre os artigos do tratado, os de número 20 e 21 incluem compromissos de que os países signatários adotem medidas legislativas para permitir que suas autoridades competentes tenham condições técnicas para gravar ou obrigar os provedores de serviço de gravarem: informações sobre o tráfego em tempo real de comunicações específicas realizadas por meio de sistemas computacionais; conteúdo em tempo real de comunicações transmitidas por sistemas computacionais, no caso de crimes considerados graves (CONSELHO DA EUROPA, 2001).

Até dezembro de 2011, 32 países assinaram e ratificaram a convenção, dentre eles: Alemanha, Dinamarca, Espanha, Estados Unidos, Finlândia, França, Holanda, Itália, Noruega, Portugal, Reino Unido, Suécia e Suíça. A Rússia, apesar de participar do Conselho, não assinou ou ratificou a convenção. Da mesma forma que a Rússia, procederam outros países que não são membros, como Brasil, Argentina, Chile e China (CONSELHO DA EUROPA, 2011).

Como resultado da assinatura desse tratado, alguns países signatários criaram ou atualizaram suas legislações (BALOO, 2003). Na Tabela 3.1, o cenário de alguns países europeus é apresentado (KOOPS, 2010; UTIMACO, 2009).

Tabela 3.1 - Dispositivos legais e padrões de países europeus sobre interceptação de dados.

País	**Legislações e Padrões**
Alemanha	• *G10 Law*, 2001*;* • *Strafprozessordnung (StPO)*, 2002*;* • *Gesetz über das Zollkriminalamt und die Zollfahndungsämter, (Zollfahndungsdienstgesetz - ZFdG)*, 2002*;* • *Technical Directive: Requirements for implementing statutory telecommunications interception measures v.4.0*, feito pelo *Regulatory Authority for Telecommunications and Post*, 2003; • *Telecommunications Act (TKG)*, 2004*;* • *Telekommunikationsüberwachungsverordnung (TKÜV)*, 2005.
França	• *Loi n° 91-636 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications*, 1991*;* • *Décret n° 93-119 du 28 janvier 1993, Décret relatif à la désignation des agents qualifiés pour la réalisation des opérations matérielles nécessaires à la mise en place des interceptions de correspondances émises par voie de télécommunications autorisées par la loi n° 91-646 du 10 juillet 1991*, 1993; • *Loi n°2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne*, 2001; • *Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme*, 2006.
Holanda	• *Tijdelijke regeling aftappen openbare telecommunicatienetwerken en –diensten*, 1998; • *Telecommunicatiewet*, 1998*;* • *Transport of Intercepted IP Traffic (TIIT) V1.0.0 (2002-09)*, criado pelo *Directorate General for Telecommunication and Post of the Ministry of Economic Affairs*, 2002; • *Wet van 22 april 2004 tot wijziging van de Telecommunicatiewet*, 2004.

Itália	• *Intercettazioni di conversoni o communicazione, Art. 266 – 271, Code di Procedura Penale,* 1988*;* • *Decreto del presidente della repubblica del 19 settembre 1997, n. 318: Regolamento per l'attuazione di direttive comunitarie nel settore delle telecomunicazioni,* 1997; • *Decreto-legge 18 ottobre 2001, n. 374: Disposizioni urgenti per contrastare il terrorismo Internazionale,* 2001; • *Decreto del Ministero delle comunicazioni 26 aprile 2001,* 2001. • *Legge 20 novembre 2006, n.281,* 2006.
Reino Unido	• *Regulation of Investigatory Powers Act (RIPA),* 2000*;* • *The Regulation of Investigatory Powers (Maintenance of Interception Capability) Order,* 2002*;* • *National Handover Interface Specification v1.0,* produzido pelo *Home Office,* 2002.
Rússia	• *Law on Operational Investigations, 1995.* • *SORM I (Sistema Operativno-Rozysknykh Meropriyatii), 1995* • *SORM II,* 2000.

3.4.3. Diretiva 2006/24/CE

No ano de 2006, o Parlamento Europeu e o Conselho da Europa aprovaram a Diretiva 2006/24/CE (PARLAMENTO EUROPEU; CONSELHO DA EUROPA, 2006) referente ao armazenamento de dados gerados ou processados durante uma conexão por meio de serviços ou redes de telecomunicação disponíveis ao público em geral. Tal diretiva não abrange o conteúdo das comunicações, somente seus metadados.

No que diz respeito ao acesso à Internet, e-mails e chamadas por VoIP, devem ser armazenados dados necessários para identificar a origem, destino e hora, tais como: nome, endereço e número da linha do assinante; endereço IP utilizado; data e hora de início e fim das conexões; identificador do usuário; número de telefone usado para chamada VoIP; número de telefone do destinatário de chamadas; nome e endereço do destinatário de e-mails; data e hora dos e-mail e chamadas; duração das ligações. Os dados relativos a e-mails e chamadas por VoIP só deverão ser armazenados pelos próprios provedores desses serviços (PARLAMENTO EUROPEU; CONSELHO DA EUROPA, 2006).

Ainda de acordo com essa diretiva, cada país membro do Conselho da Europa deve aprovar lei nacional que obrigue seus provedores de telecomunicação a armazenar dados referentes a comunicações por um período não inferior a seis meses e não superior a dois anos.

3.4.4. Padrões e especificações técnicas do ETSI

O *European Telecommunications Standards Institute* (ETSI) é uma organização sem fins lucrativos que tem como membros operadores de rede e fabricantes de equipamentos de telecomunicação. Ele é responsável por desenvolver padrões de telecomunicações e tecnologia da informação.

O ETSI publicou padrões e especificações técnicas relacionadas à interceptação de dados. As mais importantes são:

- Padrão ETSI ES 201 158 (ETSI, 2002): contém requisitos gerais para prestadores de serviços de telecomunicações relativos à interceptação legal de dados telemáticos;
- Padrão ETSI ES 201 671 (ETSI, 2007) e Especificação Técnica TS 101 671 (ETSI, 2011a): especificam uma interface de entrega de dados de tráfego interceptado por provedores de serviço de telecomunicações a OSPIIs;
- Especificação técnica ETSI TS 101 331 (ETSI, 2009): contém um conjunto de requisitos técnicos relativos à interface de entrega de dados interceptados, do ponto de vista dos órgãos de segurança que os recebem;
- Especificações técnicas ETSI TS 102 232:
    - *part* 1: v2.7.1 (2011-08) – *Handover Specification for IP Delivery* (ETSI, 2011b);
    - *part* 2: v2.6.1 (2011-08) – *Service-specific details for E-mail services* (ETSI, 2011c);
    - *part* 3: v2.3.1 (2011-08) – *Service-specific details for Internet access services* (ETSI, 2011d);
    - *part* 4: v2.3.1 (2010-08) – *Service-specific details for Layer 2 services* (ETSI, 2010a);
    - *part* 5: v2.5.1 (2010-10) – *Service-specific details for IP Multimedia Services* (ETSI, 2010b);
    - *part* 6: v2.3.1 (2008-08) – *Service-specific details for PSTN/ISDN services* (ETSI, 2008);
    - *part* 7: v2.2.1 (2011-03) – *Service-specific details for Mobile Services* (ETSI, 2011e).

3.4.4.1. ETSI ES 201 158

Em 2002, o ETSI aprovou o padrão ES 201 158, que indica os requisitos gerais para prestadores de serviços de telecomunicação, operadores de redes e provedores de acesso à Internet, relativos à interceptação autorizada de dados trafegados (ETSI, 2002). Nesse padrão, há uma referência especial à interface de entrega de dados. A título de comparação, no contexto do Serviço de Comunicação Multimídia (SCM) brasileiro, as funções de prestadores de serviços de telecomunicação e operadores de redes são consideradas equivalentes (ANATEL, 2001).

No ETSI ES 201 158, são definidos os papéis e o fluxo de ações que devem ser executadas para realizar uma interceptação telemática, conforme mostrado na Figura 3.3 e descrito em seguida.

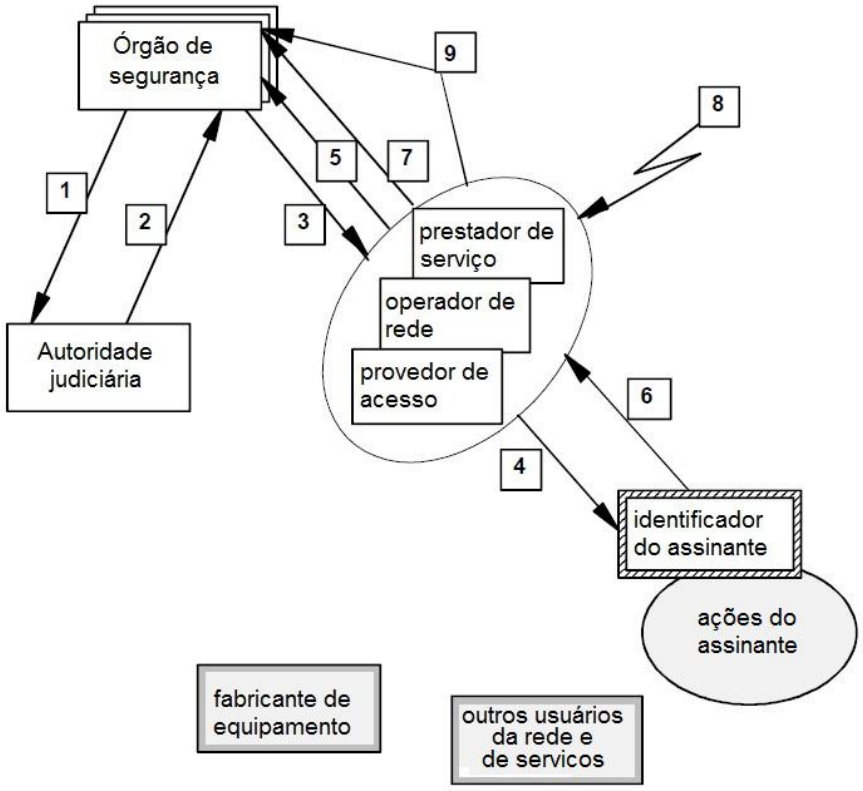


Figura 3.3 - Principais envolvidos e seus papéis – adaptado de (ETSI, 2002).

Caso um OSPII queira realizar uma interceptação telemática, ele deve solicitar uma autorização legal de uma autoridade judiciária competente (1). É possível que essa autorização especifique as informações referentes à interceptação (*intercept related information* – IRI) e o conteúdo da comunicação (*content of communication* – CC) que possam ser entregues aos investigadores.

Se a autorização for concedida (2), o órgão apresentará essa autorização ao prestador de serviço de telecomunicação ou provedor de acesso à Internet (3). A autorização contém os identificadores do assinante alvo, tais como seu nome, endereço residencial, linha telefônica ou endereço IP. Não há comunicação direta entre a autoridade que fornece a autorização legal e os prestadores de serviço de comunicação ou provedores de acesso. Além disso, os OSPIIs não podem ter acesso direto aos elementos da rede do assinante ou provedor.

Em seguida, a empresa ou entidade responsável, contatada pelo OSPII, identifica seu assinante com base nas informações recebidas (4) e informa ao requisitante o recebimento da autorização e quais medidas foram adotadas (5).

Posteriormente, informações referentes à interceptação (IRI) e o conteúdo da comunicação (CC) são coletadas (6) e entregues ao OSPII (7).

Finalmente, mediante pedido do OSPII ou no fim do prazo definido para interceptação, ela é interrompida (8) e sua interrupção é comunicada ao organismo de segurança (9).

Outros envolvidos no processo são os fabricantes, que fornecem equipamentos para os provedores empregarem em suas redes e os demais assinantes, que não devem conseguir detectar que uma interceptação esteja em curso.

O padrão estabelece que uma mesma autorização pode estar dirigida a múltiplos provedores de telecomunicação e acesso, dependendo da conexão do assinante. Além disso, um único assinante pode ser objeto de interceptação de dados por diferentes equipes de investigação, em OSPIIs distintos, com autorizações concedidas por diferentes autoridades judiciais e com restrições diversas (ETSI, 2002).

Para conseguir ativar uma interceptação, deve ser definido um identificador do assinante alvo da escuta, parâmetros de conexão com as instalações de monitoramento do OSPII e identificadores dos prestadores de serviços de telecomunicação, operadores de redes e provedores de acesso à Internet (ETSI, 2002).

O ETSI ES 201 158 define uma interface de entrega (*Handover Interface* – HI) entre o OSPII e prestadores de serviços de telecomunicação, operadores de redes e provedores de acesso à Internet. Ela deve ser configurada de acordo com exigências de leis nacionais, bem como regulamentos específicos de um órgão de segurança.

É sugerido que haja autenticação mútua entre os interlocutores da HI e transmissão segura entre as partes. Ademais, os dados devem ser disponibilizados já decifrados às autoridades competentes, quando a cifragem tiver sido oferecida ao assinante pelos provedores e prestadores de serviço.

A interface HI adota uma estrutura com três canais (ou interfaces): um para troca de informações administrativas (canal HI1), outro para informações referentes à interceptação (HI2) e um terceiro com o conteúdo da comunicação (HI3). Esses canais estão separados da forma apresentada na Figura 3.4.

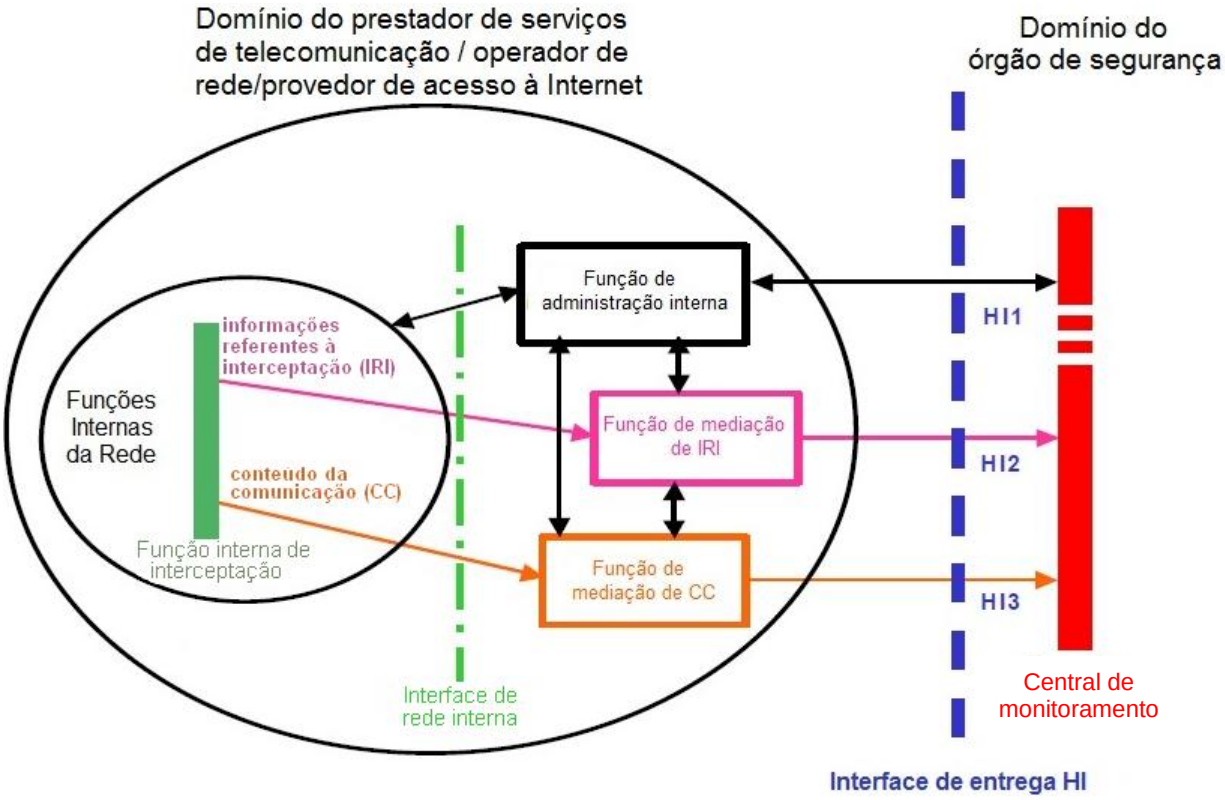


Figura 3.4 - Diagrama funcional da Interface de Entrega – adaptado de (ETSI, 2002).

O canal HI1 leva informações administrativas entre OSPII e os prestadores de serviço de telecomunicação ou provedores de acesso à Internet, tais como solicitações de início e fim de interceptações e suas confirmações de recebimento. Mensagens de erro de transmissão de dados, falhas de conexão e mudanças de configuração do assinante também são conduzidas por meio do HI1. Nesse canal, pode haver transmissões eletrônicas ou manuais e é a única interface bidirecional.

A interface HI2 transporta as informações relativas à interceptação e associadas aos serviços do assinante alvo. Alguns exemplos são: identificação do alvo, tipo de serviço usado, direção da comunicação, localização, data e hora do evento, início e fim de conexão.

O conteúdo das comunicações é transportado por meio do canal HI3 aos OSPIIs. Esse conteúdo deve ser apresentado como uma cópia integral não modificada do fluxo de informação transmitida durante uma comunicação do assinante alvo. Em casos de falha no transporte, como por congestionamento na rede ou indisponibilidade da central de monitoramento, o conteúdo é perdido, já que não há sua gravação pela rede. Quando esse canal é estabelecido, identificadores do assinante alvo devem ser passados de forma que seja possível associar o conteúdo do canal HI3 com as informações recebidas pelo HI2.

As funções internas da rede são a comutação, roteamento e gerenciamento do processo de comunicação. São dessas funções que são produzidos os resultados da interceptação (IRI e CC) para a interface de rede interna.

As funções de mediação são os mecanismos que fazem a passagem da informação da rede interna para a interface de entrega. Caso haja necessidade de se proceder a conversões de formatos de dados, decifragem de pacotes ou outras transformações nos dados originalmente interceptados, tais procedimentos devem ser realizados no âmbito das funções de mediação.

As funções administrativas são as responsáveis por converter as tarefas relativas à interceptação recebidas pela interface HI1 em ações internas e comandos para os equipamentos de rede.

3.4.4.2. ETSI ES 201 671 e TS 101 671

A versão 3.1.1 do padrão ES 201 671 foi definida pelo ETSI em 2007 (ETSI, 2007). Da mesma forma que a especificação técnica TS 101 671 (ETSI, 2011a), ela apresenta um fluxo genérico de informações, assim como os procedimentos, protocolos e serviços relativos à interceptação de telecomunicações de dados ou voz.

Os princípios básicos da interface de entrega, seus requisitos legais e funcionais são os mesmos do ETSI ES 201 158 (ETSI, 2002). Além disso, no ES 201 671 e na TS 101 671, é utilizado como referência o mesmo diagrama funcional de bloco da interface de entrega descrito no ES 201 158 e apresentado na Figura 3.4.

Quanto à interface administrativa HI1, é reforçada a ideia de que os OSPIIs não devem ter acesso direto às funções de comutação da rede interna dos provedores. Além disso, os provedores devem se encarregar da ativação, desativação e modificação de uma interceptação em suas funções internas (ETSI, 2007, 2011a).

Para ativar uma interceptação, os OSPIIs devem fornecer as seguintes informações: identificação do assinante alvo; o LIID (descrito posteriormente); o início e fim ou a duração da interceptação; tipo de informações que devem ser fornecidas (IRI, CC ou ambos); endereço da central de monitoramento para envio dos resultados da interceptação; parâmetros de entrega a serem usados pelas interfaces HI2 e HI3; referência para a autorização legal; contato técnico para resolução de problemas que possam surgir (ETSI, 2007, 2011a).

Cada serviço de um assinante interceptado deve estar associado a um identificador (*Lawful Interception IDentifier* – LIID), em comum acordo com o OSPII, consistindo de caracteres alfanuméricos, contendo referência ao assinante, à autorização legal e a sua data de emissão. Esse identificador é utilizado nos procedimentos de entrega do conteúdo da comunicação e de informações referentes à interceptação, servindo para identificar e correlacionar os dados com cada assinante alvo (ETSI, 2007, 2011a).

Notificações à central de monitoramento do OSPII (*Law Enforcement Monitoring Facility* - LEMF) devem ser enviadas quando há uma ativação, desativação ou modificação de uma interceptação, além de outros casos excepcionais (ETSI, 2007, 2011a).

No que se refere à HI2, as informações referentes à interceptação devem ser enviadas imediatamente quando disponíveis por meio de protocolos de rede amplamente usados, como o FTP. Essas informações só devem ser acumuladas para envio posterior em casos extremos, como falhas de comunicação. Os parâmetros individuais de IRI devem ser codificados usando ASN.1 (*Abstract Syntax Notation One*) e BER (*Basic Encoding Rules*) (ETSI, 2007, 2011a).

Nas definições da interface HI3 para envio do conteúdo da comunicação, a TS 101 671 complementa a ES 201 671, definindo que os dados devem ser encaminhados decifrados aos OSPIIs quando os provedores procederem aos serviços de criptografia. Alternativamente, os dados podem ser entregues cifrados, acompanhados das respectivas chaves e algoritmos para decifragem. Por outro lado, procedimentos criptográficos que não tenham sido fornecidos pelos provedores não precisam ser desfeitos por eles (ETSI, 2011a).

Alguns atributos de segurança para designar um canal como seguro são confidencialidade, integridade, autenticidade e disponibilidade. Contudo, o padrão ES 201 671 e a especificação técnica TS 101 671 não exigem que os canais utilizados tenham essas propriedades.

O padrão e a especificação técnica contêm ainda informações detalhadas sobre a implementação da entrega em redes por comutação de circuitos e de pacotes, a estrutura dos dados enviados, nomes de arquivos, dentre outras.

3.4.4.3. ETSI TS 101 331

A especificação técnica ETSI TS 101 331 contém um conjunto de requisitos relativos à interface de entrega de dados interceptados a OSPIIs, de acordo com o ponto de vista destes órgãos. Além disso, ela apresenta orientações para cooperação entre prestadores de serviços de telecomunicação, operadores de redes e provedores de acesso à Internet (ETSI, 2009).

As exigências da especificação técnica e definições do tráfego que deve ser interceptado estão sujeitas a normativos nacionais e tratados internacionais (CONSELHO DA EUROPA; PARLAMENTO EUROPEU, 1995, 2001, 2006).

