UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

ESTUDO DE VIABILIDADE TÉCNICA E JURÍDICA DE UMA METODOLOGIA PARA OBTENÇÃO DE ÁUDIO EM DISPOSITIVOS SOBRE CANAIS CRIPTOGRAFADOS

EDUARDO ZACCHI

ORIENTADOR: ANDERSON CLAYTON ALVES NASCIMENTO

DISSERTAÇÃO DE MESTRADO EM ENGENHARIA ELÉTRICA

PUBLICAÇÃO: PPGENE.DM – 108/2012

BRASÍLIA / DF: JULHO – 2012

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

ESTUDO DE VIABILIDADE TÉCNICA E JURÍDICA DE UMA METODOLOGIA PARA OBTENÇÃO DE ÁUDIO EM DISPOSITIVOS SOBRE CANAIS CRIPTOGRAFADOS

EDUARDO ZACCHI

DISSERTAÇÃO DE MESTRADO PROFISSIONALIZANTE 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.

APROVADA POR:

ANDERSON CLAYTON ALVES NASCIMENTO, Dr., ENE/UNB
(ORIENTADOR)

FLÁVIO ELIAS GOMES DE DEUS, Dr., ENE/UNB
(EXAMINADOR INTERNO)

RAFAEL TIMÓTEO DE SOUSA JÚNIOR, Dr., ENE/UNB
(SUPLENTE)

BRASÍLIA/DF, 12 DE JULHO DE 2012.

FICHA CATALOGRÁFICA

ZACCHI, EDUARDO
Estudo de Viabilidade Técnica e Jurídica de uma Metodologia para Obtenção de Áudio em Dispositivos sobre Canais Criptografados [Distrito Federal] 2012.
xiv, 110p., 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. VoIP
3. Canais Criptografados
4. Sigilo
5. Cadeia de Custódia

I. ENE/FT/UnB.
II. Título (Série)

REFERÊNCIA BIBLIOGRÁFICA

ZACCHI, E. (2012). Estudo de Viabilidade Técnica e Jurídica de uma Metodologia para Obtenção de Áudio em Dispositivos sobre Canais Criptografados. Dissertação de Mestrado, Publicação PPGENE.DM – 108/2012, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 110p.

CESSÃO DE DIREITOS

NOME DO AUTOR: Eduardo Zacchi

TÍTULO DA DISSERTAÇÃO: Estudo de Viabilidade Técnica e Jurídica de uma Metodologia para Obtenção de Áudio em Dispositivos sobre Canais Criptografados.

GRAU: Mestre ANO: 2012

_____

Eduardo Zacchi
Rua Vinte e Um de Abril, 180
CEP 88131-150 – Palhoça – SC - Brasil

Dedico este trabalho a todos que trabalham
pela Justiça e pela evolução tecnológica
visando a ela.

AGRADECIMENTOS

Agradeço a Deus pela vida e pela minha saúde e de minha família.

Ao Professor João Gondim pela motivação, direcionamento e busca incessante pela melhoria da qualidade do trabalho.

À minha família, que sempre me apoiou e incentivou para que esse trabalho chegasse ao fim e pela paciência e tolerância nas minhas ausências.

Aos amigos George Linhares e Gustavo Roberge Goedert, por terem auxiliado na obtenção dos entendimentos jurídicos referentes ao estudo de viabilidade jurídica do sistema proposto.

Ao Perito Criminal Federal Hélvio Pereira Peixoto, e demais envolvidos, pelo empenho e comprometimento para que esse curso de Mestrado se tornasse realidade.

A todos, os meus sinceros 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.

RESUMO

ESTUDO DE VIABILIDADE TÉCNICA E JURÍDICA DE UMA METODOLOGIA PARA OBTENÇÃO DE ÁUDIO EM DISPOSITIVOS SOBRE CANAIS CRIPTOGRAFADOS.

Autor: Eduardo Zacchi

Orientador: Anderson Clayton Alves Nascimento

Programa de Pós-graduação em Engenharia Elétrica

Brasília, julho de 2012

Cada vez mais as pessoas utilizam a Internet para se comunicar. E o acesso ao teor das comunicações possui grande importância para o conhecimento de ações desempenhadas por investigados, comunicações entre pessoas, seus hábitos, dentre outras informações relevantes a uma investigação criminal.

Os criminosos tem conhecimento que muitas provas são obtidas a partir da quebra do sigilo das comunicações. Para evitar que os órgãos de investigação possam interceptar as suas comunicações, criminosos utilizam sistemas de comunicações criptografados.

A legislação permite a quebra do sigilo das comunicações telefônicas e telemáticas em situações especiais. Quando é realizada a interceptação de canais de voz não criptografados as informações são transmitidas em claro e têm serventia para a investigação, por outro lado, quando se intercepta um canal criptografado, as informações são embaralhadas, não sendo possível na maioria dos casos torná-las inteligíveis.

Esse trabalho apresenta um método para obtenção de áudio em dispositivos que utilizam canais criptografados. O método foi proposto levando em conta as dificuldades técnicas na obtenção das informações propondo uma alternativa para contornar essas dificuldades além de preocupar-se com o aspecto legal, de forma que as informações obtidas tenham validade probatória para a determinação de dinâmica e autoria de um delito.

Após a proposição do sistema, com a definição de seus requisitos e características, foi feita análise de viabilidade jurídica a fim de avaliar a validade probatória das informações obtidas; e análise de viabilidade técnica, buscando identificar situações em que o sistema proposto será possível de ser instalado nos dispositivos, obtendo informações necessárias e encaminhando-as ao órgão de investigação sem ser percebido pelo investigado.

Em consulta com diversos operadores do direito, foi constatado que o sistema pode ser implementado, desde que atendidos os requisitos previstos em lei, sendo considerado que o sistema proposto é considerado análogo às interceptações telefônicas e telemáticas.

Foram consideradas as técnicas de segurança dos dispositivos onde possivelmente será instalado o sistema proposto, e foi considerado que o ponto fraco é o usuário, sendo que é possível a instalação do sistema.

ABSTRACT

ANALYSIS TECHNICAL AND LEGAL ABOUT A METHODOLOGY FOR OBTAINING AUDIO IN DEVICES USING ENCRYPTED CHANNELS

Author: Eduardo Zacchi

Supervisor: Anderson Clayton Alves Nascimento

Electrical Engineering Post-graduate Program

Brasilia, July of 2012

More and more people use the Internet to communicate. The access to the contents of communications has great importance for the understanding of actions performed by investigated, the communications between people, their habits, among other information relevant to a criminal investigation.

Criminals understands that much evidence are obtained from the breach of confidentiality of communications. To prevent the investigating agencies can intercept their communications, criminals using encrypted communications systems.

The legislation allows the breaking of the confidentiality of telephone communications and telematics in special situations. When the trap is made of voice channels unencrypted information is transmitted in clear and are use for investigation, on the other hand, when it intercepts an encrypted channel, the information is scrambled, making them intelligible.

This paper presents a method for obtaining audio in devices using encrypted channels. The method was proposed considering the technical difficulties in obtaining the information, proposing an alternative to overcome these difficulties as well as worry about the legal aspect, so that the information obtained has validity in the courts for the determination of dynamic and authorship of a crime.

After the proposition of the system, defining its requirements and features, viability analysis in law was made in order to assess the validity of evidence obtained, and analysis of technical feasibility in order to identify situations in which the proposed system will be able to be installed on devices, obtaining necessary information and forwarding them to the investigative agency without being perceived by the criminal.

In consultation with several law enforcement officers, it was found that the system can be implemented, since it met the requirements prescribed by law, considered that the proposed system is considered as similar to telephone intercepts and telematics.

Were considered the security techniques used in devices where possible the proposed system will be installed, and was considered the weak point is the user, and it is possible to install the system.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE SÍMBOLOS, NOMENCLATURA E ABREVIAÇÕES

3D - Três Dimensões

3G - *3rd Generation*

ADPCM - *Adaptive Differential Pulse Code Modulation*

AES - *Advanced Encryption Standard*

AI - *Administration Interface*

A_{ID} – Número de identificação do alvo

ANATEL – Agência Nacional de Telecomunicações

CBC - *Cypher Block Chaining*

CCC - *Call Content Channel*

CD – *Compact Disc*

CDC - *Call Data Channel*

CELP - *Codebook-Excited Linear Prediction*

CNJ – Conselho Nacional de Justiça

CODEC – C*oder-Decoder*

Dec - Representação da função Decifrar

DVD - *Digital Versatile Disc*

DH - *Diffie-Helman*

DIF_{tempo} - Diferença de tempo entre relógio local e o obtido no servidor de NTP

EAX - *Environmental Audio Extensions*

ECDH - *Elliptic Curve Diffie-Hellman*

EDGE - *Enhanced Data for Global Evolution*

Enc – Representação da função Cifrar

EUA - *Estados Unidos da América*

FTP – *File transfer protocol*

GPRS - *General Packet Radio Service*

HSPA - *High Speed Packet Access*

HTML5 - *Hypertext Markup Language, versão 5*

HW_{ID} - Identificador de Hardware

IMA - *Interactive Multimedia Association*

IP – *Internet Protocol*

$K_{analise}$ - chave da máquina de análise

K_{alvo} - chave da máquina do alvo

LEA – *Law Enforcement Agency*

LPC - *Linear Prediction Coding*

MD5 - *Message Digest Algorithm*

MIC - microfone

MP3 - *MPEG 1 Layer-3*

NSA - *National Security Agency*

NTP - *Network Time Protocol*

OAM&P - *Operation, Administration, Maintenance and Provisioning*

PADO - Procedimento para Apuração de Descumprimento de Obrigação

PC – *Personal Computer*

QoS - *Quality of Service*

RAM - Randon Access Memory

RSA - *Rivest, Shamir e Adleman*

SCM – Serviço de Comunicação Multimídia

SHA - *Secure Hash Algorithm*

SPK - *speaker*

TCP - *Transmission Control Protocol*

Ts - Tempo de aquisição do sinal

UDP - *User Datagram Protocol*

UMTS - *Universal Mobile Telecommunications System*

V – Número da versão do sistema da máquina do alvo

VoIP – *Voice over Internet Protocol*

WMA – *Windows Media Audio*

WAV - *Waveform audio format*

WiFi - *Wireless Fidelity*

1. INTRODUÇÃO

Um dos mais importantes meios de investigação atualmente usado pela polícia é a interceptação telefônica e de dados efetuada com a devida autorização judicial.

Desde os primórdios dos sistemas de comunicação, os sinais da voz eram convertidos em sinais elétricos sendo transmitidos de forma analógica. Com o desenvolvimento da tecnologia digital, os sistema de comunicação passaram a utilizar essa tecnologia. O som da voz, para ser transmitido em um sistema digital deve ser codificado para o formato digital antes de ser transmitido através do meio e decodificado no outro lado para a sua forma analógica original para que o ouvinte possa compreendê-lo. (COSTA, 2007)

Qualquer informação analógica que precisa ser armazenada em um computador ou transmitida por um sistema de comunicação digital, passa necessariamente por um processo de codificação ou digitalização do sinal, que permite grandes vantagens, tais como, os sinais digitais são muito menos sensíveis a interferências ou ruídos e podem ser enviados diretamente a computadores, que são equipamentos que utilizam sistemas digitais. (COSTA, 2007)

O que é visto hoje é uma transformação geral em todo processo de telefonia e informática, onde ambos estarão eternamente ligados. (COSTA, 2007)

Para haver comunicação entre dois pontos é necessário o estabelecimento de uma conexão. Na comunicação analógica e em alguns casos na comunicação digital é necessário o estabelecimento de uma conexão baseada em comutação por circuitos. Nesse sistema, a transmissão de voz só pode ser realizada se existir um caminho dedicado entre dois terminais, geralmente chamados de terminal A, para quem origina a chamada, e terminal B, para quem recebe a chamada. Na comutação de circuitos, o caminho alocado durante a fase de estabelecimento da conexão permanece dedicado a estes terminais até que um deles, ou ambos, decida desfazer o circuito. (DÍGITRO, s.d.)

Durante a fase de conversação, caso o tráfego entre os dispositivos não seja contínuo e constante, ou seja, apresente períodos de inatividade, a capacidade do meio físico é bastante desperdiçada. Em outras palavras, o processo de transmissão é bastante

dispendioso, já que mantém alocado o circuito durante 100% do tempo, apesar de não se utilizá-lo o tempo todo, em períodos de silêncio, por exemplo. (DÍGITRO, s.d.)

A outra modalidade de comutação é a comutação de pacotes. Nas tecnologias de comutação de pacotes, os dados a serem transmitidos são fragmentados e organizados em unidades lógicas menores, chamadas de pacotes, com tamanhos variáveis, porém dentro dos limites máximos de transmissão fixados por um protocolo de rede. (DÍGITRO, s.d.)

A comutação de pacotes é baseada no endereçamento de pacotes ao destino, ou seja, diferentemente da comutação de circuitos, não é necessário o estabelecimento de caminhos físicos dedicados entre os terminais ou estações participantes da comunicação. A informação a ser enviada pode viajar por caminhos diferentes até seu destino. (DÍGITRO, s.d.)

A digitalização dos sinais de voz e vídeo e a tecnologia de comutação de pacotes possibilitaram a convergência de vários serviços utilizando uma mesma infra-estrutura.

Para operar num ambiente integrado, a forma mais viável foi através de tecnologias de transmissão de voz sobre dados ou voz sobre pacotes, como também são chamadas, pois trabalham sob o princípio da comutação de pacotes. (DÍGITRO, s.d.)

Neste sistema, antes de operar num ambiente de dados, a voz é digitalizada, comprimida e transformada em pacotes através de elementos denominados *CODECS*. E depois, a voz é transmitida na forma de dados juntamente com os demais dados da rede. (DÍGITRO, s.d.)

Existem várias tecnologias que podem operar num ambiente convergindo voz e dados, uma delas é a chamada voz sobre *IP*.

A comunicação de voz em redes *IP*, chamada de *VoIP*, consiste no uso das redes de dados que utilizam o conjunto de protocolos das redes *IP* (*TCP/UDP/IP*) para a transmissão de sinais de voz em tempo real na forma de pacotes de dados. (CAMPOS, 2007)

A Internet utiliza a pilha de protocolos *TCP/IP* para estabelecer comunicação entre os computadores a ela conectados. (TITTEL, 2002)

Quando um tráfego de dados é enviado de uma máquina para outra (e-mails, mensagens de *ICQ*, navegação, *ftp*, etc) os dados passam por várias máquinas até atingir o seu destino. Se

alguém instalar algum capturador de pacotes (*sniffer*) em alguma das máquinas da rota os dados poderão ser facilmente visualizados. (SILVA, 2002)

É sabido que a Internet não é considerada um ambiente seguro. Uma maneira de impedir que uma pessoa não autorizada tenha acesso as informações que cruzam uma rede, é tornar o conteúdo das mensagens ilegível, só podendo ser compreendido pelo destinatário pretendido (TITTEL, 2002). Esse processo de tornar as mensagens ilegíveis a todos, exceto para o destinatário, é chamado de criptografia.

A fim de garantir a confidencialidade das mensagens transmitidas, os usuários utilizam aplicativos que implementam funções de criptografia, como exemplo podemos citar o aplicativo de comunicação por voz *Skype*.

Os projetistas do *Skype* não hesitaram em empregar criptografia, a fim de estabelecer uma base de confiança, autenticidade e confidencialidade para os seus serviços ponto a ponto. Os programadores do *Skype* implementaram as funções criptográficas corretamente e eficientemente. Como resultado, a confidencialidade de uma sessão do *Skype* é muito maior do que o oferecido por um telefonema com ou sem fio ou por e-mail e anexos de e-mail. (BERSON, 2005).

Assim como o *Skype*, outras soluções oferecem segurança e privacidade para as comunicações, como exemplo cita-se a proteção contra escuta telefônica oferecido pela empresa *SecVoice* (SECVOICE). A solução provê comunicação segura cifrada por voz e mensagens de texto criptografadas para *Windows* e é compativel com *PCs desktop*, *notebooks*, *subnotebooks* e *smartphones* com *Windows Mobile* (SECVOICE).

Outro sistema semelhante é *PhoneCrypt* que utiliza a tecnologia em nível militar para assegurar conversas telefônicas em tempo real. A tecnologia avançada cifra conversas de telefone celular para telefone celular, de telefone fixo para telefone fixo, de telefone celular para telefone fixo e vice-versa.

Por outro lado, a interceptação telefônica e de dados (telemática) é prevista pela legislação brasileira como meio legal de prova em processos criminais. (PERON, 2011).

A interceptação autorizada de chamadas consiste no processo de interceptar e monitorar a comunicação telefônica (voz e dados associados à chamada) estabelecida por um indivíduo e seu(s) interlocutor(es), por um órgão de monitoração, mediante autorização judicial, para

fins de investigação criminal e instrução processual penal. Esse tipo de interceptação deve ser legalmente autorizado e conduzido de forma tal que os interlocutores da chamada não tenham ciência da monitoração (LEITE, 2006)

Conforme (LEITE, 2006) o serviço de interceptação de chamadas telefônicas constitui-se no processo de acessar continuamente o conteúdo (voz ou dados) que trafega no canal de comunicação e os dados de identificação da chamada envolvendo um determinado assinante de uma central telefônica. O assinante monitorado é denominado assinante alvo de interceptação, o qual através de uma ordem judicial, previamente expedida, terá suas informações telefônicas monitoradas.

O assinante que se comunica com o assinante alvo é denominado assinante associado. O ponto de acesso de interceptação é a central telefônica na qual o assinante alvo está hospedado. Também pode ser chamado de central alvo de interceptação. É na central alvo que será realizado todo o processo de interceptação de chamadas em estudo.

Já a central associada hospeda o assinante associado, com o qual o assinante alvo se comunica. As informações de interesse da interceptação podem ser classificadas em dois tipos:

Conteúdo da chamada (*Call Content*): É todo conteúdo de áudio e dados trocados entre o assinante alvo e o assinante associado.

Dados Associados à Chamada (*Call Data*): São os dados de identificação da chamada monitorada (ex. número dos assinantes, hora de início e fim da chamada, identificador da chamada, indicador de serviços suplementares, etc.).

As informações da interceptação são enviadas à agência de monitoração que tem a função de coletar e processar os dados para os fins da investigação autorizada. A administração é responsável por todas as atividades de operação, administração, manutenção e provisionamento da monitoração.

A fig. 1.1, extraída de (LEITE, 2006) ilustra as entidades e interfaces utilizadas pelo serviço de monitoração.

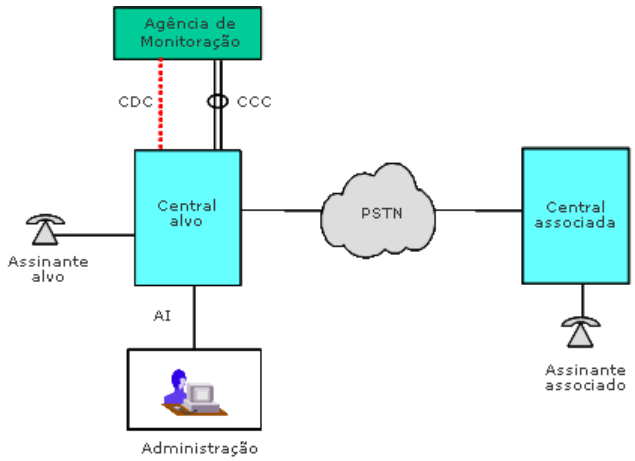

Figura 1.1: Arquitetura do serviço de interceptação de chamadas

A interface de conteúdo (*CCC - Call Content Channel*) é utilizada para transmissão do conteúdo de voz e dados, trocados entre os interlocutores da chamada, à agência de monitoração. Podem ser utilizados canais de áudio dedicados ou circuitos comutados na rede de telefonia pública.

A interface de dados (*CDC - Call Data Channel*) é utilizada para transmissão de dados de identificação da chamada. As mensagens *CDC* são encapsuladas em pacotes *TCP/IP* e enviadas à agência de monitoração através da rede *IP*.

A interface de administração (*AI - Administration Interface*) é utilizada para comunicação entre o sistema de gerência e a central alvo. É através desta interface que são realizadas as atividades de *OAM&P* referentes à interceptação de chamadas na central. A conexão entre o sistema de administração e a central telefônica pode ser realizada através conexão *IP* ou linha discada (dial-up).

O 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).

Com a popularização do acesso à Internet, muitas pessoas tem conexão permanente em casa ou no trabalho. O número total de pessoas com acesso à Internet em qualquer

ambiente (domicílios, trabalho, escolas, *lan houses* ou outros locais) atingiu 79,9 milhões no quarto trimestre de 2011. (IBOPE, 2012)

O uso da internet em casa ou no local de trabalho também se manteve em crescimento em 2012. No primeiro trimestre, o acesso em casa ou no trabalho atingiu 66 milhões de pessoas. Dessas pessoas com acesso, 48,7 milhões foram usuários ativos em fevereiro, o que significou um crescimento de 2,5% sobre o mês de janeiro, de 18% sobre os 41,4 milhões de fevereiro de 2011 e de 33% sobre 36,7 milhões de fevereiro de 2010. (IBOPE, 2012)

De acordo com uma pesquisa realizada pela KPMG, 20% dos brasileiros pretendem deixar de lado o telefone fixo em 2012 e passar a usar somente o celular para fazer e receber ligações. (CIRIACO, 2012)

Apesar de não ter sido tratado na pesquisa, outro método que também pode ser uma "ameaça" aos telefones fixos tradicionais é a ligação via VoIP, com a popularização de programas tipo *Skype*. (CIRIACO, 2012)

Ao que tudo indica, a *Microsoft* está preparando uma versão do *Skype* que deve ser menos dependente de sistemas operacionais e vai rodar em navegadores. A suspeita se deve as quatro vagas de emprego que foram postadas em seu site de talentos. De acordo com as ofertas, a empresa está a procura de engenheiros experientes especializados em *HTML5* e *Javascript* para portar o conhecido programa de *VoIP* para a *web*. (MORENO, 2012).

Assim, está havendo uma migração das formas de comunicação tradicionais para a rede de dados. (MARCHETTI, 2008).

Ao longo desse trabalho, será utilizada a sigla *LEA* (*Law Enforcement Agency*) com referência às forças policiais, agências de inteligência, o Ministério Público (quando exercendo seu poder de investigação) e demais entidades possam exercer legalmente funções e investigação.

1.1. DEFINIÇÃO DO PROBLEMA

A escuta telefônica tem se revelado o principal, senão o único, meio de prova disponível para a constatação da materialidade de determinados delitos e de sua autoria, notadamente

aqueles que não deixam rastros materiais a serem identificados por outros meios. (SIQUEIRA FILHO, 1997)

A interceptação telefônica é fundamental para produzir provas em investigações complexas (ITAGIBA, 2009). Sabedores disso, criminosos passaram a utilizar a Internet como forma de comunicação, mantendo comunicações através de diversos meios como e-mail, redes sociais, aplicativos de chat e *VoIP*.

A sofisticação e o profissionalismo de certos criminosos, principalmente, quando integram quadrilhas estruturadas, equipadas e organizadas, reclamam, obviamente, o emprego de mecanismo também modernos de investigação criminal. (SIQUEIRA FILHO, 1997)

Os grupos que se dedicam ao tráfico de drogas, contrabando, roubo a instituições financeiras, corrupção, procuram, a cada dia, aperfeiçoar, mais a mais, a prática delitiva, buscando eliminar ou reduzir ao máximo os riscos do insucesso. (SIQUEIRA FILHO, 1997)

Dada à vulnerabilidade, quanto ao acesso indevido por terceiros ao conteúdo das mensagens transmitidas pela Internet, surgiu a necessidade da utilização de sistemas de criptografia. (SILVA, 2006)

No entanto, com a utilização de criptografia nas comunicações, tornou-se inviável inclusive para as LEA identificarem as mensagens transmitidas através da Internet. A obtenção dos dados que trafegam pelo *link* do alvo é possível, no entanto, em várias situações esses dados estão cifrados tornando inviável a obtenção da mensagem. Dentre algumas aplicações que utilizam criptografia pode-se citar o aplicativo para comunicação por *VoIP*, *Skype*.

Essa característica de algumas aplicações, de cifrar os dados antes de transmití-los, é de conhecimento geral, inclusive dos criminosos, que passam a utilizá-las de modo a inviabilizar uma possível interceptação de suas comunicações.