Parte dos requisitos já haviam sido indicados em uma resolução do Conselho da Europa (CONSELHO DA EUROPA, 1995). Alguns dos contidos na especificação técnica são:

- Todo o conteúdo da comunicação de um assinante alvo de interceptação deve ser interceptável ao longo do período da autorização legal, sendo excluídas comunicações sem relação com o referido na ordem de judicial. Ademais, o conteúdo destinado ou originado de uma infraestrutura de armazenamento, tais como arquivos e correio eletrônico, também deve ser capturável;
- A entrega de informação relativa à interceptação e de conteúdo da comunicação deve ser feita de forma confiável. No caso de essa informação não ser entregue imediatamente, ela deve ser acumulada até que seja entregue. Entretanto, esses dados não podem ser analisados ou armazenados permanentemente pelos provedores de comunicação e de serviços;
- O resultado da interceptação disponibilizados por meio de uma interface de entrega deve receber um identificador único. Além disso, esse resultado deve ser entregue em tempo real ou com atraso mínimo;

- Os dados interceptados devem ser entregues decodificados e decifrados, quando os provedores procederem aos serviços de codificação e criptografia, ou, alternativamente, devem ser fornecidos os meios necessários para executar essas operações. Ademais, a entrega deve ser feita usando rotas, protocolos, formatos e princípios de codificação amplamente disponíveis;
- As informações referentes à interceptação (IRI) devem ser fornecidas quando há tentativa, estabelecimento ou encerramento de uma conexão, da mesma forma quando há mudança de status, serviço ou localização. Essas IRIs devem conter a identidade do assinante, detalhes do serviço, seu estado e a hora do registro;
- Informações do modo que medidas de interceptação são conduzidas ou dos sujeitos interceptados não devem ser disponibilizadas a pessoas não autorizadas;
- As interceptações não podem ser detectadas por pessoas não autorizadas. Assim, não deve haver mudança na qualidade de serviço, tempo de resposta ou outra característica do serviço oferecido;
- Cada assinante alvo de interceptação deve possuir um identificador único, relacionado ao conteúdo de sua comunicação e informações referentes à interceptação;
- Os OSPIIs devem ser informados quando da ativação, desativação, indisponibilidade ou qualquer alteração na interceptação realizada;
- No que tange a cooperação entre diferentes entidades, deve haver o mínimo de envolvimento com terceiros e cada parte envolvida deve saber somente o estritamente necessário para realizar suas tarefas;
- Deve haver a possibilidade de que um determinado assinante tenha suas transmissões interceptadas simultaneamente por mais de um OSPII, sem que um tenha conhecimento do trabalho do outro.

3.4.4.4. ETSI TS 102 232

A partir de sua versão 2.1.1, a especificação técnica ETSI TS 102 232 foi desmembrada em um conjunto de especificações, uma voltada para pacotes IP em geral e outras com detalhamento para serviços individuais (ETSI, 2011b), conforme mostrado na Figura 3.5.

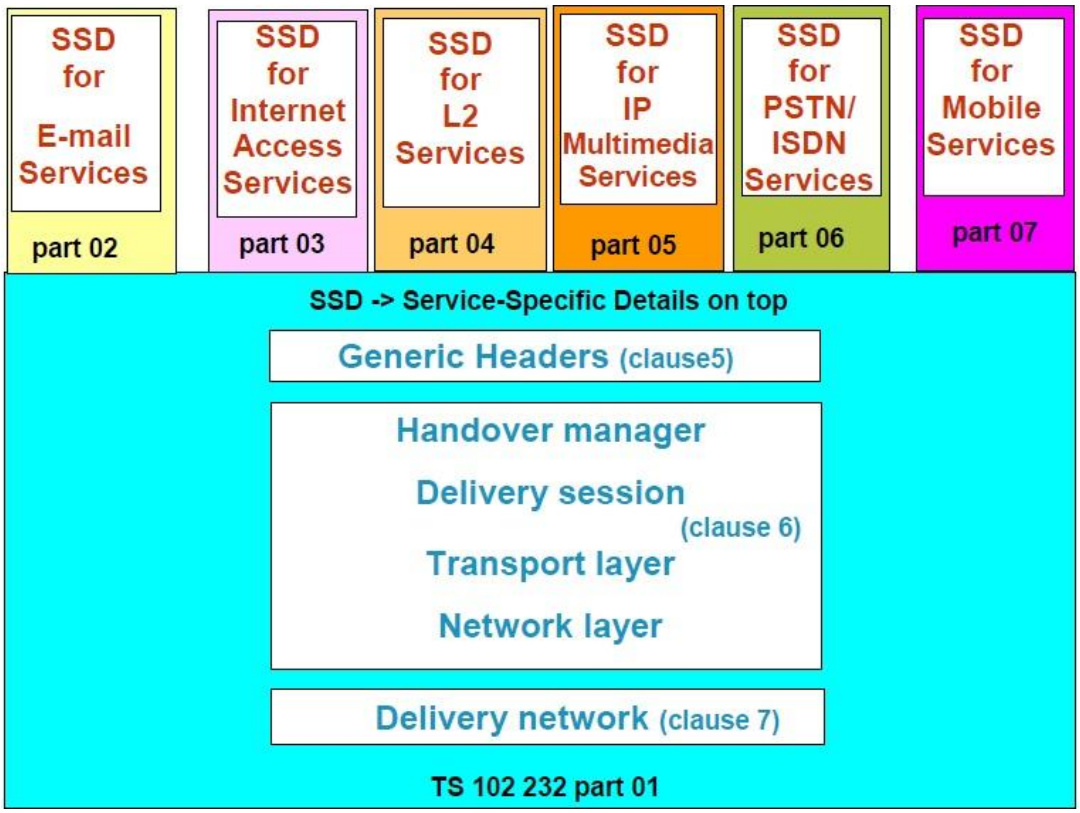


Figura 3.5 - Conjunto de especificações técnicas da série TS 102 232 (ETSI, 2011b).

A ETSI TS 102 232-1, por exemplo, aborda a entrega de dados interceptados de uma rede IP de um provedor de serviço de telecomunicação para um centro de monitoramento de um OSPII. Mais especificamente, seu foco é o transporte de informações referentes à interceptação, por meio da interface HI2, e de conteúdo de comunicação, pela interface HI3. As informações de gerenciamento da interface HI1 não são discutidas no documento (ETSI, 2011b).

O documento também especifica a abordagem modular usada para especificar as interfaces de entrega, os cabeçalhos para serem adicionados ao IRI e CC, além dos protocolos de transferência que devem ser utilizados (ETSI, 2011b).

Os estágios gerais da interceptação de dados telemáticos são: criar ou separar dados interceptados e criar IRI; formatar e transportar os resultados da interceptação da função de mediação do provedor de telecomunicações para uma central de monitoramento (LEMF); receber, interpretar e exibir o resultado da interceptação. Somente o segundo estágio está no escopo da ETSI TS 102 232-1. Ademais, é gerenciada somente a entrega de dados interceptados das camadas de rede (pacotes IP) e aplicação (dados no formato do serviço) (ETSI, 2011b).

Toda informação enviada através das interfaces HI2 e HI3 obrigatoriamente deve ter os seguintes campos identificadores em seu cabeçalho: versão do cabeçalho, LIID, código do país autorizador, identificador único da comunicação, número sequencial, data e hora, direção da comunicação, tipo de conteúdo (IRI ou CC) e tipo da interceptação. O cabeçalho deve ser codificado usando BER e de acordo com o ASN.1 (ETSI, 2011b).

A ETSI TS 102 232-1 contém uma pilha de camadas para a interface de entrega. Elas são de entrega, de sessão e de transporte. Suas funções e definições estão indicadas na específicação técnica.

Os requisitos de segurança para a interface de entrega são confidencialidade, autenticidade e integridade. Tais requisitos podem ser alcançados usando uma aplicação de rede privada virtual (*Virtual Private Network* – VPN). Alternativamente, para atingir confidencialidade e autenticidade, é sugerido o uso do protocolo TLS (*Transport Layer Security*), mais especificamente com encriptação do modo TLS_RSA_WITH_RC4_128_SHA ou TLS_RSA_WITH_AES_256_CBC_SHA. E para garantir a integridade dos dados, periodicamente a função de entrega deve executar o algoritmo SHA-1 sobre pacotes e introduzir datagramas de verificação de integridade no fluxo de pacotes.

As especificações técnicas TS 102 232-2 a TS 102 232-7 contêm definições quanto à entrega de tráfego relativo a serviços específicos de um provedor de serviços ao centro de monitoramento de um OSPII. De acordo com as normas brasileiras, os provedores de SVA seriam equivalentes aos provedores de serviços.

Os serviços descritos em tais especificações são: correio eletrônico (ETSI, 2011c); acesso à Internet (ETSI, 2011d); acesso na camada 2 à rede IP pública (ETSI, 2010a); Multimídia baseada nos protocolos SIP (*Session Initiation Protocol*), RTP (*Real Time Transport Protocol*) e MSRP (*Message Session Relay Protocol*) (ETSI, 2010b); serviços do STFC (PSTN) e RDSI (ISDN) usando técnicas baseadas em pacotes (ETSI, 2008); serviços de redes móveis UMTS, GPRS e CDMA2000 (ETSI, 2011e).

As especificações técnicas TS 102 232-2 a TS 102 232-7 não serão abordadas em detalhes nesta dissertação.

3.4.5. A diretiva alemã: *Requirements for implementing statutory telecommunications interception measures*

Em abril de 2003, a *Regulatory Authority for Telecommunications and Post*, agência regulatória de telecomunicações alemã, aprovou a diretiva técnica *Requirements for implementing statutory telecommunications interception measures* (ALEMANHA, 2003). Ela contém detalhes técnicos para implementação de operações de monitoramento de telecomunicações.

A diretiva abrange as seguintes redes:

- De circuito comutado: PSTN, ISDN, GSM, UMTS-CS, DCS 1800, TETRA, TFTS, VPN e IN;
- De comutação de pacotes: IP, UMTS-PS, GPRS, ITU-T X.25, *frame relay*, ISDN, ATM, ADSL e *packet over* SDH;
- Sistema de chamadas de pessoas (*radio paging*);
- De cabo para serviços de banda larga.

A diretiva divide a comunicação monitorada em conteúdo da comunicação (CC) e informação referente à interceptação (IRI). Ela contém especificações detalhadas dos mecanismos de interceptação para redes de circuito comutado.

No entanto, a versão atual da diretiva técnica só contém regras para conteúdo multimídia e correio eletrônico por meio de UMTS e GPRS. Além disso, é definido que as ações para monitoramento de telecomunicações em redes de comutação de pacotes devem ser acordadas entre a agência de monitoramento e o provedor de serviço de comunicação e cada caso avaliado individualmente. Ou seja, da mesma forma que ocorre no Brasil, na Alemanha ainda não existe padrões definidos para envio de dados interceptados oriundos de redes de pacotes IP.

3.4.6. A especificação holandesa: *Transport of Intercepted IP Traffic*

O primeiro país europeu a definir uma especificação técnica para envio de tráfego interceptado de redes IP foi a Holanda. Em setembro de 2002, o *Directorate General for Telecommunication and Post* do Ministério da Economia holandês publicou a versão 1.0.0 do *Transport of Intercepted IP Traffic* (TIIT) (HOLANDA, 2002).

O documento contém a especificação de uma interface para a função de interceptação de uma rede IP para uma central de monitoramento de um OSPII a fim de que os dados sejam fornecidos no contexto de uma interceptação telemática (HOLANDA, 2002). Essa interface tem como escopo principal o envio do conteúdo da comunicação (CC).

O documento também apresenta uma arquitetura conceitual que pode permitir a execução de interceptações de dados de forma distribuída. Tal arquitetura serve como referência de como entregar os dados interceptados de forma segura aos OSPIIs (HOLANDA, 2002).

A especificação holandesa define um protocolo projetado para transportar tráfego IP interceptado por um ponto de interceptação de um provedor de serviço de telecomunicação a uma central de monitoramento de um OSPII (LEMF), cumprindo os seguintes requisitos:

- Proteger o tráfego para esconder de pessoas não autorizadas informações sobre o número de interceptações em curso, os assinantes que estão com seu tráfego interceptado e a entidade que requisitou a interceptação dos assinantes;
- Minimizar o número de pessoas envolvidas nas atividades de interceptação;
- Permitir uma transmissão autenticada e segura de dados confidenciais por meio de uma rede IP insegura, tal como a Internet;
- Fazer com que a transmissão seja robusta a erros de comunicação em camadas de redes mais baixas;
- Gerar registros históricos para prevenir e rastrear uso malicioso de interceptações;
- Usar apenas padrões abertos para implementação de software.

No TIIT, é especificada uma interface de entrega dividida em três partes, de forma similar ao definido nos documentos do ETSI:

- Interface de entrega 1 (HI1): utilizada para rotinas administrativas relativas às interceptações, por exemplo, envio de chaves criptográficas, ordens judiciais, renovações e interrupção de interceptações;
- Interface de entrega 2 (HI2): envia informação sobre a comunicação de um assinante, como eventos de início e fim de sessões e conexões;
- Interface de entrega 3 (HI3): envia o conteúdo da comunicação à central de monitoramento, como tráfego IP interceptado originado ou destinado ao assinante interceptado e os resultados de autenticação do conteúdo (*hashes*).

Os tráfegos das interfaces HI2 e HI3 podem ser enviados através de um mesmo canal seguro, caso isso ofereça vantagens técnicas ou econômicas. No entanto, a interface HI1 deve utilizar um canal separado.

A arquitetura geral necessária para um transporte confiável para as interfaces HI2 e HI3 está apresentada na Figura 3.6.

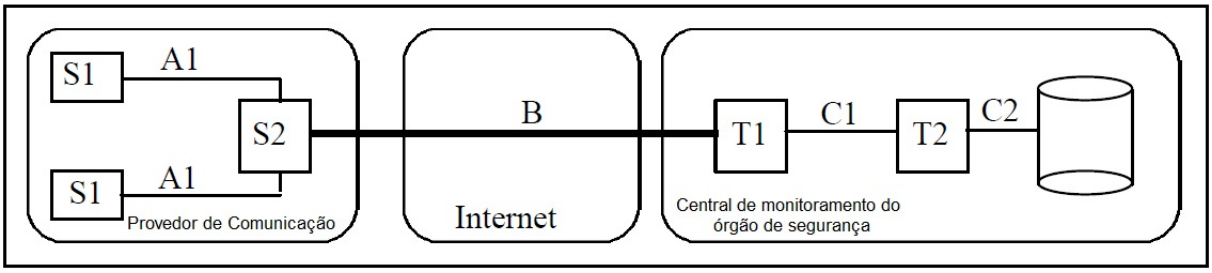


Figura 3.6 - Arquitetura geral do TIIT – adaptado de (HOLANDA, 2002).

As entidades funcionais definidas na Figura 3.6 como S1 e S2 implementam duas funções distintas nas instalações do provedor de serviço de comunicação. S1 é o ponto de interceptação de todo o tráfego originado ou destinado ao assinante interceptado. Tipicamente, S1 pode ser um *sniffer* ou a função de interceptação de um servidor de correio eletrônico ou roteador. S1 deve gerar uma marca temporal sobre cada pacote interceptado e aplicar a função de *hash* SHA-1 para cada 64 pacotes interceptados de um fluxo de tráfego interceptados. Além disso, deve cifrar o tráfego usando uma chave conhecida, definida na autorização judicial.

A função S2 agrupa o tráfego de uma ou mais entidades S1, encaminha-o para uma LEMF e gerencia conexões entre o provedor e a central. Essas conexões devem ser feitas por meio de um túnel TLS/SSLv3, cujas chaves são negociadas pela interface HI1. Alternativamente, pode-se utilizar uma conexão de TCP/IPSec com IKE autenticando S2 e T1. Caso as funções S1 e S2 fiquem em equipamentos distintos, o caminho A1 deve ser feito por meio de um canal seguro, com autenticação mútua.

As funções T1 e T2, por sua vez, são implementadas nas instalações da LEMF. T1 é a função de coleta de dados, que aceita conexões de uma ou mais funções S2 dos provedores previamente conhecidos. T2 é a função que armazena os dados interceptados para análise e uso posterior.

O canal B mostrado na arquitetura da Figura 3.6 é seguro sobre uma infraestrutura insegura. Assim, deve ser um canal cifrado. Da mesma forma, o canal C1 também é seguro e não deve estar na Internet ou outra rede pública. O canal C2 não é especificado no TIIT.

3.4.7. A especificação britânica: *National Handover Interface Specification*

Em maio de 2002, o *Home Office* do governo britânico aprovou a *National Handover Interface Specification* (NHIS) (REINO UNIDO, 2002). A especificação abrange a entrega de todo conteúdo interceptado legalmente de Internet de provedores de serviço de telecomunicações para uma central de monitoramento de um OSPII. O conteúdo interceptado inclui e-mails, fluxos de tráfego IP e outros serviços de Internet.

De forma semelhante aos padrões do ETSI, a interface de entrega é dividida em três níveis (REINO UNIDO, 2002):

- Interface de entrega 1 (HI1): utilizada para atribuição de tarefas e gerenciamento, ou seja, para comunicação entre os provedores de serviço de comunicação e a central de monitoramento sobre o assinante alvo, o início e o fim das interceptações. Essa interface é a única bidirecional;
- Interface de entrega 2 (HI2): envia informação referente a interceptação, sendo utilizada para que o provedor de serviço envie dados adicionais sobre a interceptação, como hora e duração das conexões;
- Interface de entrega 3 (HI3): envia o conteúdo da comunicação à central de monitoramento.

A especificação divide o conteúdo de interceptação em fluxos e lotes. Os fluxos são referentes a um conteúdo de tráfego obtido de uma sessão web ou VoIP, por exemplo. Já os conteúdos em lotes são aqueles cuja informação é suprida em blocos discretos e completos, tais como mensagens de correio eletrônico, grupos de notícias e arquivos armazenados (REINO UNIDO, 2002).

A NHIS contém ainda especificações detalhadas do encapsulamento que o tráfego IP interceptado deve receber antes de ser enviado em tempo-real à central de monitoramento do OSPII. Além disso, são definidos o formato e conteúdo dos cabeçalhos dos pacotes, critérios para gerenciamento de *sockets*, transmissão de dados e tratamento de erros.

Finalmente, a especificação contém o detalhamento do formato que deve ser utilizado para envio de conteúdo em lote, como mensagens de correio eletrônico e grupos de notícias. Cada item do lote deve ser salvo em arquivo no formato XML e enviado à central de monitoramento por meio de FTP.

O documento não contém definições sobre a rede de comunicação por onde será feita a entrega ou sobre procedimentos de segurança.

3.5. SÍNTESE DO CAPÍTULO

Neste capítulo, apresentou-se o cenário da interceptação telemática em alguns países. Foram descritas legislações, normas, padrões e especificações técnicas de referência. Baseado nisso, a fim de proverem capacidade de interceptação e estarem em conformidade com requisitos legais e técnicos internacionais, fabricantes de hardware e software projetam e adaptam seus produtos. Alguns deles são utilizados em provedores de telecomunicação brasileiros, cujas características técnicas serão descritas no próximo capítulo.

4. A ESTRUTURA DOS PROVEDORES BRASILEIROS PARA CONEXÃO À INTERNET

Diferentes tecnologias são utilizadas para que um assinante se conecte à Internet no Brasil. Em dezembro de 2011, havia mais de 58 milhões de usuários com conexão à Internet em banda larga no País (TELEBRASIL, 2012). Os dados referentes aos acessos a serviços de comunicação multimídia por tecnologia em setembro de 2011 no Brasil estão listados na Tabela 4.1.

Tabela 4.1 - Quantidade de acessos SCM por tecnologia (TELECO, 2011a).

Total de acessos SCM por Tecnologia (Milhares)												
Tecnologia	ATM	Cable Modem	Ethernet	Fibra	FR	FWA	HFC	MMDS	SAT	Spread Spectrum	WiMAX	xDSL
Acessos	377	4.461	808	188	22	195	131	9	32	653	45	10.713

A distribuição de tipos de tecnologia para acesso à Internet em domicílios por região do País, renda familiar e classe social pode ser vista na Tabela 4.2.

Tabela 4.2 - Tipo de conexão para acesso à Internet no domicílio (CETIC.BR, 2010).

Percentual (%)		**Acesso discado**	**Banda Larga Fixa**					**Banda larga móvel (modem 3G)**	**Não sabe/Não respondeu**
			TOTAL Banda larga fixa	**Modem digital via linha telefônica (tecnologia DSL)**	**Modem via cabo**	**Conexão via rádio**	**Conexão via satélite**		
TOTAL BRASIL		13	68	30	25	12	3	10	10
REGIÕES DO PAÍS	SUDESTE	15	67	29	28	8	3	8	12
	NORDESTE	12	64	16	27	20	2	15	9
	SUL	9	78	38	18	19	2	9	5
	NORTE	21	53	21	15	14	3	16	10
	CENTRO-OESTE	9	66	35	12	18	2	17	11
RENDA FAMILIAR	Até 1 SM	14	64	24	27	11	2	8	14
	1 SM - 2 SM	17	65	25	21	18	3	8	11
	2 SM - 3 SM	13	69	34	21	12	3	9	10
	3 SM - 5 SM	13	65	28	24	12	2	10	14
	5 SM - 10 SM	10	76	31	33	11	3	11	6
	10 SM ou +	8	70	34	31	3	3	21	8
CLASSE SOCIAL	A	8	81	39	31	8	5	14	8
	B	11	72	33	27	10	3	11	8
	C	15	64	27	22	13	3	9	12
	DE	14	59	17	18	24	1	7	20

Nas seções a seguir, serão apresentadas algumas das principais tecnologias existentes no País para acesso à grande rede, mostrando a disposição dos entes envolvidos e seus equipamentos.

4.1. PROVEDOR WIMAX

O padrão IEEE 802.16 especifica uma interface aérea de sistemas combinados de acesso a redes sem fio metropolitanas (*Wireless Metropolitan Area Network* - WMAN). Ele recebeu o nome WiMAX, que é a sigla referente a *Worldwide Interoperability for Microwave Access* ou em tradução livre "Interoperabilidade Mundial para Acesso por Micro-ondas" (IEEE 802.16 WORKING GROUP, 2011). Por meio do uso desse padrão, pode-se disponibilizar uma rede de acesso sem fio em escala metropolitana, com maior taxa de transmissão e cobertura que outros padrões sem fio, tais como o Wi-Fi e 3G (AQSACOM, 2010a).

O padrão WiMAX representa uma evolução das redes Wi-Fi (IEEE 802.11), tanto pelo seu maior alcance como pelas altas taxas de transmissão. O padrão oferece velocidades de até 40 Mbit/s para clientes móveis e pode chegar até 1 Gbit/s para clientes fixos com a especificação IEEE 802.16m (IEEE 802.16 WORKING GROUP, 2011). Ademais, seu sinal é capaz alcançar 50 km com visada direta ou ainda cobrir um raio de 8 km sem visada. Outra vantagem dessa tecnologia é o relativo baixo custo de implantação, quando comparado com outras tecnologias de última milha, como ADSL, cabo, GSM ou fibra ótica. Com isso, é possível oferecer acesso à Internet em regiões isoladas onde antes não era viável economicamente, como em áreas rurais e ilhas (HANCOCK, 2009).

A topologia típica de um provedor de acesso à Internet que faça uso de redes WiMAX encontra-se exibida na Figura 4.1 (WIMAX FORUM, 2009).

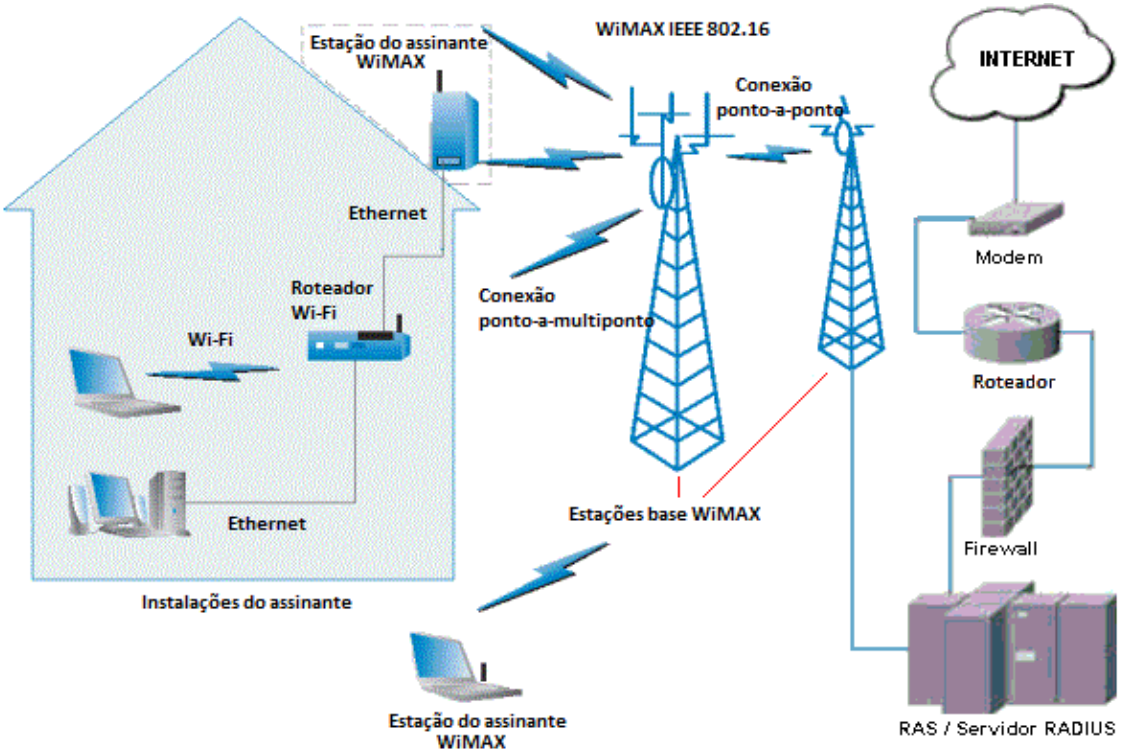


Figura 4.1 - Topologia de provimento de acesso à Internet via WiMAX.

Tipicamente, há uma estação base (*base station* - BS) conectada a um servidor RADIUS que faz a autenticação dos assinantes. Esse servidor pode estar conectado a outros elementos, tais como firewall, roteador ou modem com conexão a um enlace de dados de Internet. A estação base retransmite o sinal para outra estação base por intermédio de uma conexão WiMAX ponto-a-ponto (PPP). Essa base redistribui o sinal via WiMAX ponto-a-multiponto (PMP) no meio aéreo. Outro elemento no diagrama é a estação do assinante (*subscriber station* - SS), que recebe os dados provenientes da base, e que normalmente está conectada a um roteador Wi-Fi, que envia os dados pelo meio aéreo a estações de trabalho que possuam interfaces de rede sem fio e via conexão cabeada Ethernet para máquinas que possuam esse tipo de interface.

Computadores pessoais e notebooks que possuam interface de rede WiMAX também podem receber o sinal diretamente de uma base e assumir desta forma o papel de estação do assinante (SÍCOLI, 2010).

4.1.1. Um exemplo de provedor: Wixx

A empresa Wixx (BRXNQ Telecomunicações LTDA) começou a oferecer conexão à Internet em Brasília por meio do uso de WiMAX em 2010. A empresa presta o serviço de valor adicionado de conexão à Internet (SCI) e ainda tem autorização da ANATEL para oferecer o

serviço de comunicação multimídia (SCM) em todo o território nacional. Sua sede fica na região central da capital federal, onde está localizada sua estação base com conexão à rede mundial de computadores (PAIVA, 2010). A área de cobertura da empresa são as regiões administrativas de Águas Claras, Asa Norte, Asa Sul, Sudoeste e Taguatinga, que ficam a até 20 km de sua sede.

Na configuração padrão, faz-se uso de um equipamento com interface de rede WiMAX localizado nas instalações do assinante e fornecido pela empresa (*customer premises equipment* - CPE). Por um lado, o CPE se comunica com a estação base localizada na sede da Wixx, que está ligada à infraestrutura fixa do servidor de autenticação (RAS e RADIUS), de correio eletrônico e também ao enlace de Internet. Por outro, o CPE está ligado a um roteador sem fio, que retransmite o tráfego de Internet por meio de Wi-Fi a estações com interfaces de rede sem fio ou por meio de conexão cabeada Ethernet. A topologia do serviço está organizada de maneira semelhante ao apresentado na Figura 4.1.

A autenticação na rede da Wixx é feita por meio de servidores RAS (*Remote Access Server*) e RADIUS. Inicialmente, quando um usuário tenta acessar um recurso de Internet, o RAS detecta que o usuário ainda não está autorizado e provoca a abertura de uma página de autenticação no navegador do usuário. Assim, o usuário deve se autenticar por meio da página do RAS, que encaminha os dados de usuário para que o servidor RADIUS verifique as credenciais fornecidas. Estas são verificadas em sua base de dados e, caso o usuário seja autorizado, o servidor RADIUS comunica de volta ao servidor RAS que concede ao usuário acesso à Internet.

O público-alvo da empresa para os serviços de acesso a Internet são condomínios e empresas pequenas e médias. A Wixx também oferece a seus assinantes *hotspots* Wi-Fi em locais públicos de grande circulação de pessoas, como *shopping centers* e no aeroporto internacional da cidade. Os *hotspots* Wi-Fi estão conectados a estações WiMAX, que recebem os dados da estação base da empresa e os redistribuem.

A rede WiMAX da Wixx trabalha na faixa de frequência não licenciada de 5,8 GHz e utiliza equipamentos compatíveis com o padrão IEEE 802.16d dos fabricantes Alvarion e Airspan (PAIVA, 2010).

4.2. PROVEDOR ADSL

A tecnologia ADSL (*Asymmetric Digital Subscriber Line* ou "Linha Digital Assimétrica para Assinante") é utilizada para prover uma transmissão de dados digitais de alta velocidade por meio de linhas telefônicas comuns de cobre (MIAO, 2004). O termo “assimétrica” do nome indica que as velocidades de *download* e *upload* são diferentes, já que a tecnologia usa uma faixa de frequência mais estreita para o *upload*. Conforme, mostrado na Tabela 4.1, é a tecnologia de transmissão de banda larga mais utilizada no País.

O ADSL funciona nas linhas telefônicas existentes sem causar impactos negativos nos serviços de chamadas tradicionais (NUNES, 2006). Os sinais de voz analógicos e dados são separados por meio de um filtro ou divisor, que vai introduzir o sinal de dados do ADSL em uma faixa de frequência mais alta que a de voz (HENZ, 2008). Dessa forma, os serviços de voz e dados podem funcionar ao mesmo tempo. Do ponto de vista do assinante, basta que ele conecte seu computador a um modem ligado a sua linha telefônica para que tenha acesso à grande rede.

Na central telefônica da operadora, também há um tipo de divisor. Desta forma, no caso de chamadas telefônicas, o sinal de voz é encaminhado para a rede de comutação de circuitos da companhia telefônica (STFC). Por outro lado, o sinal de dados é enviado ao DSLAM (*Digital Subscriber Line Access Multiplexer*), e seguirá o caminho da rede de dados e Internet, conforme mostrado na Figura 4.2.

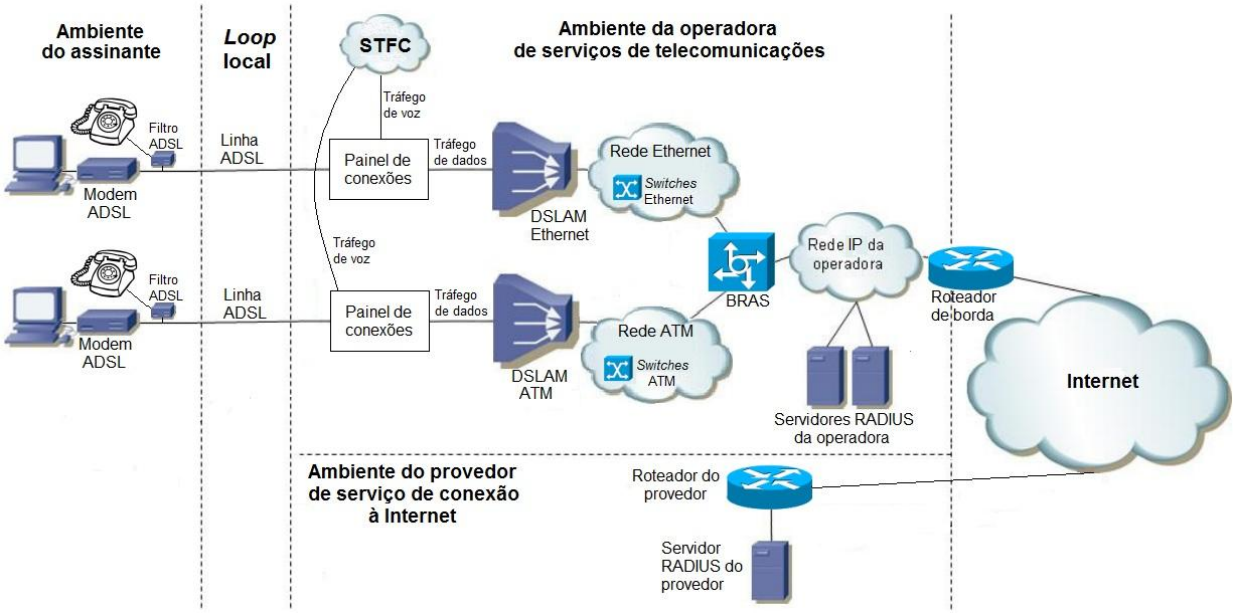


Figura 4.2 - Principais elementos de uma conexão ADSL – adaptado de (GRUSZYNSKI, 2008).

Nas seções a seguir, serão descritas as funções dos principais elementos existentes para viabilizar uma conexão ADSL à Internet.

4.2.1. Filtro ADSL

O filtro ADSL, também conhecido como divisor, é o dispositivo responsável por separar o sinal analógico de voz, que funciona em uma faixa de frequência mais baixa (menor que 4 kHz) dos dados digitais de Internet. Ele permite que os sinais de dados não interfiram com os de voz e vice-versa (NUNES, 2006). Cada aparelho telefônico ligado a uma linha com ADSL deve possuir um filtro entre ele e a linha (KITZ, 2004).

4.2.2. Modem ADSL

O modem ou roteador ADSL é o transceptor que conecta a linha ADSL a um computador ou outro dispositivo que se queira conectar à Internet. Embora o equipamento tenha o nome de "modem", ele não modula ou demodula sinais analógicos e digitais, apenas trabalha com sinais digitais (GALLO; HANCOCK, 2002).

4.2.3. *Loop* local

O *loop* local, também conhecido como linha de assinante ou "última milha", é o caminho que a linha telefônica percorre entre a residência do assinante e a central telefônica. Normalmente os cabos são de cobre e podem passar por cima de postes ou ainda por meio de dutos subterrâneos. A distância entre a residência do assinante até a central telefônica vai definir a velocidade máxima de transmissão da linha. Quanto mais longe da central, maior a atenuação do sinal e, consequentemente, menor a velocidade suportada pela linha. A distância máxima do *loop* local é de aproximadamente 5 km (HENZ, 2008).

As conexões ADSL usam enlaces ponto-a-ponto dedicados, ou seja, o enlace até a central telefônica é de uso exclusivo de um único assinante (GALLO; HANCOCK, 2002).

4.2.4. Painel de Conexões

Os painéis de conexões (*patch panels*) são concentradores de cabos que ficam na central telefônica. Todas as linhas ADSL são conectadas a estes painéis, que normalmente têm uma referência ao cartão de linhas e DSLAM aos quais estão conectados. Eles também dividem e filtram o sinal recebido, encaminhando o sinal de voz para o sistema telefônico comum (STFC) e o de dados para o DSLAM (HENZ, 2008).

4.2.5. Cartões de linhas

Os cartões de linha são peças encaixadas nos DSLAM. Cada cartão de linha tem um número determinado de linhas conectadas, normalmente 8, 16, 24 ou 32 (KITZ, 2004).

A velocidade máxima da linha é configurada por meio de *jumpers* nos cartões de linha.

4.2.6. DSLAM

O DSLAM (*Digital Subscriber Line Access Multiplexer*) é o equipamento responsável por concentrar e multiplexar as conexões de vários usuários em uma única conexão do *backbone* ATM ou Ethernet (HENZ, 2008). Ele é formado por várias placas com circuitos e cartões de linhas, podendo conter centenas de portas (GRUSZYNSKI, 2008).

Os DSLAMs podem se conectar ao *Broadband Remote Access Server* (BRAS) por meio de interfaces para redes ATM ou Ethernet.

4.2.7. *Switch* ATM ou Ethernet

Um *switch* ATM ou Ethernet é o equipamento que agrupa um conjunto de DSLAMs ao BRAS (HENZ, 2008).

4.2.8. BRAS

O *Broadband Remote Access Server* (BRAS) é o equipamento responsável por agregar ou terminar as conexões provenientes de um ou mais DSLAMs. Ele é um servidor que termina a sessão PPP do assinante e designa a ele um endereço IP válido (HENZ, 2008), estabelecendo uma conexão do equipamento do cliente com a rede da operadora (GRUSZYNSKI, 2008), possibilitando assim seu acesso à Internet.

O BRAS recebe chamadas de clientes que desejam acessar a rede de dados. Ele é responsável pela verificação das credenciais de usuários, por meio de consulta a servidores de autenticação, autorização e contabilização (*Accounting, Authorization, Authentication – AAA*), tais como os servidores RADIUS.

O BRAS localiza-se em um ponto de presença dos provedores de serviços de telecomunicação. Ele concede acesso a recursos remotos da rede, sendo, desta forma, um *Network Access Server* (NAS).

4.2.9. Servidor RADIUS

O servidor RADIUS é um equipamento que implementa o protocolo RADIUS (*Remote Authentication Dial In User Service*), definido na RFC 2865, para prover um serviço de Autenticação, Autorização e Contabilização (*Authentication, Authorization and Accounting - AAA*) para equipamentos que desejam se conectar à Internet (RIGNEY et al., 2000). Os clientes dos servidores RADIUS podem ser um BRAS, servidores de VPN ou *switches*.

As principais funções de um servidor RADIUS são: autenticar usuários ou dispositivos antes de conceder acesso a uma rede; autorizá-los para determinados serviços; contabilizar o uso dos serviços acessados; delimitar a velocidade, o tempo e o volume de dados que os usuários podem trafegar (NUNES, 2006).

Por meio de um servidor RADIUS, pode-se definir que um usuário somente poderá se conectar com determinado endereço MAC. É possível também definir um endereço IP fixo que sempre será atribuído a determinado usuário.

O software para servidor RADIUS mais utilizado no mundo é o FreeRADIUS (THE FREERADIUS SERVER PROJECT, 2010).

De acordo com as normas vigentes no País (ANATEL, 2001), uma conexão ADSL de uma operadora de serviço de telecomunicações só pode ser fornecida com a utilização de um provedor de serviços de conexão à Internet (PSCI). Dessa forma, para o estabelecimento de uma conexão à Internet, os servidores de AAA da operadora de SCM devem consultar os servidores de AAA dos PSCIs a fim de buscar informação de autenticação dos clientes e conceder ou não o acesso (HENZ, 2008).

4.2.10. Roteadores de borda

São dispositivos posicionados nos limites da rede de um provedor e que fazem o roteamento de dados de sua rede local para *backbones* de Internet. Eles se comunicam pelo protocolo eBGP com outro dispositivo em outro provedor ou ainda a se conectam a outro sistema autônomo (BERKOWITZ et al., 2005).

4.2.11. Um exemplo de serviço: Speedy da Telefônica

O Speedy é um serviço de acesso à Internet banda larga fixa da empresa Telefônica. Ele usa a tecnologia ADSL e é oferecido no Brasil e em outros países da América Latina com esse mesmo nome comercial. No País, atualmente são oferecidos planos de 256 kbit/s a 8 Mbit/s (TELEFÔNICA, 2011).

No terceiro trimestre de 2011, a Telefônica tinha 22,3% de participação no mercado de Internet banda larga no Brasil, contando com cerca de 3,6 milhões de assinantes (TELECO, 2012).

A rede da empresa Telefônica, utilizada para prover o serviço Speedy, é formada pelas três grandes redes mostradas na Figura 4.3.

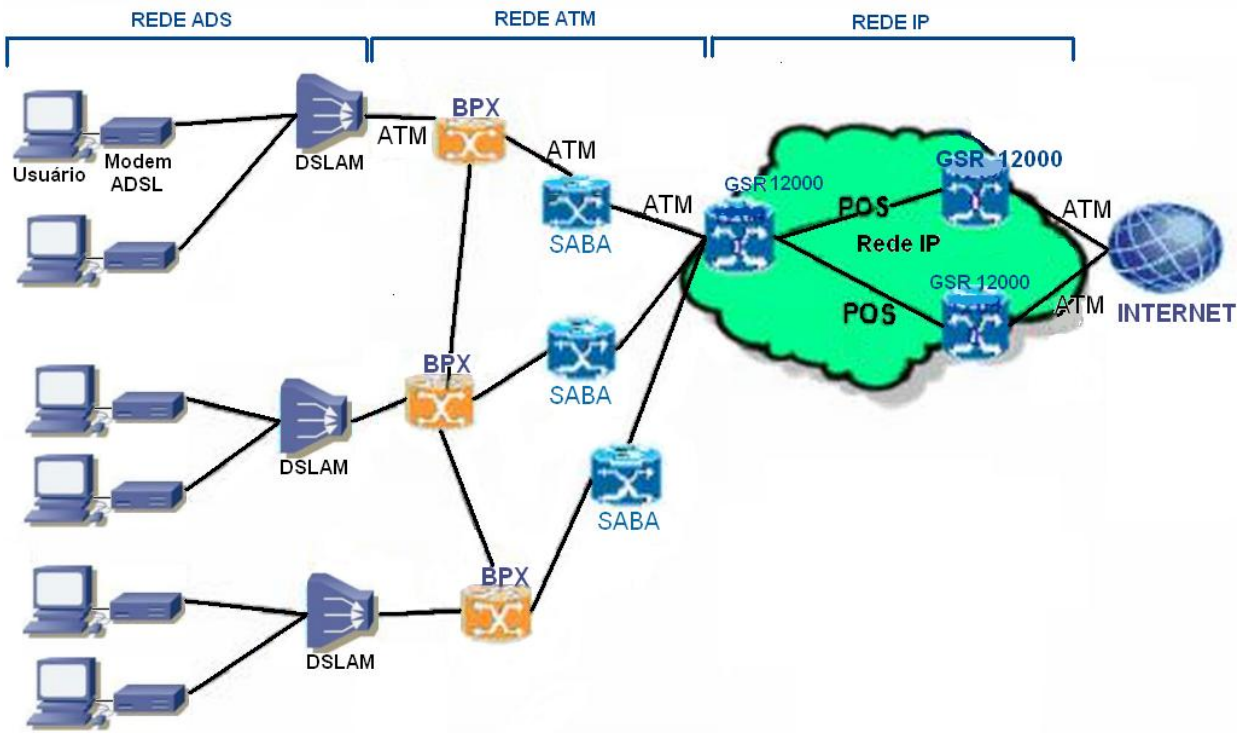


Figura 4.3 - Arquitetura simplificada do serviço Speedy da Telefônica.

A primeira rede, a ADS, é formada pelos elementos de hardware e software que vão desde a residência do usuário ao DSLAM, tais como modem, loop local, cabos de cobre e painéis de conexões.

A Rede ATM, por sua vez, inclui a estrutura que vai desde a saída do DSLAM, passa pelo BPX (*Broadband Packet Exchange*), pelo SABA (*Servidor del Acceso Banda Ancha*, também conhecido como BRAS), e vai até o roteador de borda, que faz a interface com a rede IP.

Vários DSLAMs estão conectados a um concentrador, que tem um VPI (*Virtual Path Identifier*) ou VCI (*Virtual Channel Identifier*) em comum, que trafegam pela rede ATM por meio da mesma entrada do BPX.

O BPX é o equipamento onde estão configuradas as linhas e os VPs e VCs de cada cliente. Ele é um switch ATM de grande porte, como por exemplo, da série Cisco BPX 8600. A rede ATM tem duas conexões ATM, a *master* e a *slave*. A primeira conecta o DSLAM ao BPX. Já a segunda, conecta o BPX ao SABA.