A polícia italiana tem reclamado de que o serviço de Voz sobre *IP Skype* está inviabilizando o uso de escutas telefônicas em investigações criminais. (DUNM, 2009)

As autoridades em Milão admitiram que o crime organizado na Itália está cada vez mais utilizando as sessões criptografadas do *Skype* para comunicações críticas como uma forma de obstruir a vigilância remota. (DUNM, 2009)

Policiais e fiscais dizem ter ouvido um traficante de drogas recomendando o uso do *Skype* para discutir detalhes confidenciais de um lote, tornando impossível para as autoridades interceptá-lo. (DUNM, 2009)

O *Skype* é conhecido por ser uma frustração para as autoridades em todo o mundo. Um ano atrás, um documento vazado no site *Wikileaks* mostrou que as autoridades alemãs estavam tão preocupadas com o uso do *Skype* que eles haviam contratado uma empresa de software para desenvolver cavalos de tróia capazes de gravar dados do *Skype* nos *PCs* dos investigados para análise posterior. (DUNM, 2009)

O problema é que o *Skype* utiliza um esquema de criptografia forte, e as chamadas são criadas e implementadas com criptografia que é proprietária e é considerada pela empresa um segredo comercial. (DUNM, 2009)

Nos EUA, relatos não confirmados surgem de tempos em tempos, alegando que a *NSA* (National Security Agency) está preocupada com o *Skype* e está ativamente tentando quebrar sua criptografia. (DUNM, 2009)

Um desses relatos, fez a afirmação improvável de que autoridades dos EUA estariam dispostas a oferecer "bilhões" para qualquer um que pudesse encontrar uma maneira de contornar isso. A mesma história também relatou que a *NSA* estava prestes a "quebrar" a criptografia do *Skype*. (DUNM, 2009)

Foi noticiado também pelo site inglês *The Register* que a Agência de Segurança Americana (*NSA*) estaria oferecendo bilhões de dólares por uma tecnologia que a permita "grampear" ligações utilizando o software de Voz sobre *IP Skype*. Estas informações teriam sido passadas por um executivo de uma empresa especializada em tecnologias para interceptação telemática em uma feira desta indústria, em Londres. (SÜFFERT, 2011)

A polícia alemã não conseguiu decifrar a criptografia usada no software de telefonia pela Internet, *Skype* para monitorar chamadas de suspeitos de crimes e terroristas, afirmou a principal autoridade policial da Alemanha. (REUTERS, 07)

Apesar da limitação tecnológica em interceptar o tráfego de dados e decifrar informações que trafegam em canais criptografados, como no caso do *Skype*; há a possibilidade de obter os sinais de áudio antes de serem criptografados; é como funciona um *trojan* para o *Skype*, capaz de extrair chamadas de voz na forma de arquivos *MP3* e enviá-los para terceiros (EDGE, 2009).

Entretanto não basta obter os sinais de áudio, é necessário que os mesmos tenham validade probatória. Considerando a grande capacidade técnica e jurídica em que alguns indiciados tem de se defender, se faz necessária a criação de um mecanismo que mantenha a cadeia de custódia das provas obtidas, garantindo assim a integridade e validade das mesmas durante todo o processo inquisitório e processual.

Em alguns casos, por falta de uma cadeia de custódia confiável e de garantias de autenticidade e integridade do tráfego (MONTENEGRO; BUENO; NUSDEO, 2007), ocorre anulação e desconsideração das informações como prova no processo criminal pelo Judiciário e Ministério Público, frustrando o trabalho de investigação das LEA e promovendo a impunidade (RONCAGLIA, 2008).

No Brasil, as leis que definem a interceptação telefônica e telemática são 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). No entanto, não foram encontrados registros em legislação e em decisões judiciais relativas às provas obtidas através de ferramentas diversas àquelas usualmente implementadas, que em geral se baseiam no desvio de tráfego por parte das operadoras.

1.2. OBJETIVO DA DISSERTAÇÃO

O objetivo dessa dissertação é definir os requisitos necessários ao sistema de obtenção de áudio em equipamentos computacionais de forma a garantir a (1) integridade, ou seja, a informação recebida no sistema da LEA é a mesma obtida nos canais de áudio do computador do alvo; a (2) confidencialidade, ou seja, somente quem tem permissão poderá acessar os registros de áudio; e a (3) autenticação, ou seja, será possível no sistema da LEA identificar que a informação foi realmente gerada pelo alvo.

Uma vez definidos os requisitos, será realizada uma análise jurídica e técnica, buscando identificar a viabilidade de implementação do aplicativo a fim de determinar se (1) é possível tecnicamente desenvolver um aplicativo furtivo, capaz de obter os registros de áudio do dispositivo do alvo e disponibilizá-los no sistema da LEA e (2) se o aplicativo furtivo, implementado atendendo aos requisitos elencados, é capaz de obter os áudios e os mesmos terão validade probatória.

1.3. HIPÓTESE DE PESQUISA

Para realizar a interceptação das comunicações de áudio em canais criptografados, uma possibilidade é obter o áudio antes do mesmo ser criptografado e disponibilizá-lo nos sistemas da LEA.

Para garantir integridade, confidencialidade e autenticação devem ser utilizados artifícios de criptografia na transmissão a armazenamento das informações.

Após elencadas as características do aplicativo é feita uma análise jurídica, inclusive com pareceres dos operadores do direito a fim de verificar a viabilidade jurídica das provas obtidas. Além da análise jurídica é feita uma análise a fim de verificar a viabilidade técnica do aplicativo no tocante a capacidade furtiva e não detecção.

1.4. MÉTODO

Para a realização desse trabalho, inicialmente foi realizada uma pesquisa a fim de verificar a existência de aplicativos capazes de realizar a obtenção de áudio em dispositivos computacionais. Foram feitas buscas em periódicos científicos e conferências, em material disponível nos tribunais e em sites de notícias. Não sendo encontrados sistemas que atendessem todas as características necessárias.

Em seguida, foi feita busca detalhada nos tribunais por jurisprudências a respeito da matéria, buscando inclusive situações diferentes mas que mantivessem alguma relação com a filosofia da obtenção de provas. Nesse sentido, também não foi encontrado material que pudesse subsidiar uma análise jurídica contundente.

Considerando tratar-se de uma matéria nova, antes de buscar efetivamente a viabilidade jurídica, foram elencados os principais requisitos a serem atendidos e definido um método para especificar a forma como esses requisitos seriam atendidos.

Considerando a inexistência de decisões e jurisprudências a respeito da matéria, foi realizada uma consulta jurídica sendo elaborado um texto e repassado a alguns operadores do direito, como advogados, membros do Ministério Público, magistrados, e Defensores Públicos. Devido à impossibilidade de magistrados fornecerem pareceres em casos hipotéticos, foram marcadas audiências a fim de conhecer o entendimento dos magistrados sobre a matéria.

A análise de viabilidade técnica foi realizada com base nos sistemas atualmente disponíveis e como os mesmos implementam o seu esquema de segurança.

Para finalizar, foi feita uma compilação das informações obtidas quando da consulta jurídica, que possibilitou concluir quanto a viabilidade jurídica da proposta; e foram apresentados os cenários em que é viável tecnicamente a implementação da proposta.

1.5. ESTRUTURA DA DISSERTAÇÃO

Essa dissertação foi dividida em seis capítulos. Neste capítulo foi apresentada uma introdução ao trabalho. Aqui é apresentada a importância das comunicações por voz nas investigações criminais, a evolução dessas formas de comunicação e os problemas advindos dessa evolução com foco na investigação.

O capítulo 2 apresenta o contexto legal da interceptação de dados telefônicos e telemáticos no Brasil. O terceiro capítulo descreve os requisitos a serem atendidos e os detalhes do sistema a ser implementado de forma a atender aos requisitos.

O capítulo 4 apresenta a forma como foi realizada a consulta jurídica e os resultados obtidos. O quinto capítulo apresenta as limitações técnicas quanto a implementação da proposta e possíveis alternativas para viabilizá-la.

E finalmente, o capítulo 6 contém as conclusões do trabalho, apresentando uma síntese dos resultados obtidos através da consulta jurídica e da análise técnica, avaliando se é viável a implementação da proposta com base nesses aspectos.

2. ASPECTOS LEGAIS E NORMATIVOS

No Brasil, o direito ao sigilo das telecomunicações é garantido pela constituição, sendo no entanto relativizado. Nesse sentido, existem diversos instrumentos legais que tratam desse tema, são eles: a Constituição Federal, leis específicas, jurisprudências, normas e resoluções da Agência Nacional de Telecomunicações (ANATEL) e documentos do Poder Judiciário e Ministério Público.

Existem algumas formas de quebrar o sigilo das comunicações, sendo a interceptação telefônica, a gravação clandestina e a gravação ambiental.

A interceptação telefônica ocorre quando um terceiro capta a comunicação telefônica alheia, sem o conhecimento dos interlocutores. Na gravação clandestina, um dos interlocutores (ou alguém a seu mando) grava sua própria conversa telefônica com o outro, sem que este saiba. A gravação ambiental é aquela que capta uma conversa alheia, não telefônica, feita por um terceiro, valendo-se de qualquer meio de gravação. É uma conversa ocorrida em um gabinete, reunião, ou residência, por exemplo (GRANDINETTI, 2006, p. 79 apud MOLLMAN, COLL, 2011).

Apenas as interceptações telefônicas encontram amparo na norma do inciso XII do artigo 5º, do texto constitucional, e estão regulamentadas pela Lei n. 9.296/96. Por outro lado, as gravações clandestinas e ambientais estão regulamentadas, em parte, pela Lei n. 9.034/95, a qual prevê a admissibilidade como meio investigatório e de formação de prova quando aquelas versarem sobre ilícito praticado por organizações criminosas, ou quando comprovada a ocorrência de alguma excludente de ilicitude que possa vir a ser utilizada pelo interessado para defender seus direitos. (MOLLMAN, COLL, 2011).

Fora das hipóteses supracitadas, essas espécies de captação de comunicações (interceptações telefônicas, gravações clandestinas e ambientais) são, em princípio, proibidas justamente por violarem o dispositivo constitucional (MENDES, 2008, p. 646-647 apud MOLLMAN, COLL, 2011).

2.1. CONSTITUIÇÃO FEDERAL

A Constituição da República Federativa do Brasil de 1988, que define os direitos e garantias fundamentais dos cidadãos, em seu artigo 5º, inciso XII, apresenta o direito à privacidade conforme abaixo. (BRASIL, 1988).

> art. 5º, XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

Como citado, a regra é a garantia do direito do cidadão. A exceção é a autorização judicial da interceptação, em casos específicos e nunca de ofício. O essencial na discussão jurídica da questão é determinar exatamente em que casos e mediante qual procedimento se dará a interceptação.

A redação dessa norma constitucional não foi suficientemente clara. Não há dúvida que a comunicação telefônica pode ser interceptada, desde que por ordem judicial. Porém, o inciso já não é tão claro e inequívoco quando o intérprete se propõe determinar se a exceção (realização de escuta judicial) abarca somente as comunicações telefônicas ou inclui também as comunicações telegráficas, de dados, ou ambientais.

Uma parte da comunidade jurídica defende que a Constituição, ao incluir a expressão "no último caso", refere-se à possibilidade de quebra de sigilo para fins de investigação criminal para todas as modalidades de comunicação, exceto a correspondência por carta convencional, que é englobada pelo termo "correspondência" no início do inciso.

Outros entendem que a expressão "no último caso" refere-se somente à última das modalidades de comunicação elencadas, ou seja, as comunicações telefônicas. Estariam, portanto, fora do alcance das interceptações, mesmo autorizadas judicialmente, além da carta convencional, as comunicações telegráficas e de dados.

Outros, ainda, afirmam que não há direitos absolutos, e mesmo a correspondência convencional, bem como qualquer outra modalidade de comunicação, poderia, com a devida justificação e autorização judicial, ser objeto de quebra de sigilo. Na

jurisprudência do Supremo Tribunal Federal se confirmou a admissibilidade de interceptação de correspondência de preso pela administração carcerária, com base no argumento de que "a inviolabilidade do sigilo epistolar não pode constituir instrumento de salvaguarda de práticas ilícitas".(MELLO, 1994)

Existe ainda hoje, mesmo muito tempo após a promulgação da Constituição de 1988, discussão na doutrina jurídica a esse respeito. Na prática, pelo menos até agora, prevalece o entendimento de que o sigilo das comunicações telefônicas não é absoluto, embora, a definição do que seja correspondência e comunicação telefônica, num mundo em que o correio eletrônico, a telefonia sobre *IP* e as redes convergentes são cada vez mais difundidos, não fica isenta de polêmica.

Os direitos fundamentais, segundo a moderna doutrina constitucional, não podem ser entendidos em sentido absoluto, em face da natural restrição resultante do princípio da convivência das liberdades públicas, sendo que não se permite que qualquer delas seja exercida de modo danoso à ordem pública e às liberdades alheias. (KISTENMACHER , VANDRESEN, 2009)

As jurisprudências têm mostrado a possibilidade da quebra de sigilo telefônico nas hipóteses estabelecidas em lei conforme cita (PENTEADO, 2011)

> (…) A Constituição Federal giza que o sigilo das comunicações telefônicas poderá ser quebrado por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal" (artigo 5º, inciso XII), tendo em vista que, em determinados casos, o direito individual é relativizado frente ao interesse público, que prepondera sobre aquele. Havendo previsão legal para que se promova a interceptação de comunicações telefônicas, não se evidencia vício nesse tipo de prova, desde que observados os respectivos preceitos legais.
>
> "As prorrogações da interceptação telefônica, autorizadas pelo Juízo, de fato não podem exceder 15 dias; porém, podem ser renovadas por igual período, não havendo qualquer restrição legal ao número de vezes, em que possa ocorrer a renovação, desde que comprovada a necessidade" (HC nº 34.701/SP, STJ, 6ª Turma, rel. Min. Hélio Quaglia Barbosa, DJU, ed. 19-12-2005, p. 473).(...)

(TRF4, ACR 0014752-96.2008.404.7000, Oitava Turma, Relator Luiz Fernando Wowk Penteado, D.E. 14/04/2011)

2.2. LEI DAS INTERCEPTAÇÕES TELEFÔNICAS E DE DADOS

A norma constitucional depende de norma infraconstitucional regulamentadora, sendo esta a Lei n. 9.296/96 que traça o procedimento devido para a quebra do sigilo das comunicações telefônicas, sendo que sua inobservância vicia a prova obtida de forma circunstância, caracterizando assim prova ilícita e portanto, inadmissível. (KISTENMACHER, VANDRESEN, 2009)

A Lei nº 9.296, de 24 de julho de 1996, popularmente conhecida como a Lei da Interceptação, (KISTENMACHER , VANDRESEN, 2009) regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal e define em seu Art. 1º que a interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça. (BRASIL, 1996).

No parágrafo único do Art. 1º é determinado que o disposto na referida lei se aplica também à interceptação do fluxo de comunicações em sistemas de informática e telemática. (BRASIL, 1996).

No Art. 2º a lei em comento vedou a realização de interceptação das comunicações telefônicas quando não houver indícios razoáveis da autoria ou participação em infração penal ou a prova puder ser feita por outros meios disponíveis. (KISTENMACHER , VANDRESEN, 2009)

Não resta dúvida acerca da possibilidade da utilização da interceptação telefônica como meio probatório, desde que devidamente autorizada pelo magistrado competente, por decisão fundamentada, para fins de investigação ou instrução processual penal, quando não seja possível a formação do conjunto probatório por outros meios legais (KISTENMACHER , VANDRESEN, 2009)

A lei indica que a interceptação das telecomunicações deve ser utilizada somente quando houver indícios do cometimento de um crime que tenha pena de detenção e que a

interceptação seja direcionada a algum suspeito específico. Desta forma, não se pode fazer uso de mecanismos que monitorem constantemente as redes de comunicação em busca de indícios de crimes.

É fundamental, pois, que determinados elementos deixem transparecer uma razoável suspeita de que alguém tenha colaborado com a tentativa ou a prática delituosa, como autor ou partícipe, e a escuta seja exigida pelas circunstâncias, a fim de elucidar a verdade material. É lógico que não se exige a certeza, mas a simples presença de indícios. (SIQUEIRA FILHO, 1997)

Com relação à possibilidade de obtenção de prova por outros meios legais, (SIQUEIRA FILHO, 1997) entende que esta regra não exclui a possibilidade de se recorrer ao expediente em tela, a título complementar, quando os outros meios de prova não esclarecem, em plenitude, os fatos objeto da investigação ou da instrução criminal. Em contrapartida, se os outros meios oferecem condições para uma bem-sucedida apuração integral dos fatos, é vedada a adoção da escuta telefônica. (SIQUEIRA FILHO, 1997)

No Art. 3º, é indicado que a interceptação telefônica pode ser determinada pelo juiz, de ofício ou requerida pela autoridade policial na investigação criminal ou representante do Ministério Público na investigação criminal e na instrução processual penal. (BRASIL, 1996)

No Art. 4° a lei indica que o pedido de interceptação de comunicação telefônica deve conter a demonstração de que a sua realização é necessária à apuração de infração penal e a indicação dos meios a serem empregados, sendo que excepcionalmente, o juiz poderá admitir que o pedido seja formulado verbalmente, desde que estejam presentes os pressupostos que autorizem a interceptação, caso em que a concessão será condicionada à sua redução a termo. O juiz, no prazo máximo de vinte e quatro horas, decidirá sobre o pedido. (BRASIL, 1996)

No Art. 5° a lei especifica os requisitos da autorização, sendo que decisão será fundamentada, sob pena de nulidade, indicando também a forma de execução da diligência, que não poderá exceder o prazo de quinze dias, renovável por igual tempo uma vez comprovada a indispensabilidade do meio de prova. (BRASIL, 1996)

Com relação à fundamentação da decisão, trata-se de um registro totalmente dispensável, pois todas as decisões judiciais devem conter fundamentação. (SIQUEIRA FILHO, 1997)

Ao se reportar a igual tempo, parece admitir apenas uma renovação. Mas, na verdade, não se pode tolerar a restrição à renovação do prazo, por tantas vezes quantas necessárias à apuração. dos fatos, caso, como antedito, for evidenciada a indispensabilidade do emprego da escuta. (SIQUEIRA FILHO, 1997)

Considerando a forma de execução da diligência, o juiz decidirá se aceita 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, podendo redefinir tais meios.

Em sendo deferido o pedido, o Art. 6º define que a autoridade policial conduzirá os procedimentos de interceptação, dando ciência ao Ministério Público, que poderá acompanhar a sua realização. No caso de a diligência possibilitar a gravação da comunicação interceptada, será determinada a sua transcrição. Cumprida a diligência, a autoridade policial encaminhará o resultado da interceptação ao juiz, acompanhado de auto circunstanciado, que deverá conter o resumo das operações realizadas. Recebidos esses elementos, o juiz determinará a providência do Art. 8°, ciente o Ministério Público. (BRASIL, 1996)

No Art. 7° a lei define que para os procedimentos de interceptação de que trata esta Lei, a autoridade policial poderá requisitar serviços e técnicos especializados às concessionárias de serviço público.(BRASIL, 1996). Ao falar em requisitar, o art. 7 impôs, por conseguinte, à concessionária a obrigação de colaborar com a elucidação dos fatos, com as repercussões daí decorrentes. (SIQUEIRA FILHO, 1997)

No Art. 8° a lei define que a interceptação de comunicação telefônica, de qualquer natureza, ocorrerá em autos apartados, apensados aos autos do inquérito policial ou do processo criminal, preservando-se o sigilo das diligências, gravações e transcrições respectivas. A apensação somente poderá ser realizada imediatamente antes do relatório da autoridade, quando se tratar de inquérito policial ou na conclusão do processo ao juiz. (BRASIL, 1996)

A interceptação ocorre em autos apartados, de modo a assegurar a proteção à intimidade e à vida privada das pessoas envolvidas. (SIQUEIRA FILHO, 1997)

O objetivo da escuta telefônica consiste na colheita de elementos probatórios para a demonstração da materialidade e/ou da autoria delitivas. Em face de tal premissa, avulta abusiva a preservação da gravação de trechos de comunicações que não interessem, precisamente, à elucidação dos fatos objeto da investigação ou da instrução criminal. (SIQUEIRA FILHO, 1997)

Por este motivo, o Art. 9°, define que a gravação que não interessar à prova será inutilizada por decisão judicial, durante o inquérito, a instrução processual ou após esta, em virtude de requerimento do Ministério Público ou da parte interessada. (BRASIL, 1996)

O dispositivo não fez alusão à possibilidade de o juiz, de ofício, determinar a inutilização em tela. Na verdade, não é prudente deliberar a respeito da questão sem a oitiva das partes envolvidas. Se o magistrado reputa desnecessária e, até, inconveniente (no que atine à intimidade das pessoas cujas conversações foram gravadas) a preservação dos registros, deve consultar as partes interessadas na produção da prova, inclusive, obviamente, o acusado e, se elas não se opuserem ou, em se opondo à destruição, não oferecerem argumentos razoáveis para tal posicionamento, determinar a providência que, lhe parecer oportuna . (SIQUEIRA FILHO, 1997)

Por medida de segurança, para evitar a destruição de trechos que possam interessar ao deslinde do feito, a inutilização será assistida pelo representante do Ministério Público, que, obviamente, é o interessado na produção da prova cabal a demonstrar a infração penal, considerando que ao acusado basta a dúvida sobre os fatos, facultando-se a presença do acusado ou de seu representante legal, que, para o exercício de tal prerrogativa, deverão ser regularmente intimados. (SIQUEIRA FILHO, 1997)

No Art. 10. a lei define como crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei, com pena de reclusão, de dois a quatro anos, e multa. (BRASIL, 1996)

Não é cabível o emprego do mecanismo em análise para instruir feitos de outra natureza, que não aquele definido na autorização judicial, muito menos para divulgar, sem a

permissão das pessoas envolvidas, aspectos da intimidade e da vida privada das mesmas. (SIQUEIRA FILHO, 1997)

2.3. LEI GERAL DAS TELECOMUNICAÇÕES

A Lei 9472 de 16 de julho de 1997, conhecida como Lei Geral das Telecomunicações, dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais, nos termos da Emenda Constitucional nº 8, de 1995. (BRASIL, 1997)

A referida Lei em seu Art. 3º define que o usuário de serviços de telecomunicações tem direito à inviolabilidade e ao segredo de sua comunicação, salvo nas hipóteses e condições constitucional e legalmente previstas. (BRASIL, 1997)

No Art. 19. a Lei define que à Agência compete adotar as medidas necessárias para o atendimento do interesse público e para o desenvolvimento das telecomunicações brasileiras, atuando com independência, imparcialidade, legalidade, impessoalidade e publicidade, e especialmente expedir normas sobre prestação de serviços de telecomunicações no regime privado. (BRASIL, 1997)

A Agência referida no artigo 19 trata-se da Agência Nacional de Telecomunicações (ANATEL) que é uma Autarquia especial criada pela Lei Geral de Telecomunicações (Lei 9.472, de 16 de julho de 1997). (ANATEL, 1997). Cabe à ANATEL organizar e definir regras referentes a exploração dos serviços de telecomunicações no Brasil.

A LGT define em seu Art. 60 que Serviço de telecomunicações é o conjunto de atividades que possibilita a oferta de telecomunicação, sendo que Telecomunicação é a transmissão, emissão ou recepção, por fio, radioeletricidade, meios ópticos ou qualquer outro processo eletromagnético, de símbolos, caracteres, sinais, escritos, imagens, sons ou informações de qualquer natureza. (BRASIL, 1997)

2.4. LEI Nº 9.034, DE 3 DE MAIO DE 1995

A Lei 9.034, de 3 de maio de 1995 dispõe sobre a utilização de meios operacionais para a prevenção e repressão de ações praticadas por organizações criminosas. Essa lei regula e admite a possibilidade de utilização de escuta ambiental como meio de prova.

Em seu Art. 1º a Lei define e regula meios de prova e procedimentos investigatórios que versem sobre ilícitos decorrentes de ações praticadas por quadrilha ou bando ou organizações ou associações criminosas de qualquer tipo. (BRASIL, 1995)

O Art. 2º permite em qualquer fase de persecução criminal, sem prejuízo dos já previstos em lei, os seguintes procedimentos de investigação e formação de provas: a ação controlada, que consiste em retardar a interdição policial do que se supõe ação praticada por organizações criminosas ou a ela vinculado, desde que mantida sob observação e acompanhamento para que a medida legal se concretize no momento mais eficaz do ponto de vista da formação de provas e fornecimento de informações; o acesso a dados, documentos e informações fiscais, bancárias, financeiras e eleitorais; a captação e a interceptação ambiental de sinais eletromagnéticos, óticos ou acústicos, e o seu registro e análise, mediante circunstanciada autorização judicial; infiltração por agentes de polícia ou de inteligência, em tarefas de investigação, constituída pelos órgãos especializados pertinentes, mediante circunstanciada autorização judicial. A autorização judicial será estritamente sigilosa e permanecerá nesta condição enquanto perdurar a infiltração. (BRASIL, 1995)

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

O Conselho Nacional de Justiça (CNJ), criado em 31 de dezembro de 2004 e instalado em 14 de junho de 2005, é um órgão do Poder Judiciário com sede em Brasília/DF e atuação em todo o território nacional, que visa, mediante ações de planejamento, à coordenação, ao controle administrativo e ao aperfeiçoamento do serviço público na prestação da Justiça. (CNJ, 2004)

A interceptação das comunicações é motivo de grande celeuma seja no Congresso Nacional por ocasião da apresentação à Câmara dos Deputados do Projeto de Lei n.

3.272/08, que objetiva limitar o uso da interceptação telefônica, bem como diante da instauração da CPI das Escutas Clandestinas, seja no Supremo Tribunal Federal quando alguns Ministros dessa Corte levantaram a hipótese de terem sofrido, eles próprios, a exceção de maneira ilegal. (KISTENMACHER , VANDRESEN, 2009)

Em 2008 o Conselho Nacional de Justiça publicou a Resolução nº 59, de 09 de setembro de 2008, que disciplina e uniformiza as rotinas visando ao aperfeiçoamento do procedimento de interceptação de comunicações telefônicas e de sistemas de informática e telemática nos órgãos jurisdicionais do Poder Judiciário, a que se refere a Lei no 9.296, de 24 de julho de 1996 (CNJ, 2008).

A Resolução inicialmente trata da distribuição e encaminhamento dos pedidos de interceptação visando o sigilo, sendo que em seu Art 1º define que as rotinas de distribuição, registro e processamento das medidas cautelares de caráter sigiloso em matéria criminal, cujo objeto seja a interceptação de comunicações telefônicas, de sistemas de informática e telemática, observarão disciplina própria, na forma do disposto na Resolução. (CNJ, 2008).