O SABA também é um roteador de grande porte que possui interfaces STM-1 e STM-4. Alguns desses equipamentos são da série Cisco 6400. Os roteadores de borda têm capacidade superior ao SABA. Alguns deles são dos fabricantes Juniper Networks, série ERX, e Cisco, série 12000.

Finalmente, na rede IP, estão outros equipamentos, tais como roteadores, *switches* e servidores de autenticação.

4.2.12. Outro exemplo de serviço ADSL: Velox da Oi

O Velox é o serviço de acesso à Internet banda larga via ADSL da empresa Oi. O serviço começou a ser comercializado pela empresa Brasil Telecom sob o nome “Turbo” a partir de 2000 nas cidades de Brasília e Curitiba (SILVA, 2010). Atualmente, a empresa oferece planos com velocidade de 1 a 15 Mbit/s em aproximadamente 300 cidades (OI, 2012).

No levantamento realizado no terceiro trimestre de 2011, o serviço era o maior entre os acessos à Internet banda larga no País, com cerca de 4,8 milhões de assinantes, o que representava 29,9% de participação no mercado (TELECO, 2012).

A arquitetura simplificada da rede ADSL da operadora Oi foi exibida na Figura 4.4 a seguir.

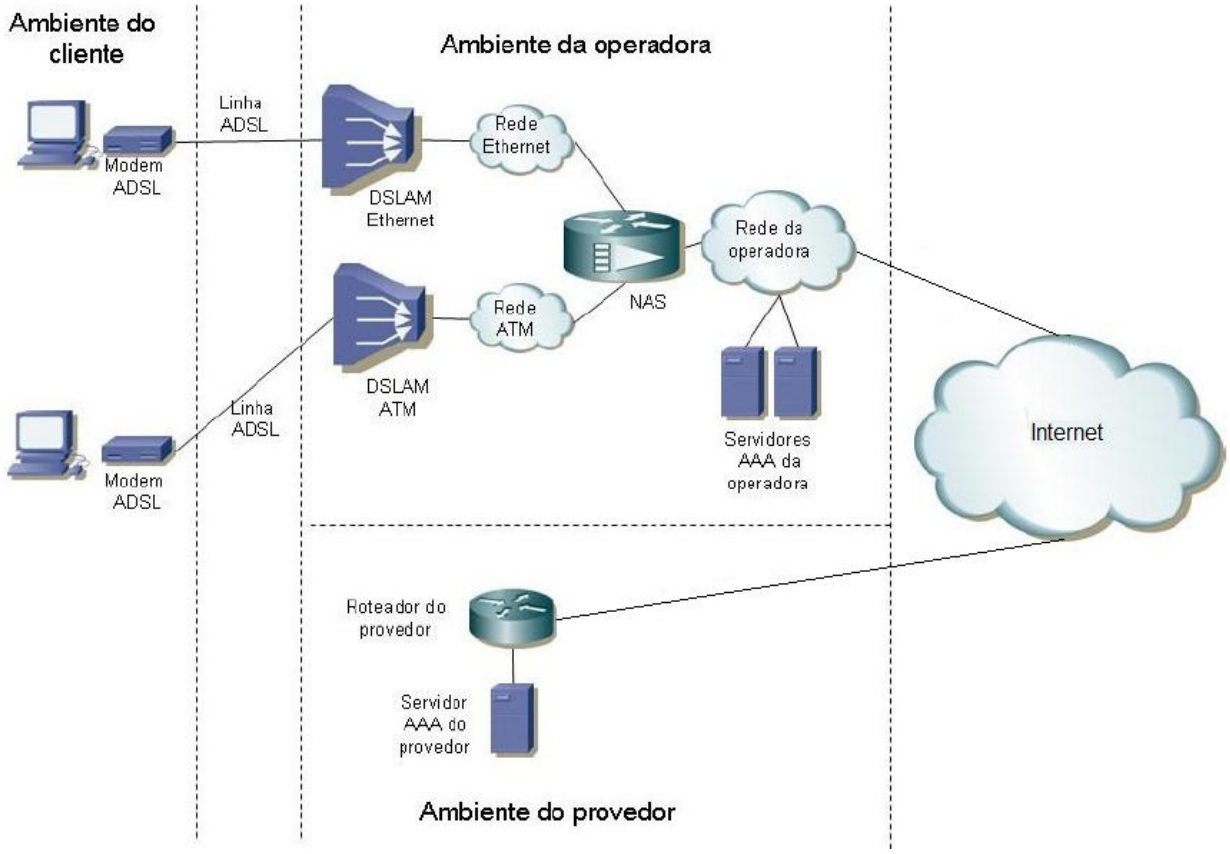


Figura 4.4 - Arquitetura simplificada do serviço Velox da Oi (GRUSZYNSKI, 2008).

A Oi possui portas de acesso banda larga do tipo ADSL, ADSL2 e ADSL2+. Além disso, tem em operação DSLAMs do tipo Ethernet e ATM. Em 2008, a operadora possuía os equipamentos instalados constantes da Tabela 4.3 a seguir (HENZ, 2008).

Tabela 4.3 – Equipamentos da empresa Oi (Brasil Telecom).

Tipo	Fabricante	Modelo	Quantidade	Total de portas
DSLAM ATM	Alcatel	7300 ASAM	926	178.254
DSLAM ATM	Cisco	6120	109	12.984
DSLAM ATM	Inovia	-	88	17.403
DSLAM ATM	Lucent	Stinger	644	440.581
DSLAM ATM	Huawei	MA5100, MA5103 e MA5105	2.726	459.270
DSLAM Ethernet	Huawei	MA5100, MA5300 e MA5600	1.824	514.151
DSLAM Ethernet	Ericsson	HM 130	462	89.297
DSLAM Ethernet	UTStarcom	B820 e B1000	1.955	494.592
DSLAM Ethernet	Siemens	HiX5635	263	102.484
BRAS	Cisco	10008	43	1.579.127
BRAS	Juniper	ERX	19	729.889

Os dois modelos de BRAS utilizados pela Oi têm suporte a funções de interceptação telemática. O Cisco modelo 10008, assim como todos da série 10000, é compatível com o padrão ANSI J-STD-025 (CISCO SYSTEMS, 2010d). Por sua vez, os BRASs da Juniper série E têm a capacidade de espelhamento de pacotes, podendo ter como filtro uma determinada interface ou assinante, replicando o tráfego para uma estação de análise (JUNIPER, 2010).

4.3. PROVEDOR POR CABO

Alguns provedores oferecem o acesso à Internet utilizando a mesma infraestrutura de TV a cabo, a CATV (*Community Antenna Television*), para trafegar dados (KOS; GRGIC; MANDIC, 2003). Para tal propósito, é utilizado o padrão DOCSIS (*Data Over Cable Service Interface Specification*), definido pelo ITU-T (*International Telecommunications Union Telecommunications Standardization Sector*). Suas especificações permitiram o desenvolvimento e implantação de transmissão de dados por cabos de forma não proprietária, com múltiplos fabricantes de equipamentos, o que garante interoperabilidade para transferência de tráfego IP entre o assinante e o provedor de acesso à Internet (CISCO SYSTEMS, 2004). A versão mais recente do padrão é o DOCSIS 3.0, que foi ratificado pela Recomendação J.222 do ITU-T (ITU-T, 2007b). Na Europa, é utilizada uma versão modificada do padrão, o EuroDOCSIS. Os provedores por cabo brasileiros utilizam o DOCSIS original.

Da mesma forma que ocorre com a tecnologia ADSL, há uma divisão do espectro de frequências para que os canais sejam transmitidos em uma faixa de frequência e os dados em outra (KOS; GRGIC; MANDIC, 2003). Os dados são transmitidos em por meio de um ou mais canais com faixas de frequência que podem ter 6 MHz (DOCSIS) ou 8 MHz (EuroDOCSIS) (ITU-T, 2007b). Como no padrão europeu são utilizados canais de 8 MHz, podem-se obter taxas de transferência superiores.

Antigamente, quando era utilizado o padrão DOCSIS 1.0, as redes de TV a cabo não suportavam o canal de retorno. Dessa forma, o *upload* de dados era feito por meio da rede telefônica convencional. Atualmente, são utilizados os padrões DOCSIS 1.1 ou superiores, com conexão bidirecional entre as instalações do provedor e o modem a cabo do assinante.

A arquitetura DOCSIS 3.0 possui alguns componentes principais, mostrados na Figura 4.5.

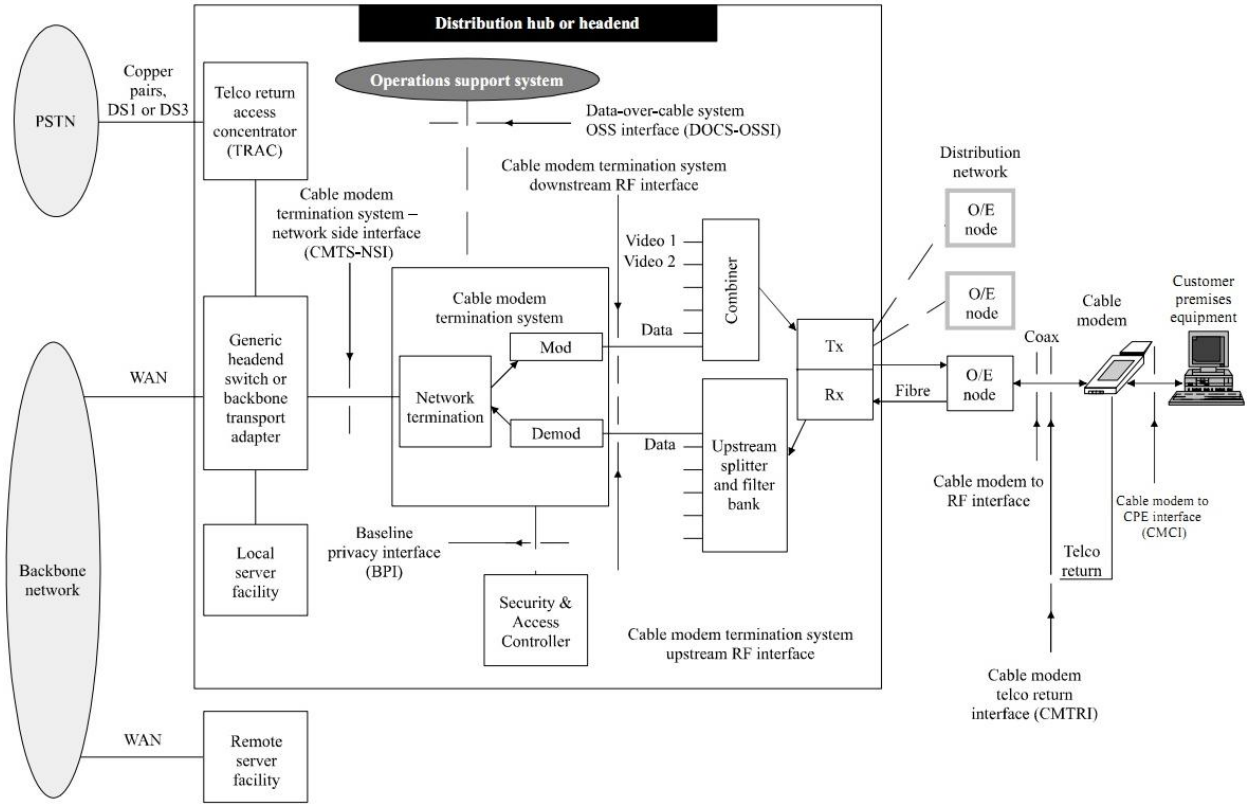


Figura 4.5 - Arquitetura do DOCSIS 3.0 para Internet a cabo (ITU-T, 2007b).

No lado das instalações do provedor, está o cabeçal principal (*master headend*), que é a central mais importante da empresa de TV a cabo. Esta central possui equipamentos para recebimento da programação televisiva (antenas parabólicas, receptores via satélite, moduladores, amplificadores e videocassetes) e para conexão com a Internet (roteadores, servidores) (SEC, 2011).

O cabeçal pode estar conectado a alguns centros de distribuição (*distribution hub*). É lá onde fica o *Cable Modem Termination System* (CMTS), que trabalha de forma análoga ao DSLAM em uma rede ADSL (SCHADEN; SILVA, 2008). Suas principais funções são demodular, rotear e modular (YRIODA, 2002). O CMTS faz a interface entre a rede de dados do provedor e a rede de distribuição que vai até a casa do assinante, podendo servir dezenas de milhares de residências (CABLE EUROPE LABS, 2009).

De acordo com o padrão DOCSIS 3.0, os CMTS podem ser da arquitetura integrada (I-CMTS – *Integrated* CMTS) ou modular (M-CMTS – *Modular* CMTS). Os da primeira têm todos os componentes necessários para sua operação integrados no mesmo equipamento. Os da arquitetura M-CMTS utilizam também um ou mais equipamentos EQAM (*Edge Quadrature*

Amplitude Modulator) e um servidor de sincronização para utilizar múltiplos canais (CISCO SYSTEMS, 2010b).

A rede de distribuição pode ser formada somente por cabos coaxiais ou ser uma rede híbrida com cabos coaxiais e fibra ótica (HFC – *Hybrid Fiber Coaxial*) (ITU-T, 2007b). No segundo caso, um nó ótico ou EQAM recebe dados do CMTS pela fibra ótica e os convertem em sinais de rádio frequência para um ou mais cabos coaxiais, que percorrem o caminho até os modems dos assinantes (ITU-T, 2006). Em geral os nós óticos estão conectados aos CMTS em uma topologia em anel (CABLE EUROPE LABS, 2009). Um mesmo nó ótico pode servir de 500 a 2.000 assinantes (BOLZANI, 2004).

Ao contrário da tecnologia ADSL, na tecnologia de acesso à Internet por cabo, diferentes assinantes compartilham um mesmo meio de transmissão, dividindo entre eles a capacidade de transmissão do segmento em que estão conectados (CABLE EUROPE LABS, 2009).

Do lado do assinante, há o modem a cabo, que recebe os sinais de rádio frequência pelo cabo coaxial e convertem-nos em sinais digitais para outro equipamento do assinante (CPE), tipicamente um computador ou roteador, por meio de interface Ethernet ou USB (ITU-T, 2007a). O modem utiliza seu endereço MAC para se autenticar no CMTS, que lhe envia parâmetros de configuração, tais como: versão do padrão DOCSIS a ser utilizada; velocidades máximas de *downstream* e *upstream*; QoS; endereço IP; *gateway*; servidores de DNS, TFTP e TOD; frequências de transmissão e parâmetros criptográficos (VOLPE, 2005).

4.3.1. Um exemplo de empresa: NET Serviços

A NET Serviços de Comunicação S.A. é uma empresa brasileira que oferece televisão por assinatura, acesso à Internet e telefonia VoIP. O serviço de acesso à Internet passou a ser oferecido pela empresa em abril de 2000 sob o nome "NET Vírtua". No final de 2010, o serviço estava presente em 90 cidades brasileiras (SEC, 2011). Já no terceiro trimestre de 2011, o NET Vírtua era o segundo maior provedor de acesso à Internet de banda larga do País e o primeiro dentre os que proveem acesso via cabo, tendo cerca de 4,2 milhões de assinantes, o que representava 26,0% de participação no mercado de Internet banda larga no Brasil (TELECO, 2012).

Em março de 2006, a NET Serviços lançou em parceria com a Embratel o serviço de telefonia denominado "NET Fone Via Embratel", que contava com 3,2 milhões de assinantes no final

de 2010 (SEC, 2011). Nesse serviço, utiliza-se a tecnologia de voz sobre IP (VoIP) para realização de chamadas.

No ano de 2008, começou a ser oferecido o "NET Vírtua 5G" em São Paulo e no Rio de Janeiro, com velocidades de até 60 Mbit/s com o uso de tecnologia DOCSIS 3.0, que permite o uso de quatro ou mais canais simultaneamente para transferência de dados.

No final de 2009, a rede da empresa tinha 5.867 nós de fibra ótica, cada um recebendo dezesseis fibras e alimentando em média 1.837 residências (SEC, 2010). A arquitetura permitia uma possível migração para uma distribuição de 250 residências por nó ótico (SEC, 2011).

Já em setembro de 2011, a empresa oferecia planos de acesso à Internet com taxas de transferência de até 100 Mbit/s (NET, 2011).

A arquitetura simplificada da rede da NET Serviços está ilustrada na Figura 4.6 a seguir (SEC, 2010).

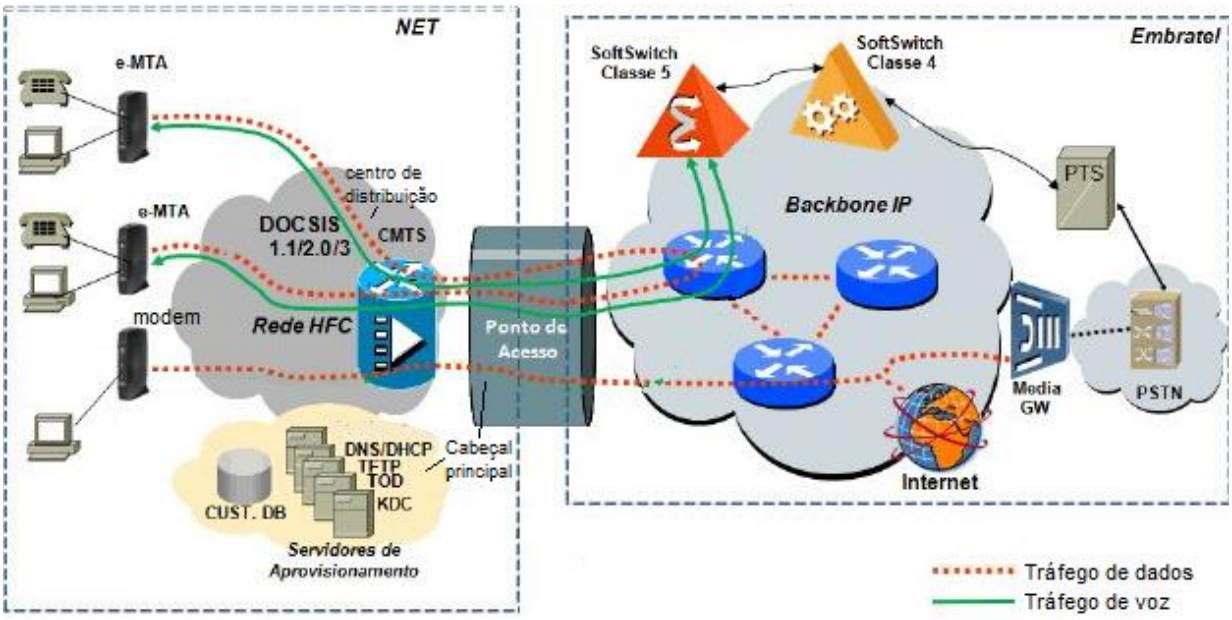


Figura 4.6 - Arquitetura simplificada da NET Serviços (SEC, 2010).

O cabeçal principal da empresa tem conexão com a Internet por meio de *backbones* da empresa Embratel. No cabeçal, há servidores de aprovisionamento, tais como *Time of Day* (TOD), *Domain Name Server* (DNS), *Dynamic Host Configuration Protocol* (DHCP), *Trivial File Transfer Protocol* (TFTP), *Key Distribution Center* (KDC) e RADIUS (SEC, 2011). O cabeçal principal também tem conexões com os centros de distribuição.

A NET usa uma rede híbrida com fibra ótica e cabos coaxiais (HFC) com cerca de 66.000 km de extensão. Grande parte dos centros de distribuição tem conexão à Internet por meio de cabos de fibra ótica dedicados da Embratel, sem compartilhamento de banda, totalizando uma capacidade total de transmissão de 45 GB/s (SEC, 2010, 2011), por onde trafegam os pacotes de dados e VoIP. Desses centros de distribuição, são enviados sinais luminosos por meio de cabos óticos até os nós óticos, que os convertem para sinais de RF para serem transmitidos pelos cabos coaxiais. Estes cabos são subdivididos até chegar às instalações dos assinantes, que têm equipamentos tais como modems a cabo, e-MTAs, roteadores sem fio e decodificadores (SEC, 2011).

4.3.1.1. Os CMTS

Em matéria de equipamentos, a NET utiliza CMTS de diferentes marcas, como Arris (ARRIS, 2008), Cisco (NET, 2008) e Motorola (LR CABLE, 2009). Unidades do CMTS Arris C4 foram adquiridas pela empresa em 2008 (ARRIS, 2008). No final do mesmo ano, CMTS Cisco uBR10012 passaram a ser utilizados com o objetivo de que fossem oferecidas velocidades de até 60 Mbit/s no Rio de Janeiro (NET, 2008). Já no ano seguinte, foi anunciada a compra de unidades do CMTS Motorola BSR6400 (LR CABLE, 2009).

Os CMTS Cisco uBR10012, que utilizam o sistema operacional IOS, são compatíveis com a legislação estadunidense de interceptação de dados CALEA (CISCO SYSTEMS, 2011). Por meio do comando "*cable intercept*", é possível direcionar todo o tráfego oriundo ou destinado a um determinado modem a cabo, baseado em seu endereço MAC e interface do CMTS, para uma estação de coleta de dados. Os pacotes são encapsulados no protocolo UDP e redirecionados para uma determinada porta da estação de coleta (CISCO SYSTEMS, 2011). Além disso, o comando "show packetcable event df-group" mostra informações sobre os servidores com a Função de Entrega (*Delivery Function* – DF) que estejam configurados no CMTS, para recebimento de mensagens de eventos e tráfego (CISCO SYSTEMS, 2011).

4.3.1.2. Roteadores e outros equipamentos

Algumas das marcas de roteadores utilizadas pela NET são Cisco e Huawei, com uso dos modelos Cisco 7606 e 7206, por exemplo.

Os roteadores da série Cisco 7600 oferecem suporte ao CALEA e o J-STD-025-B a partir da versão 12.2SRB do Cisco IOS (CISCO SYSTEMS, 2007a). A interceptação pode ser feita por diferentes atributos dos pacotes IPv4, tais como endereço IP de origem, destino ou ainda uma faixa de endereços. O tráfego interceptado é encapsulado em pacotes UDP e encaminhado para um dispositivo de mediação. Por sua vez, os roteadores Cisco 7206, com o IOS versão 12.4(4)XD ou superior, também oferecem suporte a interceptação de dados trafegados (CISCO SYSTEMS, 2007b).