No Art. 2° é definido que os pedidos de interceptação de comunicação telefônica, telemática ou de informática, serão encaminhados à Distribuição em envelope lacrado contendo o pedido e documentos necessários (CNJ, 2008). O Art. 3°. define que na parte exterior do envelope será colada folha de rosto contendo somente as seguintes informações "medida cautelar sigilosa", delegacia de origem ou órgão do Ministério Público, e comarca de origem da medida (CNJ, 2008). O Art. 4°. veda a indicação do nome do requerido, da natureza da medida ou qualquer outra anotação na folha de rosto e o Art. 5°. define que no envelope referido no Art. 3º deverá ser anexado outro envelope menor, também lacrado, contendo em seu interior apenas o número e o ano do procedimento investigatório ou do inquérito policial (CNJ, 2008). No Art. 6°. é vedado ao Distribuidor e ao Plantão Judiciário receber os envelopes que não estejam devidamente lacrados conforme definido anteriormente (CNJ, 2008).

Os artigos 2º a 6º visam garantir o sigilo quanto às informações referentes ao feito e ao investigado de modo que tais informações se tornem disponíveis apenas ao juiz que tomará a decisão em relativizar ou não a inviolabilidade do sigilo.

Os artigos 7º a 9º tratam da rotina de recebimento dos envelopes pela serventia como o procedimento a ser adotado para cadastro e distribuição do envelope.

O Art. 10 trata do deferimento da medida cautelar de interceptação e caso sejam atendidos os requisitos legalmente previstos para deferimento da medida o Magistrado fará constar expressamente em sua decisão: a indicação da autoridade requerente; os números dos telefones ou o nome de usuário, e-mail ou outro identificador no caso de interceptação de dados; o prazo da interceptação; a indicação dos titulares dos referidos números; a expressa vedação de interceptação de outros números não discriminados na decisão; os nomes das autoridades policiais responsáveis pela investigação e que terão acesso às informações; os nomes dos funcionários do cartório ou secretaria responsáveis pela tramitação da medida e expedição dos respectivos ofícios, podendo reportar-se à portaria do juízo que discipline a rotina cartorária. (CNJ, 2008).

Para os casos de formulação de pedido verbal de interceptação previstos no artigo 4o, § 1o, da Lei no 9.296/96, o funcionário autorizado pelo magistrado deverá reduzir a termo os pressupostos que autorizem a interceptação, tais como expostos pela autoridade policial ou pelo representante do Ministério Público e a decisão judicial será sempre escrita e fundamentada. (CNJ, 2008).

O Art. 11 trata da expedição de ofícios às operadoras que em cumprimento à decisão judicial que deferir a medida cautelar sigilosa deverão ser gerados pelo sistema informatizado do respectivo órgão jurisdicional ou por meio de modelos padronizados a serem definidos pelas respectivas Corregedorias locais, dos quais deverão constar: número do ofício sigiloso; número do protocolo, data da distribuição; tipo de ação; número do inquérito ou processo; órgão postulante da medida (Delegacia de origem ou Ministério Público); número dos telefones que tiveram a interceptação ou quebra de dados deferida; a expressa vedação de interceptação de outros números não discriminados na decisão; advertência de que o ofício-resposta deverá indicar o número do protocolo do processo ou do Plantão Judiciário, sob pena de recusa de seu recebimento pelo cartório ou secretaria judicial, e advertência da regra contida no artigo 10 da Lei no 9.296/96 (CNJ, 2008).

O Art 12 trata das obrigações das operadoras de telefonia . Recebido o ofício da autoridade judicial a operadora de telefonia deverá confirmar com o Juízo os números cuja efetivação

fora deferida e a data em que efetivada a interceptação, para fins do controle judicial do prazo.

Semestralmente as operadoras indicarão em ofício a ser enviado à Corregedoria Nacional de Justiça os nomes das pessoas, com a indicação dos respectivos registros funcionais, que por força de suas atribuições, têm conhecimento de medidas de interceptações telefônicas deferidas, bem como os dos responsáveis pela operacionalização das medidas, arquivando-se referido ofício em pasta própria na Corregedoria Nacional. Sendo que sempre que houver alteração do quadro de pessoal, será atualizada a referida relação. (CNJ, 2008)

O Art. 13 trata das medidas apreciadas pelo Plantão Judiciário que durante o mesmo, as medidas cautelares sigilosas apreciadas, deferidas ou indeferidas, deverão ser encaminhadas ao Serviço de Distribuição da respectiva comarca, devidamente lacradas, porém, não será admitido pedido de prorrogação de prazo de medida cautelar de interceptação de comunicação telefônica, telemática ou de informática durante o plantão judiciário, ressalvada a hipótese de risco iminente e grave à integridade ou à vida de terceiros, bem como durante o Plantão de Recesso previsto artigo 62 da Lei no 5.010/66. Na Ata do Plantão Judiciário constará, apenas, a existência da distribuição de "medida cautelar sigilosa", sem qualquer outra referência, não sendo arquivado no Plantão Judiciário nenhum ato referente à medida. (CNJ, 2008)

O Art. 14 trata dos pedidos de prorrogação de prazo , sendo que quando da formulação de eventual pedido de prorrogação de prazo pela autoridade competente, deverão ser apresentados os áudios (CD/DVD) com o inteiro teor das comunicações interceptadas, as transcrições das conversas relevantes à apreciação do pedido de prorrogação e o relatório circunstanciado das investigações com seu resultado. Sempre que possível os áudios, as transcrições das conversas relevantes à apreciação do pedido de prorrogação e os relatórios serão gravados de forma sigilosa encriptados com chaves definidas pelo Magistrado condutor do processo criminal. Os documentos acima referidos serão entregues pessoalmente pela autoridade responsável pela investigação ou seu representante, expressamente autorizado, ao Magistrado competente ou ao servidor por ele indicado. (CNJ, 2008)

O Art. 15 define que o transporte dos autos para fora das unidades do Poder Judiciário deverá atender à seguinte rotina: serão os autos acondicionados em envelopes duplos; no envelope externo não constará nenhuma indicação do caráter sigiloso ou do teor do documento, exceto a tipificação do delito; no envelope interno serão apostos o nome do destinatário e a indicação de sigilo ou segredo de justiça, de modo a serem identificados logo que removido o envelope externo; o envelope interno será fechado, lacrado e expedido mediante recibo, que indicará, necessariamente, remetente, destinatário e número ou outro indicativo do documento; e o transporte e a entrega de processo sigiloso ou em segredo de justiça serão efetuados preferencialmente por agente público autorizado. (CNJ, 2008)

Os artigos 16 e 17 tratam da obrigação de sigilo e da responsabilidade dos agentes públicos, sendo que o Art. 16. define que no recebimento, movimentação e guarda de feitos e documentos sigilosos, as unidades do Poder Judiciário deverão tomar as medidas para que o acesso atenda às cautelas de segurança previstas nesta norma, sendo os servidores responsáveis pelos seus atos na forma da lei. No caso de violação de sigilo de que trata a Resolução, o magistrado responsável pelo deferimento da medida determinará a imediata apuração dos fatos. (CNJ, 2008)

E o Art. 17 define que não será permitido ao magistrado e ao servidor fornecer quaisquer informações, direta ou indiretamente, a terceiros ou a órgão de comunicação social, de elementos sigilosos contidos em processos ou inquéritos regulamentados pela Resolução, sob pena de responsabilização nos termos da legislação pertinente. (CNJ, 2008)

A fim de prestar informações sigilosas às Corregedorias-Gerais o Art. 18 define que mensalmente, os Juízos investidos de competência criminal informarão à Corregedoria Nacional de Justiça, por via eletrônica, em caráter sigiloso, a quantidade de interceptações em andamento.

O Art. 19 define que a Corregedoria Nacional de Justiça exercerá o a companhamento administrativo do cumprimento da Resolução.

O Art. 20 define que o Conselho Nacional de Justiça desenvolverá, conjuntamente com a Agência Nacional de Telecomunicações - ANATEL, estudos para implementar rotinas e

procedimentos inteiramente informatizados, assegurando o sigilo e segurança dos sistemas no âmbito do Judiciário e das operadoras.

2.6. PL 3272/2008

O Projeto de Lei 3272 apresentado em 16/04/2008 visa regulamentar a parte final do inciso XII do art. 5o da Constituição e dar outras providências, e quando aprovada revogará a Lei no 9.296, de 24 de julho de 1996, conforme Art. 26. (BRASIL, 2008)

No Art. 1º a Lei disciplina a quebra, por ordem judicial, do sigilo das comunicações telefônicas de qualquer natureza, para fins de investigação criminal e instrução processual penal. Para os fins desta Lei, considera-se quebra do sigilo das comunicações telefônicas de qualquer natureza todo ato que intervém no curso dessas comunicações com a finalidade de conhecer as informações que estão sendo transmitidas, incluindo a interceptação, escuta e gravação. O registro, a análise e a utilização da informação contida nas comunicações, objeto de quebra de sigilo por ordem judicial, sujeitam-se, no que couber, ao disposto nesta Lei. O disposto nesta Lei aplica-se ao fluxo de comunicações em sistemas de tecnologia da informação e telemática. (BRASIL, 2008)

O Art. 2º define que a quebra do sigilo das comunicações telefônicas de qualquer natureza é admissível para fins de investigação criminal e instrução processual penal relativas aos crimes apenados com reclusão e, na hipótese de crime apenado com detenção, quando a conduta delituosa tiver sido realizada por meio dessas modalidades de comunicação. Em nenhuma hipótese poderão ser utilizadas as informações resultantes da quebra de sigilo das comunicações entre o investigado ou acusado e seu defensor, quando este estiver atuando na função. (BRASIL, 2008)

Esta Lei se aplica apenas às comunicações de terceiros, ou seja, a gravação de conversa própria, com ou sem conhecimento do interlocutor, não se sujeita às disposições desta Lei., conforme Art. 3º. (BRASIL, 2008)

O Art. 4º define que o pedido de quebra de sigilo das comunicações telefônicas de qualquer natureza será formulado por escrito ao juiz competente, mediante requerimento do Ministério Público ou representação da autoridade policial, ouvido, neste caso, o

Ministério Público, e deverá conter: a descrição precisa dos fatos investigados; a indicação da existência de indícios suficientes da prática do crime objeto da investigação; a qualificação do investigado ou acusado, ou esclarecimentos pelos quais se possa identificá-lo, salvo impossibilidade manifesta devidamente justificada; a demonstração de ser a quebra de sigilo da comunicação estritamente necessária e da inviabilidade de ser a prova obtida por outros meios; e a indicação do código de identificação do sistema de comunicação, quando conhecido, e sua relação com os fatos investigados. (BRASIL, 2008)

Art. 5º O requerimento ou a representação será distribuído e autuado em separado, sob segredo de justiça, devendo o juiz competente, no prazo máximo de vinte e quatro horas, proferir decisão fundamentada, que consignará de forma expressa, quando deferida a autorização, a indicação dos indícios suficientes da prática do crime; dos indícios suficientes de autoria ou participação no crime, salvo impossibilidade manifesta devidamente justificada; do código de identificação do sistema de comunicação, quando conhecido, e sua relação com os fatos investigados; e do prazo de duração da quebra do sigilo das comunicações., sendo que este não poderá exceder a sessenta dias, permitida sua prorrogação por iguais e sucessivos períodos, desde que continuem presentes os pressupostos autorizadores da medida, até o máximo de trezentos e sessenta dias ininterruptos, salvo quando se tratar de crime permanente, enquanto não cessar a permanência. O prazo correrá de forma contínua e ininterrupta e contar-se-á a partir da data do início da quebra do sigilo das comunicações pela prestadora responsável pela comunicação, que deverá comunicar este fato, imediatamente, por escrito, ao juiz. Para cada prorrogação será necessária nova decisão judicial fundamentada. Durante a execução da medida de quebra de sigilo, caso a autoridade policial identifique que o investigado ou acusado passou a fazer uso de outro número, código ou identificação em suas comunicações, poderá formular, em caráter de urgência, pedido oral, que será reduzido a termo, de nova interceptação ao juiz, cuja decisão deverá ser proferida no prazo máximo de vinte e quatro horas, sendo que os autos seguirão para manifestação do Ministério Público e retornarão à autoridade judiciária que, então, reapreciará o pedido. (BRASIL, 2008)

O Art. 6º define que contra decisão que indeferir o pedido de quebra de sigilo caberá recurso em sentido estrito do Ministério Público, podendo o relator, em decisão fundamentada, conceder liminarmente o pedido de quebra. O recurso em sentido estrito

tramitará em segredo de justiça e será processado sem a oitiva do investigado ou acusado, a fim de resguardar a eficácia da investigação. (BRASIL, 2008)

O Art. 7º define que o mandado judicial que determinar a quebra do sigilo das comunicações deverá constar a qualificação do investigado ou acusado, quando identificado, ou o código de identificação do sistema de comunicação, quando conhecido. O mandado judicial será expedido em duas vias, uma para a prestadora responsável pela comunicação e outra para a autoridade que formulou o pedido de quebra do sigilo das comunicações e poderá ser expedido por qualquer meio idôneo, inclusive o eletrônico ou similar, desde que comprovada sua autenticidade. (BRASIL, 2008)

A prestadora responsável pela comunicação deverá implementar a quebra do sigilo autorizada, indicando ao juiz o nome do profissional responsável pela operação técnica, no prazo máximo de vinte e quatro horas, contado do recebimento da ordem judicial, sob pena de multa até o efetivo cumprimento da ordem, sem prejuízo das demais sanções cabíveis., conforme definido no Art 8º da lei. A prestadora não poderá alegar como óbice para a implementação da quebra do sigilo questão relativa ao ressarcimento dos custos pelos serviços de sua responsabilidade prestados para esse fim, que serão gratuitos. (BRASIL, 2008)

No Art. 9º a lei define que a decretação da quebra de sigilo de comunicação caberá ao juiz competente para o julgamento do crime investigado ou responsável pelo inquérito. (BRASIL, 2008)

Já o Art. 10 define que a execução das operações técnicas necessárias à quebra do sigilo das comunicações será efetuada sob a supervisão da autoridade policial e fiscalização do Ministério Público. (BRASIL, 2008)

Finalizadas as operações técnicas, a autoridade policial encaminhará, no prazo máximo de sessenta dias, ao juiz competente, todo o material produzido, acompanhado de auto circunstanciado, que deverá conter o resumo das operações realizadas., conforme Art 11 da lei. Decorridos sessenta dias do encaminhamento do auto circunstanciado, a autoridade policial inutilizará qualquer material obtido em virtude da quebra do sigilo das comunicações, salvo determinação judicial em contrário. (BRASIL, 2008)

O Art. 12. define que recebido o material produzido, o juiz dará ciência ao Ministério Público para que, se julgar necessário, requeira, no prazo de dez dias, diligências complementares. (BRASIL, 2008) Caso não haja requerimento de diligências complementares ou após a realização das que tiverem sido requeridas, o juiz intimará o investigado ou acusado para que se manifeste, fornecendo-lhe cópia identificável de todo o material produzido, conforme preconiza o Art 13. (BRASIL, 2008)

O Art. 14. define que as dúvidas a respeito da autenticidade ou integridade do material produzido serão dirimidas pelo juiz, aplicando-se, no que couber, o disposto nos arts. 145 a 148 do Código de Processo Penal. (BRASIL, 2008)

Conforme Art. 15 serão conservadas em cartório, sob segredo de justiça, as fitas magnéticas ou quaisquer outras formas de registro das comunicações cujo sigilo fora quebrado até o trânsito em julgado da sentença, quando serão destruídos na forma a ser indicada pelo juiz, de modo a preservar a intimidade dos envolvidos, sendo que enquanto for possível a revisão criminal, não se procederá a destruição. (BRASIL, 2008)

Caso a quebra do sigilo das comunicações telefônicas de qualquer natureza revelar indícios de crime diverso daquele para o qual a autorização foi dada e que não lhe seja conexo, a autoridade deverá remeter ao Ministério Público os documentos necessários para as providências cabíveis, conforme definido no Art. 16. (BRASIL, 2008)

O Art. 17 define que a prova obtida por meio da quebra de sigilo das comunicações telefônicas de qualquer natureza realizada sem a observância desta Lei não poderá ser utilizada em qualquer investigação, processo ou procedimento, seja qual for sua natureza. (BRASIL, 2008)

O Art. 18 define que correrão em segredo de justiça os inquéritos e processos que contiverem elementos informativos ou provas obtidos na forma desta Lei. (BRASIL, 2008)

As gravações ambientais são tratadas na lei conforme o Art. 20. que define que as gravações ambientais de qualquer natureza, quando realizadas pela autoridade policial, sujeitam-se às disposições da Lei, no que couber. (BRASIL, 2008)

O Art. 21. define que fica o Poder Executivo autorizado a instituir, para fins exclusivamente estatísticos e de planejamento de ações policiais, sistema centralizado de informações sobre quebra de sigilo de comunicações telefônicas de qualquer natureza, na

forma do regulamento. O referido sistema não conterá o conteúdo das comunicações realizadas nem os códigos de identificação ou outros elementos e meios capazes de identificar os envolvidos, inclusive investigados e acusados. (BRASIL, 2008)

Segundo o Art. 22. A Agência Nacional de Telecomunicações - ANATEL regulamentará, no prazo de cento e oitenta dias, o padrão dos recursos tecnológicos e facilidades necessárias ao cumprimento desta Lei, a serem disponibilizados gratuitamente por todas as prestadoras responsáveis pela comunicação. (BRASIL, 2008)

O Art. 23. altera o Código Penal, em seu Art. 151 com a seguinte redação Art. 151-A. Violar sigilo de comunicação telefônica de qualquer natureza, sem autorização judicial ou com objetivos não autorizados em lei. Pena - reclusão, de dois a quatro anos, e multa. Incorre na mesma pena quem violar segredo de justiça de quebra do sigilo de comunicação telefônica de qualquer natureza.” (BRASIL, 2008)

Na justificativa para a proposição do Projeto de Lei é levado em conta o respeito ao princípio da reserva de lei proporcional, a regulamentação da matéria há de resultar da escrupulosa ponderação dos valores em jogo, observado o princípio da proporcionalidade, entendido como justo equilíbrio entre os meios empregados e os fins a serem alcançados, que deve levar em conta os seguintes elementos: a) adequação: a aptidão da medida para atingir os objetivos pretendidos; b) necessidade: como exigência de limitar um direito para proteger outro, igualmente relevante; c) proporcionalidade estrita: a ponderação entre a restrição imposta (que não deve aniquilar o direito); e d) a vantagem alcançada. (BRASIL, 2008)

O requerimento de quebra de sigilo das comunicações passa a ser disciplinado de forma mais rigorosa e objetiva, diferente da Lei atual que sequer exige a forma escrita para tal. Este procedimento mais detalhado é fruto do entendimento sobre a quebra do sigilo telefônico, pois se por um lado é importante meio de prova, por outro deve ser disciplinado de forma precisa, considerando que não deixa de ser odioso meio de interferência estatal na vida do particular. (BRASIL, 2008)

2.7. NORMAS E RESOLUÇÕES DA ANATEL

A ANATEL criada para disciplinar o modelo das telecomunicações no Brasil conforme LGT, publicou alguns documentos que disciplinam questões relativas ao provimento de serviços de telecomunicações bem como questões relativas ao sigilo das comunicações e quebra das mesmas.

Em 2005, já havia preocupação da agência com relação aos sigilos, após ter conhecimento de problemas dessa natureza em uma reunião foi destacado que à Anatel cumpre zelar pela prática, pela não prática, por esse tipo de comportamento, e o que chama a atenção é que hoje já há uma constituição democrática, princípios de se resguardar pela privacidade e a empresa deveria resguardar essa ética, também foi destacado por um conselheiro que a ANATEL não deve ter atitudes passivas ou esperar que o problema venha afetar o usuário para depois tomar decisões. (ANATEL, 2005)

Conforme notícia veiculada no site da ANATEL (ANATEL, 2008) em depoimento à Comissão Parlamentar de Inquérito com a Finalidade de Investigar Escutas Telefônicas Clandestinas/Ilegais - mais conhecida como CPI da Escuta, o então presidente da Agência Nacional de Telecomunicações (ANATEL), Ronaldo Sardenberg, afirmou que a Agência e as empresas de telefonia têm preocupação constante com a segurança das redes de telecomunicações, mas que a inviolabilidade do sigilo das telecomunicações é de responsabilidade das operadoras. Sardenberg também esclareceu aos parlamentares que a Agência não tem conhecimento prévio das solicitações de interceptações de comunicação. "A ordem judicial, até por questões de sigilo, é apresentada diretamente à operadora e não à Anatel", afirmou. (ANATEL, 2008)

Os principais pontos abordados pelo presidente da Anatel foram os aspectos legais: Artigo 5º da Constituição Federal de 1988; Lei nº 9.296/96, Lei de Interceptação Telefônica; Lei n° 9.472/97; Lei Geral de Telecomunicações (LGT). “O usuário tem direito à inviolabilidade e ao segredo de sua comunicação, salvo nas hipóteses e condições legalmente previstas". O mesmo artigo garante aos usuários de telecomunicações o respeito à privacidade nos documentos de cobrança e na utilização de dados pessoais pela prestadora dos serviços. (ANATEL, 2008)

Outro ponto abordado foi a Regulamentação e inviolabilidade do sigilo, que é regida pelos regulamentos do Serviço Telefônico Fixo Comutado (Resolução 426/2005) e do Serviço Móvel Pessoal (Resolução 477/2008) que estabelecem as obrigações das operadoras quanto à inviolabilidade do sigilo. A prestadora é responsável pela inviolabilidade do sigilo das comunicações em suas redes, exceto nos segmentos instalados no imóvel do assinante da telefonia fixa. Cabe à prestadora zelar pelo sigilo inerente ao serviço por ela prestado e pela confidencialidade quanto aos dados e informações, com o emprego de meios e tecnologia que assegurem este direito do usuário. (ANATEL, 2008)

Foi tratado ainda que o atendimento às solicitações judiciais é obrigatório e a ordem judicial é apresentada diretamente à operadora (e não à ANATEL). A prestadora deve tornar disponíveis os recursos tecnológicos e as facilidades necessárias à suspensão de sigilo de telecomunicações, determinada por autoridade judiciária ou legalmente investida desses poderes. Cabe à prestadora manter controle permanente de todos os casos, acompanhar a efetivação dessas determinações e zelar para que elas sejam cumpridas dentro dos estritos limites autorizados. Caso a solicitação judicial não seja atendida, e independentemente das medidas jurídicas que o Judiciário tomar, a ANATEL determina a abertura de 'Procedimento para Apuração de Descumprimento de Obrigação' (PADO) que pode resultar em aplicação de advertência, multa, suspensão temporária, caducidade ou declaração de inidoneidade. (ANATEL, 2008)

Sardenberg citou ainda que a ANATEL dispõe de procedimentos de fiscalização para averiguar o cumprimento da regulamentação, pela operadora, sobre inviolabilidade, principalmente na rede externa do STFC. Nos trechos de rede externa, os armários de distribuição devem ser mantidos invioláveis pelas prestadoras e são, por essa razão, objeto de fiscalização programada da Agência. A ANATEL tem realizado ações de fiscalização para averiguar o estágio de segurança da rede externa das operadoras. Trata-se de operação constante, com vistas a coibir o acesso de pessoas não autorizadas às linhas telefônicas dos usuários em centrais de comutação, em armários de distribuição e em pontos de terminação de rede. (ANATEL, 2008)

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

Apesar da ANATEL não receber as ordens judiciais autorizando a quebra de sigilo dos investigados, a ela recai a atribuição de normatizar e fiscalizar os procedimentos para a referida quebra. O Regulamento dos Serviços de Telecomunicações que foi aprovado pela Resolução nº 73, de 25 de novembro de 1998, reitera em seu Art. 9º, inciso V que são assegurados aos usuários dos serviços de telecomunicações o direito a inviolabilidade e o segredo de sua comunicação, salvo nas hipóteses e condições constitucionais e legalmente previstas. (ANATEL, 1998)

O Art. 26. define novamente que a Prestadora observará o dever de zelar estritamente pelo sigilo inerente aos serviços de telecomunicações e pela confidencialidade quanto aos dados e informações, empregando todos os meios e tecnologia necessárias para assegurar este direito dos usuários. (ANATEL, 1998)

Considerando a possibilidade de quebra de sigilo o parágrafo único do Art 26. define que a Prestadora tornará disponíveis os recursos tecnológicos necessários à suspensão de sigilo de telecomunicações determinada por autoridade judiciária ou legalmente investida desses poderes e manterá controle permanente de todos os casos, acompanhando a efetivação destas determinações e zelando para que elas sejam cumpridas dentro dos estritos limites autorizados. (ANATEL, 1998)

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

A resolução da ANATEL 272, de 9 de agosto de 2011, abrange novamente a questão do sigilo das comunicações e seu afastamento. No Art. 57. fica definido que a prestadora observará o dever de zelar estritamente pelo sigilo inerente aos serviços de telecomunicações e pela confidencialidade quanto aos dados e informações do assinante, empregando todos os meios e tecnologia necessárias para assegurar este direito dos usuários. (ANATEL, 2001)

E em seu parágrafo único deixa claro que a prestadora tornará disponíveis os dados referentes à suspensão de sigilo de telecomunicações para a autoridade judiciária ou legalmente investida desses poderes que determinar a suspensão de sigilo. (ANATEL, 2001)

No art. 59. é definido que o assinante do SCM têm direito, sem prejuízo do disposto na legislação aplicável à inviolabilidade e ao segredo de sua comunicação, respeitadas as hipóteses e condições constitucionais e legais de quebra de sigilo de telecomunicações;

O capítulo 2 desse trabalho traz um apanhado geral da legislação aplicada ao sigilo e à possibilidade de interceptação das comunicações. Conforme apresentado, a preocupação do legislador é focada no direito à privacidade do cidadão. Apesar da privacidade ser considerada um direito fundamental, existe a possibilidade de quebra do sigilo das comunicações conforme definido na Constituição. Para regular a forma como o sigilo pode ser quebrado, existem diversas restrições definidas por normas infraconstitucionais que tem o objetivo principal de evitar que os grampos ilegais e em justificativa sejam efetivados.