Também são utilizados servidores DHCP da Cisco e Incognito, além de *switches* da Foundry, Cisco, Extreme e Summit. Além desses, o *switch* "Arbor Networks Ellacoya E30" é utilizado em alguns pontos de sua rede entre seus CMTS e os roteadores de borda.

4.4. PROVEDOR POR CONEXÃO DISCADA

O acesso à Internet por meio de uma conexão discada é ainda muito popular no País entre as classes sociais menos favorecidas da população (CETIC.BR, 2010). Os clientes dessa tecnologia fazem grande uso do acesso à noite, principalmente de meia-noite às seis da manhã ou outros horários de tarifação reduzida, quando algumas operadoras de telefonia cobram um valor fixo para manter a conexão, independente da sua duração (FÄRBER; BODAMER; CHARZINSKI, 1998).

A tecnologia é também utilizada por alguns sistemas para contingência no acesso à grande rede, ou seja, quando outras conexões estejam fora do ar.

A linha telefônica fica ocupada quando em uso para transmissão de dados, não podendo ser utilizada simultaneamente para serviços de voz. As taxas de transmissão por meio dessa tecnologia chegam normalmente a 56 kbit/s.

Os principais elementos envolvidos nesse tipo de conexão podem ser vistos na Figura 4.7.

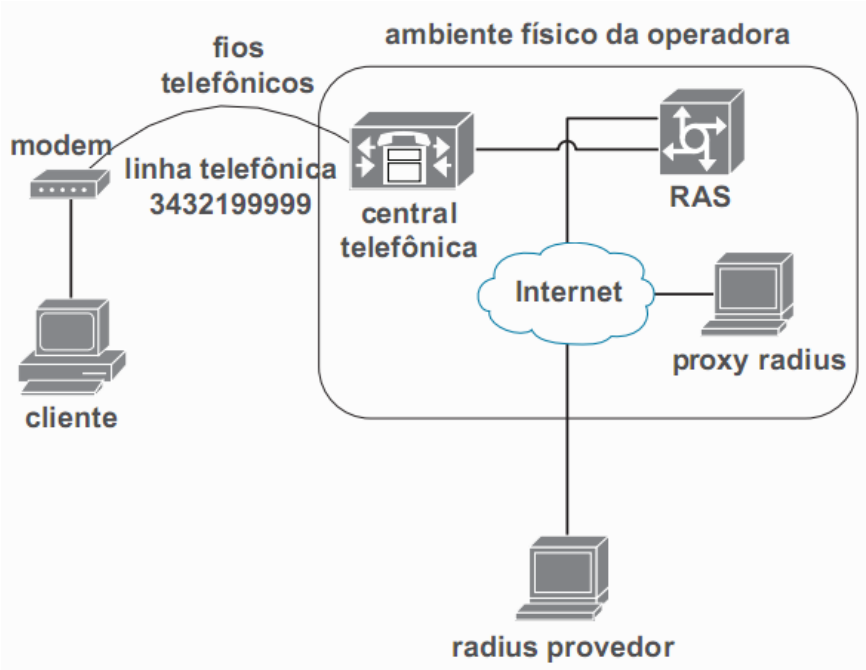


Figura 4.7 - Topologia de acesso à Internet através de conexão discada (SCHADEN; SILVA, 2008).

Para estabelecer sua conexão à rede mundial de computadores, o usuário precisa ter um modem, que fica ligado ao seu computador e a uma linha telefônica. O modem fará a modulação e demodulação dos dados enviados por meio da linha telefônica, que vai de seu imóvel até a central telefônica da operadora.

A central possui uma ligação com o *Remote Access Server* (RAS), que demodula os dados recebidos do modem do usuário. Além disso, o RAS possui os parâmetros de configurações dos endereços IP que podem ser alocados aos usuários, assim como os endereços dos servidores RADIUS, que gerenciam a autenticação dos usuários. Tipicamente, para se conectar, um usuário informa um número telefônico de conexão, juntamente com seu nome de usuário e senha. Estas credenciais são enviadas por meio da linha telefônica até a central da operadora de telefonia, que verifica o número telefônico de conexão e encaminha a chamada utilizando este número para o RAS. Este recebe a chamada e negocia os parâmetros de conexão com o modem do usuário.

Caso esta negociação seja bem sucedida, o RAS identifica o equipamento para o qual deve encaminhar as credenciais de autenticação do usuário para validar o acesso. As credenciais normalmente são enviadas para um servidor RADIUS da operadora de telefonia chamado Proxy RADIUS, que as repassa para autenticação a um servidor RADIUS do provedor de acesso à Internet ao qual o usuário está vinculado.

Caso haja uma confirmação da autenticação, o servidor RADIUS do provedor encaminhará ao Proxy RADIUS da operadora a resposta positiva que em seguida será encaminhada ao RAS, para que este tenha conhecimento do sucesso da autenticação. Posteriormente, o RAS aloca um endereço IP ao usuário, que receberá um endereço para acessar a Internet. A conexão é então estabelecida e será gerado um bilhete de início de conexão para o Proxy RADIUS e para o servidor RADIUS do provedor (SCHADEN; SILVA, 2008).

4.5. PROVEDOR POR GPRS/EDGE/3G

Para permitir uma conexão móvel à Internet, alguns provedores do Serviço Móvel Pessoal (SMP) utilizam tecnologias de transmissão sem fio, tais como o GPRS (*General Packet Radio Service*), EDGE, HSPA, HSPA+ e UMTS (*Universal Mobile Telecommunication System*) (EKEROTH; HEDSTRÖM, 2000).

As tecnologias GPRS e UMTS são consideradas uma evolução do *Global System for Mobile Communications* (GSM) (CISCO SYSTEMS, 2010a). O GSM é o padrão de comunicação sem fio mais utilizado no mundo. Ele é utilizado predominantemente na Europa, Ásia e América do Sul.

O GPRS é um padrão de comunicação 2,5G definido pelo ETSI e 3GPP (*Third Generation Partnership Program*) que permite que provedores de serviço ofereçam a seus assinantes serviços de dados baseados em pacotes por meio de uma rede GSM. Alguns desses serviços são: acesso à Internet e a intranets corporativas; comunicação instantânea; mensagens multimídia.

Quando o GPRS é combinado com o EDGE, tem-se o EGPRS, que permite taxas de transferência de até 200 kbit/s, atingindo os requisitos de velocidade do IMT2000 para 3G. No entanto, o EDGE é comumente oferecido como uma tecnologia “2,5G” (AQSACOM, 2010a).

O UMTS, por sua vez, é uma tecnologia de comunicação móvel de terceira geração (3G) definida pelo 3GPP, que utiliza o WCDMA (*Wide-band Code Division Multiple Access*), o TD-SCDMA, HSPA ou ainda o HSPA+. O UMTS permite maiores taxas de transmissão que o GPRS, podendo chegar ao limite teórico de 84 Mbit/s (AQSACOM, 2010a). A tecnologia suporta serviços em tempo real, qualidade de serviço fim-a-fim e foi projetado para transmitir fotos, vídeos, conteúdo multimídia, voz e dados aos assinantes (CISCO SYSTEMS, 2010a).

O diagrama de uma rede GPRS/UMTS foi exibido na Figura 4.8.

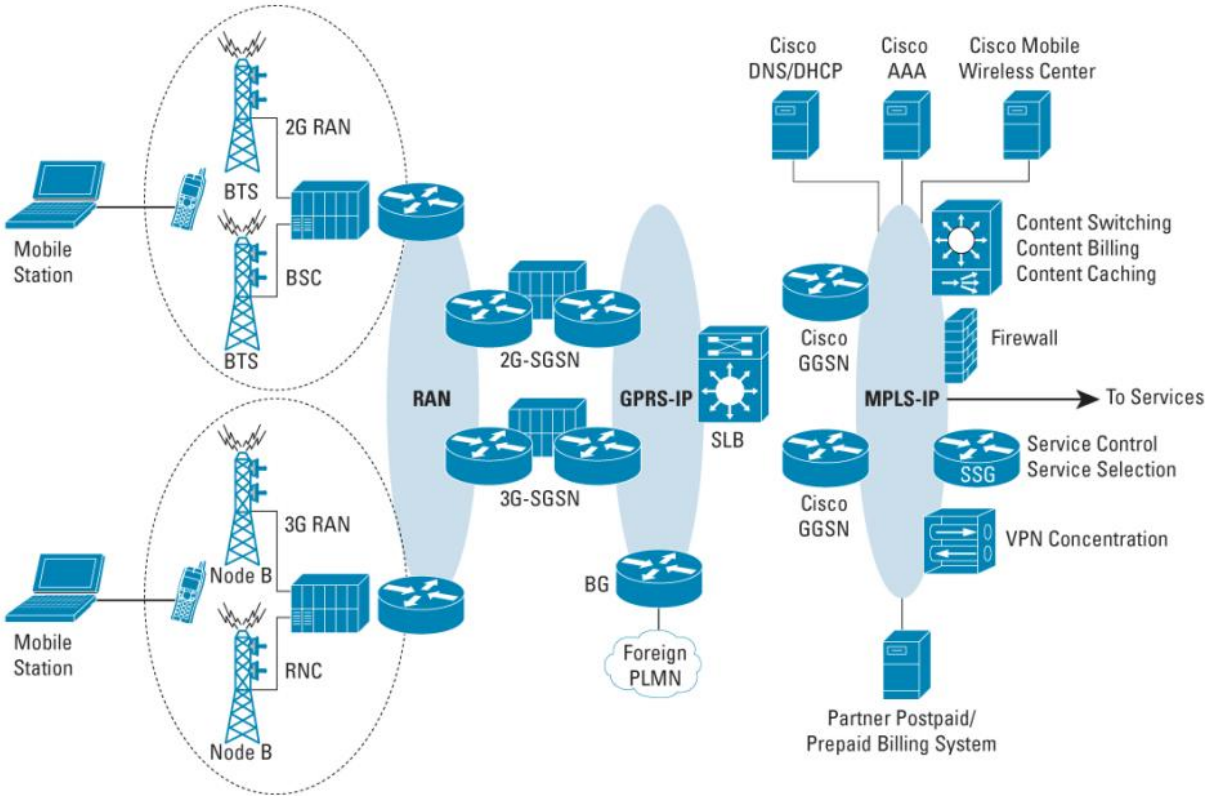


Figura 4.8 - Componentes de uma rede GPRS/UMTS (CISCO SYSTEMS, 2010a).

Conforme mostrado na Figura 4.8, a Rede de Acesso de Rádio (*Radio Access Network* – RAN) é composta por componentes diferentes em uma rede GPRS (2,5G) e uma UMTS (3G). Na primeira, a RAN é formada por clientes móveis que se conectam a uma Estação Base Transceptora (*Base Transceiver Station* - BTS), que por sua vez está conectada a um Controlador de Estação Base (*Base Station Controller* – BSC). Por outro lado, em uma rede UMTS, a RAN é composta por clientes móveis que se conectam a um *NodeB*, que então está ligado a um Controlador de Rede de Rádio (*Radio Network Controller* – RNC) (CISCO SYSTEMS, 2010a).

Os principais elementos do núcleo da rede são o *Serving GPRS Support Node* (SGSN) e o *Gateway GPRS Support Node* (GGSN). Os SGSNs roteiam pacotes com origem e destino da rede celular enquanto os GGSNs fazem a interface com a rede IP externa e a Internet (EKEROTH; HEDSTRÖM, 2000), por meio de um *gateway* de borda (*Border Gateway* – BG) (TATEOKI, 2007). O SGSN conecta a RAN ao núcleo da rede GPRS/UMTS e direciona os dados das sessões dos usuários para o GGSN. Dentre as funções do SGSN, estão: enviar e receber dados das estações móveis (MS), gerenciar sessões de usuários; cifrar e decifrar

informações transmitidas, manter informação da localização dos clientes móveis para *roaming* e mudança de estação base (EKEROTH; HEDSTRÖM, 2000). Além disso, o SGSN faz a interface entre as estações móveis e o GGSN. Este, por sua vez, é um *gateway* para rede IP privada do provedor e para a Internet. Além disso, é responsável pela alocação de endereços IP aos clientes móveis. Os endereços podem ser fornecidos diretamente pelo GGSN por meio de DHCP ou ainda por meio de um servidor RADIUS escolhido (CISCO SYSTEMS, 2010a). Neste caso, o GGSN contém um cliente que fornece ao servidor RADIUS informações de autenticação do cliente, que fornecerá um endereço IP caso a autenticação seja bem-sucedida (EKEROTH; HEDSTRÖM, 2000).

A RAN se conecta ao núcleo da rede GPRS/UMTS por meio de um SGSN, que encaminha as sessões de usuário ao GGSN, que funciona como um *gateway* para as redes de serviços e Internet (CISCO SYSTEMS, 2010a). Esse encaminhamento é feito por meio do encapsulamento de pacotes em um protocolo de tunelamento chamado *GPRS Tunneling Protocol* (GTP), que roda sobre o IP. O núcleo da rede GPRS/UMTS pode ser formado por redes IP ou MPLS, dependendo da operadora (CISCO SYSTEMS, 2010a).

4.6. SÍNTESE DO CAPÍTULO

Neste capítulo, foram apresentadas estruturas e características técnicas das principais tecnologias utilizadas para provimento de acesso à Internet no Brasil. Foram citados alguns exemplos de empresas que prestam esse serviço, com a indicação de equipamentos utilizados por elas. Tais equipamentos incorporam funções de interceptação de dados baseadas em leis e padrões internacionais. As características desses equipamentos, suas funções de interceptação e as leis e padrões com os quais eles são compatíveis foram utilizadas na definição do modelo de interceptação telemática descrito no capítulo a seguir.

5. O MODELO PROPOSTO

Este capítulo é dedicado a descrever o modelo proposto para transmissão de dados interceptados dos provedores de Internet aos órgãos de segurança pública, investigação e inteligência (OSPIIs).

Para a proposição do modelo, foram considerados três componentes principais, discutidos nos primeiros capítulos desta dissertação: a legislação e normas vigentes; soluções adotadas em outros países; a estrutura tecnológica das entidades que proveem o acesso à Internet no Brasil.

Cabe ressaltar que foi verificado que as soluções e modelos existentes internacionalmente para transmissão de dados interceptados não são totalmente adequados às peculiaridades e necessidades do País, quando observados os três componentes citados, justificando, portanto, a proposição de um novo modelo.

5.1. EXIGÊNCIAS LEGAIS

No capítulo 2 desta dissertação, foi apresentada uma descrição de leis, resoluções e normas vigentes acerca da interceptação de fluxos telemáticos no País. Os principais elementos a serem considerados na solução proposta foram listados a seguir:

- Os meios a serem empregados para a execução da interceptação devem estar contidos no pedido de interceptação, feito pela autoridade policial ou representante do Ministério Público (MP). No entanto, fica a cargo do juiz a decisão de aceitar ou redefinir os meios a serem empregados para sua execução, como recursos tecnológicos e humanos, com a indicação dos papéis a serem desempenhados pelos agentes da lei e empresas de telecomunicação envolvidas (BRASIL, 1996);
- O Judiciário deve expedir ofícios às operadoras para que deem cumprimento à decisão judicial de suspensão de sigilo das telecomunicações. Esses ofícios devem conter as informações necessárias para que as operadoras possam cumprir a decisão judicial, como o número do procedimento investigativo, tipo de ação e dados do assinante (CNJ, 2008);
- Os procedimentos de interceptação devem ser conduzidos pelas forças policiais. Para realizar esses procedimentos, a autoridade policial poderá requisitar às concessionárias de serviços de telecomunicação serviços e profissionais especializados. É obrigação da

concessionária atender essa requisição, podendo ser responsabilizada criminalmente pelo seu não cumprimento (BRASIL, 1996);

- A prestadora de serviço de telecomunicações deverá cuidar do sigilo inerente aos serviços prestados e da confidencialidade dos dados trafegados e informações dos seus assinantes. Para assegurar esse direito a seus assinantes, a prestadora deverá empregar todos os meios e tecnologias necessários (ANATEL, 1998, 2001);
- A prestadora deve disponibilizar todos os recursos tecnológicos necessários para suspender o sigilo de telecomunicações, quando determinado por autoridade judiciária ou outra legalmente investida desses poderes, e disponibilizar os dados das telecomunicações requeridas de seus assinantes à autoridade que tenha sido designada para tal diligência (ANATEL, 1998, 2001);
- A prestadora de serviço de telecomunicações deve manter um controle permanente de todos os casos, acompanhar a efetivação das determinações judiciais e zelar para que elas sejam cumpridas estritamente dentro dos limites autorizados. É também sua obrigação garantir que somente o tráfego dos assinantes autorizados seja interceptado e que o prazo da quebra do sigilo não ultrapasse o determinado na ordem judicial (ANATEL, 1998);
- As operadoras de telecomunicações devem comunicar o Judiciário da data de efetivação da interceptação, para que seja controlado o prazo das medidas (CNJ, 2008);
- O MP deve ter acesso aos registros de autorizações judiciais para quebra de sigilo de comunicações. Além disso, deve fiscalizar o cumprimento e acompanhar a realização das atividades de interceptação junto aos órgãos policiais e provedores de acesso à Internet (BRASIL, 1996; CNMP, 2007);
- O resultado da interceptação, com o inteiro teor das comunicações interceptadas, deverá ser encaminhado ao Juiz para sua ciência, com um resumo das ações realizadas (BRASIL, 1996; CNJ, 2008).

5.2. LIMITAÇÕES DOS MODELOS EXISTENTES

No capítulo 3 desta dissertação, foram apresentados alguns dos principais modelos existentes para entrega de dados interceptados, notadamente os contidos nos padrões do ETSI, ANSI J-STD-025-B e TIIT. Mostrou-se também o contexto legal em que eles estavam situados.

No entanto, existem algumas peculiaridades do sistema brasileiro que impedem a adoção desses modelos de forma direta. A seguir, foram elencadas as principais características que demandariam ajustes para sua implementação no País.

5.2.1. Padrões e especificações técnicas do ETSI

Nos padrões ETSI ES 201 158, ES 201 671 e nas especificações técnicas TS 101 331 e TS 101 671 e da série TS 102 232, os órgãos judiciários enviam a ordem para interceptação telemática ao OSPII que o solicitou. No entanto, conforme resolução do CNJ (CNJ, 2008), essa determinação judicial é enviada pelo Poder Judiciário diretamente à empresa de telecomunicações responsável pela execução da interceptação da comunicação de seus assinantes.

Ainda de acordo com os normativos brasileiros, outra comunicação direta que deve ocorrer entre as operadoras de telecomunicações e o Judiciário é a relativa à data de efetivação da interceptação (CNJ, 2008).

De acordo com os padrões do ETSI, não há qualquer comunicação direta entre a autoridade que fornece a autorização legal e os prestadores de serviço de comunicação ou provedores de acesso.

Além disso, não há qualquer menção nos documentos do ETSI de algum órgão que também pudesse ter acesso às informações sobre as interceptações, que é o papel de controle externo à atividade policial desempenhado pelo Ministério Público (MP). De acordo com nossa legislação, o MP também pode solicitar à autoridade judicial autorização para uma interceptação, o que não é previsto pelo ETSI.

Outra questão que deve ser apontada é que, nos documentos do ETSI, não há qualquer previsão de envio do conteúdo interceptado a outro destino que não seja uma central de monitoramento de um órgão de segurança (LEMF). No entanto, de acordo com requisitos legais do País, o inteiro teor das comunicações interceptadas deve ser encaminhado ao Poder Judiciário (BRASIL, 1996; CNJ, 2008).

5.2.2. Diretivas e especificações da Alemanha, Holanda e Reino Unido

Em termos gerais, tais documentos apresentam as mesmas limitações dos documentos definidos pelo ETSI, nos quais foram baseados.

A diretiva técnica alemã (ALEMANHA, 2003) é a menos avançada, quando afirma que as ações para monitoramento de telecomunicações em redes por comutação de pacotes devem ser definidas caso a caso, em comum acordo entre a agência de monitoramento e o provedor de serviço de comunicação.

Apesar de suas inadequações com o sistema legal brasileiro, a especificação técnica holandesa (HOLANDA, 2002) se destaca positivamente pela importância dada às rotinas de segurança em todas as atividades executadas relativas à interceptação de dados. São constantemente utilizadas funções de autenticação dos dados e das entidades envolvidas. Outro ponto importante é que as transmissões de dados são feitas sempre por meio de canais seguros. Além disso, algoritmos e suítes criptográficas são especificadas no padrão, todas de padrões abertos e com bom nível de segurança.

A especificação britânica (REINO UNIDO, 2002) inova por distinguir o conteúdo interceptado em fluxos e lotes. No entanto, para o escopo dessa dissertação, somente o tratamento dado aos fluxos é considerado, área em que a especificação não apresenta nenhuma contribuição relevante.

5.2.3. O padrão ANSI J-STD-025-B

Ao contrário dos documentos do ETSI, o padrão ANSI J-STD-025-B prevê que a ordem judicial para interceptação telemática seja encaminhada simultaneamente ao OSPII e à empresa de telecomunicações, o que satisfaz parte dos requisitos do CNJ (CNJ, 2008).

A Função de Entrega do padrão dá suporte ao envio da comunicação interceptada a uma ou mais Funções de Coleta. Estas funções, no entanto, só são previstas de serem implementadas em OSPIIs (LEAs). Dessa forma, frustram requisitos legais brasileiros, como a necessidade de encaminhamento ao Judiciário do inteiro teor das comunicações interceptadas (BRASIL, 1996; CNJ, 2008) e ainda o envio das informações sobre as interceptações ao Ministério Público (CNMP, 2007).

Outro ponto a ser ressaltado é que o ANSI J-STD-025-B não tem como requisito uma comunicação confiável entre as Funções de Coleta e Entrega de dados, inviabilizando uma correta cadeia de custódia, com rastreabilidade e garantia de autenticidade e integridade do tráfego utilizado como vestígio (DIAS FILHO, 2009). O padrão não requer, desta maneira, qualquer validação de que o que está sendo enviado pelo provedor é o mesmo que está sendo

recebido pelo órgão policial. Ademais, não há verificação de integridade das mensagens do protocolo LAESP. Dessa forma, um congestionamento do canal CDC pode gerar a corrupção ou perda de mensagens.

Além disso, como as mensagens do protocolo LAESP não contêm uma numeração sequencial, sua perda pode não ser detectada pelo OSPII que recebe os dados. Finalmente, já que as mensagens do protocolo LAESP definem o início e fim das ligações e conexões, a perda dessas mensagens pode causar falhas na gravação do conteúdo dos fluxos de dados e áudio de chamadas (SHERR et al., 2009).

5.3. PRINCIPAIS REQUISITOS DO MODELO PROPOSTO

O modelo de entrega de dados interceptados proposto tem como principais requisitos:

- Estar de acordo com as necessidades impostas pela legislação e normas vigentes, apontadas no capítulo 2 e na seção 5.1;
- Adotar as melhores práticas do padrão ANSI J-STD-025-B e dos padrões especificações técnicas do ETSI e TIIT, utilizando-os como referência e aplicando as alterações necessárias;
- Os provedores devem assinar digitalmente o conteúdo capturado por eles, para que posteriormente seja possível verificar sua autenticidade e integridade. Assim, pode-se garantir que os dados foram efetivamente produzidos por aquele provedor e que nenhuma alteração foi introduzida neles;
- Os dados devem ser cifrados de forma que somente quem for autorizado possa ter acesso ao seu conteúdo (CASEY, 2004);
- Realizar autenticação mútua em todas as transmissões entre diferentes entidades;
- Minimizar o número de pessoas envolvidas nas atividades de interceptação, automatizando ao máximo as tarefas e fazendo com que elas exijam o mínimo de intervenções humanas (BROADWAY; TURNBULL; SLAY, 2008);
- Proteger as rotinas de interceptação e seus dados do acesso de pessoas não autorizadas (CASEY, 2004; LEITE, 2005);
- Gerar registros históricos para prevenir e rastrear uso malicioso de interceptações (CASEY, 2004);
- Garantir uma correta cadeia de custódia dos dados interceptados (CASEY, 2004);

- Ter o mínimo impacto na estrutura dos provedores de comunicação, aproveitar a compatibilidade de seus equipamentos com os padrões de interceptação e entrega de dados do ETSI e ANSI J-STD-025-B;
- Fazer uso preferencial de padrões abertos e de software livre;
- Adotar medidas estruturais para minimizar a perda de pacotes de dados interceptados, dando maior disponibilidade à solução e aos dados interceptados (PERON; DEUS; SOUSA JUNIOR, 2011);
- Ser escalável e modular, podendo ser ampliado por meio da incorporação de mais elementos de acordo com a demanda.

5.4. ESCOPO

A arquitetura proposta tem como objetivo definir interfaces de entrega de tráfego interceptado de redes de dados informáticos, tais como a Internet, capturado em um provedor de serviços de telecomunicações mediante uma autorização judicial, e informações sobre as interceptações. De acordo com o sistema legal brasileiro, as entidades que se relacionam com os provedores são o Poder Judiciário, o Ministério Público (MP) e órgãos de segurança pública, investigação e inteligência (OSPIIs).

Estão fora do escopo do modelo proposto:

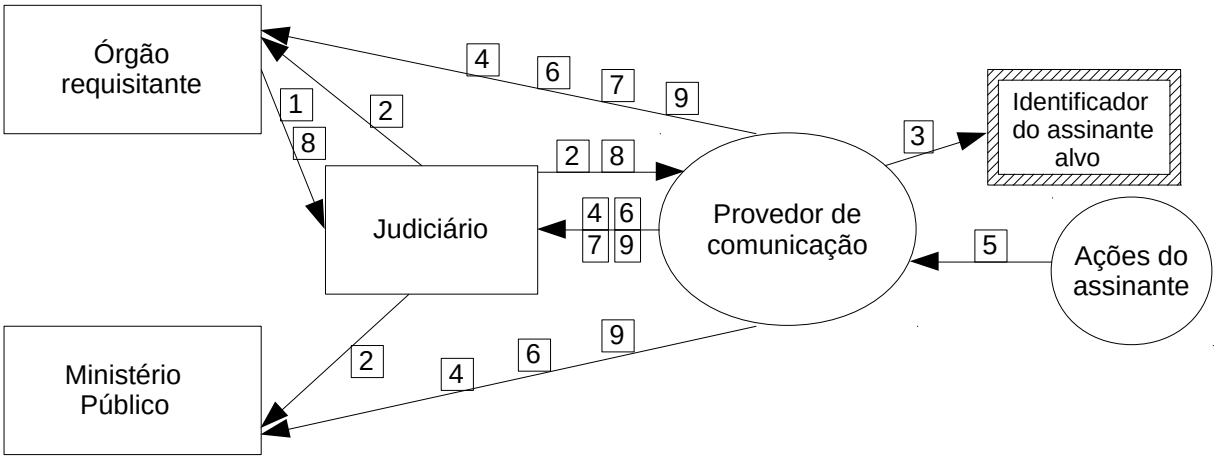
- Dados relativos a interceptações telefônicas;
- Dados diretamente extraídos da camada de aplicação, provenientes de provedores de serviços de valor adicionado, tais como provedores de conteúdo, webmail, armazenamento remoto de arquivos e instituições bancárias;
- O processamento e visualização de tráfego interceptado e informações sobre a interceptação, após seu recebimento por OSPIIs, Poder Judiciário e MP;
- As rotinas de administração das interceptações, configuração de equipamentos e acesso aos dados em provedores de serviço de telecomunicações;
- O relacionamento entre provedores de serviço de comunicação multimídia e de valor adicionado.

5.5. ARQUITETURA DO MODELO PROPOSTO

A arquitetura do modelo proposto é formada por três principais componentes: um fluxograma que contém as principais tarefas e entidades envolvidas na interceptação; a descrição da interface de entrega; a definição das entidades funcionais relativas à interface de entrega.

5.5.1. Fluxograma de rotinas desempenhadas pelas entidades

O fluxograma com as principais rotinas que devem ser executadas para realizar uma interceptação telemática é mostrado na Figura 5.1. Além disso, o relacionamento entre as entidades envolvidas e seus papéis também é apresentado e descrito em seguida.



Legenda:

1 – Solicitação de interceptação;
2 – Encaminhamento de ordem judicial;
3 – Identificação do assinante e configuração de equipamentos;
4 – Informar início da interceptação;
5 – Coleta de conteúdo da comunicação (CC) e informação referente à interceptação (IRI);
6 – Entrega de IRI;
7 – Entrega de CC;
8 – Interrupção da interceptação;
9 – Informar a interrupção.

Figura 5.1 - Fluxo de rotinas entre os principais envolvidos na interceptação telemática.

A primeira ação a ser desempenhada é o pedido de autorização judicial para interceptação telemática por uma autoridade policial ou representante do Ministério Público (MP) (1). Esse pedido deve ser encaminhado a uma autoridade judiciária competente e deve conter informações sobre o assinante cujo tráfego se queira interceptar e sobre os meios a serem empregados para a execução da interceptação.

Se a autorização for concedida, o órgão judiciário encaminhará essa autorização ao provedor de serviço de telecomunicação, ao órgão que solicitou a diligência e ao MP (2). A autorização

conterá as informações necessárias para que os provedores possam cumprir a decisão judicial, como os meios a serem empregados na interceptação, o número do procedimento investigativo, tipo de ação e os identificadores do assinante alvo, tais como seu nome, endereço residencial, linha telefônica ou endereço IP.

Em seguida, a empresa ou entidade responsável identifica seu assinante com base nas informações recebidas e realiza a configuração de seus equipamentos para a interceptação (3). Posteriormente, informa ao Judiciário, MP e órgão requisitante o recebimento da autorização, quais medidas foram adotadas e data do efetivo início da interceptação (4).

Na etapa seguinte, a informação referente à interceptação (IRI) e o conteúdo da comunicação (CC) são coletados (5). Em seguida, IRI é entregue ao OSPII requisitante, Poder Judiciário e MP (6). Adicionalmente, CC é entregue aos OSPIIs e Judiciário (7).

Finalmente, mediante pedido do OSPII ou no fim do prazo definido para interceptação, ela é interrompida (8) e sua interrupção é comunicada ao organismo de segurança, Judiciário e MP (9).

5.5.2. A interface de entrega

A interface de entrega (HI) será definida de maneira semelhante ao descrito nos padrões e especificações técnicas do ETSI, TIIT e NHIS. Ela será dividida nas três partes descritas a seguir:

- Interface de entrega 1 (HI1): utilizada para rotinas administrativas acerca das interceptações. Por meio dela são enviadas ordens judiciais, ofícios, solicitações de renovações e interrupção de interceptações, avisos de início, fim de interceptações, erros nos procedimentos e gerenciamento de chaves criptográficas. É a única interface bidirecional;
- Interface de entrega 2 (HI2): envia informação sobre a comunicação de um assinante alvo, como informações de geolocalização, eventos de início, fim e tentativas de estabelecimento de sessões e conexões;
- Interface de entrega 3 (HI3): envia o conteúdo da comunicação à central de monitoramento do OSPII, ou seja, o tráfego IP originado ou destinado ao assinante interceptado.

Caso isso produza vantagens técnicas ou econômicas, os tráfegos das interfaces HI2 e HI3 podem ser enviados por meio de um mesmo canal seguro. Entretanto, a interface HI1 necessariamente deve utilizar um canal separado.

5.5.3. Entidades funcionais

A arquitetura geral necessária para um transporte confiável para a interface de entrega foi apresentada na Figura 5.2. São utilizadas funções de *hash*, infraestrutura de chaves públicas, algoritmos de cifragem, assinatura digital, desencapsulamento, descompactação, transmissão, dentre outros.

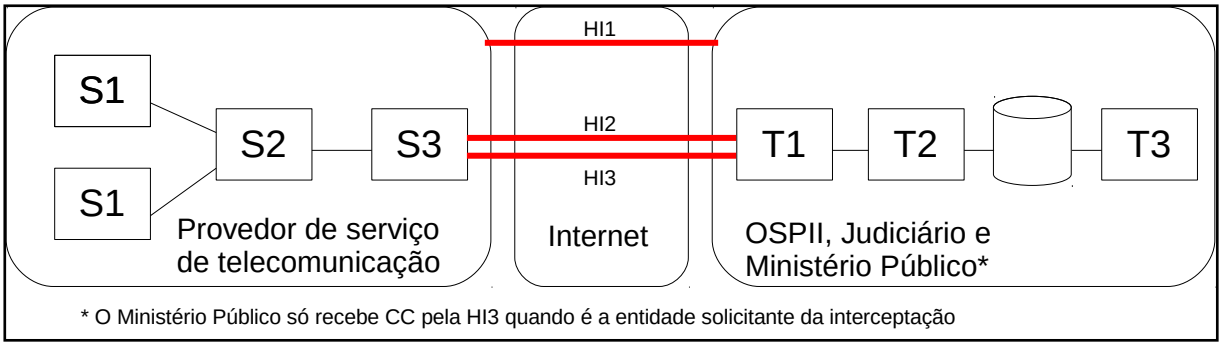


Figura 5.2 - Arquitetura geral das entidades funcionais para a interface de entrega.

Na Figura 5.2, as entidades funcionais definidas como S1, S2 e S3 implementam três funções distintas nas dependências do provedor de serviço de comunicação. S1 é o ponto de acesso de interceptação de todo o tráfego originado ou destinado ao assinante interceptado. A função S1 pode ser realizada por um programa *sniffer*, por um equipamento específico de interceptação ou ainda pela função de interceptação de um roteador ou *switch*, por exemplo.

A função S2 agrupa o tráfego de uma ou mais entidades S1 e gera um identificador temporal para cada arquivo criado contendo fluxo de tráfego interceptado. Esses arquivos devem estar descompactados, decifrados (caso a cifragem tenha sido feita no âmbito do provedor), com fluxo desencapsulado e convertido para o formato padrão “libpcap” (WIRESHARK, 2011).

Posteriormente, S2 aplica uma função de *hash* sobre os arquivos e assina digitalmente o resultado da função, cifrando-o com uma chave privada do provedor de serviços de telecomunicação, com intuito de garantir a autenticidade e integridade dos arquivos. Com isso, pretende-se dar garantia de que aqueles arquivos foram produzidos pelo provedor e adicionar mecanismos de detecção de modificação do conteúdo. Finalmente, os arquivos em

si são cifrados, utilizando os algoritmos e chaves definidos na autorização judicial, com o objetivo de que somente quem for autorizado tenha acesso ao conteúdo dos arquivos.

A função S3 gerencia conexões entre o provedor e os OSPIIs, Ministério Público e Judiciário. Além disso, encaminha os arquivos gerados pela função S2 a essas entidades e gerencia os arquivos que já foram transferidos. A função S3 deve ter como componente um servidor de transferência de arquivos.

As funções S1, S2 e S3 podem ser executadas por um único equipamento, caso isso implique em uma simplificação técnica ou economia de recursos.

Para realização dos procedimentos de forma segura, sugere-se minimamente: o algoritmo AES no modo CBC com chave de 256 bits para criptografia simétrica; o RSA com chave de 2048 bits para criptografia assimétrica; para função de *hash*, o SHA-256; um servidor de transferência de arquivos, como o SFTP sobre SSH-2, de modo que aceite conexões, autentique sessões e transfira arquivos de forma segura.

No âmbito das instalações das centrais de monitoramento dos OSPIIs, Judiciário e Ministério Público, existem as funções T1, T2 e T3. A função T1 é a de coleta de dados. Ela estabelece conexões com uma ou mais funções S3 de provedores previamente conhecidos. T2 é a função que verifica a integridade e autenticidade dos arquivos, além de decifrar e armazenar os dados interceptados. Finalmente, a T3 faz uso posterior dos dados armazenados, como, por exemplo, a análise por meio de ferramentas de interpretação e visualização de tráfego capturado.

Com o objetivo de se obter economia de recursos ou simplificação técnica, de forma análoga ao que ocorre no âmbito dos provedores, as funções T1, T2 e T3 podem ser executadas por um único equipamento.

5.6. SÍNTESE DO CAPÍTULO

Neste capítulo, foram discutidas limitações de modelos existentes internacionalmente para interceptação de dados. Além disso, foi proposto um modelo de interceptação, com a indicação de requisitos e premissas utilizadas em seu desenvolvimento, suas características gerais e o escopo de sua aplicação. A partir desse modelo foi criado um protótipo, cuja descrição e avaliação serão apresentadas no próximo capítulo.

6. IMPLEMENTAÇÃO E TESTES

A fim de avaliar o modelo proposto no capítulo anterior e testar funcionalidades, foi criado um protótipo, que foi aplicado para entrega de dados interceptados de empresas de telecomunicações que utilizam três tecnologias de transmissão diferentes para provimento de acesso à Internet.

6.1. O PROTÓTIPO

O escopo para o protótipo criado foi a execução das funções S2 e S3, que são realizadas no âmbito dos provedores de serviço de telecomunicação, e das funções T1 e T2, que são realizadas pelos OSPIIs, Judiciário e Ministério Público, conforme mostrado na Figura 6.1.

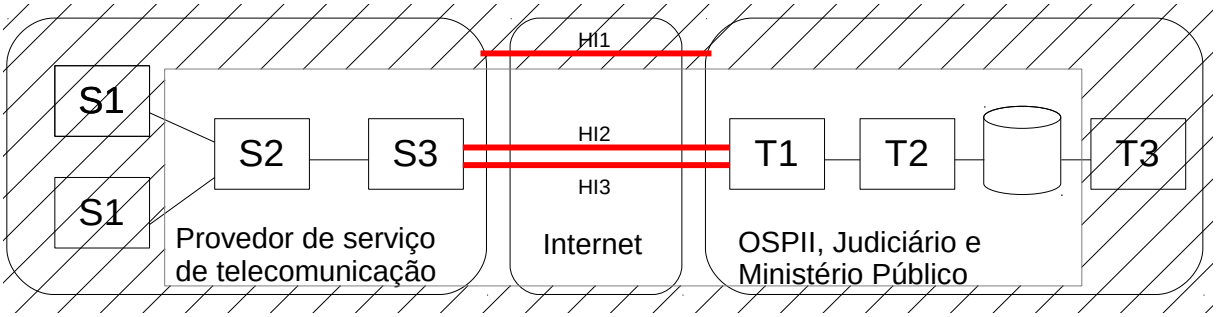


Figura 6.1 - Funções realizadas pelo protótipo, indicadas na área destacada.

O protótipo foi criado em conformidade com os seguintes provedores de serviços de telecomunicações:

- Oi (Velox) e GVT (Power), que utilizam tecnologia ADSL;
- NET Serviços (Vírtua), que utiliza a rede de TV a cabo;
- Vivo (Internet Brasil), que utiliza transmissão com tecnologia celular 3G.

Para realizar as funções S2, S3, T1 e T2, foram utilizados computadores com processador Intel Core i3 de 2,13 GHz, 4 GB de memória RAM e 500 GB de disco rígido com uma interface de rede Gigabit Ethernet. Os computadores que realizavam a função S2 tinham como diferencial a utilização de quatro interfaces de rede Gigabit Ethernet.

O sistema operacional escolhido para os equipamentos foi o “Fedora” versão 16, devido a ele ser baseado no Linux, possuir suporte a um bom número de aplicativos e funções de segurança, ter código aberto, ser gratuito e por já conter alguns dos aplicativos que seriam

utilizados. Os principais elementos de software utilizados em cada função do protótipo estão descritos em seguida.

6.1.1. A função S2

A função S2 deve receber o tráfego de uma ou mais entidades S1, que realizam a função de interceptação. Além disso, ela gera um identificador temporal para cada arquivo criado contendo fluxo de tráfego interceptado, que deve estar descompactado, decifrado, ter seu fluxo desencapsulado e convertido para o formato padrão "libpcap". Ademais, os arquivos devem ser assinados digitalmente e cifrados utilizando os algoritmos e chaves definidas na autorização judicial.

Para cada provedor, foi utilizado um conjunto de aplicativos já existentes ou especialmente desenvolvidos para realizar as tarefas desejadas, conforme descrito nas seções a seguir.

6.1.1.1. Oi (Velox)

A função S1 da prestadora Oi, que fornecia acesso à Internet via ADSL, encaminhava o tráfego do assinante interceptado em tempo real imediatamente após encapsulá-lo com o protocolo GRE (*Generic Routing Encapsulation*).

Para essa prestadora, foi criado um gerenciador de capturas, que recebia como entrada um banco de dados com as seguintes informações: o nome da estação de captura, a interface de rede de captura, endereço IP que encaminha o tráfego interceptado, identificador do assinante alvo, tamanho ou tempo máximo para gravação de cada arquivo de pacotes, data de início e fim da interceptação. Com base nesses dados, o gerenciador iniciava processos do programa "TCPDump", que faz a captura dos dados encaminhados em tempo real e grava os pacotes recebidos em arquivos. Para que os dados fossem disponibilizados para análise em tempo quase real, um novo arquivo era gerado a cada trinta segundos. Ao final do prazo para interceptação, o processo de captura era interrompido pelo gerenciador. Posteriormente, esses arquivos eram submetidos ao programa "Bittwiste", que retirava o encapsulamento GRE dos pacotes e deixava os arquivos no formato "libpcap", já desencapsulados.

Uma das interfaces de rede da máquina era utilizada para seu gerenciamento e transferência de arquivos. As outras interfaces eram utilizadas apenas para recebimento de pacotes interceptados. Estas interfaces eram configuradas de forma a não enviarem qualquer datagrama.

6.1.1.2. GVT (Power)

Para a prestadora GVT, foi utilizado um servidor de SFTP contido na suíte livre e de código aberto “OpenSSH” versão 5.8 para receber os arquivos das funções S1. Posteriormente, foram utilizados os aplicativos “Tshark” e “Bittwiste” com o intuito de converter os arquivos recebidos para o formato “libpcap”, retirando o encapsulamento PPPoE sobre VLAN do tipo IEEE 802.1Q.

6.1.1.3. NET Serviços (Vírtua)

Para a empresa NET Serviços, foi utilizado o cliente de SFTP contido no pacote “OpenSSH” versão 5.8 para coletar os arquivos com tráfego de uma ou mais funções S1, dos diferentes alvos. Posteriormente, foram utilizados os aplicativos “Tshark” e “Bittwiste”, com o objetivo de remover o encapsulamento UDP e converter os arquivos recebidos para o formato “libpcap”.

6.1.1.4. Vivo (Internet Brasil)

Para a operadora Vivo, utilizou-se o servidor de SFTP contido no pacote “OpenSSH” versão 5.8 para receber os arquivos da função S1. Posteriormente, utilizou-se o aplicativo “Editcap”, que faz parte do programa “Wireshark”, de forma a retirar a compressão “gzip” e converter os arquivos recebidos do formato “Snoop” para o formato “libpcap”.

6.1.1.5. Etapas finais

Após os arquivos estarem decifrados, desencapsulados e convertidos para o formato “libpcap”, ainda era necessário executar algumas etapas.

Para assinar digitalmente e cifrar os arquivos, utilizou-se o programa "gpg2" do sistema “GNU Privacy Guard” (GnuPG) versão 1.4.11, que implementa o protocolo OpenPGP (CALLAS et al., 2007). O "gpg2" foi utilizado com os parâmetros "--sign", "--digest-algo", "--encrypt", "--cipher-algo" e "--recipient". Foram escolhidos algoritmos que fossem considerados seguros e que fossem compatíveis com a versão 8 do PGP. Para cifragem, foi utilizado o algoritmo RSA com chaves de 2048 bits e o AES com chave de 256 bits. O algoritmo de *hash* escolhido foi o SHA-256. O RSA era utilizado com a chave privada do

provedor e as chaves públicas das entidades que receberiam o arquivo. Dessa forma, podia se garantir a autenticidade, integridade e a confidencialidade do conteúdo dos arquivos.

Em seguida, tais arquivos cifrados e acompanhados de sua assinatura eram transportados para outro computador, que realizava a função S3. Este transporte se deu por meio de um cliente SFTP, do pacote "OpenSSH".

6.1.2. A função S3

A principal atribuição da função S3 é gerenciar conexões entre o provedor e os OSPIIs, Ministério Público e Judiciário. Além disso, ela recebe os arquivos encaminhados a essas entidades pela função S2 e gerencia os arquivos que já foram transferidos.

Foi utilizado o servidor de SFTP contido na suíte "OpenSSH". Esse servidor fazia a autenticação das máquinas que faziam a função S2 e T1. Além disso, com o auxílio de um programa feito na linguagem Perl para ler os dados de uma base de dados e atualizar as configurações e permissões do servidor, fazia-se o gerenciamento de que tipo de conteúdo cada função T1 dos OSPIIs, Ministério Público e Judiciário poderia receber e o gerenciamento dos arquivos que já tinham sido transferidos.