A legislação vigente, seja a Constituição, Leis ou Normas não definem a ferramenta que deve ser utilizada para a obtenção dos sinais de áudio resultantes da interceptação, nem tampouco fazem qualquer restrição quanto as formas de interceptação.

As Normas definem que as operadoras tem a obrigação de fornecer meios para possibilitar a quebra do sigilo, mas quando se trata de comunicações de utilizando rede de dados e o fluxo de dados trafega criptografado, as operadoras podem apenas fornecer os dados da forma como trafegam, ou seja, criptografados. As operadoras não são capazes de fornecer a informação já que não possuem as chaves necessárias para decifrar os dados.

3. METODOLOGIA PROPOSTA

O sistema proposto deve atender a duas principais premissas que são, fomentar a investigação com os registros de áudio de comunicações ponto a ponto e ambientais e garantir a validade probatória dos registros gerados. Os requisitos jurídicos e técnicos para o atendimento a essas premissas são citados a seguir

3.1. REQUISITOS

3.1.1. REQUISITOS LEGAIS

Os requisitos legais para o desenvolvimento do sistema passam pela (1) autorização judicial para instalação do sistema atendendo ao art. 5º, inciso XII, seguindo o que regem as normas infraconstitucionais constantes na Lei 9.296/96 e na Resolução nº 59/08 do CNJ, além de outras normas aplicáveis.

Além da necessidade de haver autorização para implementação da interceptação, é necessário garantir que o áudio seja válido como prova. Assim como qualquer vestígio, o áudio deve atender a (2) manutenção da cadeia de custódia ou seja, deve ser garantida a integridade, a confidencialidade e autenticidade e não-repúdio.

3.1.2. REQUISITOS TÉCNICOS

Um dos requisitos técnicos a ser atendido no sistema é que o mesmo seja de (1) difícil detecção, para que o investigado não saiba que está sendo monitorado, pois caso contrário, o processo de investigação poderá ser frustrado.

Para obter o áudio em conversações através de *VoIP* é necessário (2) adquirir o áudio do microfone e do alto-falante separadamente. Para possibilitar a reconstrução correta do áudio, que será armazenado em amostras, é necessário (3) definir marcadores de tempo em cada amostra de áudio e para garantir a confidencialidade deve-se (4) cifrar as amostras de áudio antes de (5) armazená-las em memória de massa.

Uma vez armazenadas, as amostras de áudio poderão ser (6) transmitidas para a máquina de análise, sendo que os registros já transmitidos devem ser (7) marcados no dispositivo onde foram obtidos.

3.2. VISÃO GERAL

As seções seguintes constantes nesse capítulo apresentam uma possível forma de implementar o sistema de forma que os requisitos elencados sejam atendidos, sendo que o sistema pode ser implementado de outras maneiras, desde que os requisitos sejam atendidos.

A fig. 3.1 ilustra o diagrama em blocos geral do sistema proposto, sendo que no decorrer do capítulo os blocos serão abordados individualmente descrevendo as suas funções dentro do sistema como um todo.

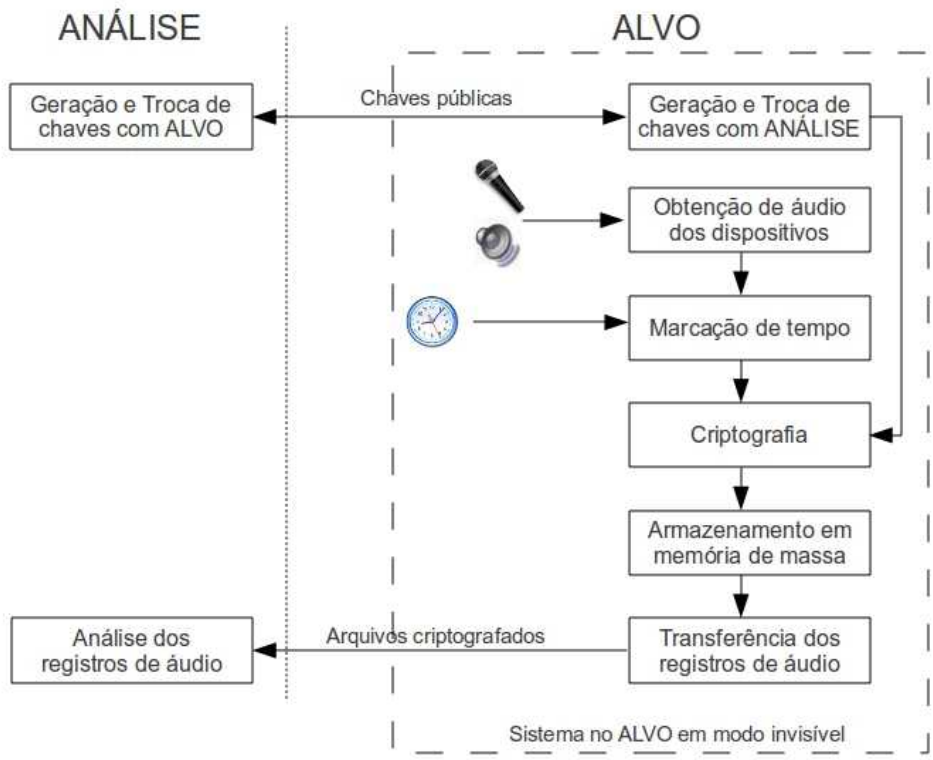

Figura 3.1 - Visão Geral do Sistema

Esse trabalho visa a obtenção de registros de áudio, armazenamento e transmissão se for possível e necessário. O sistema na máquina do alvo pode rodar em modo invisível para reduzir a possibilidade do mesmo ser descoberto, podendo ser em nível de *kernel*, de *driver* ou mesmo em nível de usuário.

Algumas definições do sistema do alvo que são importantes para o sistema de aquisição de áudio serão apresentadas a seguir.

3.3. PREPARAÇÃO

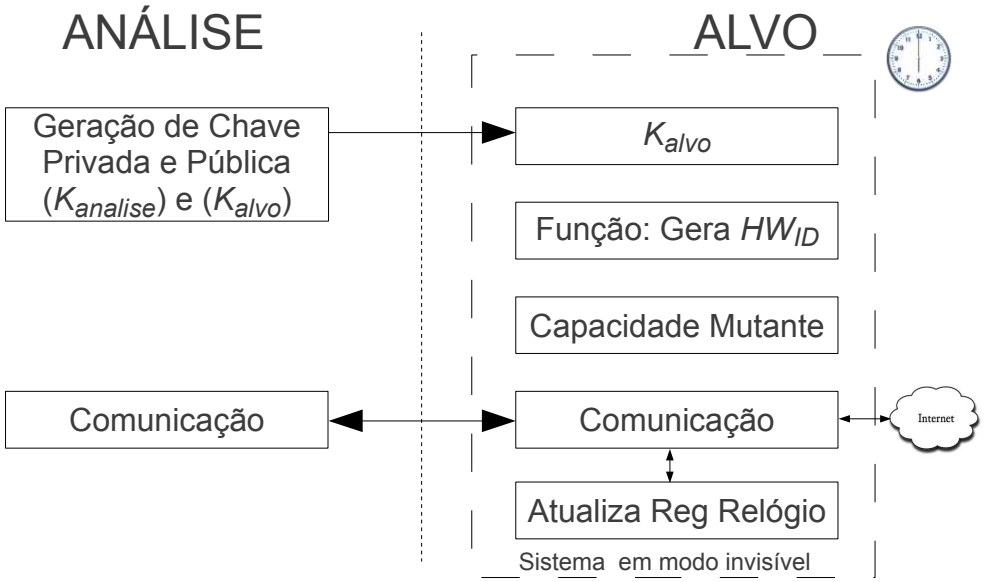

Figura 3.2 - Sistemas antes da instalação do sistema invisível

Considerando a comunicação entre o sistema da análise e o sistema alvo, há a necessidade de desenvolvimento além do sistema invisível no alvo, um sistema na análise de modo a receber, validar e disponibilizar os registros aos agentes da investigação.

A fig. 3.2 ilustra as características dos sistemas na máquina de análise e na máquina alvo antes dos mesmos realizarem a aquisição de áudio. Os sistemas ilustrados são os que devem estar disponíveis na máquina análise e prontos para serem instalados na máquina do alvo.

No sistema de análise será gerado um par de chaves, $K_{analise}$ e K_{alvo}, do esquema *RSA*, onde $K_{analise}$ é a chave privada da análise e K_{alvo} a chave pública da análise, que será incluída no código do sistema invisível no alvo. Além da chave K_{alvo} o sistema da máquina alvo terá um número que o identifica, que será doravante referido por A_{ID}, sendo este inalterado durante todo o processo e um número de versão, que será doravante referido por V, que identifica a versão do sistema instalado na máquina alvo, sendo que este número é alterado a cada alteração realizada no sistema na máquina alvo. A chave K_{alvo}, e os números A_{ID} e V são incluídos no código do sistema da máquina do alvo.

O sistema na máquina alvo deve ser capaz de obter informações do hardware e características do sistema operacional e gerar um número com base nessas informações; esse número será doravante chamado de HW_{ID}.

O relógio do sistema na máquina alvo deve ser atualizado através de um servidor de *NTP*. Todas as vezes que o sistema na máquina alvo inicializar este deverá consultar o servidor *NTP* a fim de identificar o horário a ser considerado, em seguida calcula a diferença entre o horário obtido do servidor de *NTP* e o horário do hardware da máquina alvo e armazena esta diferença em memória de massa, sendo que essa diferença será doravante referida por DIF_{tempo}. Uma vez existente o DIF_{tempo} no sistema da máquina do alvo, caso a máquina do alvo não tenha disponível conexão com Internet no momento da inicialização, o DIF_{tempo} poderá ser utilizado para estimar o horário do servidor *NTP* com base no horário local da máquina do alvo. Logo na instalação do sistema invisível na máquina do alvo o valor de DIF_{tempo} será zero, e logo após a instalação o sistema na máquina alvo tentará realizar conexão com o servidor *NTP* e em caso de sucesso atualizará o DIF_{tempo}. O servidor de *NTP* utilizado pode estar disponível na própria máquina de análise, caso o sistema da máquina do alvo não consiga conexão com a máquina de análise poderá tentar conexão com outros servidores de *NTP* disponíveis na Internet.

A comunicação entre o sistema na máquina alvo e o sistema na máquina análise é feita sempre através de uma solicitação do sistema na máquina alvo, que possui em seu código o endereço *IP* da máquina da análise. As comunicações são feitas de forma similar às comunicações feitas pelos navegadores nas quais o sistema da máquina do alvo solicita ao sistema de análise instruções a serem executadas. O sistema da máquina de análise nunca abre comunicação com o sistema da máquina do alvo de modo a evitar detecções. Considerando que as instruções são enviadas pelo sistema da máquina de análise e que o mesmo não inicia qualquer conexão com o sistema da máquina alvo, o sistema da máquina do alvo deve em intervalos de tempos definidos fazer uma verificação no sistema da máquina de análise se há alguma instrução a ser executada, esse intervalo de tempo pode ser alterado e inicialmente é definido em 5 minutos. O sistema da máquina alvo mantém em seu módulo de comunicação um *log* de eventos de forma a identificar toda a comunicação entre sistema da máquina alvo e sistema da máquina de análise, bem como as

instruções enviadas pelo sistema da máquina de análise, possibilitando que posteriormente seja feita auditoria no sistema identificando todas as ações executadas.

O sistema da máquina alvo será mutante, ou seja terá a funcionalidade de alterar algumas funções internas, ou até mesmo o sistema completamente. Essa funcionalidade possibilitará a instalação de funções e tende a reduzir a possibilidade de ataque através de engenharia reversa, além de possibilitar a atualização periódica da chave K_{alvo} e das demais variáveis do sistema.

3.3.1. Plugins disponíveis para instalação no sistema alvo

O sistema na máquina alvo, inicialmente deve ser o menor possível, sendo basicamente um *downloader* de modo a tornar rápido e imperceptível o *download* e instalação. Porém, é necessário que as funcionalidades básicas estejam disponíveis para que o sistema possa atender aos requisitos. A capacidade mutante do sistema da máquina alvo lhe permite dentre outras coisas, instalar módulos de funcionalidades que estarão disponíveis no sistema na máquina de análise.

Um dos módulos a ser instalado no sistema da máquina do alvo tem a função de obter informações da máquina do alvo. O referido m deverá ser capaz de obter informações relativas aos dispositivos de som instalados, como marca, modelo, endereçamento, interrupção, bem como informações dos *drivers* instalados no sistema operacional que acessam esses dispositivos. Além dos dispositivos de áudio é importante que se tenha conhecimento dos dispositivos de rede instalados na máquina alvo bem como a largura de banda disponível, isso auxiliará na decisão da forma mais adequada para a transmissão dos dados; também quais as características do *hardware* da máquina alvo tais como processador, quantidade de memória volátil e quantidade de memória de masa, utilizada e disponível. Os detalhes de memória de massa são relevantes para a determinação da "autonomia" de gravação e da necessidade ou não de compactação dos dados obtidos.

Além do módulo para obtenção das informações da máquina alvo, existem os outros módulos para aquisição do áudio, codificação, criptografia, dentre outros que serão abordados em seções específicas nesse trabalho.

3.4. PRIMEIRO ACESSO

Após instalado o sistema na máquina alvo, o mesmo irá iniciar automaticamente cada vez que o sistema operacional da máquina alvo for inicializado.

3.4.1. Ajuste do relógio na máquina alvo

Sempre que o sistema na máquina alvo inicializar, irá buscar no servidor de *NTP* o registro de data e hora atual, realizará comparação com o registro de data e hora da máquina alvo e essa diferença será comparada com a variável DIF_{tempo}, caso a DIF_{tempo} não seja igual a diferença entre horários, DIF_{tempo} será atualizada e haverá um registro nos *logs*.

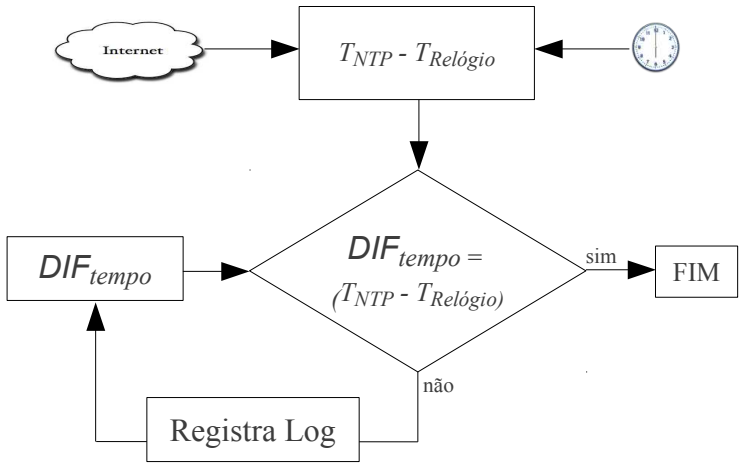

Figura 3.3 - Ajuste do relógio no sistema da máquina alvo

3.4.2. Geração do número de identificação de máquina (HW_{ID})

O sistema na máquina alvo gerará um número HW_{ID} que será gerado com base nos componentes instalados na máquina do alvo, em especial aqueles utilizados pelo sistema. O objetivo do HW_{ID} é evitar que em cada conexão entre o sistema da máquina alvo e o sistema de análise seja necessário o envio de todas as informações dos dispositivos e respectivos *drivers*. O HW_{ID} será baseado nos dispositivos de áudio, de rede, discos rígidos e seus respectivos *drivers*. A forma para a geração do HW_{ID} pode ser através de cálculos de *hash* simples utilizando por exemplo o algoritmo *SHA1*, dessa forma são obtidas *strings* das especificações dos dispositivos e seus *drivers* e calculados os *hashes* com base nas mesmas, gerando assim o HW_{ID}, sendo que essa variável não é armazenada em memória

de massa sendo mantida em memória *RAM* enquanto não for encaminhada ao sistema da análise.

3.5. COMUNICAÇÃO COM O SISTEMA DA ANÁLISE

O sistema de análise não abrirá comunicação com o sistema da máquina alvo, de modo a evitar detecção por um possível sistema de proteção instalado na máquina do alvo. As comunicações entre sistema de análise e sistema da máquina do alvo serão iniciadas pelo sistema da máquina do alvo. O sistema da máquina alvo, que possui em seu código o endereço *IP* da máquina de análise abre uma conexão para esse endereço. Para responder às solicitações realizadas pela máquina do alvo, o sistema da máquina de análise possui um servidor através do qual são passados os comandos a serem executados no sistema da máquina do alvo.

A fig. 3.4 ilustra os eventos de cada conexão que é aberta entre o sistema da máquina alvo e o sistema da máquina de análise, sendo que o sistema da máquina alvo envia no início da conexão (1) o número de identificação A_{ID}, e o número da versão do sistema, V utilizando a chave K_{alvo}, sendo a mensagem transmitida $M=A_{ID}||Enc(K_{alvo},V, A_{ID})$. Com essa mensagem o sistema da análise identifica (2) o alvo, através do A_{ID}, seleciona a chave $K_{analise}$ referente ao AID recebido e decifra (3) a mensagem Dec($K_{analise}$, Enc(K_{alvo},V, AID) = V, AID; depois compara (4) o número de identificação AID que foi recebido em claro e cifrado para verificar a integridade do mesmo, se forem iguais o sistema de análise considera que o sistema da máquina alvo é o sistema que possui o identificador do alvo A_{ID}. A partir desse momento, todas as comunicações entre o sistema da máquina alvo e o sistema de análise serão cifradas através do par de chaves K_{alvo} e $K_{analise}$. O sistema de análise compara o número de versão recebido com o número existente na base de dados na máquina de análise e envia (5) ao sistema da máquina alvo o identificador de hardware, HW_{ID}, cifrado com a chave $K_{analise}$.

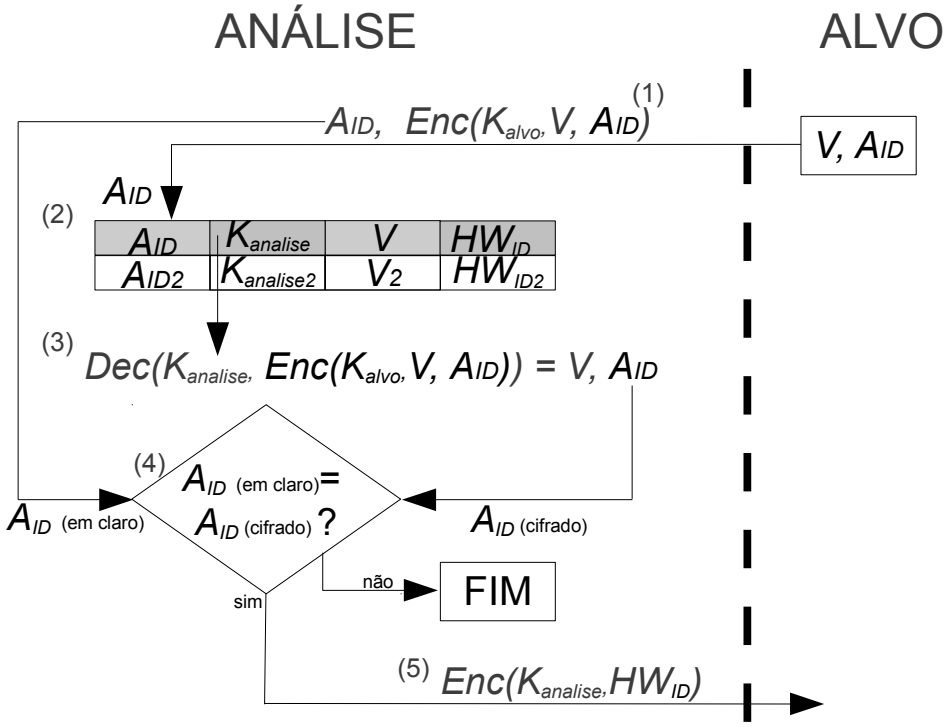

Figura 3.4 - Comunicação entre sistema de análise e alvo

A fig. 3.5 ilustra os eventos após a máquina alvo receber o HW_{ID} cifrado. A máquina alvo gera (1) o número identificador de *hardware* e recebe (2) o número identificador armazenado na base de dados da máquina de análise, conforme (5) da fig. 3.4. A máquina alvo decifra (3) a mensagem com K_{alvo} e obtém HW_{ID}. Em seguida compara (4) $HW_{IDgerado}$ com número HW_{ID} recebido, se forem diferentes o sistema da máquina alvo envia (5) o novo identificador de hardware gerado e os dados dos dispositivos e *drivers* cifrados com a chave $K_{analise}$, se forem iguais o sistema da máquina alvo envia (6) apenas o HW_{ID} cifrado com a chave $K_{analise}$.

O sistema da máquina de análise, decifra a mensagem, sendo esse processo não ilustrado na figura, e deve ser considerado implícito, e obtém HW_{ID}. Em seguida verifica se HW_{ID} é igual ao identificador armazenado em sua base de dados, caso igual, aguarda (7) o próximo contato do sistema da máquina alvo. Caso HW_{ID} seja diferente do identificador existente na base de dados da máquina de análise o sistema realizará (8) a atualização da sua base de dados com HW_{ID} e dados de dispositivos para atualizar também na base de dados da máquina de análise.

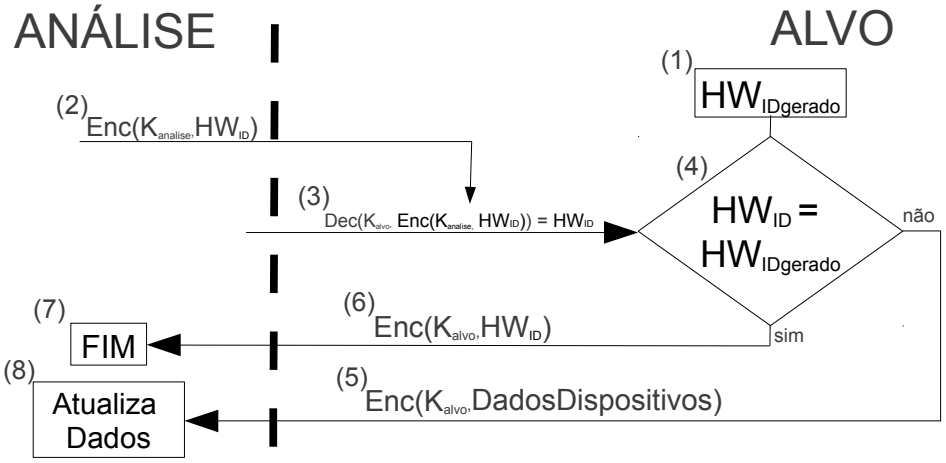

Figura 3.5: Atualização de dados de hardware

Após as comunicações realizadas entre o sistema da máquina alvo e o sistema de análise conforme ilustrado nas fig. 3.4 e 3.5, o sistema de análise entrará em espera aguardando uma comunicação do sistema da máquina do alvo.

O agente de análise poderá definir no sistema da máquina de análise uma sequência de ações que deseja realizar, tais como atualizar o sistema furtivo na máquina do alvo, atualizar as chaves, fazer *download* de amostras de áudio, dentre outras.

A sequência de ações referida ficará armazenada em uma "fila de ações". O sistema da máquina do alvo em intervalos de tempos periódicos abrirá uma conexão com o sistema da máquina de análise buscando ações a serem realizadas; a cada solicitação o sistema de análise irá enviar a primeira ação existente na "fila de ações".

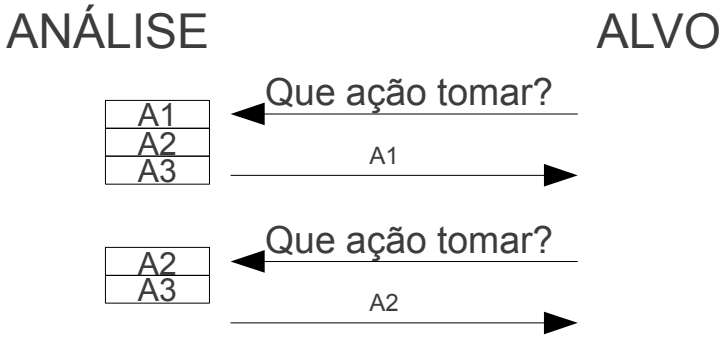

Figura 3.6: Ações a serem executadas

3.6. ATUALIZAÇÃO DO SISTEMA DA MÁQUINA ALVO

O sistema da máquina alvo inicialmente será o menor possível de modo que o *download*, se necessário, seja rápido evitando que usuário alvo desconfie que está ocorrendo o *download* e instalação do sistema furtivo. A função mutante do sistema da máquina alvo permite que funcionalidades e *plugins* necessários sejam instalados posteriormente, de acordo com as necessidades específicas da investigação e das características técnicas do sistema do alvo.

Com as informações dos dispositivos existentes na máquina alvo, o sistema de análise seleciona os *plugins* a serem encaminhados ao sistema da máquina alvo, tais como pacote de acesso aos dispositivos, de obtenção de áudio, de compressão, de criptografia e de transmissão.

Baseado nas informações dos dispositivos da máquina do alvo, o sistema da máquina de análise verifica se existem disponíveis *plugins* disponíveis para esses dispositivos e os disponibiliza para o sistema da máquina do alvo instalá-los. Em certos casos, o conhecimento das informações dos dispositivos é irrelevante, como por exemplo, para o caso em que o acesso aos dispositivos de áudio, de armazenamento e rede ocorrerem através de bibliotecas existentes nos sistemas operacionais, tornando transparente o acesso independente do tipo de dispositivo.

Por outro lado, caso haja a necessidade de o sistema furtivo acessar os dispositivos de *hardware* diretamente a informação dos dispositivos do alvo será relevante para a definição correta do *plugin* que fará o acesso aos dispositivos.

Caso não haja *plugins* referentes aos dispositivos da máquina do alvo na biblioteca do sistema da máquina de análise, o sistema de análise fará uma notificação ao analista informando a necessidade de desenvolvimento dos *plugins* necessários.

Caso exista na base de dados os *plugins* referentes aos dispositivos instalados na máquina alvo, a máquina de análise irá encaminhá-los para serem instalados no sistema da máquina alvo. Essa instalação é feita pelo sistema da máquina alvo, através da característica mutante que o mesmo possui.

3.6.1. Módulo de Obtenção de Áudio

O módulo de obtenção de áudio deve ser capaz de abrir como leitura qualquer dispositivo de áudio instalado na máquina do alvo e armazenar o áudio em memória. A obtenção do áudio deve ser feita em cada dispositivo separadamente, porém é necessário que seja mantida a possibilidade de sincronização temporal entre os diversos dispositivos. A sincronização é feita através da indicação do tempo em que a amostra foi obtida, e é armazenada junto com a mesma. De modo a reduzir a memória de massa necessária para o armazenamento do áudio obtido, o áudio será compactado utilizando técnicas de compressão de áudio conhecidas, tais como *IMA ADPCM, MP3*, *SILK* ou outro método que atenda as necessidades, sendo que a escolha de qual método de compressão será utilizado, dependerá principalmente da quantidade de memória de massa disponível, da largura de banda disponível e da capacidade computacional da máquina do alvo.

Além dos parâmetros da máquina do alvo, a decisão de qual a técnica de compressão será utilizada, levará em conta a qualidade do sinal de voz disponível. O sinal de áudio a ser obtido deve ter qualidade suficiente para a realização futura de um exame de verificação de locutor, através do qual é possível atribuir de quem é a voz existente no áudio. Assim, é preciso que a técnica utilizada na compactação do áudio tenha um compromisso entre capacidade da máquina do alvo e qualidade do sinal, já que a maioria das técnicas de compactação geram perdas de sinal.

3.6.1.1. Forma de acesso aos dispositivos

Inicialmente será necessário obter o áudio dos dispositivos da máquina alvo, seja o microfone, fone ou outros dispositivos de áudio disponíveis. A leitura do dispositivo pode ser feita em diversas camadas, através do acesso direto ao dispositivo, ou utilizando bibliotecas nativas do sistema operacional ou ainda utilizando bibliotecas multiplataformas para acesso a dispositivos.

Para a leitura dos dispositivos realizando acesso direto ao mesmo, é necessário conhecer os parâmetros técnicos de cada dispositivo a ser aberto, como endereçamento e interrupção, o processo é transparente não sofrendo interferência do sistema operacional, porém, para cada modelo de dispositivo deverá ser desenvolvido um código específico. A dificuldade

inerente a esse tipo de acesso é que o sistema furtivo deverá rodar ou em modo *kernel* ou como um *driver* de dispositivo, tornando mais complexo o desenvolvimento e inoculação na máquina do alvo.

Para a leitura dos dispositivos utilizando bibliotecas nativas dos sistemas operacionais será necessário atentar para a possibilidade do sistema operacional realizar algum tipo de bloqueio de acesso por parte do sistema da máquina alvo, uma vez que quem fará o controle propriamente dito do dispositivo é o sistema operacional. A grande vantagem dessa escolha é que o código desenvolvido poderá ser utilizado com qualquer dispositivo, desde que a máquina do alvo execute o sistema operacional que tenha a biblioteca utilizada.

É possível ainda desenvolver o sistema de modo que acesse os dispositivos através de bibliotecas desenvolvidas para esse fim, como o *DirectSound*, que possui suporte a diversos sistemas operacionais e tem evoluído e mantendo a compatibilidade com as versões antigas. A utilização dessas bibliotecas, da mesma forma como nas bibliotecas nativas, poderá experimentar problemas devido ao controle do sistema operacional. Geralmente o *DirectSound* possui uma menor latência, o que pode ser interessante na etapa de tomada de decisão de quais sinais armazenar.

O *DirectSound* é uma interface de programação de aplicativos (*API*) que provê uma interface de baixa latência com o *driver* da placa de som dos dispositivos, suportando mixagem e gravação de várias *streams* de áudio. (MICROSOFTb, s.d) O *DirectSound* é usado principalmente para o desenvolvimento de jogos, porém pode ser usado em outras aplicações que utilizem os dispositivos de áudio.

Utilizando a interface do *DirectSound* é possível tocar sons no formato *WAV*, tocar múltiplos sons simultaneamente, associar sons de alta prioridade à *buffers* controlados por *hardware*, utilizar som em ambiente *3D*, incluir efeitos como *echo* e alterar parâmetros de efeitos dinamicamente e capturar sons no formato *wav* de microfone ou outra entrada de áudio. (MICROSOFTc, s.d)

DirectSound funciona no *Windows 98*, *Windows 2000,* e sistemas operacionais *Windows* mais novos. Algumas funcionalidade estão disponíveis apenas no *Windows XP* ou mais novos. (MICROSOFTc, s.d)

No *Windows Vista* a camada de abstração de hardware para áudio foi retirada, o que limitou os desenvolvedores de jogos. Com a decisão da *Microsoft* de remover a camada de *hardware* para áudio, os jogos existentes que utilizavam *DirectSound 3D* não mais utilizam algoritmos de *hardware 3D* para áudio, ao contrário passaram a utilizar um novo *mixer* feito no *Windows Vista*. Esse novo mixer oferece aos usuários suporte básico para áudio para seus jogos antigos, mas como não há camada de *hardware*, todos os efeitos *EAX* serão perdidos. (OPENAL, 2008)

3.6.1.2. Aquisição dos sinais

Uma vez definida a forma de acesso aos dispositivos, é necessário realizar a aquisição do sinal e determinar por quanto tempo o mesmo será mantido em memória. Em seguida é feita uma análise para avaliar se o sinal adquirido deve ou não ser armazenado na memória de massa.

O primeiro passo é definir um intervalo de tempo para a aquisição do sinal, *Ts*, que pode ser por exemplo 3 segundos. Com o intervalo definido então são definidas posições de memória (*buffer*) para os sinais provenientes de cada dispositivo. Durante o intervalo de tempo definido, deve ser armazenada nas posições de memória o *stream* proveniente de cada dispositivo e em seguida realizar a análise.

Em geral, os dispositivos de som utilizados num computador são apenas dois, sendo um de entrada no qual é conectado um microfone e um de saída onde é ligado um fone, entretanto é possível que existam outros dispositivos que são utilizados. Nas comunicações de voz, bastam dois dispositivos que é um de entrada e um de saída, sendo que se for possível identificar quais dos dispositivos de áudio são utilizados para as comunicações de áudio, os demais podem ser ignorados. No presente trabalho, os dispositivos utilizados para comunicação de voz serão referidos como *MIC* para o dispositivo de entrada e *SPK* para o dispositivo de saída.

É necessário definir as características de captura de modo a manter um comprometimento entre qualidade de sinal aceitável para um futuro exame de verificação de locutor e a necessidade de espaço de armazenamento e largura de banda de rede. Considerando que a qualidade do sinal empregado na telefonia é suficiente para o exame de verificação de

locutor e que o sinal que trafega na telefonia se concentra na faixa de 300 a 3400Hz, uma frequência de corte de 4KHz é um valor suficiente para a realização da captura, o que exigirá uma taxa de amostragem de pelo menos 8KHz, de modo a satisfazer o Teorema da amostragem. Para que não haja perda de informação, segundo o teorema de *Nyquist*, a frequência de amostragem deve ser pelo menos duas vezes maior do que a maior frequência contida no espectro do sinal (KUTWAK, 1999). Com relação a taxa de bits de modo a garantir uma boa qualidade do sinal o valor de 32 bits é suficiente, sendo que poderia ainda ser utilizada codificação *IMA ADPCM* ou codificação *MP3* que são formas de codificação com compressão com perdas, mas as perdas são aceitáveis para um exame de verificação de locutor.

3.6.1.3. Análise das Amostras

A análise para a tomada de decisão do armazenamento ou não da *stream* se baseia em duas situações: (1) a ausência de sinal ou (2) a coincidência de sinais entre *SPK* e *MIC*.

A ausência de sinal tanto em *MIC* quanto em *SPK* é considerada quando o sinal obtido nesses dispositivos tiver amplitude inferior a um limite previamente definido (*squelch*) durante todo o período de aquisição. Quando ocorre a ausência de sinal, a *stream* é ignorada e portanto não será gravada em arquivo.

A coincidência aqui referida leva em consideração que em certas situações a saída do sinal de áudio é o sinal ambiente quando utilizados alto-falantes e não fones de ouvido. Nesse caso o sinal de áudio de saída realimenta o microfone e gerará uma coincidência entre o sinal de saída e de entrada, podendo haver um pequeno atraso entre os sinais. Esses sinais, podem ser descartados pois não terão qualquer utilidade para a investigação.

A identificação da coincidência de sinais obtidos é feita através da identificação de um padrão de forma de onda obtida em *SPK* e na busca por esse padrão em *MIC*. Havendo coincidência pode-se descartar a entrada *MIC*. A fig. 3.7 ilustra o mecanismo utilizado para o desprezo ou não das amostra adquiridas.

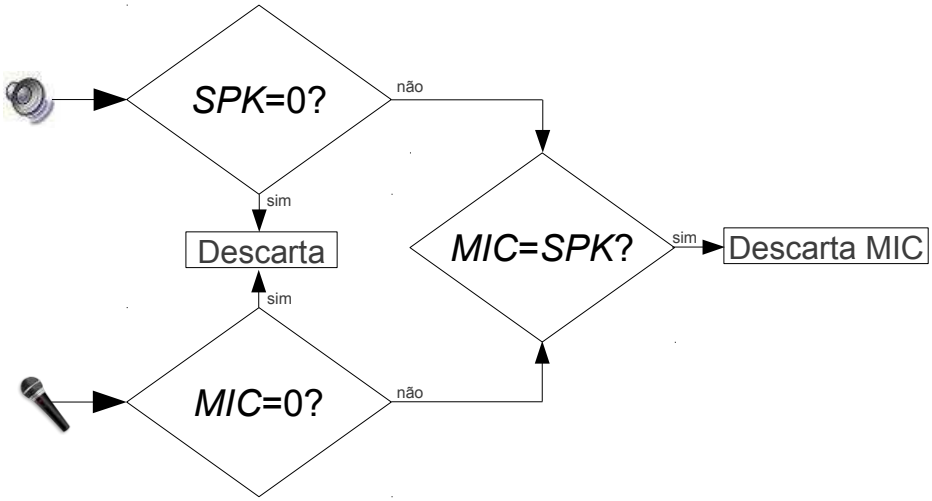

Figura 3.7 - Desprezo de amostras irrelevantes

3.6.2. Módulo de Identificação das amostras

As amostras que não são descartadas devem ser cifradas e armazenadas em memória de massa, possibilitando posterior envio ao sistema da máquina de análise ou acesso aos dados quando da apreensão da máquina do alvo. Antes de serem armazenadas em arquivo, as amostras devem ser identificadas, de modo que possam ser adequadamente recuperadas na estação de análise. O objetivo de identificar as amostras é definir a ordem em que as mesmas foram obtidas e em que tempo. A fim de atender a esse requisito cada amostra receberá um carimbo que contém um número sequencial e o tempo em que a amostra foi obtida. O número da amostra será formado por um número sequencial e um número representativo de tempo capaz de fornecer precisão, conforme o padrão *TIMESTAMP*. A parte indicativa do número sequencial é composta de 16 bits e a parte indicativa do tempo utilizará o padrão *TIMESTAMP* e será composta por 32 bits. A fig. 3.8 ilustra o formato do cabeçalho de cada amostra.

$N_{amostra}$	Tempo	Áudio

Figura 3.8: Formatação das amostras antes de cifradas

O campo de áudio das amostras contém o áudio propriamente dito referente ao período definido na variável *Ts*. O tempo de aquisição *Ts* é definido com base nas características do sistema de arquivos da máquina do alvo, especialmente no tamanho do bloco do sistema de arquivos, no processo de codificação do áudio e no processo de criptografia utilizado antes

de armazenar as amostras. Seguindo a sequência apresentada, cabe ressaltar que até o momento não há armazenamento em memória de massa, uma vez que os dados ainda não foram cifrados.

3.6.3. Módulo de criptografia e armazenamento das amostras.

De modo a garantir a cadeia de custódia, especificamente a confidencialidade e integridade do sinal obtido, as amostras de áudio obtidas antes de serem armazenadas em memória de massa serão cifradas, de modo que somente quem possui a chave poderá ter acesso às mesmas.

Considerando que a obtenção e tratamento das amostras de áudio é realizada em tempo real, e considerando ainda que o sistema não deve ser perceptível ao usuário alvo, é necessário evitar o uso de técnicas que demandam grande processamento o que pode causar lentidão no sistema da máquina do alvo. Devido a isso, não foi utilizada a criptografia assimétrica com a chave K_{alvo}, para que as amostras sejam decifradas na máquina de análise utilizando a chave $K_{analise}$; em vez disso, foi utilizada criptografia simétrica podendo ser utilizada cifra de fluxo com o esquema *RC4*, ou cifra de bloco com o esquema *AES*, ou ainda outro esquema que seja julgado mais interessante quando do desenvolvimento do sistema.

Apesar do esquema de criptografia com *RC4* ser considerado melhor que o *AES* (SINGHAL, RAINA, 2011) em termos de performance, para a nossa aplicação o uso do *AES* não trará grandes implicações de performance.

No estudo realizado por (SINGHAL, RAINA, 2011) utilizando um laptop com *CPU* de 2,99GHz e 2GB de memória *RAM*, foram consideradas algumas métricas sendo de nosso interesse : o tempo necessário para cifrar e decifrar um pacote e dados, a quantidade de recurso de processamento e quantidade de memória. Como exemplo, serão citadas as métricas para a criptografia de um pacote de dados de por exemplo 2MB : o tempo para cifrar/decifrar é de 218/219,7ms no *RC4* e 345,3/346ms no AES ECB, a quantidade de memória utilizada está disponível apenas em gráfico e aparentemente é de cerca de 10MB no *RC4* e 15MB no *AES*, e o tempo de utilização da *CPU* também está disponível apenas em gráfico e aparentemente é de 300ms no *RC4* e de 390ms no *AES*. Considerando esses valores e os recursos computacionais disponíveis nos dispositivos atualmente, tanto na

utilização do *RC4* quanto do *AES* provavelmente serão atendidas as necessidades, mas o *AES* é considerado mais seguro que o *RC4*, tendo esse último sido trocado pelo *AES* na implementação do *WEP2* na criptografia das redes sem fio, pois é considerado mais seguro (MIYANO NETO, 2004)

Para garantir a confidencialidade da chave K_{AES}, é seguida uma sequência de eventos conforme diagrama da fig. 3.9, sendo que chave K_{AES} é gerada (1) no sistema da máquina alvo e armazenada (2) em memória *RAM* ficando armazenada durante a execução do sistema da máquina alvo. Após a geração da chave K_{AES}, o sistema da máquina do alvo cifrará (3) a chave K_{AES} com a chave K_{alvo} e tentará realizar uma conexão com o sistema da máquina de análise e enviar (4) a chave K_{AES}, cifrada com a chave K_{alvo}.

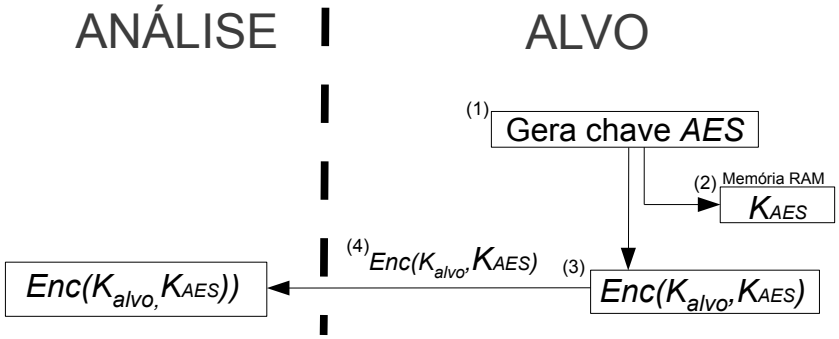

Figura 3.9: Geração e envio de K_{AES}

O diagrama da fig. 3.10 ilustra as ações tomadas na máquina de análise após receber a chave K_{AES} cifrada com K_{alvo}. O sistema da máquina de análise recebe (1) a chave K_{AES} cifrada com K_{alvo} e a decifra (2) com a chave $K_{analise}$ e armazena (3) a chave K_{AES} no banco de dados juntamente com registro de data e hora.

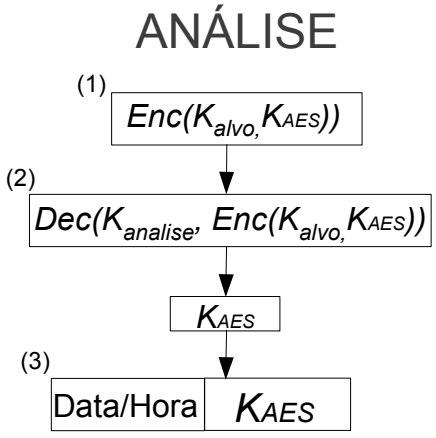

Figura 3.10: Armazenamento de K_{AES}

A fig. 3.11 ilustra as ações realizadas para a confirmação da correta transmissão da chave ou o armazenamento da mesma caso não tenha ocorrido a transmissão. Para confirmar ao sistema alvo que a chave foi recebida corretamente, o sistema de análise envia (1) novamente K_{AES} cifrada com a chave $K_{analise}$. O sistema da máquina do alvo decifra (2) utilizando K_{alvo} e compara (3) a chave K_{AES} recebida com a chave K_{AES} armazenada em memória *RAM*.

Se as chaves forem iguais é considerado que a chave está disponível na máquina de análise, e portanto não há necessidade de armazenar a chave na máquina do alvo, dessa forma é feito registro (4) nos *logs* que a transmissão da chave ocorreu com sucesso.

Se as chaves forem diferentes, significa que a máquina do alvo não conseguiu conexão com a máquina de análise. Devido a possibilidade do sistema da máquina alvo operar sem conexão com a internet e consequentemente sem conexão com o sistema de análise, é necessário que a chave K_{AES}, seja armazenada na máquina do alvo. A fim de manter a confidencialidade e integridade da chave K_{AES}, e consequentemente das amostras, a chave K_{AES} é armazenada (5) cifrada com a chave K_{alvo}, dessa forma somente o detentor da chave $K_{analise}$, que é o sistema de análise, poderá decifrar e ter acesso a chave K_{AES}.

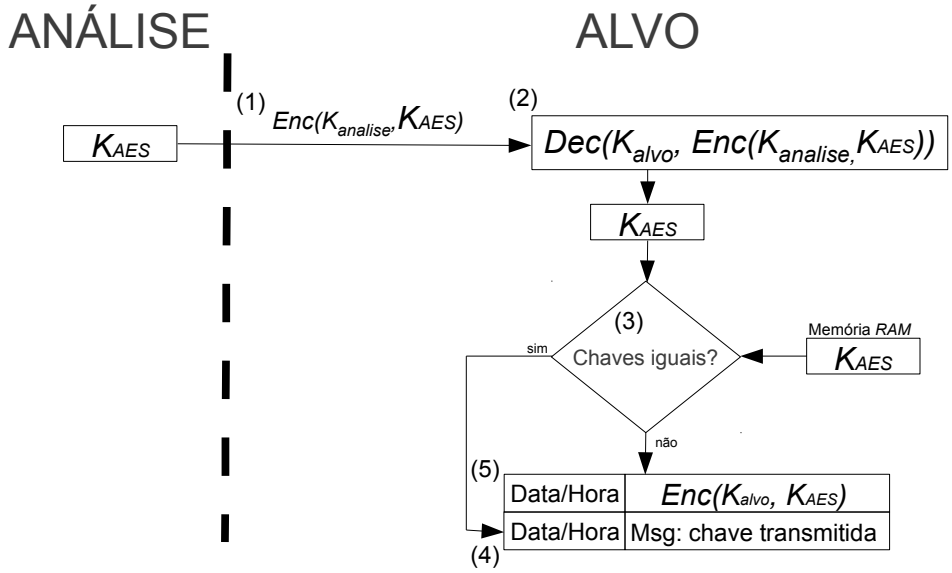

Figura 3.11: Geração e envio de K_{AES}

A chave K_{AES} é mantida em memória *RAM* e é usada para a cifrar várias amostras. A cada *N* amostras a chave K_{AES} deve ser novamente gerada no sistema do alvo conforme esquema

da fig. 3.9. O número de amostras que são cifradas com a mesma chave K_{AES} pode ser por exemplo o número de amostras que podem ser alocadas num mesmo arquivo.

O armazenamento das amostras será realizado em arquivo sendo que os arquivos serão armazenados preferencialmente em pastas onde ficam os arquivos de sistema de modo a evitar que o usuário identifique os arquivos que serão estranhos para o mesmo. Será criada uma pasta que será mantida oculta, e na mesma serão incluídos os arquivos cujo nome será definido pela data de criação dos mesmos. No momento em que o arquivo for criado, será obtido o tempo no formato *TIMESTAMP*, cujo valor possui 32bits, e o valor obtido será convertido no formato hexadecimal e cada *nibble* definirá um caractere no nome do arquivo. A fig. 3.12 ilustra a forma de nomeação dos arquivos que conterão as amostras de áudio.

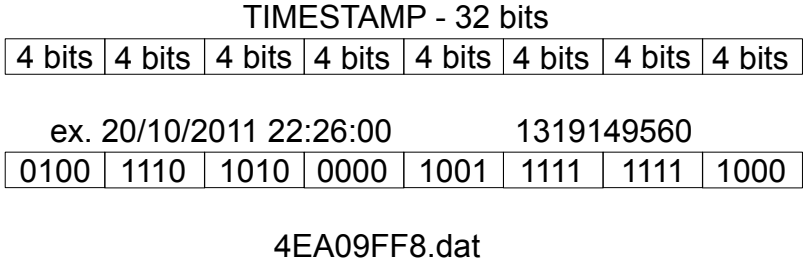

Figura 3.12 - Nome do arquivo

O arquivo gerado será mantido aberto e as amostras obtidas serão incluídas no mesmo de forma sequencial, até que o arquivo atinja o tamanho determinado, sendo que, como já citado o tamanho do arquivo depende do sistema de arquivos, especialmente do tamanho do *cluster* e da largura de banda disponível na máquina do usuário.

Quando o arquivo atingir o tamanho definido, o mesmo é fechado e é gerado um registro no *log* de eventos sendo registrado que um novo arquivo está disponível com nome do arquivo, tamanho, data e hora de registro e o hash *SHA-2* do mesmo. Através do registro de *logs* será possível identificar possíveis incoerências e falta de arquivos no sistema da máquina alvo. A extensão do arquivo é definida pelo dispositivo que gerou as amostras existentes no arquivo, dessa forma a extensão apresentada na fig. 3.12 como ".dat", é substituída por ".spk", que indica obtenção do áudio do fone, ".mic" que indica obtenção do áudio do microfone, ou "da1" que indica a obtenção de áudio de outro dispositivo de áudio.

3.6.4. Módulo de transmissão dos arquivos

A interceptação de áudio na máquina do alvo tem duas funções: determinar o *modus operandi* da operação criminosa e garantir que o áudio interceptado tenha valor probatório. Para garantir que o áudio seja aceito como prova são utilizadas as técnicas de criptografia apresentadas anteriormente no trabalho e o exame de verificação de locutor a ser realizado em momento posterior, caso a autoria da voz seja negada.

Para utilizar o áudio somente como prova, não seria necessário o envio do áudio para o sistema da máquina de análise, pois seria possível ter acesso ao áudio quando da apreensão da máquina do alvo em cumprimentos de mandados de busca e apreensão. Para determinar o *modus operandi* entretanto, se faz necessário o acompanhamento contínuo dos contatos que o alvo efetua e nesse caso, é necessário ter disponível o mais rápido possível o áudio obtido. Nesse caso o sistema da máquina do alvo envia ao sistema de análise os arquivos obtidos de modo que a partir dos mesmos o áudio seja recuperado e analisado.

Antes de realizar o envio de um arquivo o sistema da máquina do alvo irá analisar a atividade de rede, caso a atividade esteja intensa o sistema não realizará a transmissão de modo a evitar que a rede do usuário alvo fique lenta, fazendo com que o mesmo perceba que há algo de diferente na sua máquina. Caso a transmissão fosse feita durante grande atividade de rede poderia ocorrer também prejuízo na comunicação *VoIP* do usuário, já que essa demanda grande disponibilidade de rede, em especial no tocante à latência.

A fig. 3.13 ilustra as ações tomadas para o envio e verificação de sucesso do mesmo. Antes de realizar o envio de um arquivo, o sistema da máquina do alvo irá calcular (1) o *hash SHA-2* do arquivo a ser enviado. Em seguida irá enviar para a máquina de análise (2) o referido arquivo sem criptografia, já que o mesmo já foi armazenado cifrado. O *hash SHA-2* do arquivo será cifrado (3) com a chave K_{alvo}, e enviado (3) para o sistema da máquina de análise.