6.1.3. A função T1

A função T1 é a de coleta de dados, implementada nos OSPIIs, Ministério Público e Judiciário. Para essa função, foi utilizado um programa feito na linguagem Perl, que acessava um banco de dados que continha uma lista de máquinas com funções S3 ao qual tinha que se conectar e buscar arquivos. Os arquivos eram baixados para a máquina local utilizando o cliente SFTP da suíte "OpenSSH".

Esses arquivos eram então encaminhados por SFTP para outra máquina, que realizava a função T2.

6.1.4. A função T2

Primeiramente, a função T2 recebia os arquivos por meio de um servidor SFTP da suíte "OpenSSH".

Depois de baixados os arquivos, eles eram decifrados com a chave privada da entidade e a chave simétrica adequada. Além disso, era feita uma validação de cada arquivo com seu *hash* e assinatura digital, de forma a conferir a integridade e a autenticidade do conteúdo recebido.

Os arquivos eram então salvos em disco em um repositório para utilização posterior.

6.2. TESTES

Os testes foram realizados em um ambiente controlado de laboratório. Simulou-se desde o momento da expedição da ordem judicial para quebra de sigilo telemático até a fase de armazenamento de arquivos para análise ou outra utilização posterior.

Foi utilizada como premissa, a condição de que os provedores conseguiriam identificar corretamente seus assinantes alvos e realizar a função S1, interceptando todo seu tráfego de Internet.

Os testes envolveram quatro provedores (Oi, GVT, NET Serviços e Vivo), dois OSPIIs (denominados "OSPII A" e "OSPII B"), um órgão fazendo o papel do Poder Judiciário e outro o papel do Ministério Público. A disposição das máquinas que realizaram as funções do protótipo e seus principais elementos de software foram apresentados na Figura 6.2.

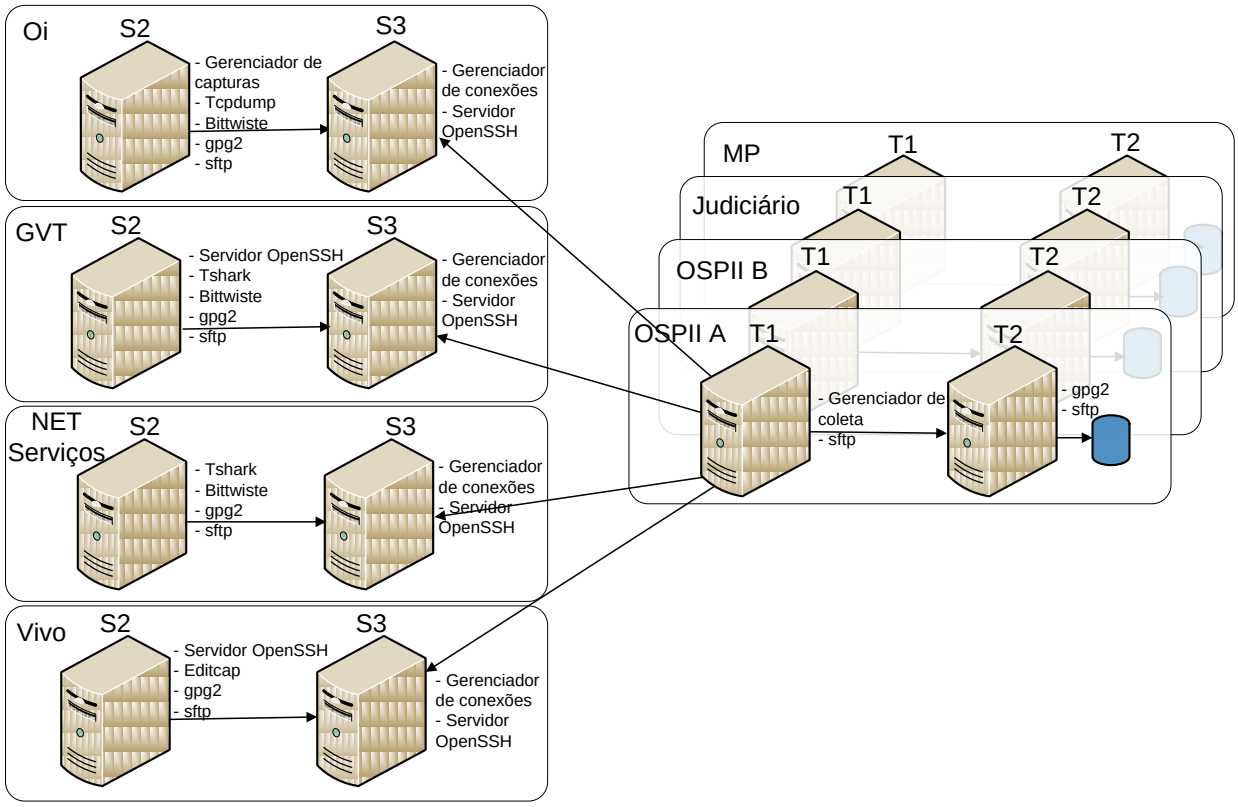


Figura 6.2 – Protótipo e principais elementos de software para realizar suas funções.

Como entrada para os testes, foram utilizados dados disponibilizados pelas prestadoras de serviços de telecomunicações, fazendo uso dos mesmos métodos efetivamente utilizados por elas em casos reais ocorridos em momentos pretéritos. Foram utilizados os tráfegos de terminais de treze assinantes, sendo dois simultaneamente acessados pelo "OSPII A" e "OSPII B", conforme Tabela 6.1.

Tabela 6.1 – Assinantes cujos terminais foram interceptados.

Assinante	Provedor	Acesso à informação referente à interceptação (IRI)	Acesso ao conteúdo da comunicação (CC)
Ass. 01	Oi	OSPII A, Judiciário, MP	OSPII A, Judiciário
Ass. 02	Oi	OSPII A, Judiciário, MP	OSPII A, Judiciário
Ass. 03	Oi	OSPII B, Judiciário, MP	OSPII B, Judiciário
Ass. 04	Oi	OSPII B, Judiciário, MP	OSPII B, Judiciário
Ass. 05	NET Serviços	OSPII A, Judiciário, MP	OSPII A, Judiciário
Ass. 06	NET Serviços	OSPII A, Judiciário, MP	OSPII A, Judiciário
Ass. 07	NET Serviços	OSPII B, Judiciário, MP	OSPII B, Judiciário
Ass. 08	NET Serviços	OSPII B, Judiciário, MP	OSPII B, Judiciário
Ass. 09	GVT	OSPII A, Judiciário, MP	OSPII A, Judiciário
Ass. 10	GVT	OSPII B, Judiciário, MP	OSPII B, Judiciário
Ass. 11	GVT	OSPII A, OSPII B, Judiciário, MP	OSPII A, OSPII B, Judiciário
Ass. 12	Vivo	OSPII A, Judiciário, MP	OSPII A, Judiciário
Ass. 13	Vivo	OSPII A, OSPII B, Judiciário, MP	OSPII A, OSPII B, Judiciário

O tráfego capturado foi processado por funções S2 de forma que, ao final, estivesse desencapsulado, decifrado e convertido para o formato padrão "libpcap". Além disso, os arquivos que armazenavam o tráfego foram assinados digitalmente, para garantir sua autenticidade e integridade, seguida da efetiva cifragem dos arquivos para impedir o acesso não autorizado do seu conteúdo.

Em seguida, as funções S3 de cada provedor gerenciaram conexões de quatro funções T1, sendo uma de cada entidade envolvida: "OSPII A", "OSPII B", Ministério Público e Judiciário.

Os arquivos foram baixados por T1 e, finalmente, foram transferidos para funções T2, que os decifraram, verificaram sua autenticidade e integridade e os armazenaram.

Todas as funções geraram arquivos com registros históricos para permitir a auditoria e a verificação dos resultados das rotinas executadas.

6.2.1. Limitações

Os testes foram realizados em um ambiente simulado de laboratório e tiveram algumas limitações. As máquinas que realizavam as funções S2 e S3 estavam instaladas em um ambiente de testes no âmbito da Polícia Federal e não nos provedores de serviços de telecomunicações. De maneira análoga, as funções T1 e T2 não foram efetivamente realizadas no Ministério Público e Judiciário.

Não se tinham disponíveis informações referentes à interceptação (IRI) das conexões interceptadas, somente o conteúdo da comunicação (CC). Dessa forma, arquivos com IRI foram gerados manualmente e enviados para S2.

Os algoritmos criptográficos e chaves não foram definidos na ordem judicial. Foram utilizados os algoritmos de cifragem de dados e *hash* recomendados, chaves simétricas aleatórias e pares de chaves assimétricas geradas especificamente para os testes.

Todas as transferências entre as funções foram feitas através de um canal seguro, assumindo que o meio era inseguro. As interfaces de rede das máquinas estavam configuradas com endereços IP válidos na Internet para a hipótese de os equipamentos não estarem dentro de uma mesma rede.

6.3. RESULTADOS E DISCUSSÃO

Finalizados os testes, verificou-se que o conteúdo interceptado recebido pelas funções S2 foi efetivamente armazenado pelas funções T2, conforme esperado.

Os testes ocorreram de acordo com os requisitos estabelecidos, com a correta transmissão dos dados entre as partes e realizando autenticação mútua entre elas. Ademais, foi seguido o fluxo de rotinas estabelecido nos dispositivos legais e utilizaram-se métodos considerados adequados com o objetivo de garantir a confidencialidade, autenticidade e integridade dos dados transmitidos. Além disso, por meio da geração de arquivos de registros históricos se tornava possível uma auditoria das rotinas. Dessa forma, os testes foram considerados bem sucedidos, conforme a Tabela 6.2, com um resumo dos requisitos propostos para o modelo.

Tabela 6.2 – Requisitos para o modelo e seu atendimento.

Requisito	Atendido
Conformidade com legislação e normas vigentes	Sim
Ter como base os padrões especificações técnicas do ANSI, ETSI e TIIT	Sim
Assinatura digital do tráfego capturado pelos provedores	Sim
Garantia de integridade, autenticidade e confidencialidade dos dados	Sim
Autenticação mútua em todas as transmissões entre diferentes entidades;	Sim
Automatização de tarefas para minimizar pessoas envolvidas	Sim
Proteção das rotinas de interceptação e seus dados do acesso de pessoas não autorizadas	Sim
Geração de registros históricos para prevenir e rastrear uso malicioso de interceptações	Sim
Garantia de cadeia de custódia dos dados interceptados	Sim
Aproveitar a compatibilidade dos equipamentos dos provedores com os padrões de interceptação do ETSI e ANSI J-STD-025-B	Sim
Uso de padrões abertos e de software livre	Sim
Adotar medidas estruturais para minimizar a perda de pacotes de dados interceptados, dando maior disponibilidade à solução e aos dados interceptados	Sim
Ser escalável e modular, podendo ser ampliado por meio da incorporação de mais elementos de acordo com a demanda.	Sim

O modelo proposto exige que sejam instalados novos elementos nos provedores de serviços de telecomunicações. Estes, de acordo com normas vigentes, têm a obrigação de fornecer todos os meios e recursos tecnológicos necessários para efetivar a interceptação de dados. Foi escolhida uma solução que fosse menos suscetível à perda de dados por indisponibilidade da central de monitoramento, congestionamento ou demais variações na Internet. Para tanto, os dados interceptados são gravados em arquivos temporariamente e passam por algumas etapas de processamento ainda no âmbito dos provedores. Ademais, na definição da arquitetura, objetivou-se que mudanças tecnológicas e reconfigurações dos equipamentos dos provedores não impactassem negativamente os procedimentos de interceptação, utilizando uma interface constante de relacionamento entre as diferentes entidades envolvidas no processo. Isto faz com que os provedores tenham a responsabilidade de possuir mecanismos que consigam interpretar os dados produzidos por seus equipamentos.

Espera-se que os benefícios gerais produzidos pela adoção de tal modelo prevaleçam sobre os custos operacionais: garantia de autenticidade e integridade da informação capturada; segurança do transporte e manipulação dos dados; aumento da capacidade de interceptação;

automatização de tarefas; otimização de recursos e maior eficiência nos OSPIIs; confiabilidade na cadeia de custódia da informação coletada. Ademais, por meio do aperfeiçoamento dos mecanismos de apuração de crimes, acredita-se que se reduza a impunidade.

7. CONCLUSÕES

Cada vez mais as pessoas utilizam mecanismos disponíveis na Internet para se comunicar. Dentre esses, se destacam correio eletrônico, comunicação instantânea, redes sociais, VoIP e *blogs*.

O acesso ao conteúdo da comunicação é uma importante ferramenta para apuração de práticas ilícitas. Esse acesso pode ser obtido por meio da interceptação telemática dos fluxos de dados e de comunicações pelo sistema telefônico tradicional.

Os órgãos de segurança pública, investigação e inteligência (OSPIIs) têm grande capacidade de interceptar o conteúdo de comunicações telefônicas. No entanto, o mesmo não ocorre com a interceptação de dados telemáticos. O que se observa é a falta de métodos e ferramentas que garantam a agilidade da execução de interceptações telemáticas, a integridade dos dados capturados e a facilidade de operação por parte dos agentes da lei. Ademais, em razão da inexistência de uma cadeia de custódia confiável e de garantias de autenticidade e integridade do tráfego interceptado, com frequência tal tráfego é desconsiderado como prova no processo criminal, o que frustra trabalhos de investigação e promove a impunidade.

Em grande parte, esse cenário é decorrente da falta de padronização dos métodos utilizados pelos provedores de serviço de telecomunicação para repassar os dados interceptados aos OSPIIs. Outros pontos negativos são a diversidade de formatos de dados utilizados e a frequente necessidade de adaptação de mecanismos de interceptação, causada por aquisições de equipamentos e mudanças nas configurações dos provedores.

Foram então pesquisadas as leis e normativos sobre a interceptação de dados telemáticos em nosso País e as tecnologias utilizadas atualmente para provimento de acesso à Internet. Posteriormente, foram avaliadas as soluções adotadas internacionalmente, para que fossem aplicadas diretamente ou servissem de referência para a criação de um modelo para transmissão de dados interceptados. Verificou-se então que os padrões existentes internacionalmente não atendiam a requisitos legais e técnicos brasileiros.

Neste trabalho, foi apresentado um modelo para entrega de dados de Internet interceptados pelas operadoras de telecomunicações. Para sua definição, foram considerados os requisitos legais e normativos brasileiros, os modelos e mecanismos utilizados em outros países, a estrutura das empresas de telecomunicações brasileiras que fornecem o acesso à rede mundial

de computadores e ainda algumas boas práticas da segurança da informação. Foram então definidos alguns requisitos para tal modelo.

A partir da especificação do modelo, foi feita a implementação de um protótipo para intermediar a relação entre os entes envolvidos em uma interceptação de dados telemáticos (Poder Judiciário, Ministério Público, OSPIIs e provedores de serviços de telecomunicação) e transferir dados entre as partes. O protótipo foi criado pela junção de ferramentas de software livre disponíveis e ainda programas que foram especialmente desenvolvidos para executar algumas das rotinas adicionais necessárias.

O protótipo foi utilizado em um ambiente de testes, que abrangia dados de quatro provedores de Internet que utilizavam algumas das tecnologias predominantes no País: ADSL, cabo e 3G. Foi então feita uma simulação de interação entre as partes envolvidas em uma interceptação, englobando as transferências de dados entre elas.

Os testes foram considerados bem sucedidos, tendo em vista que ocorreram conforme os requisitos estabelecidos. Houve a correta transferência dos dados entre as partes, que se autenticaram mutuamente, e foi seguido o fluxo de rotinas estabelecido na legislação nacional. Além disso, foram utilizadas rotinas criptográficas que objetivaram garantir a confidencialidade, autenticidade e integridade dos dados transmitidos. Por meio desses testes, foi mostrada a adequação do modelo proposto.

As principais dificuldades encontradas foram quanto à realização de testes que conseguissem efetivamente simular situações que se aproximassem de casos reais. O modelo proposto envolvia diferentes entidades. No entanto, não foi possível que as ações efetivamente fossem realizadas por todas elas. Além disso, pelo fato de a interceptação telemática se tratar de um tema sensível e com muitas restrições legais, havia rígidas restrições para que não houvesse perda de dados ou quebra de sigilo durante os testes. Outra questão é que não foi possível introduzir equipamentos nos diferentes órgãos que participariam do processo. Um ponto que também impactou significativamente o desenvolvimento do trabalho foi a dificuldade de se obter informações. Por um lado, os órgãos de segurança pública, investigação e inteligência não revelam ou documentam abertamente seus procedimentos e dificuldades enfrentadas. Já os provedores, por questões de estratégia competitiva e segredo industrial, não divulgam abertamente seus equipamentos e tecnologias utilizadas. Além desses pontos levantados, foi um grande desafio compatibilizar o modelo proposto com a grande quantidade de leis e

normas acerca do tema, produzidas por diferentes órgãos e poderes, com distintos pontos de vista, e elaboradas em épocas diversas.

É notório que a adoção do modelo proposto demandaria a introdução de novos equipamentos e rotinas nos provedores de serviços de telecomunicação e outras entidades envolvidas. Isto certamente demandaria investimentos por tais empresas e órgãos. No entanto, espera-se que os benefícios gerados pela adoção do modelo preponderem sobre os custos: mecanismos para garantir autenticidade e integridade da informação capturada; transporte e manipulação segura dos dados; ampliação da capacidade de interceptação; automatização de tarefas; melhoria na utilização de recursos e maior eficiência nos OSPIIs; manutenção da cadeia de custódia da informação coletada. Além disso, em decorrência do aperfeiçoamento dos mecanismos de apuração de crimes, é possível que se reduza a impunidade.

7.1. TRABALHOS FUTUROS

Como trabalho futuro, sugere-se que o modelo proposto seja testado para outros provedores de acesso à Internet, principalmente os que utilizam tecnologias diferentes das que foram testadas. Complementarmente, poderiam ser feitos testes de estresse do protótipo a fim de dimensionar requisitos de hardware e capacidade de transmissão para sua utilização em um ambiente de produção.

Além disso, a validação e a verificação de integridade de dados interceptados poderiam ser também aplicadas nos sistemas de interceptação de chamadas telefônicas, o que minimizaria questionamentos sobre a autenticidade e integridade das gravações utilizadas como provas e, consequentemente, a protelação e invalidação de processos criminais.

Outro possível trabalho seria a agregação de técnicas de identificação de dispositivos (*device fingerprinting*) para associar tráfegos interceptados a equipamentos específicos. Isso poderia ser obtido por meio da utilização de assimetrias de *clock* dos processadores, refletidas nos valores da opção *Timestamps* do TCP, contidos em pacotes capturados (KOHNO; BROIDO; CLAFFY, 2005).

Finalmente, tendo como base as contribuições desta dissertação, a Agência Nacional de Telecomunicações, em conjunto com as entidades envolvidas, poderia especificar uma norma que determinasse como os prestadores de serviço de telecomunicações deveriam entregar os dados aos OSPIIs.

REFERÊNCIAS BIBLIOGRÁFICAS

AGÊNCIA ESTADO. PNBL terá que ofertar 5 Mbps até 2014. **Info Online**, 2011. Disponivel em: <http://info.abril.com.br/noticias/tecnologia-pessoal/pnbl-tera-que-ofertar-5-mbps-ate-2014-01072011-2.shl>. Acesso em: 01 jul. 2011.

ALEMANHA. **Technical Directive: Requirements for implementing statutory telecommunications interception measures V4.0**. Regulatory Authority for Telecommunications and Post. Berlin, p. 102. 2003. (TR TKÜ).

ANATEL. **Norma 004/95**. Agência Nacional de Telecomunicações. Brasília. 1995.

ANATEL. **Resolução nº 73, de 25 de novembro de 1998**. Agência Nacional de Telecomunicações. Brasília, p. 27. 1998.

ANATEL. **Resolução nº 272, de 9 de agosto de 2001**. Agência Nacional de Telecomunicações. Brasília, p. 21. 2001.

ANATEL. **Estudo Técnico para Atualização da Regulamentacao das Telecomunicações no Brasil**. Agência Nacional de Telecomunicações. Brasília, p. 245. 2008a.

ANATEL. **Informe nº 427/2008/PBCPD/PVCPC/CMLCE/PBCP/PVCP/ CMLC/SPB/SPV/SCM**. Agência Nacional de Telecomunicações. Brasília, p. 165. 2008b.

ANSI. **ANSI J-STD-025-B**. American National Standards Institute. Washington, p. 268. 2006.

AQSACOM. **The USA Patriot Act**. Aqsacom Incorporated. Washington, p. 10. 2006.

AQSACOM. **Lawful Interception for 3G and 4G Networks**. Aqsacom Incorporated. Washington, p. 36. 2010a. (100458).

AQSACOM. **Lawful Interception for IP Networks White Paper**. Aqsacom Incorporated. Washington, p. 40. 2010b.

ARRIS. NET Servicos Selects ARRIS C4 CMTS to Expand Its High Speed Data & VoIP Service in Brazil. **ARRIS - Press/Events**, 2008. Disponivel em: <http://www.arrisi.com/press_events/press_releases/pressdetail.asp?id=405>. Acesso em: 10 ago. 2011.

BALOO, J. **Lawful Interception of IP Traffic: The European Context**. Las Vegas, p. 42. 2003.

BANDEIRA, G. **A Interceptação do Fluxo de Comunicações por Sistemas de Informática e Sua Constitucionalidade**. Universidade Estácio de Sá. Rio de Janeiro, p. 15. 2002.

BERKOWITZ, H. et al. **RFC 4098: Terminology for Benchmarking BGP Device Convergence in the Control Plane**. The Internet Society. Fremont, p. 36. 2005.

BITENCOURT, R. Operadoras terão 90 dias para vender internet mais barata. **Valor Econômico Online**, 2011. Disponivel em: <http://www.valoronline.com.br/impresso/empresas/102/449253/operadoras-terao-90-dias-para-vender-internet-mais-barata>. Acesso em: 01 jul. 2011.

BOLZANI, C. A. M. **Residências Inteligentes**. 1ª Edição. ed. São Paulo: Livraria da Física, 2004.

BRANCH, P. Lawful Interception of the Internet. **Australian Journal of Emerging Technologies and Society**, Melbourne, v. 1, n. 1, p. 38-51, 2003. ISSN 14490706.