O sistema da máquina de análise recebe o arquivo (2) e o *hash SHA-2* do arquivo, cifrado com K_{alvo} (3). O sistema da máquina de análise então decifra (4) com a chave $K_{analise}$, o conteúdo recebido na ação (3) e obtém o cálculo do *hash SHA-2* do arquivo. Em seguida a máquina de análise calcula (5) o *hash SHA-2* do arquivo e compara (6) com o *hash* recebido, sendo iguais o sistema de análise considera que o arquivo foi recebido

adequadamente e armazena (7) o arquivo e registra (8) nos *logs* do sistema da análise o recebimento do mesmo, com informações de nome do arquivo, data e hora de recepção e *hash SHA-2* do mesmo.

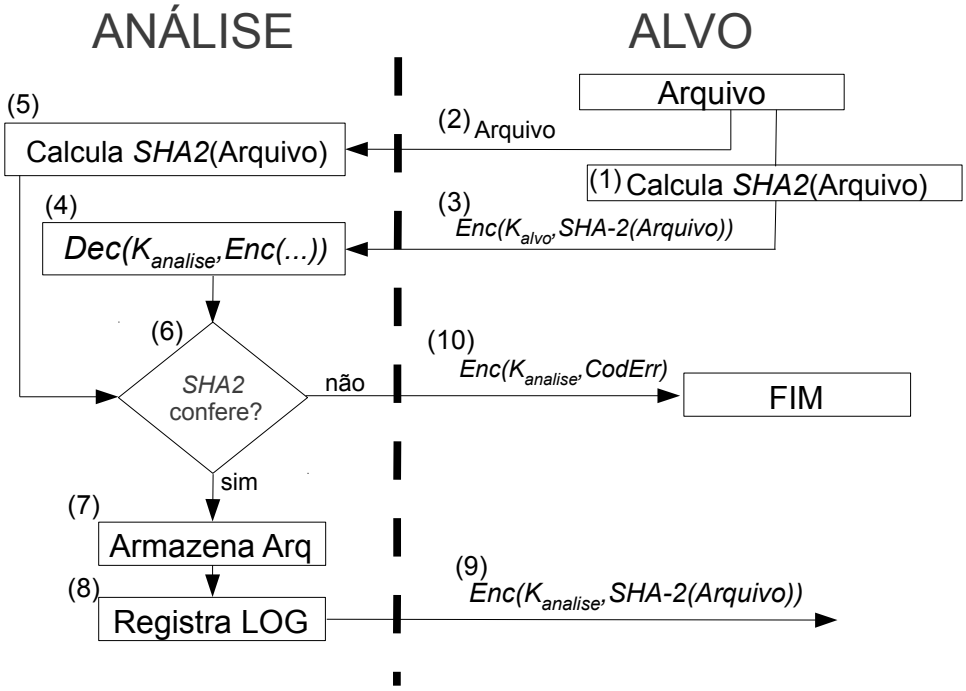

Figura 3.13 – Envio do Arquivo

Para confirmar ao sistema da máquina do alvo que o arquivo foi recebido corretamente na máquina de análise, o sistema da máquina de análise cifra o *hash SHA-2* do arquivo com a chave $K_{analise}$ e envia (9) ao sistema da máquina do alvo.

Caso o resultado da verificação de *hash* citado no item (6) seja negativo o sistema da máquina de análise não armazena o arquivo e envia (10) uma mensagem de erro para a máquina de análise.

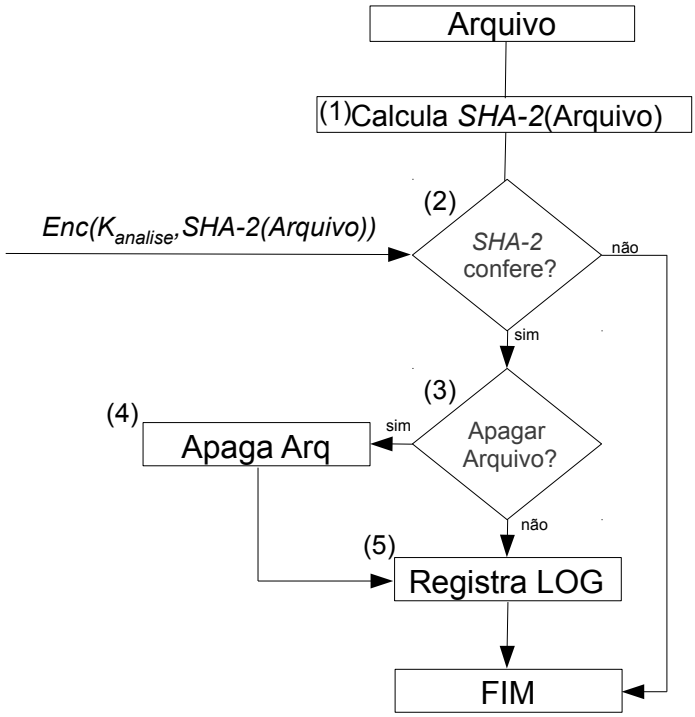

Figura 3.14 – Tratamento do Arquivo

A fig. 3.14 ilustra as ações tomadas na máquina de alvo após a confirmação do recebimento do arquivo pela máquina de análise.

O sistema da máquina do alvo calcula (1) o *hash SHA-2* do arquivo e compara (2) esse *hash* com o *hash SHA-2* cifrado com $K_{analise}$ recebido da máquina de análise conforme item (9) da fig. 3.13. Se os valores forem iguais, o sistema da máquina do alvo avalia (3) se deve apagar o arquivo conforme diretivas internas do sistema e características específicas de memória de massa do sistema do alvo.

Se a tomada de decisão for pela exclusão do arquivo, o sistema da máquina do alvo apaga (4) o arquivo e faz (5) registro em *log* da operação. Caso a tomada de decisão seja pela não exclusão do arquivo, será feito (5) apenas o registro no log.

No log serão registrados dados como data e hora do envio, nome do arquivo, hash *SHA-2* do mesmo e indicação de que arquivo foi excluído ou não da máquina do alvo.

3.6.5. Módulo de checagem de integridade – envio de *LOGs*

De modo a fornecer integridade dos dados do sistema da máquina do alvo, toda vez que o *log* do sistema da máquina do alvo atingir 10 registros o mesmo encaminha ao sistema da

máquina de análise o hash *SHA-2* dos últimos 10 registros de *log*. Com esse procedimento será possível identificar alterações realizadas nos registros de *log* feitas com o intuito de forjar a exclusão ou inclusão ou alteração de algum registro de áudio. A informação de que o *hash* dos *logs* foi transmitido, é armazenada apenas nos logs da máquina de análise. A sistemática de transmissão ocorre conforme ilustrado na fig. 3.15. O fato gerador da transmissão dos registros de *logs* do sistema da máquina do alvo é a geração do registro que fecha uma dezena, ou seja, no registro 10, 20, 30, etc. Ao ocorrer o fato gerador, o sistema da máquina do alvo calcula o *hash SHA-2* dos últimos 10 registros de *log*, o número do *log* referente, por exemplo 20 e cifra com K_{alvo}, e encaminha ao sistema de análise. O sistema de análise decifra os dados recebidos e armazena no *log* da máquina de análise o *hash SHA-2* recebido. Com o número do registro de *log* recebido o sistema da máquina de análise, verifica em seu *log* se há registros anteriores, caso haja todos os registros anteriores, responde ao sistema da máquina do alvo com um código que recebeu corretamente o registro; caso a máquina de análise não tenha em seus *logs* os registros anteriores dos *hash SHA-2* dos *logs* da máquina do alvo, o sistema da máquina de análise envia uma solicitação ao sistema da máquina alvo, informando que não possui os registros anteriores, nesse caso o sistema da máquina do alvo envia ao sistema da máquina de análise os registros não constantes no *log* do sistema da máquina de análise.

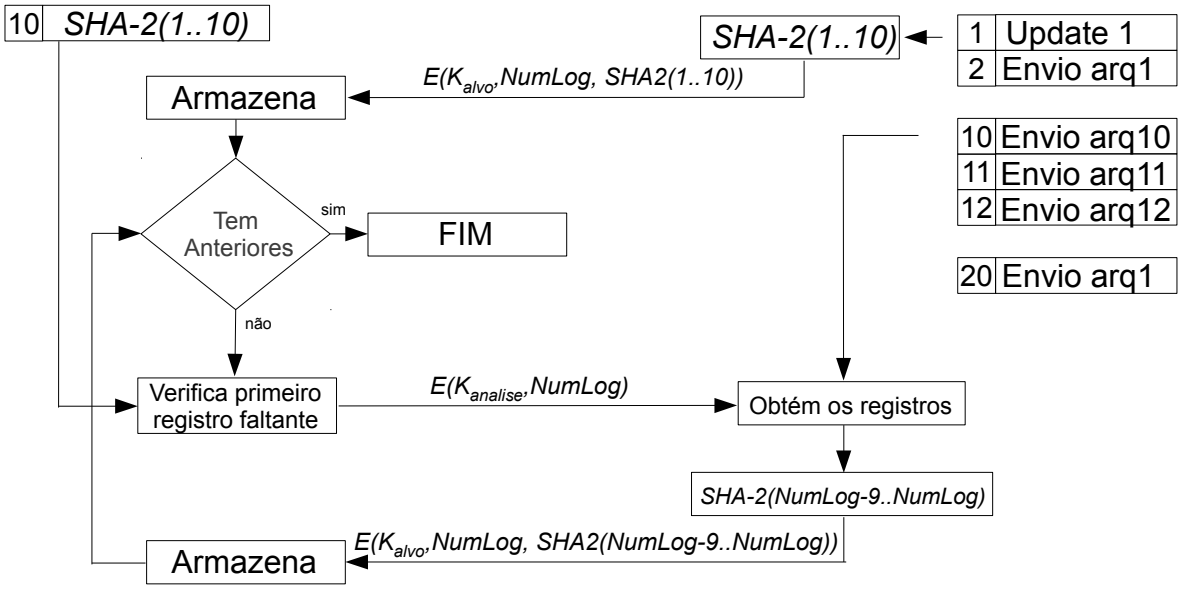

Figura 3.15: Envio dos Logs do sistema da máquina do alvo

4. ESTUDO DE VIABILIDADE JURÍDICA

O sistema proposto utiliza um método de obtenção de dados que não encontra respaldo específico na legislação e jurisprudências no ordenamento jurídico brasileiro.

A fim de determinar se os dados obtidos terão validade jurídica nos tribunais, haja vista que, de nada adiantaria investir recursos e tempo no desenvolvimento de um sistema, se o resultado por ele obtido não tiver validade probatória, foi realizada uma análise jurídica quanto a utilização do sistema proposto.

Nesse sentido, foi inicialmente feita busca em decisões nos principais tribunais, tendo como objetivo encontrar decisões transitado e julgado com provas obtidas através de aplicativos furtivos similares ao sistema proposto, não sendo encontrados casos concretos relativos a matéria.

Considerando tratar-se de uma situação nova na Justiça Brasileira, foi elaborado um artigo, no qual foram apresentadas as evoluções tecnológicas, as dificuldades que tais evoluções trouxeram para as LEA, e uma alternativa para obtenção das provas. Tal relatório foi encaminhado para diversos operadores do direito, como magistrados, advogados, defensores e membros do Ministério Público.

A referida análise foi realizada utilizando-se os métodos de hermenêutica mais adequados ao caso proposto. Visando a concretização da norma foi utilizado o método hermenêutico-concretizador de *Konrad Hesse* (parte-se da norma para a solução do problema), bem como o método normativo-estruturante de *Friedrich Müler*, que aplica uma estrutura de concretização da norma considerando doutrina e jurisprudência. [1](LINHARES, 2012)

(LINHARES,2012) cita que a Lei n° 9.296/96 foi criada para regulamentar o dispositivo Constitucional do inciso XII, art. 5°, determinando expressamente as hipóteses possíveis (art. 2°), mas foi omissa em relação à forma, mais especificamente ao meio a ser empregado, conforme se depreende do *caput* do artigo 4°.

Dessa forma a utilização do sistema proposto não é proibida, todavia deve ser especificamente indicada no momento do pedido. Para que o procedimento seja revestido

1 Como resposta à consulta, foi obtido um parecer de George Linhares ex-assessor do Centro de Apoio Operacional Criminal do Ministério Público do Estado de Santa Catarina, atualmente ocupa cargo no Poder Judiciário Catarinense.

pelo manto legal e para que se evitem alegações de nulidades é necessário que esteja detalhado, inclusive com a delimitação do campo de atuação do sistema a ser instalado (o que é captado e gravado pelo programa). Destaca-se que conhecido o procedimento pelo Magistrado competente e autorizada a interceptação telefônica, o fim justificará os meios, legalizando todo o processo de formação de prova. (LINHARES, 2012)

Quanto a natureza da comunicação telefônica, observa-se que VoIP faz as vezes da comunicação telefônica ou se retrata como a própria comunicação telefônica. Assim, não haveria óbice de ser aplicada ao caso, levando-se em conta que a própria norma permite a interceptação de comunicação telefônica de **qualquer natureza**. (LINHARES, 2012)

A problemática giraria em torno da implantação do sistema e armazenamento dos dados no computador do alvo para posterior apreensão ou transmissão, haja vista que não há óbice para que se autorize a interceptação de chamadas de voz. (LINHARES, 2012)

Assim, tendo em vista que esses pontos destacados (implantação e armazenamento) são etapas necessárias ao procedimento, não haveria ilícito penal ou civil, porquanto: 1) não há tipificação para que essa ação se considere crime (LINHARES, 2012) e 2) por meio da ponderação entre o Princípio da Intimidade e o Princípio do *In Dubio Pro Societate,* verifica-se que esse tem maior peso no caso concreto (investigação criminal ou instrução processual penal que se verifica indícios de autoria ou participação em crime punido com reclusão), devendo o primeiro princípio ceder ao último, por força do Princípio da Concordância Prática ou Harmonização, do Princípio da Proporcionalidade e do Princípio da Relatividade ou Colidência das Liberdades Públicas; (NOVELINO, 2010, apud LINHARES, 2012).

Foram encaminhadas as consultas a alguns Juízes Federais em Santa Catarina, não sendo obtidas respostas formais, devido ao fato de Juízes serem impedidos de fornecer parecer formal em casos hipotéticos. Entretanto os Juízes possibilitaram uma audiência e expuseram o seu entendimento do ponto de vista teórico e doutrinário.

Em audiência com Dr. Rafael Carmona[2], foi apresentado o problema referente a interceptação de voz e dados em canais criptografados, citando como exemplo o *skype*. A seguir foi mostrado a forma de operação do sistema proposto e então o Dr. Rafael teceu os

2 Audiência com o Dr Rafael Selau Carmona, Juiz Substituto da 2ª Vara Federal Criminal da Justiça Federal em Florianópolis, Santa Catarina, realizada em 28 de março de 2012

seguintes cometários: O sigilo das comunicações telefônicas é garantido pela Constituição Federal, no entanto o referido direito pode ser relativizado desde que alguns pressupostos sejam atendidos. O magistrado comentou que em tese não via impedimento para a implementação do sistema, já que não há legislação contrária e a lei não restringe a forma que deve ser utilizada para implementar as interceptações.

Em outra oportunidade, em audiência com Dr. Marcelo[3], foi adotada a mesma metodologia, ou seja, foi apresentado o problema referente a interceptação de voz e dados em canais criptografados, citando como exemplo o *skype* e foi mostrado a forma de operação do sistema proposto. Em seguida Dr. Marcelo informou tratar-se de comunicação similar às comunicações de dados e por conseguinte a interceptação segue a mesma sistemática daquele tipo de comunicação. Então foi feito questionamento relativo à forma como a interceptação seria feita, enfatizando que seria feita invasão do dispositivo do investigado e utilizado o dispositivo do mesmo para armazenar o áudio e transferir as informações. Então o Dr. Marcelo informou que desconhece lei que restrinja a forma como as interceptações são realizadas, e considerando que não há lei que restrinja, em princípio não há problemas quanto a validade jurídica nas provas obtidas da forma proposta.

Em audiência com Dr. Ivorí[4] foi da mesma forma exposto o problema e o sistema proposto. Inicialmente Dr Ivorí falou sobre a impossibilidade de os juízes fornecerem entendimento sobre situações hipotéticas, porém o mesmo iria indicar a seu entendimento baseado apenas na legislação e doutrinas, e que num caso real, dependendo das circunstâncias poderia ter um entendimento diverso. Passou então a comentar a respeito dos princípios legais relevantes ao sistema proposto, sendo que o direito constitucional da inviolabilidade das comunicações deve ser preservado, no entanto existe a possibilidade de relativizar o referido direito, desde que atendidos os pressupostos em lei. O Dr. Ivorí ressaltou que ainda que hoje o entendimento sobre o sistema proposto fosse pelo não reconhecimento da prova, ainda assim o sistema deveria ser implementado, já que no seu entendimento o direito vai a reboque da técnica, além do mais, tanto o direito quanto as leis são mutáveis, e o que não é válido hoje, poderá ser amanhã.

3 Em 13 de abril de 2012 foi realizada audiência com Dr. Marcelo Krás Borges, Juiz Federal Titular da 1ª Vara Federal da Justiça Federal em Florianópolis, Santa Catarina.

4 Em 13 de abril de 2012, foi realizada audiência com Dr Ivorí Luis da Silva Scheffer, Juiz Federal Titular da 2ª Vara Federal Criminal da Justiça Federal em Florianópolis, Santa Catarina

Quanto ao aspecto legal referente ao sistema proposto, Dr. Ivorí comentou que, analisando de forma teórica é preciso lembrar de dois aspectos a privacidade e a proporcionalidade. A privacidade é relativa ao direito de inviolabilidade das comunicações e que pode ser quebrado. Dr. Ivorí indicou a importância de haver a (1) necessidade de obtenção da prova, e em havendo, analisar (2) o meio como esta prova será obtida, de forma que seja o menos invasivo possível.

Para abordar um pouco mais sobre o princípio da proporcionalidade, foi realizada pesquisa sendo que o conteúdo a seguir apresentado não foi obtido na audiência com Dr. Ivorí.

O sistema normativo, não é concebido como um conjunto fechado de regras, que, para cada fato, apresentaria a consequência jurídica decorrente, mas sim, como um sistema aberto, para dar conta das peculiaridades de cada caso concreto. Isso significa uma abertura para, em certas hipóteses, tomar decisões sobre problemas jurídicos lançando mão de recursos outros, que não o das proposições normativas . (GUERRA FILHO, 2002)

O princípio da proporcionalidade tem um conteúdo que se reparte em três princípios parciais: (1) princípio da proporcionalidade em sentido estrito, (2) princípio da adequação e (3) princípio da exigibilidade ou mandamento do meio mais suave. (GUERRA FILHO, 2002)

O princípio da proporcionalidade em sentido estrito determina que se estabeleça uma correspondência entre o fim a ser alcançado por uma disposição normativa e o meio empregado, que seja juridicamente a melhor possível. Isso significa, acima de tudo, que não se fira o conteúdo essencial de direito fundamental, com o desrespeito intolerável da dignidade humana, bem como que, mesmo em havendo desvantagens para, digamos, o interesse de pessoas, individual ou coletivamente consideradas, acarretadas pela disposição normativa em apreço, as vantagens que traz para interesses de outra ordem superam aquelas desvantagens. (GUERRA FILHO, 2002)

Os subprincípios da adequação e da exigibilidade, por seu turno, determinam que, dentro do faticamente possível, o meio escolhido se preste para atingir o fim estabelecido, mostrando-se, assim, adequado. Além disso, esse meio deve se mostrar exigível, o que significa não haver outro, igualmente eficaz, e menos danoso a direitos fundamentais. (GUERRA FILHO, 2002)

Voltando às informações obtidas na audiência com o Dr. Ivorí, foi comentado pelo mesmo que na sua opinião o sistema deve ser realizado ressaltando ainda que há outros meios de obtenção de provas muito mais invasivos e que são aceitos, como exemplo citou a infiltração de agente do estado em organizações criminosas, desde que devidamente autorizados pelo juiz, para a obtenção de provas.

Em audiência realizada com Dr. Gustavo[5], sendo da mesma forma exposto o problema e o sistema proposto. O Dr. Gustavo entendeu que o mais importante a ser analisado é o direito individual do sigilo das comunicações e que, considerando que tal direito já esteja quebrado através de um mandado, a forma como será realizada a obtenção da voz ou dados é irrelevante. Foi citado ainda que no caso pode ser aplicado o princípio de quem pode o mais pode o menos, sendo que o mais se refere à quebra do sigilo das comunicações e o menos se refere à forma como a referida quebra será realizada.

4.1. MANUTENÇÃO DA CADEIA DE CUSTÓDIA

Conforme definido no capítulo 3, uma das características principais do sistema é a manutenção da cadeia de custódia das provas, sendo necessário que o áudio obtido tenha integridade, confidencialidade, autenticidade e não-repúdio.

4.1.1. Integridade

A integridade, que é a garantia de que os sinais recebidos na máquina de análise foram os obtidos na máquina do alvo, é implementada através das assinaturas de cada uma das amostras que são armazenadas no arquivo de *log* e o armazenamento dos registros de *log* tanto na máquina de análise quanto na máquina do alvo.

Além disso, a análise forense na máquina do alvo, realizada após a apreensão da mesma, pode-se verificar a inexistência de outro sistema furtivo ou aplicativo de acesso remoto rodando na máquina do alvo; ou ainda a inexistência de vestígios de que pudesse ter havido sistemas furtivos instalados.

5 Audiência realizada em 13 de abril de 2012, com o Dr. Gustavo Dias de Barcellos, Juiz Federal Substituto da 1ª Vara Federal da Justiça Federal em Florianópolis, Santa Catarina

4.1.2. Confidencialidade

A confidencialidade, que é a garantia de que as amostras de áudio somente serão ouvidas pelas pessoas autorizadas, é implementada através da chave privada armazenada na máquina de análise. As amostras são criptografadas com a chave pública, na máquina do alvo antes de serem armazenadas, ou seja, somente terá acesso às informações criptografadas quem possuir a chave privada.

4.1.3. Autenticidade e Não-Repúdio

Para os casos de investigações criminais o objetivo é determinar a dinâmica e autoria de um delito. Considerando o escopo do trabalho a garantia de que a amostra de áudio foi gerada num determinado computador não constitui prova cabal, já que não é possível garantir que determinada pessoa utilizou o computador para se comunicar.

No caso de interceptações telefônicas o fato de identificar o telefone de um dos interlocutores não imputa ao mesmo a autoria da conversação, já que poderia o telefone de alguém ser utilizado por terceiros na realização de chamadas.

De modo análogo, um computador eventualmente é utilizado por mais de uma pessoa e dessa forma, para ter valor probatório é imprescindível que o áudio obtido seja atribuído a alguém. Para atribuir um áudio como tendo sido falado por alguém não basta garantir que o mesmo foi obtido no computador do alvo, mas sim a fala de uma pessoa que gerou o referido áudio. A garantia de que um áudio foi fornecido por alguém é dada através de um exame pericial de verificação de locutor.

O exame de verificação de locutor é feito em diversas etapas e a seguir são apresentados os procedimentos realizados no âmbito da Polícia Federal conforme sugerido na capacitação nacional em fonética forense oferecida pela SENASP.

4.1.3.1. Exame de Verificação de Locutor

Para a realização de exames de Verificação de Locutor, é necessário o confronto técnico comparativo entre os materiais sonoros questionados, que são os áudios provenientes de interceptações telefônicas ou ambientais, cuja autoria da locução se deseja verificar; e

padrão que são áudios obtidos de uma pessoa, identificada, cuja autoria é irrefutavelmente conhecida.

Para a realização de um exame de verificação de locutor é necessário então a existência de suspeitos, para que se possa realizar a coleta de padrão de voz do mesmo.

Para o início dos exames de Verificação de Locutor em um áudio questionado, é necessário que seja apontando com clareza qual é o interlocutor na gravação cuja voz se deseja confirmar, bem como indicando o diálogo ou o trecho da gravação perquirida, já que nem todo o áudio é relevante para a solução do crime.

Análise do Material Questionado

Os materiais questionados a serem submetidos aos exames de verificação de locutor devem ser adequados e para tal, ter boa qualidade sonora e quantidade suficiente.

Para verificar se o material questionado disponível é adequado deve-se analisar se a quantidade do material é suficiente para a realização dos exames; verificar a relação sinal/ruído, principalmente nos trechos da gravação onde há locuções características do falante; analisar a qualidade dos espectrogramas e *LPC*s especialmente nos trechos anteriormente mencionados e confirmar a possibilidade de cálculo de *pitch*.

A qualidade do material sonoro questionado deve ser a maior possível, uma vez que quanto maior for, maior a possibilidade de identificação de elementos segmentais e supra-segmentais individualizadores da fala de um interlocutor dentre outras que, na maioria das vezes, possui as mesmas características dialetais e/ou socioletais em uma mesma comunidade de fala.

Quando o material questionado possui baixa relação sinal/ruído, resulta em pouca qualidade sonora, o que pode dificultar ou até mesmo impossibilitar a realização dos exames de verificação de locutor. A ausência de qualidade sonora pode ocorrer devido a diversos fatores como: Falta de adequabilidade no ajuste do equipamento de gravação utilizado, gerando ruídos que se sobrepõem às vozes ou a saturação do sinal; em escutas ambientais o posicionamento inadequado do microfone do sistema de gravação no ambiente em que se pretende realizar a aquisição do áudio, o que resulta em gravações muito baixas ou com destaque para outros sons, em vez do conteúdo desejado; emprego de

gravadores digitais com alta taxa de compressão do áudio, sendo que o ideal é armazenar o áudio sem compressão, ou com compressão com baixo índice de perdas.

Após a análise do material sonoro questionado e a confirmação de que o mesmo é passível de confronto, o próximo passo é a elaboração de um roteiro que direcione a coleta do material sonoro padrão.

A forma de apontar ou excluir determinada pessoa como sendo aquela que gerou o material sonoro questionado, é identificar características peculiares da sua fala e verificar se existe convergência ou divergência com o material sonoro questionado. Para realizar tais comparações é necessário que existam tanto no material sonoro questionado quanto no material sonoro padrão a realização de fonemas que demonstrem tais características. Ao identificar fonemas característicos da fala no material questionado, esses devem ser incluídos no plano de coleta de modo a tentar verificar se o fornecedor de material sonoro padrão produzirá tais fonemas da mesma forma que no material questionado.

Identificar palavras no material sonoro questionado e definir um contexto de modo que o fornecedor de padrão de voz produza tais palavras sem saber que são essas palavras que o examinador quer que sejam ditas.

Nos exames de verificação de locutor o objetivo é identificar elementos segmentais e supra-segmentais de modo a individualizar um falante dentre outros; o exame visa atribuir que as vozes existentes no material sonoro questionado foram proferidas por uma pessoa, ou ainda excluir que uma determinada pessoa tenha proferido as vozes constantes no material questionado.

Dessa forma é necessário identificar as peculiaridades da fala existente nos materiais sonoros questionados e padrão e os parâmetros que permitam confrontar, com maior grau de certeza, o locutor questionado. Nesses parâmetros técnico comparativos, busca-se não só elementos técnicos individualizadores do falante como também comuns em sua comunidade de fala, de modo a informar que tais padrões não podem ser utilizados como individualizadores.

A metodologia é baseada em parâmetros técnicos que podem ser alcançados por análises acústicas e perceptuais, verificando a forma de articulação dos segmentos.

A avaliação final deve levar em conta os resultados obtidos de diversos elementos isolados e nunca no resultado de um único elemento, seja convergente ou divergente. Em alguns casos, dependendo com quem o locutor converse, vários parâmetros são alterados; portanto se possível, o material sonoro padrão deve ser obtido em situação mais próxima possível daquela em que foi obtido o material sonoro questionado.

Análise Articulatória

O levantamento de características articulatórias pode ser obtido tanto pela análise perceptiva quanto pela análise acústica. A seguir são apresentados elementos técnicos da fala que podem ser observados para atribuir ou não a fala a algum interlocutor : tipo de voz, como áspera, tremulosa, rouquejante, sussurrada, soprosa, com instabilidade na frequência de emissão ou com características de laringalização; elementos paralinguísticos, como o tom da voz; disfemia; velocidade da fala; tendência de começar enunciados com um clique; ocorrência ou não de eructação durante a fala; uso de elementos prosódicos para marcar a estrutura da informação do discurso como: pausa, velocidade de fala, altura, extensão de tom, diferença de tom e tons de limite; vocabulário utilizado, se mediano, ou elaborado, assim como a presença de características sociolinguísticas que indiquem a origem do interlocutor; realização articulatória das locuções se clara ou não; se os plurais metafônicos são articulados; acréscimo de vogais epentéticas; predominância ou a ausência de flexões verbais e/ou nominais; ocorrência de locuções que favoreçam à nasalização, ocasionando a troca de um fonema oral por um nasal; ocorrência de locuções que favoreçam à desnasalização, ocasionando a substituição de um fonema nasal por um oral; ocorrência de metaplasmos por transposição, como metátese e hipértese; hiperbibasmos e por diástole; assimilação resultante da influência de um fonema em outro, além de outras características que sejam individualizadoras.

Análise Acústica

A análise acústica compreende principalmente a análise de formantes, análise de frequência fundamental e análise espectrográfica de comportamentos articulatórios dos materiais sonoros questionado e padrão.

Os espectrogramas que são utilizados para ilustração de convergências ou divergências e representam os fenômenos articulatórios graficamente, por exemplo, para ilustrar o

apagamento de fonemas, ou o vozeamento, ensurdecimento, laringalização, etc. Algumas vezes é interessante utilizar espectrogramas e curva de frequência fundamental para representar convergências ou divergências.

São analisados trechos do material sonoro questionado e padrão sendo mostrados os espectrogramas e um gráfico comparativo entre as curvas de resposta em frequência *LPC* resultantes das análises. As análises são feitas num mesmo contexto fonético, tanto no material padrão quanto no material questionado.

As análises *LPC* são realizadas principalmente em vogais e de preferência em trechos estáveis tomando cuidado com os efeitos de coarticulação analisando sempre trechos compatíveis no áudio padrão e questionado.

A análise de *LPC* sofre interferência da largura de banda do sinal, é bastante comum o material questionado apresentar banda limitada. Quando o material questionado é oriundo de interceptações telefônicas, é comum que os áudios estejam limitados entre 300 e 3400 Hz. A limitação de banda tem efeitos negativos na análise de formantes, principalmente nos casos em que o espectro subtraído do sinal engloba parte representativa dos mesmos.

No caso da banda passante do sistema telefônico, o corte inferior, de cerca de 300 Hz, influencia no cálculo primeiro formante, causando um resultado maior do que o que seria obtido se o sinal não tivesse sua banda limitada. Já o corte superior, de 3400 Hz, influencia no cálculo de formantes com frequências próximas a esse valor, causando resultados menores do que os obtidos sem a limitação de banda. No caso do material questionado possuir a sua banda limitada, é importante que o material sonoro padrão passe pela mesma limitação de banda, fazendo com que as comparações sejam feitas em sinais com as mesmas características.

Outro aspecto importante para a análise acústica é a presença de sinal saturado. Para as análises acústicas, a saturação é extremamente ruim, pois distorce o sinal, inserindo frequências espúrias não existentes no sinal original prejudicando bastante a observação e o cálculo das características espectrais, podendo inviabilizar o cálculo de valores de formantes.

Devido a essa característica, deve-se evitar a saturação do sinal tanto no material questionado, que geralmente não é uma variável controlada, mas no nosso caso é possível

implementar um controle de ganho, quanto no material sonoro padrão, que devido ao fato de ser obtido com o controle do próprio examinador deve-se garantir que o sinal não atinja o nível de saturação.

A compressão que também altera os sinais, está presente na grande maioria das representações digitais de sinais tanto vídeo quanto áudio. Existem praticamente dois grupos de compactadores de áudio, o grupo dos codificadores de voz e o dos codificadores de sinais de áudio em geral, como música, por exemplo. Os codificadores da áudio tratam o sinal avaliando o espectro de frequência e cortando as frequências não perceptíveis pelo ouvido humano. Os codificadores de áudio que mais se destacam atualmente são o *MP3* e o *WMA*. Os codificadores de voz, por sua vez, são em sua maioria baseados em técnicas de predição linear, que buscam a partir do sinal original identificar os parâmetros de um sistema fonte-filtro. Os codificadores de voz mais conhecidos atualmente são os do tipo *CELP*, utilizados nos sistemas atuais de telefonia celular.

Os métodos de codificação mais eficientes são processos com perdas, sendo que quanto mais eficientes são os codificadores, ou seja, quanto menor o número de *bits* necessários para representar uma informação, maior será a perda. Um sinal que passa por um processo de codificação com perdas, significa que não será idêntico ao sinal original, havendo perda de qualidade no mesmo.

Os codificadores possuem parâmetros que permitem definir o compromisso entre qualidade e tamanho final do áudio comprimido, na geração de arquivos *MP3*, por exemplo, pode-se selecionar a taxa de bits (número de bits/segundo) e a largura de banda do sinal a ser utilizada.

Sinais oriundos de interceptações envolvendo telefonia celular foram submetidos a codificação de voz do tipo *CELP*. Os codificadores de voz *CELP*, trabalham com taxas de amostragem de 8 kHz, e, por utilizarem técnicas de compressão mais eficientes, conseguem comprimir a voz com qualidade suficiente com apenas cerca de 8 kbps a cerca de 13 kbps.

Os codificadores de voz causam distorções no espectro do sinal, sendo que os trechos mais adequados para o cálculo dos formantes são os correspondentes a vogais mais alongadas e mais estáveis.

Para a definição dos parâmetros de obtenção de áudio no sistema proposto, é necessário levar em consideração a largura de banda de aquisição, sendo que quanto maior a largura de banda, mais confiável será o exame de verificação de locutor, a saturação deve ser evitada, e a compactação deve ser aquela com a menor perda possível.

Verificação automática de locutor

Atualmente existem sistemas automáticos que utilizam tecnologias de processamento digital de sinais e são capazes de contribuir com as análises de verificação de locutor.

Nesses sistemas é gerado um modelo estatístico com base no material sonoro questionado e outro com base no material sonoro padrão, sendo os modelos gerados comparados entre si e gerada uma pontuação que infere a similaridade da fala entre os materiais, sendo o resultado fornecido em termos de probabilidade.

Os sistemas automáticos realizam confrontos acústicos e fornecem resultados objetivos, e fornecem mais um elemento robustecendo o resultado final, entretanto, o sistema automático não pode ser utilizado isoladamente pois a tecnologia atual não permite tal aplicação, e nem há perceptivas para tanto.

Resultados dos Exames de Verificação de Locutor

A adequabilidade principalmente do material questionado está ligada à possibilidade de um resultado conclusivo nos exames de verificação de locutor. Quanto mais adequado for o material sonoro questionado, especialmente no tocante a quantidade de material e qualidade do áudio, maior a possibilidade de uma análise conclusiva

Os resultados finais dos exames de verificação de locutor são positivo, negativo, indicativo ou não conclusivo. Os resultados positivos ou negativos são fornecidos quando o examinador com base nos elementos técnicos obtidos nas análises perceptual, articulatória, acústica e automática se convenceu de que a voz questionada partiu ou não do trato vocal do fornecedor do material sonoro padrão.

Os resultados indicativos, não concluem com certeza de que a voz questionada partiu ou não do trato vocal do fornecedor do material sonoro padrão, porém, apresenta indícios, ainda que em quantidade insuficiente.

Existe ainda a possibilidade de não conclusão, que ocorre principalmente quando são encontradas convergências e divergências entre o material sonoro questionado e padrão, acarretando na impossibilidade de apontamento de que a voz do material questionado é ou não a mesma fornecida no material padrão.

Com base nas consultas à legislação onde não foi encontrado impedimento para a instalação do sistema proposto e também não foram encontrados casos semelhantes nas decisões dos tribunais pesquisados, foi realizada consulta jurídica com os operadores do direito. Através dessa consulta, apesar de embasada em situações acadêmicas, foi constatado que o sistema proposto é viável juridicamente desde que autorizada a quebra do sigilo das comunicações do alvo. Para evitar que advogados de defesa tenham êxito nas tentativas de desqualificação das provas obtidas, é necessário que sejam implantadas as diretivas para manutenção da cadeia de custódia. Todas as ações devem ser registradas nos *logs*, e os registro de *logs* devem ser disponibilizados aos assistentes técnicos das partes de modo que os mesmos possam analisar o material e constatar que não houve inclusão, alteração ou subtração das provas obtidas.

5. VIABILIDADE TÉCNICA

Além da necessidade de avaliar a possibilidade jurídica de utilização do áudio obtido é necessário avaliar se é possível tecnicamente utilizar o sistema proposto, especialmente no tocante a implantação do sistema de forma que o mesmo seja furtivo e de difícil detecção.

A realização de uma análise de viabilidade técnica para implantação do sistema, depende muito de qual a tecnologia o investigado utiliza, e com base na tecnologia do investigado será traçada a estratégia para desenvolvimento e introdução do sistema no dispositivo do investigado.

A abordagem utilizada dependerá da arquitetura e do sistema operacional utilizado pelo dispositivo a ser invadido. O investigado poderia utilizar, por exemplo, um computador com arquitetura *x86* e sistema operacional *Windows XP*, ou um telefone celular tipo *smartphone* com arquitetura *AMR* e sistema *Android 2.2*, ou um *tablet iPad* com sistema *iOS*, sendo que o sistema deve ser desenvolvido para o equipamento que o investigado possuir.

5.1. TÉCNICAS DE INFECÇÃO

Como já mencionado o sistema proposto deve ter capacidade furtiva e ser de difícil detecção, entretanto um dos principais desafios, é a inclusão do sistema no dispositivo do investigado.

Uma das possibilidades é ter acesso físico ao dispositivo do investigado e assim instalar o sistema, como alternativa poderiam ser utilizadas técnicas usadas por *hackers* de modo a forçar o usuário a, sem saber, instalar o aplicativo em seu sistema.

5.1.1. Conhecendo o investigado

Uma das técnicas utilizadas por *hackers* para invadir computadores dos seus alvos é através do *phishing*. *Phishing* é uma técnica que usa engenharia social para fazer vítimas, enganando-as com o objetivo de obter suas informações pessoais (geralmente de cunho financeiro) e depois causar-lhes prejuízos. (OLIVIO, 2010).

Na Internet, o *phishing* pode chegar ao alvo de várias maneiras, através de uma janela *pop-up* no navegador, de mensagens instantâneas ou de *e-mails*. Geralmente, a vítima é convencida a executar um clique de mouse, que descarregará e instalará algum *malware*, aquele pacote de ameaças que inclui *spam*, vírus, *phishing* e *spyware* (DELL, 2011) ou acessará um site fraudulento. (OLIVIO, 2010)

Vale lembrar que as principais vítimas desse tipo de programa de *phishing* são os usuários de plataforma proprietária, como o *Windows* e seus variantes. (MARCELO, 2005)

Uma das práticas *hackers* mais antigas não diz respeito à exploração de falhas em computadores, mas sim no comportamento humano (ARRUDA, 2011)

O usuário é convencido a clicar em *links* quando acredita que o conteúdo que será aberto é algo que lhe é interessante e confia no remetente.

Alguns *hackers* utilizam a técnica conhecida como engenharia social, para estudar os hábitos e o comportamento do seu alvo e assim conhecer seus interesses, obter informações pessoais e dessa forma aumentar as chances de que o alvo se interesse em clicar no *link* encaminhado.

O engenheiro social é capaz de estudar sua possível vítima por meses, procurando detalhes mínimos e brechas que o podem levar a conseguir a informação necessária. (MARCELO, PEREIRA, 2005)

O principal meio do engenheiro social explorar seu alvo é ganhar a sua confiança, sendo isto feito aos poucos, num processo de camadas, até chegar ao final. (MARCELO, PEREIRA, 2005)

Em algumas situações são utilizados apenas ataques indiretos, sem que haja a necessidade do contato direto entre vítima e engenheiro social e consequentemente não há necessidade da vítima conhecer ou confiar no engenheiro social, bastando um certo grau de curiosidade. O exemplo citado num relato do mais famoso *hacker*, Mitnik em entrevista à revista PC Brasil, exemplifica a situação (ULBRICH, 2004).

> "...Imagine que você está trabalhando para uma corporação. Ao entrar em um elevador, nota que alguém deixou cair um disquete no chão. O disco tem estampado o logo da empresa e traz uma etiqueta que diz: "Confidencial:histórico salarial de todos os funcionários". Diante disso, qual a primeira providência que você tomaria? Movidos pela curiosidade. Colocamos o disquete na máquina e abrimos o arquivo para ver seu conteúdo. Talvez exista o ícone para um documento

> do Word chamado "arquivo de folha de pagamento" ou "história salarial". Provavelmente clicaríamos para comparar nosso salário com os demais. O que acontece então? Você vê uma caixa de mensagem que diz algo como "o aplicativo não pôde ser aberto" ou "arquivo falho". O que a maioria não sabe é que um Cavalo de Tróia acaba de ser instalado, o que permitirá que o intruso invada."

Para o caso de investigações criminais, normalmente o investigado tem as suas comunicações de forma geral interceptadas legalmente, tais como as comunicações telefônicas e de dados, o que permite à investigação ter acesso às informações do cotidiano do investigado percebendo os seus gostos, suas opções de lazer, seus interesses além de possibilitar a identificação de características emocionais, o que auxilia na estratégia para desenvolvimento do sistema de intrusão.

Os desenvolvedores de *trojans* e vírus usam ferramentas que podem se anexar a um programa inocente, e quando você instala um aplicativo, estará baixando também um *trojan*. (CARMONA, 2006)

Com o conhecimento comportamental do investigado, é possível desenvolver um aplicativo que seja do interesse do mesmo e então incluir o sistema furtivo. Dessa forma, se o investigado abrir o arquivo do seu interesse, instalará também o aplicativo furtivo possibilitando a obtenção do áudio, desde que não haja outros mecanismos de proteção ativados que interfiram.

Nesse trabalho, a ideia é desenvolver um sistema direcionado ao alvo, tornando a chance de sucesso muito mais alta do que utilizando um *phishing* visando um público geral ou um pequeno grupo, porém isso requer conhecimento prévio do alvo, o que não é difícil de obter conforme já comentado.

5.1.2. Proteção dos sistemas

Segundo (FERNANDES FILHO et. al. 2011) ataques realizados por meio de *malware* tomaram uma dimensão tão grande que atividades simples como a navegação na *Web*, a participação em redes sociais digitais e o uso de celulares tornaram-se perigosas.

Existem algumas classes de *malwares*, que segundo (Szor, 2005 apud. FERNANDES FILHO et. al. 2011) podem se enquadrar em algumas das definições abaixo, ou em mais de uma delas:

Trojan: Cavalos-de-tróia são tipos comuns de *malware* cujo modo de infecção envolve despertar a curiosidade do usuário para que este o execute e comprometa o sistema. Este tipo de código malicioso também pode ser encontrado em versões modificadas de aplicações do sistema operacional, substituídas por indivíduos maliciosos. Estas versões apresentam as mesmas funcionalidades da aplicação íntegra, porém também contêm funcionalidades adicionais com a finalidade de ocultar as ações malignas.

Downloader. Um programa malicioso que conecta-se à rede para obter e instalar um conjunto de outros programas maliciosos ou ferramentas que levem ao domínio da máquina comprometida. Para evitar dispositivos de segurança instalados na vítima, é comum que *downloaders* venham anexados à mensagens de correio eletrônico e, a partir de sua execução, obtenham conteúdo malicioso de uma fonte externa, por exemplo de um *site*.

Rootkit. É um tipo especial de *malware*, pois consiste de um conjunto de ferramentas para possibilitar a operação em nível mais privilegiado. Seu objetivo é permanecer residindo no sistema comprometido sem ser detectado e pode conter *exploits*, *backdoors* e versões *trojan* de aplicações do sistema. Os *rootkits* modernos atacam o *kernel* do sistema operacional, modificando-o para que executem as ações maliciosas de modo camuflado. Este tipo de *rootkit* pode inclusive interferir no funcionamento de mecanismos de segurança.

No âmbito da defesa, a mera identificação de um arquivo executável como sendo um *malware* conhecido (já coletado, analisado e talvez combatido) permite a tomada de contra-medidas de maneira rápida e eficiente. Isto facilita a contenção de danos, minimiza prejuízos e reduz a possibilidade de infecção em redes e sistemas ainda intactos por meio de regras de bloqueio ou aplicação de *patches* de segurança. (FERNANDES FILHO et. al. 2011)

Com isso, é necessário haver meios de se identificar *malware* para que ações defensivas possam ser coordenadas, ao mesmo tempo em que sejam obtidos conhecimentos sobre o comportamento de um certo *malware* e sobre a possível extensão dos danos aos sistemas comprometidos por este código específico. A solução mais tradicional para identificação de *malware* ainda é o uso de antivírus. (FERNANDES FILHO et. al. 2011).

Segundo (FERNANDES FILHO et. al. 2011), o antivírus que é um dos mecanismos de defesa contra *malware* mais populares, pode ser explicado basicamente como um programa que varre arquivos ou monitora ações pré-definidas em busca de indícios de atividades maliciosas. Em geral, os antivírus operam de duas formas para identificar código malicioso: correspondência de padrões em bancos de dados de assinaturas ou heurísticas comportamentais. Na detecção por assinatura, um arquivo executável é dividido em pequenas porções (*chunks*) de código, as quais são comparadas com a base de assinaturas do antivírus. Assim, se um ou mais *chunks* do arquivo analisado estão presentes na base de assinaturas, a identificação relacionada é atribuída ao referido arquivo. Na detecção por heurística, um arquivo sob análise é executado virtualmente em um emulador minimalista e os indícios de comportamento suspeito são avaliados a fim de se verificar se a atividade realizada pelo programa pode ser considerada normal ou se um alerta deve ser emitido.

O grande problema dos antivírus é o surgimento frequente e crescente de variantes de *malware* previamente identificados, cujas ações modificadas visam evadir a detecção. Essas variantes precisam ser tratadas muitas vezes individualmente (e manualmente), no caso da confecção de uma assinatura para um antivírus. Além disso, pode ser preciso alterar a heurística de detecção para que esta seja capaz de identificar a variante, verificando se a modificação não vai gerar mais falsos-positivos, fazendo com que programas que não são *malwares* sejam detectados como tal. (FERNANDES FILHO et. al. 2011)

Para implementar proteção dos sistemas contra *malwares*, a cada novo *malware* são feitas análises de código visando o entendimento profundo do funcionamento do mesmo - como atua no sistema operacional, que tipo de técnicas de ofuscação são utilizadas, quais fluxos de execução levam ao comportamento principal planejado, se há operações de rede, *download* de outros arquivos, captura de informações do usuário ou do sistema, entre outras atividades. (FERNANDES FILHO et. al. 2011)

Existem basicamente dois tipos de análises, a análise estática e a análise dinâmica. Na análise estática o código é examinado sem executá-lo, utilizando técnicas de análise de *strings* e engenharia reversa; já na análise dinâmica o código é executado em ambiente controlado, sendo utilizadas ferramentas para verificar os processos que estão sendo

executados, arquivos criados e acessados, registros, atividades de rede, chamadas de sistemas, dentre outras.

Embora o *modus operandi* dos antivírus ainda seja majoritariamente a identificação com base em assinaturas, tem crescido o interesse por heurísticas. Para gerar uma heurística que identifique um exemplar de *malware* (ou uma classe), é necessário conhecer primeiro o seu comportamento, isto é, quais são as ações realizadas no sistema operacional alvo que denotam uma atividade anormal ou suspeita. (FERNANDES FILHO et. al. 2011)

Os sistemas de análise dinâmica de *malware*, embutidos nos antivirus, conhecidos como *SandBoxes*, lançam mão de uma variedade de técnicas para monitorar a execução de um *malware* de maneira controlada, utilizando desde a instrumentação de emuladores complexos até a interceptação de chamadas ao *kernel* do sistema operacional monitorado. (FERNANDES FILHO et. al. 2011)

Os sistemas de proteção além de realizarem análise do arquivo suspeito, através da obtenção da assinatura e verificação se esta encontra-se na base de dados de *malwares* conhecidos, realizam análise comportamental. Essa análise visa proteger o sistema contra *malwares* ainda desconhecidos, mas que realizem ações suspeitas.

Além disso, a *microsoft* implementou nas versões mais novas do *windows* a exigência de utilização somente de *drivers* assinados digitalmente.

Um *driver* assinado é um *driver* de dispositivo que inclui uma assinatura digital. Uma assinatura digital é uma marca de segurança eletrônica que pode indicar o editor do *software* e se alguém alterou o conteúdo original do pacote de *driver*. Se um *driver* tiver sido assinado por um editor que verificou sua identidade com uma autoridade de certificação, o *driver* é confiável, provém realmente desse editor e não foi alterado. (MICROSOFT, 2012)

O *Windows* emite um alerta se um *driver* não estiver assinado, tiver sido assinado por um editor que não tenha verificado sua identidade com uma autoridade de certificação ou tiver sido alterado desde o lançamento (MICROSOFT, 2012)

Caso haja tentativa de instalação de um *driver* não assinado, uma possível mensagem recebida pelo usuário é “Um *driver* sem assinatura digital válida, ou que foi alterado após

ter sido assinado, não pode ser instalado em versões baseadas no *x64* do *Windows*." (MICROSOFT, 2012).

Essa restrição visa proteger o sistema contra *malware* que são projetados para serem executados em nível de *driver*, o que lhes confere acesso privilegiado ao sistema.

Entretanto existe um subterfúgio para burlar essa restrição, através da alteração do registro *DDISABLE_INTEGRITY_CHECKS*, que pode ser feita através da execução do comando *bcdedit /set loadoptions DDISABLE_INTEGRITY_CHECKS* como administrador.

5.1.3. Alternativas para invasão

A medida que as estratégias de proteção contra *malwares* evoluem, os desenvolvedores de *malwares* buscam alternativas para burlar os mecanismos de proteção desenvolvidos.

As técnicas de *Advanced Persistent Threat (APT)* estão sendo utilizadas para invadir sistemas, sendo que segundo (ANDRESS, 2011, tradução nossa) o *NIST* definiu *APT* como sendo um adversário que possui níveis sofisticados de conhecimentos e recursos significativos que lhe permitem criar oportunidades para atingir seus objetivos usando múltiplos vetores de ataque. A *APT* (1) persegue os seus objetivos repetidamente ao longo de um período prolongado de tempo, (2) adapta-se a esforços de defesa para resistir a eles, e (3) é definida para manter o nível de interação necessário para executar os seus objetivos.

Segundo a definição do *NIST*, o *APT* pode ser dividido em três componentes:

1- *Advanced* - O atacante faz uso de uma variedade de ferramentas de ataque e podem ter recursos para desenvolver ou comprar vulnerabilidades *zero-day* e *malwares*, ou ferramentas de ataque, a fim de evitar as medidas de detecção e prevenção. Esse componente se refere a "adapta-se a esforços de defesa para resistir a eles" constante na definição do *NIST* (ANDRESS, 2011, tradução nossa).