BRANCH, P.; PAVLICIC, A.; ARMITAGE, G. Using MAC Addresses in the Lawful Interception of IP Traffic. **Australian Telecommunications Networks & Applications Conference**, Sydney, 8 dez. 2004. 449-452.

BRASIL. **Constituição da República Federativa do Brasil (1988)**. Brasília: Centro Gráfico do Senado Federal, 1988.

BRASIL. **Lei nº 9.296, de 24 de julho de 1996**. Presidência da República. Brasília. 1996.

BRASIL. **Lei nº 9.472, de 16 de julho de 1997**. Presidência da República. Brasília. 1997.

BROADWAY, J.; TURNBULL, B.; SLAY, J. Improving the Analysis of Lawfully Intercepted Network Packet Data Captured For Forensic Analysis. **The Third International Conference on Availability, Reliability and Security**, Barcelona, 04 mar. 2008. 1361-1368.

CABLE EUROPE LABS. **Cable Network Handbook**. Cable Europe. Bruxelas, p. 27. 2009. (CEL-TR-HFC-HANDBOOK-V4_3-091001).

CALLAS, J. et al. **RFC 4880: OpenPGP Message Format**. Network Working Group. [S.l.], p. 90. 2007. (RFC 4880).

CANADÁ. **Criminal Code (R.S.C., 1985, c. C-46)**. Department of Justice. Ottawa. 1985.

CASEY, E. Network traffic as a source of evidence: tool strengths, weaknesses, and future needs. **Digital Investigation**, Amsterdam, v. 1, n. 1, p. 28-43, fev. 2004. ISSN 1742-2876.

CECÍLIO, E. L. **Acesso residencial em banda larga**. Universidade Federal do Rio de Janeiro. Rio de Janeiro, p. 33. 2000.

CETIC.BR. **TIC Domicílios e Usuários 2010**. Centro de Estudos sobre as Tecnologias da Informação e da Comunicação. São Paulo. 2010.

CHERRY, S. M. IM Means Business. **IEEE Spectrum Online, vol. 39**, p. 28-32, 2002.

CHILE. **Decreto 142: Reglamento Sobre Interceptación y Grabación de Comunicaciones Telefónicas y de Otras Formas de Telecomunicación**. República do Chile. Santiago, p. 2. 2005.

CISCO SYSTEMS. **Internetworking Technologies Handbook**. 4. ed. San Jose: Cisco Press, 2004.

CISCO SYSTEMS. **Cisco 7600 Lawful Intercept Configuration Guide**. Cisco Systems, Inc. San Jose, p. 29. 2007a. (OL-12352-02).

CISCO SYSTEMS. **Cisco IOS Software Release 12.4(4)XD**. Cisco Systems, Inc. San Jose, p. 6. 2007b. (PB3264).

CISCO SYSTEMS. **Cisco GGSN Release 10.0 Configuration Guide**. Cisco Systems, Inc. San Jose, p. 452. 2010a. (OL-19936-05).

CISCO SYSTEMS. **Cisco DOCSIS 3.0 Downstream Solution Design and Implementation Guide**. Cisco Systems, Inc. San Jose, p. 156. 2010b. (OL-10705-06).

CISCO SYSTEMS. **Cisco 10000 Series Router Lawful Intercept Configuration Guide**. Cisco Systems, Inc. San Jose, p. 22. 2010d. (OL-3426-06).

CISCO SYSTEMS. **Cisco IOS CMTS Cable Command Reference**. Cisco Systems, Inc. San Jose, p. 2470. 2011. (OL-15510-14).

CLAYTON, R. The Limits of Traceability. **University of Cambridge**, 2001. Disponivel em: <http://www.cl.cam.ac.uk/~rnc1/The_Limits_of_Traceability.html>. Acesso em: 12 jul. 2009.

CNJ. **Resolução nº 59, de 09 de agosto de 2008**. Conselho Nacional de Justiça. Brasília. 2008.

CNMP. **Resolução nº 20, de 28 de maio de 2007**. Conselho Nacional do Ministério Público. Brasília. 2007.

CNT; SENSUS. **Pesquisa de Opinião Pública Nacional - Rodada 111**. Confederação Nacional do Transporte e Sensus Pesquisa e Consultoria. Brasília, p. 33. 2011.

CONSELHO DA EUROPA. **Council Resolution of 17 January 1995 on the lawful interception of telecommunications**. Conselho da Europa. [S.l.], p. 3. 1995. (96/C 329/01).

CONSELHO DA EUROPA. **Convention on Cybercrime**. Conselho da Europa. Budapeste, p. 32. 2001. (European Treaty Series - No. 185).

CONSELHO DA EUROPA. Convention on Cybercrime - CETS nº 185. **Conselho da Europa**, 2011. Disponivel em: <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=31/12/2011&CL=ENG>. Acesso em: 31 dez. 2011.

COSTA, C. O Guardião na escuta - A arma secreta da Polícia Federal. **A Notícia**, 2007. Disponivel em: <http://www.an.com.br/2007/jun/24/0pot.jsp>. Acesso em: 11 jul. 2009.

DAY, M.; J., R. **RFC 2778: A Model for Presence and Instant Messaging**. Internet Engineering Task Force. [S.l.], p. 17. 2000.

DIAS FILHO, C. R. Cadeia de custódia: do local de crime ao trânsito em julgado; do vestígio à evidência. **Revista dos Tribunais**, São Paulo, v. 98, n. 883, p. 436-451, maio 2009. ISSN 0034-9275.

EKEROTH, L.; HEDSTRÖM, P.-M. GPRS Support Nodes. **Ericsson Review No. 3**, Estocolmo, 28 ago. 2000. 156-169.

ETSI. **ETSI ES 201 158 V1.2.1: Requirements for network functions**. European Telecommunications Standards Institute. Nice, p. 27. 2002. (RES/SEC-003015).

ETSI. **ETSI ES 201 671 V3.1.1: Handover Interface for the Lawful Interception of Telecommunications Traffic**. European Telecommunications Standards Institute. Nice, p. 124. 2007. (RES/LI-00037).

ETSI. **ETSI TS 102 232-6 V2.3.1: Handover Interface and Service-Specific Details (SSD) for IP delivery - Part 6: Service-specific details for PSTN/ISDN services**. European Telecommunications Standards Institute. Nice, p. 14. 2008. (RTS/LI-00053-6).

ETSI. **ETSI TS 101 331 V1.3.1: Requirements of Law Enforcement Agencies**. European Telecommunications Standards Institute. Nice, p. 30. 2009. (RTS/LI-00062).

ETSI. **ETSI TS 102 232-4 V2.3.1: Handover Interface and Service-Specific Details (SSD) for IP delivery - Part 4: Service-specific details for Layer 2 services**. European Telecommunications Standards Institute. Nice, p. 28. 2010a. (RTS/LI-00074-4).

ETSI. **ETSI TS 102 232-5 V2.5.1: Handover Interface and Service-Specific Details (SSD) for IP delivery - Part 5: Service-specific details for IP Multimedia services**. European Telecommunications Standards Institute. Nice, p. 26. 2010b. (RTS/LI-00078-5).

ETSI. **ETSI TS 101 671 V3.8.1: Handover Interface for the Lawful Interception of Telecommunications Traffic**. European Telecommunications Standards Institute. Nice, p. 157. 2011a. (RTS/LI-00085).

ETSI. **ETSI TS 102 232-1 V2.7.1: Handover Interface and Service-Specific Details (SSD) for IP delivery - Part 1: Handover specification for IP delivery**. European Telecommunications Standards Institute. Nice, p. 50. 2011b. (RTS/LI-00086-1).

ETSI. **ETSI TS 102 232-2 V2.6.1: Handover Interface and Service-Specific Details (SSD) for IP delivery - Part 2: Service-specific details for E-mail services**. European Telecommunications Standards Institute. Nice, p. 45. 2011c. (RTS/LI-00086-2).

ETSI. **ETSI TS 102 232-3 V2.3.1: Handover Interface and Service-Specific Details (SSD) for IP delivery - Part 3: Service-specific details for internet access services**. European Telecommunications Standards Institute. Nice, p. 50. 2011d. (RTS/LI-00086-3).

ETSI. **ETSI TS 102 232-7 V2.2.1: Handover Interface and Service-Specific Details (SSD) for IP delivery - Part 7: Service-specific details for Mobile services**. European Telecommunications Standards Institute. Nice, p. 13. 2011e. (RTS/LI-00081-7).

EUA. **Communications Assistance For Law Enforcement Act - Title 47 -Telegraphs, Telephones, And Radiotelegraphs - Chapter 9 - Interception Of Digital And Other Communications**. U.S. House of Representatives. Washington. 1994. (47 U.S.C. § § 1001-1021).

FÄRBER, J.; BODAMER, S.; CHARZINSKI, J. Measurement and Modelling of Internet Traffic at Access Network. **Proceedings of the EUNICE '98 - Open European Summer School on Network Management and Operation**, Munique, p. 196-203, ago. 1998.

GALLO, M. A.; HANCOCK, B. M. **Networking explained**. 2a Edição. ed. Woburn: Digital Press, 2002.

GRUSZYNSKI, A. **Mecanismo Funcional Escalável para Contabilização de Uso de Serviços Residenciais em Rede de Acesso em Banda Larga Utilizando Tecnologia ADSL**. Universidade de Brasília. Brasília, p. 182. 2008. (PPGENE.DM-056/2008).

HANCOCK, M. Global WiMAX network deployments surpass 500. **WiMAX Forum**, 2009. Disponivel em: <http://www.wimaxforum.org/node/1724>. Acesso em: 4 out. 2010.

HENZ, L. **Proposta e Implementacao de Arquitetura para Identificação Física e Lógica de Acessos Banda Larga Utilizando Tecnologia ADSL**. Universidade de Brasília. Brasília, p. 99. 2008. (PPGENE.DM-57/2008).

HOLANDA. **Transport of Intercepted IP Traffic V1.0.0**. Directorate General for Telecommunication and Post of the Ministry of Economic Affairs. Amsterdã, p. 32. 2002. (TIIT V1.0.0 (2002-09)).

IEEE 802.16 WORKING GROUP. **IEEE Std 802.16m-2011: Part 16: Air Interface for Broadband Wireless Access Systems - Amendment 3: Advanced Air Interface**. IEEE. Nova Iorque, p. 1106. 2011. (ISBN 978-0-7381-6595-0).

ITU-T. **Downstream RF interface for cable modem termination systems**. International Telecommunication Union Telecommunication Standardization Sector. Genebra, p. 50. 2006. (ITU-T Rec.J.210).

ITU-T. **Second-generation transmission systems for interactive cable television services - IP cable modems**. International Telecommunication Union Telecommunication Standardization Sector. Genebra, p. 514. 2007a. (ITU-T Rec.J.122).

ITU-T. **Third-generation transmission systems for interactive cable television services – IP cable modems: Physical layer specification**. International Telecommunication Union Telecommunication Standardization Sector. Genebra, p. 184. 2007b. (ITU-T Rec.J.222.1).

JUNIPER. **JUNOSe Software for E Series Broadband Services Routers: Policy Management Configuration Guide, Release 11.0.x**. Juniper Networks, Inc. Sunnyvale, p. 272. 2010. (162-01708-00).

KISSWANI, N. M. Telecommunications (interception and access) and its Regulation in Arab Countries. **Journal of International Commercial Law and Technology**, Sydney, v. 5, n. 4, p. 225-239, 2010. ISSN 19018401.

KITZ. ADSL - How ADSL Works. **KITZ**, 2004. Disponivel em: <http://www.kitz.co.uk/adsl/equip.htm>. Acesso em: 2 jul. 2011.

KNIJFF, R. V. D. **Handbook of Computer Crime Investigation, Chapter 11 Embedded Systems Analysis**. [S.l.]: Academic Press, 2001.

KOHNO, T.; BROIDO, A.; CLAFFY, K. C. Remote physical device fingerprinting. **IEEE Transactions on Dependable and Secure Computing**, Oakland, v. II, n. 2, p. 93-108, abr. 2005. ISSN 15455971.

KOOPS, B.-J. Cybercrime Legislation in the Netherlands. **Country report for the 18th International Congress on Comparative Law**, Antwerp, p. 595-633, jul. 2010. ISSN SSRN-ID 1633958.

KOS, T.; GRGIC, M.; MANDIC, L. CATV broadband technologies. **4th EURASIP Conference focused on Video/Image Processing and Multimedia Communications**, Zagreb, 11 ago. 2003. 829-834 vol.2.

LAUBACH, M. Residential Area CATV Broadband Internet Technology: Current Status. **The Internet Protocol Journal**, San Jose, v. 1, n. 3, p. 13-26, dez. 1998.

LEITE, L. H. D. M. **Modelo de Interceptação Autorizada de Chamadas para o Sistema Telefônico Brasileiro**. Universidade Federal de Minas Gerais. Belo Horizonte, p. 135. 2005.

LOPES, M.; GABRIEL, M. M.; BARETA, G. M. S. **Cadeia de Custódia:** Uma Abordagem Preliminar. Curitiba: Departamento de Medicina Forense e Psiquiatria, Universidade Federal do Paraná. 2007.

LR CABLE. NET Picks Moto for Wideband. **Light Reading Cable**, 2009. Disponivel em: <http://www.lightreading.com/document.asp?doc_id=169974&site=lr_cable>. Acesso em: 10 jul. 2011.

MARCHETTI, B. R. B. Um método simples para detecção on-the-fly de arquivos e suas mutações aplicado ao combate à pedofilia e outros crimes na Internet. **Proceedings of the Third International Conference of Forensic Computer Science**, Rio de Janeiro, v. 3, n. 1, p. 31-35, jul. 2008. ISSN 1980-1114.

MIAO, Y. ADSL & PPPoE & RADIUS. **Wintersemester 2004/2005**, Freiburg, nov. 2004. 19.

MISSIUNAS, R. D. C. Controle da atividade policial pelo Ministério Público. **Consultor Jurídico**, 2009. ISSN 1809-2829. Disponivel em: <http://www.conjur.com.br/2009-fev-20/controle-externo-atividade-policial-ministerio-publico>. Acesso em: 2010 out. 20.

MONTENEGRO, M. D. H.; BUENO, F. J.; NUSDEO, L. A. D. O. **Relatório do Grupo de Atuação Especial de Controle Externo da Atividade Policial de 21 de junho de 2007**. Ministério Público do Estado de São Paulo. São Paulo, p. 19. 2007.

NET. NET Virtua 5G amplia área de cobertura e oferece banda larga mais rápida do Rio de Janeiro. **NET - Institucional - Sala de Imprensa - Press Releases**, 2008. Disponivel em: <http://netcombo.globo.com/static/html/institucional/sala_imprensa/press_release/pdf/02_-_Release_UBB_Rio.pdf>. Acesso em: 10 jul. 2011.

NET. NET - Banda Larga - Planos - Tabela Comparativa. **NET**, 2011. Disponivel em: <http://www.netcombo.com.br/netPortalWEB/appmanager/portal/desktop?_nfpb=true&_pageLabel=tabela_comparativa_page>. Acesso em: 10 set. 2011.

NUNES, M. S. D. S. **Redes de Acesso Multi-serviço**. Lisboa: Instituto Superior Técnico da Universidade Técnica de Lisboa, 2006.

OI. Banda larga - Oi Velox. **Oi**, 2012. Disponivel em: <http://www.oi.com.br/oi/oi-pra-voce/internet/planos/oi-velox-pra-casa>. Acesso em: 02 jan. 2012.

PAIVA, F. Wixx quer alcançar 20 mil clientes de WiMax em Brasília este ano. **TELETIME**, 2010. Disponivel em: <http://www.teletime.com.br/29/03/2010/wixx-quer-alcancar-20-mil-clientes-de-wimax-em-brasilia-este-ano/tt/173775/news.aspx>. Acesso em: 4 nov. 2010.

PALUDO, J.; LIMA, C. F. D. S.; ARAS, V. **Forças-Tarefas:** Direito Comparado e Legislação Aplicável. Brasília: ESMPU, 2011. 128 p. ISBN 9788588652361.

PARLAMENTO EUROPEU; CONSELHO DA EUROPA. **Directive 2006/24/EC of 15 March 2006**. Parlamento Europeu; Conselho da Europa. Strasbourg, p. 10. 2006. (COD(2005)0182).

PERON, A.; DEUS, F. E. G. D.; SOUSA JUNIOR, R. T. D. Ferramentas e Metodologia para Simplificar Investigações Criminais Utilizando Interceptação Telemática. **Proceedings of the Sixth International Conference on Forensic Computer Science**, Florianópolis, 05 out. 2011. 30-42.

PINGDOM. Internet 2010 in numbers. **Pingdom**, 2011. Disponivel em: <http://royal.pingdom.com/2011/01/12/internet-2010-in-numbers/>. Acesso em: 17 jan. 2011.

POLCAK, L. et al. Designing Lawful Interception in IPv6 Networks. **Security and Protection of Information 2011**, Brno, 2011. 114-126.

REINO UNIDO. **National Handover Interface Specification V1.0**. Home Office. London, p. 16. 2002.

RIGNEY, C. et al. **RFC 2865: Remote Authentication Dial In User Service (RADIUS)**. The Internet Society. Freemont, p. 76. 2000.

RONCAGLIA, D. Falhas técnicas invalidam grampos como prova judicial. **Consultor Jurídico**, 2008. ISSN 1809-2829. Disponivel em: <http://www.conjur.com.br/2008-jun-08/falhas_tecnicas_invalidam_grampos_prova_judicial>. Acesso em: 09 maio 2010.

SCHADEN, S.; SILVA, G. M. D. Mecanismos de Rastreabilidade de Acesso à Internet (Junho 2008). **Proceedings of the Third International Conference of Forensic Computer Science**, Rio de Janeiro, v. 3, n. 1, p. 89-96, jul. 2008. ISSN 1980-1114.

SCHWARTZ, P. M. Keeping Track of Telecommunications Surveillance. **Communications of the ACM**, v. 52, n. 9, p. 24-26, setembro 2009a. ISSN DOI 10.1145/1562164.1562175.

SCHWARTZ, P. M. Warrantless Wiretapping, FISA Reform, and the Lessons of Public Liberty: A Comment on Holmes's Jorde Lecture. **California Law Review**, v. 97, p. 407-432, abril 2009b.

SEC. **NETC Annual Report 2009 – Form 20-F**. U.S. Securities and Exchange Comission. Washington, p. 124. 2010.

SEC. **NETC Annual Report 2010 – Form 20-F**. U.S. Securities and Exchange Commission. Washington, p. 225. 2011.

SHERR, M. et al. Can They Hear Me Now?: A Security Analysis of Law Enforcement Wiretaps. **ACM Conference on Computer and Communications Security**, Chicago, n. 16, 9 nov. 2009. 512-523.

SÍCOLI, F. C. **Segurança em Redes WiMAX (IEEE 802.16)**. Universidade Federal Fluminense. Niterói, p. 34. 2010.

SILVA, D. J. R. D. **Uso dos dados de contabilização do Radius para faturamento e para geração de informações gerenciais e operacionais de serviços em banda larga**. Universidade de Brasília. Brasília, p. 136. 2010. (PPGENE.DM-422/2010).

TATEOKI, G. T. **Monitoramento de Dados via Internet Baseado em Telefonia Celular**. Universidade Estadual Paulista. Ilha Solteira, p. 123. 2007.

TELEBRASIL. **A Situação da Banda Larga no Brasil: Avaliação do Diagnóstico Realizado pelo IPEA**. TELEBRASIL. Rio de Janeiro, p. 46. 2010.

TELEBRASIL. Brasil fecha 2011 com 58 milhões de acessos em banda larga. **TELEBRASIL Online**, 2012. Disponivel em: <http://www.telebrasil.org.br/artigos/artigos.asp#1202>. Acesso em: 02 fev. 2012.

TELECO. Seção: Banda Larga - Serviço Comunicação Multimídia (SCM). **Teleco Inteligência em Telecomunicações**, 2011a. Disponivel em: <http://www.teleco.com.br/scm.asp>. Acesso em: 30 set. 2011.

TELECO. Seção: Banda Larga - Estatísticas de Banda Larga no Brasil - Dados Trimestrais. **Teleco Inteligência em Telecomunicações**, 2012. Disponivel em: <http://www.teleco.com.br/blarga.asp>. Acesso em: 02 jan. 2012.

TELEFÔNICA. Banda Larga - Speedy - Home. **Telefônica**, 2011. Disponivel em: <http://www.telefonica.com.br/residencial/speedy>. Acesso em: 24 nov. 2011.

THE FREERADIUS SERVER PROJECT. FreeRadius - Survey Results. **The FreeRADIUS Server Project**, 2010. Disponivel em: <http://freeradius.org/press/survey.html>. Acesso em: 01 set. 2011.

THOROGOOD, R.; BROOKSON, C. Lawful Interception. **Telektronikk 2.2007**, Fornebu, v. 2, n. 1, p. 33-36, 2007. ISSN 0085-7130.

TOGNOLLI, C. J. MP, Abin, PF e empresas privadas compraram um Guardião. **Consultor Jurídico**, 2007. ISSN 1809-2829. Disponivel em: <http://www.conjur.com.br/2007-jul-31/mp_abin_pf_empresas_ privadas_compraram_guardiao>. Acesso em: 12 jul. 2009.

UTIMACO. **Lawful Interception in the Digital Age: Vital Elements of an Effective Solution**. Utimaco Safeware AG. Aachen, p. 26. 2009.

VALENTE, J. J. **Internet - Contextos de Mercado e Regulatório**. Agência Nacional de Telecomunicações. Brasília, p. 20. 2007.

VOLPE, B. Cable Modem Registration Through the Eyes of a DOCSIS Protocol Analyzer. **Cable360.net**, 2005. Disponivel em: <http://www.cable360.net/technology/advancedsvcs/15072.html>. Acesso em: 05 set. 2011.

WIMAX FORUM. **WiMAX Forum Network Architecture - Architecture Tenets, Reference Model and Reference Points**. WiMAX Forum. Beaverton, p. 167. 2009. (WMF-T32-003-R010v05).

WIRESHARK. Libpcap File Format. **The Wireshark Wiki**, 2011. Disponivel em: <http://wiki.wireshark.org/Development/LibpcapFileFormat>. Acesso em: 04 nov. 2011.

YRIODA, F. A. T. **Tecnologias de Comunicação de Dados em Altas Velocidades sobre Plataformas MMDS**. Universidade de Brasília. Brasília, p. 149. 2002.