2- *Persistent* - O ataque está sendo executado na busca de um objetivo específico, e não de uma descoberta aleatória de uma vulnerabilidade ou apenas por diversão. Os ataques continuam até que esse objetivo seja alcançado, sendo que o atacante irá manter o acesso ao ambiente. Isso se refere a "persegue os seus objetivos repetidamente ao longo de um período prolongado de tempo" e "é definida para manter o nível de interação necessário

para executar os seus objetivos" nas definições de *NIST*. O atacante também irá tomar medidas abrangentes para evitar a detecção. (ANDRESS, 2011, tradução nossa)

3- *Threat* - Ameaças em *APT* não são aqueles vistos na forma de *scripts* realizando a varredura de porta, ou o ataque de *SQL injection* vindo através de uma aplicação *web* mal feita. Ataques *APT* representam um esforço mais concentrado e dirigido. Eles não são realizados ao acaso. Este tipo de ataque implica na motivação para cumprir as metas específicas do atacante. Ataques com este grau de foco representam tanto um grau maior de perigo e quanto um maior nível de dificuldade para se defender do que as típicas técnicas de defesas. (ANDRESS, 2011, tradução nossa)

Com relação às técnicas de defesa contra *APTs*, segundo (ANDRESS, 2011) defender-se contra ataques que são propositadamente furtivos e refletem um alto nível de habilidade técnica pode ser na melhor das hipóteses um desafio. Uma grande quantidade de dinheiro pode ser gasto na compra de *firewalls*, *IDS*/*IPS*, software de monitoramento e outras ferramentas semelhantes, além dos recursos necessários para implementar e gerenciar; porém essas medidas podem ser ignoradas por um atacante habilidoso. Isso vale em dobro para os produtos anunciados para se defender contra *APT* especificamente. Um *post* no *blog* do chefe do *Computer Security Incident Response Team Cisco* (*CSIRT*) resume bem a situação: "Se alguém tentar vender um hardware ou solução de *software* para o *APT*, ou eles não entendem *APT*, ou não entendem como funcionam os computadores, ou estão mentindo, ou eventualmente, todos os três" a própria definição de *APT* impede a fácil detecção e mitigação de ataques através das medidas-padrão utilizadas para filtrar as ameaças mais simples.

Embora as ferramentas são importantes e têm definitivamente um lugar, elas podem ser subvertidas por um atacante hábil de várias maneiras. É necessário avaliá-las para descobrir essas maneiras e mitigá-los antes que sejam encontradas por um invasor. Um dos principais passos para se defender contra os ataques sutis que fazem parte do *APT* é ter as ferramentas adequadas. *Firewall* padrão, *IDS*, etc, pode não ser suficiente para revelar a presença de um atacante altamente qualificado. Pior ainda, muitas dessas medidas são compradas, ligadas, e talvez apenas ocasionalmente atualizadas. Atacantes contam com estas ferramentas que estão sendo simplesmente conectadas e ignoradas, e não estão sendo

capazes de detectar a engenharia social ou ataques de *zero-day* que os atacantes estão usando. (ANDRESS, 2011, tradução nossa)

As ferramentas necessárias, a partir de uma perspectiva *APT*, são aquelas que permitem registrar e monitorar o que é realizado, e depois examinar os resultados. Ser capaz de avaliar a situação atual dos *hosts*, redes, dispositivos de fronteira, e o tráfego fluindo de, e para eles, a qualquer momento é crítico, bem como ter acesso aos dados históricos. Se a capacidade de examinar os registros do que aconteceu nos ambientes que estão sendo protegidos não existe, torna-se muito difícil de detectar como o atacante conseguiu entrar, o que os ataques estavam fazendo e por quanto tempo os sistemas foram comprometidos. Com os registros de *log*, pode não ser possível encontrar vestígios de um ataque no *firewall*, *IDS*, ou registros de *host*. (ANDRESS, 2011, tradução nossa)

Desenvolver um padrão das atividades normais de rede e *host* pode ser fundamental na detecção de ataques *APT*. Tais padrões podem representar o tráfego de rede, os processos, ou uma combinação de muitas medidas. Quando em ambientes que são objeto de ataques que para serem furtivos requerem grande atividade, esses ataques não irão necessariamente sinalizar nos *firewalls* e *IDSs* que são utilizados para a proteção. Um bom padrão de atividades normais no ambiente pode permitir a detecção de atividades anormais nos ambientes específicos. Entretanto, essa técnica pode ser prejudicial devido a possibilidade de falsos positivos. (ANDRESS, 2011, tradução nossa)

Esses recursos podem permitir identificar tráfego de rede incomum gerado por um *trojan* e informações através do *firewall*, ou um *rootkit* modificando arquivos críticos do sistema, ou outra atividade. Muitos fornecedores, estão oferecendo produtos com esses conjuntos de recursos, mas é importante estar ciente de que eles não são bolas de cristal. (ANDRESS, 2011, tradução nossa)

Muitos ataques recentes, sejam eles especificamente classificados como *APT* ou de outra forma, não teriam sido evitados com técnicas de segurança. Nos ataques em *RSA* e *Oak Ridge National Labs*, os ataques por *phishing* foram utilizados como parte dos esforços de ataque. Em combinação com as vulnerabilidades de *zero-day* usadas no ataque, esses esforços se mostraram altamente bem sucedidos. (ANDRESS, 2011, tradução nossa)

Olhando para os ataques contra o *Google*, *RSA*, e *Oak Ridge National Labs*, todos eles têm um tema comum: o uso de *phishing* simples e ataques de engenharia social. Esses ataques têm diminuído, ou sido frustrados completamente devido um maior nível de conscientização de segurança por parte dos empregados e administradores das empresas. (ANDRESS, 2011, tradução nossa)

Tecnicamente é necessário investir em defesas de fora pra dentro, podendo ser implementadas medidas como *firewalls* e e *DMZs* na entrada externa da rede da organização, *firewalls* e *IDS*/*IPS* na rede interna, ferramentas de anti-virus e *anti-malware*, além de *firewalls* e *HIDS*/*HIPS* nas estações, controle de acesso e *login* nas aplicações e por fim a criptografia dos dados. (ANDRESS, 2011, tradução nossa)

Esses esforços isolados não são suficientes para proteção contra ataques *APT*. Os atacantes leem os mesmos livros e artigos, e assistem às mesmas conferências de segurança que os defensores, os atacantes são capazes de compensar muitas das medidas que poderiam estar implantadas para implementação de uma defesa. (ANDRESS, 2011, tradução nossa)

Os ataques *APT* são eficientes em corporações que em geral adotam medidas para implementar segurança. Em ambientes pessoais, nos quais que em geral o usuário não possui conhecimentos técnicos suficientes para identificar um ataque, provavelmente serão também bem sucedidos.

Com o uso dos *smartphones* os ataques não ficam restritos aos computadores, mas também a outros dispositivos. Foi relatado que um determinado número de sites legítimos mas comprometidos devido a ações maliciosas, foram vistos oferecendo *malwares* para *Android* tendo como alvo os visitantes menos atentos, de acordo com uma advertência feita pela especialista em segurança *Lookout*. O *download* do *malware*, que se apresenta como uma atualização do sistema, é feito automaticamente graças ao código oculto malicioso (*iFrame* ou *JavaScript*) localizado na parte inferior de cada página. O *download* é acionado, apenas se o usuário visitar a página com um navegador com a palavra "*Android*" em seu cabeçalho *user-agent*. (ZORZ, 2012)

A instalação do *app* - na verdade um cavalo de Tróia chamado de "*NotCompatible*" - será bloqueado pelo dispositivo se a configuração desconhecida estiver habilitada (significando que a instalação de aplicativos a partir de outras fontes procuradas no *Google* é permitida).

O cavalo de tróia deve pedir ao usuário permissão para ser instalado, mas isso não significa muito se o destino for um usuário inexperiente no assunto. (ZORZ, 2012)

5.2. DESENVOLVIMENTO DO SISTEMA

O sistema proposto pode ser desenvolvido para dispositivos que utilizam sistema operacional *Linux*, *Windows*, *iOS* e *Android*. A seguir será apresentada uma compilação de bibliotecas que podem ser utilizadas para o desenvolvimento do sistema.

5.2.1. Aquisição de Áudio

O desenvolvimento do módulo de aquisição de áudio pode acessar os dispositivos de áudio utilizando códigos disponíveis nos sistemas operacionais. O *Windows* tem o *DirectSound*, *WinKS*, *WASAPI*, *Windows Multimedia Library* e *ASIO*, o Linux tem o *FFADO*, *ALSA* e *OSS* e o *MacOS* tem o *Sound Manager*, *ASIO* e *Core Audio*. Implementar um software que funcione em tudo isto pode ser transtorno (SCHIAVONI, 2012).

Existem algumas alternativas que parecem viáveis como *JUCE*, *SDL*, *OpenAL*, *RTAudio* e *PortAudio*. (SCHIAVONI, 2012).

O *JUCE* (*Jules' Utility Class Extensions*) é uma biblioteca para *C++* para o desenvolvimento de programas multi-plataforma. Ela contém praticamente tudo o que é provável que você precisa para criar a maioria das aplicações, e é particularmente adequado para a construção de *GUIs* altamente personalizada, e para lidar com gráficos e som. (JUCE, 2010)

JUCE pode ser utilizado nas seguintes plataformas: (JUCE, 2010)

- *Mac OSX* - Aplicações e *plugins VST/AudioUnit/RTAS/NPAPI* podem ser compilados com o *Xcode* para *OSX 10.4* ou posterior.

- *iOS* - *iPhone* nativa e *iPad* pode ser construído com o *Xcode*.

- *Windows* - Aplicações e *plugins VST/RTAS/NPAPI/ActiveX* podem ser construídos usando o *MS Visual Studio*. Os resultados são totalmente compatíveis com o *Windows XP, Vista* ou *Win7*.

- *Linux* - Aplicações e *plugins* podem ser construídos para qualquer *kernel 2.6* ou posterior.

- *Android* - Aplicações para *Android* podem ser construídas usando *Ant* e *Eclipse.*

Para todas as plataformas acima, o código que você escreve é o mesmo, e você não precisa se preocupar com os detalhes específicos da plataforma. Se o *C++* é portátil, então você precisa simplesmente re-compilar sua aplicação para executá-lo em outros sistemas operacionais.(JUCE, 2010)

A *OpenAL* é uma *API* de áudio *3D* multi-plataforma apropriada para uso com aplicativos de jogos e muitos outros tipos de aplicações de áudio. (OPENAL, s.d)

As seguintes plataformas atualmente trabalham com implementação de *OpenAL* (OPENAL, 2008b)

Tabela 5.1 : Plataformas do OpenAL

Plataforma	**Dispositivos**	**Licensa**
BSD	nativos	*Open Source (LGPL)*
IRIX	nativos	*Open Source (LGPL)*
Solaris	nativos	*Open Source (LGPL)*
Linux	*ALSA*	*Open Source (LGPL)*
	OSS	*Open Source (LGPL)*
Macintosh OS 8/9	*Sound Manager*	*Open Source (LGPL)*
Macintosh OS X	*Core Audio*	*Open Source (Apple)*
Microsoft Windows	*Creative Audigy*	*Creative Labs, Inc.*
	Creative Audigy 2	*Creative Labs, Inc.*
	Creative Audigy 4	*Creative Labs, Inc.*
	Creative X-Fi	*Creative Labs, Inc.*
	DirectSound	*Open Source (LGPL)*
	DirectSound3D	*Open Source (LGPL)*
	MMSYSTEM	*Open Source (LGPL)*
	NVIDIA nForce	*Open Source (LGPL)*
Microsoft Xbox	nativos	*Creative Labs, Inc.*
Microsoft Xbox 360	nativos	*Creative Labs, Inc.*

PortAudio é uma biblioteca para áudio, livre, multi-plataforma e de código aberto. Ela permite escrever simples programas de áudio em '*C*' ou *C++* que irá compilar e rodar em muitas plataformas, incluindo *Windows*, *Macintosh OS X* e *Unix (OSS / ALSA)*. Alguns aplicativos utilizam *PORTAUDIO*, como *Audacity* e *VLC*. (PORTAUDIO, s.d)

A utilização dessas bibliotecas multi-plataformas, minimizam o trabalho de desenvolvimento, já que o mesmo código pode ser utilizado em diversos dispositivos.

5.2.2. Codificação de Áudio

Para realizar a codificação do áudio obtido, existem algumas opções disponíveis como *SILK*, *ILBC*, *G.711*, *G.723.1*, *G.729* sendo todos os *codecs* especificados pelo *ITU-T*. Como o interesse do sistema é utilizar o áudio da voz, qualquer *codec* otimizado para voz pode ser utilizado.

O *Skype* utiliza um *codec* de áudio de alta qualidade e o licenciou para desenvolvedores gratuitamente. (IDGNOW, 2009)

O *codec*, chamado de *SILK*, foi introduzido na versão do *Skype 4.0* para *Windows* e oferece qualidade sonora que captura o som total da voz humana, de acordo com o gerente para áudio e vídeo do *Skype*, Jonathan Christensen. (IDGNOW, 2009)

Sistemas telefônicos convencionais usam uma faixa estreita para voz que permite qualidades equivalentes a taxas de 64 Kbps, o que leva a problemas para diferenciar os sons do "F" e do "S", por exemplo. (IDGNOW, 2009)

O *VoIP* faz chamadas em canais mais amplos, que permitem qualidades maiores graças a *codecs*. Com o *Silk*, o *Skype* pode reproduzir todas as frequências audíveis da voz humana, afirma Christensen, o que ajuda na identificação de participantes de uma chamada coletiva, por exemplo. (IDGNOW, 2009)

A companhia está oferecendo o *codec* gratuitamente para desenvolvedores para que usem em qualquer aparelho ou aplicação, com ou sem o *Skype*, explica Christensen. (IDGNOW, 2009)

O *SILK* pode rodar em *chipsets x86* para sistemas *Windows*, *Macintosh* e *Linux* e ser usado em *softwares* que rodam nas plataformas *Arm* e *MIP*s, diz o *Skype*. (IDGNOW, 2009)

Já o *ILBC* (*Internet Low Bitrate Codec*) é um *codec* de voz grátis adequado para comunicação de voz sobre *IP.* O *codec* foi feito para ser utilizado em banda estreita e resulta em uma taxa de bits de 13,33kbit/s, com um comprimento de quadro de 30ms e 15.20kbps com um comprimento de quadro de 20ms. O *codec iLBC* permite a degradação

da qualidade de fala aceitável, no caso de quadros perdidos, o que ocorre em conexão com perda ou atraso de pacotes. (WEBRTC, s.d)

Além desses *codecs* citados existem outros que podem ser utilizados. Os *codecs* terão a função de compactação das amostras, já que é o objetivo dos mesmos quando utilizados na transmissão de voz sobre dados.

É importante levar em conta o tratamento que os *codecs* fazem quanto ao silêncio durante a obtenção do áudio, de forma a não causar perda de sincronia com a base de tempo, podendo sugerir alegações de edição do áudio.

5.2.3. Criptografia, Armazenamento e Transmissão

Para implementar as funcionalidades de criptografia, pode ser desenvolvido um módulo próprio ou ainda utilizar *APIs* disponíveis nos sistemas. Para o *Windows* existe a *CryptoAPI* que implementa funções de criptografia.

A *API* de criptografia contém funções que permitem a aplicativos cifrar ou assinar digitalmente os dados de uma forma flexível, oferecendo proteção para dados importantes do usuário. Todas as operações criptográficas são executadas por módulos independentes, conhecidos como provedores de serviços de criptografia (*PSC*s). Um *PSC*, o *Microsoft Base Provider RSA*, está incluído com o sistema operacional. (COLERIDGE, 1996)

Cada *PSC* fornece uma implementação diferente da camada de *API* de criptografia. Alguns fornecem algoritmos criptográficos mais fortes, enquanto outros contêm componentes de hardware. Além disso, alguns *PSCs* podem ocasionalmente comunicar com os utilizadores diretamente, tal como quando as assinaturas digitais são realizadas utilizando a chave de assinatura privada do utilizador. (COLERIDGE, 1996)

Há outras bibliotecas com funções criptográficas, como por exemplo a *CryptoSys API*. A *API* fornece quatro dos principais algoritmos de codificação de bloco: *AES*, *DES*, *Triple DES* e *Blowfish*, uma cifra de fluxo compatível com *RC4*; algoritmos de *hash SHA-1*, *SHA-224, SHA-256, SHA-384, SHA-512, MD5 e MD2*, o *HMAC* e algoritmos de autenticação de mensagens *CMAC*, compressão de dados, e um gerador de números aleatórios seguro. Inclui interfaces para *Visual Basic*, *VBA*, *VB.NET/VB2005/8/x*, *C/C+*

+/C# e *ActiveX/COM/ASP*, *VB.NET* e *ActiveX*. Há também uma versão *Linux* disponível. (CRYPTOSYS, 2011)

O armazenamento das amostras obtidas pode ser feita através da criação de um arquivo e inclusão dos dados cifrados no interior do mesmo, sendo que existem bibliotecas que desempenham essas funções incluídas nas principais linguagens de programação. O mesmo ocorre com a obtenção de dados dos dispositivos de *hardware*, obtenção da base de tempo e acesso ao dispositivo de redes para realizar a transmissão dos dados.

As alternativas apresentadas constituem opções que podem ou não ser utilizadas para o desenvolvimento do sistema, sendo que podem ser utilizadas outras linguagens de programação e bibliotecas que não foram citadas no trabalho e que podem constituir alternativas mais apropriadas.

6. CONCLUSÕES

Um dos mais importantes meios de obtenção de provas em investigações criminais é a escuta telefônica. Em várias investigações as escutas telefônicas são essenciais ou até mesmo as únicas provas que incriminam determinado alvo.

Sabedores disso, os criminosos evitam utilizar o telefone em suas comunicações relativas à atividade criminosa a fim de evitar que os órgãos de investigação descubram seu *modus operandi* e formem um conjunto probatório capaz de fomentar condenação futura.

O crescente uso das comunicações através de *VoIP* e de equipamentos computacionais, como os próprios computadores, *smartphones* e *tablets* possibilitam com facilidade a utilização de sistemas de criptografia para as comunicações.

Com isso, a interceptação telemática da forma como é feita atualmente torna-se infrutífera quando na tentativa de obter as informações que trafegam nesses canais criptografados.

Os sistemas que possibilitam comunicação criptografada são oferecidos por empresas, sendo que algumas soluções são pagas e outras soluções são gratuitas como por exemplo o *skype*.

Com a utilização de comunicações criptografadas pelas quadrilhas do crime organizado se faz necessária a evolução das técnicas atuais de investigação de modo a obter de alguma forma as informações transmitidas pelos canais criptografados.

A legislação atual prevê a interceptação telefônica e telemática e atribui às operadoras a obrigação do fornecimento das informações referentes à essas interceptações. No entanto, em comunicações *VoIP* que utilizam canais criptografados, não há possibilidade técnica para a operadora fornecer as informações aos órgãos de investigação já que o sinal trafega criptografado por todo o canal de comunicação sendo cifrado e decifrado apenas nos equipamentos dos usuários envolvidos fim.

Considerando que o sinal trafega criptografado nos canais de comunicação, existem basicamente duas maneiras de ter acesso à informação cifrada: ter acesso à chave de criptografia utilizada, ou obter a informação antes de ser criptografada. A primeiro opção, pode ser inviável, já que as chaves são alteradas a cada intervalo de tempo.

A proposta desse trabalho é acessar a informação no dispositivo do investigado antes da mesma ser cifrada, e então transmiti-la para uma máquina de análise.

O acesso ao dispositivo do investigado deve ser feito de maneira oculta sem que o investigado perceba, pois caso isso ocorra, poderá frustrar a investigação.

É necessário que o áudio seja obtido do microfone e fone, e tratado de modo que sejam mantidas algumas premissas mantendo a cadeia de custódia. É necessário que o áudio seja armazenado e transmitido criptografado para evitar que pessoas não autorizadas tenham acesso ao áudio e para garantir a integridade do áudio, ou seja que o áudio disponibilizado nos sistema de análise é o mesmo obtido no dispositivo do investigado.

Na proposta foram definidos os requisitos e as formas para atendê-los. A legislação permite a interceptação das comunicações mas não define a forma como essa deve ser feita, e em pesquisas em decisões judiciais não foram encontrados registros de provas obtidas com sistemática similar à proposta. Devido não haver legislação e jurisprudência formada sobre a matéria, foi feita consulta jurídica a operadores do Direito a fim de avaliar se as provas obtidas pelo sistema proposto tem validade jurídica, pois de nada adiantaria desenvolver o sistema se as provas obtidas não forem válidas nos tribunais. O resultado da pesquisa jurídica é que devido ao fato da legislação permitir a interceptação não definindo a forma como será feita, o sistema proposto pode ser utilizado para a obtenção das provas. Esse entendimento é baseado apenas na doutrina, sendo que num caso concreto, havendo outras circunstâncias a serem analisadas o entendimento do Judiciário pode ser diverso.

Além do aspecto jurídico, outro ponto abordado foi a análise técnica do sistema, definindo possíveis estratégias de implementação de modo que o sistema seja furtivo e não seja detectável.

O grande desafio é a instalação do sistema no dispositivo do investigado sem que o mesmo se dê conta do que está sendo feito. A estratégia proposta é a de técnicas similares às utilizadas pelos *hackers*, ou seja, utilizar a curiosidade do investigado ou fornecer a ele uma oportunidade que possa motivá-lo a abrir um aplicativo que seja do seu interesse e esse aplicativo constitui um cavalo de tróia estando o sistema furtivo embutido no mesmo.

A estratégia proposta se diferencia nas utilizadas pelos *hackers* exatamente no aspecto motivacional. Os *hackers* em geral buscam a infecção de grande quantidade de usuários e

não tem alvos específicos, para tal utilizam situações do cotidiano e que possam despertar o interesse dos alvos, como atualizações bancárias, fotos de casos policiais emblemáticos, etc.

No caso do sistema proposto existe um ou poucos alvos específicos que devem ter o seu sigilo telefônico e telemático quebrado. Com o conhecimento do teor das comunicações telefônicas e telemáticas do alvo a equipe de análise tem conhecimento do cotidiano dos alvos, seus gostos, seus hábitos e seus interesses. Com base nisso, é possível desenvolver um aplicativo ou sistema ou site com foco no alvo, aumentando assim a possibilidade de sucesso na infecção.

O desenvolvimento do aplicativo deve ser feito para o dispositivo utilizado pelo alvo. O sistema pode ser desenvolvido em linguagem de programação *C++* com bibliotecas existentes na própria linguagem de programação e bibliotecas adicionais que implementam a aquisição, codificação, criptografia, armazenamento e transmissão. Há bibliotecas livres que implementam tais funções o que permite a implementação do sistema.

6.1. LIMITAÇÕES

A limitação do sistema consiste na infecção do dispositivo do alvo. Existem investigados que tem conhecimento técnico suficiente para saber que não devem acessar certos aplicativos, o que exigirá muita criatividade para desenvolver um sistema capaz de ludibriar o alvo, infectando seu dispositivo, podendo até não conseguir.

Nesse caso, uma possibilidade não descartada é ter acesso físico ao dispositivo, por exemplo com a entrada na casa ou local onde se encontra o dispositivo usado pelo alvo num momento em que não esteja presente, o que traz uma série de outros riscos, tais como o agente ser visto, haver sistema de vigilância, etc.

Pode haver situações em que todas as tentativas sugeridas nessa proposta falhem, mas dependendo da importância do alvo na investigação, justifica outras alternativas, como por exemplo um prêmio fictício oferecido ao alvo, sendo um equipamento que já seja entregue com os sistemas instalados.

6.2. TRABALHOS FUTUROS

O trabalho futuro desse, é o desenvolvimento do sistema com base nas especificações feitas nesse projeto e o teste de estratégias de infecções buscando obter áudio em comunicações *VoIP*, ou ainda simplesmente obter áudio do dispositivo, perfazendo assim uma escuta ambiental. Após a implementação será possível avaliar e validar a metodologia certamente após refinamentos contínuos.

REFERÊNCIAS BIBLIOGRÁFICAS

ANATEL, Ata da 71ª Reunião do Conselho Consultivo, Brasília, 2005. <http://www.anatel.gov.br/Portal/exibirPortalRedireciona.do?codigoDocumento=110189> Acesso em: 5 mai. 2012.

ANATEL, Sigilo das telecomunicações é responsabilidade das empresas, Brasília, 28 mar 2008. <http://www.anatel.gov.br/Portal/exibirPortalPaginaEspecialPesquisa.do?acao=&tipoConteudoHtml=1&codNoticia=15733> Acesso em: 5 mai. 2012.

ANATEL. Resolução nº 73, de 25 de novembro de 1998. Agência Nacional de Telecomunicações. Brasília, 1998 e seu anexo Regulamento dos Serviços de Telecomunicações. <http://www.anatel.gov.br/Portal/verificaDocumentos/documento.asp?numeroPublicacao=9435&assuntoPublicacao=Regulamento%20dos%20Servi%E7os%20de%20Telecomunica%E7%F5es%20(Anexo%20Resolu%E7%E3o%20n%BA%2073/1998)&caminhoRel=Cidadao-Biblioteca-Acervo%20Documental&filtro=1&documentoPath=biblioteca/regulamentos/regulamento_resolucao73_1998.pdf> Acesso em: 6 mai. 2012.

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

ANATEL. Missão, atribuições e características. Agência Nacional de Telecomunicações. <http://www.anatel.gov.br/Portal/exibirPortalInternet.do?acao=linkInt&src=http://www.anatel.gov.br/Portal/exibirPortalPaginaEspecial.do?acao=%26codItemCanal=801%26codigoVisao=8%26nomeVisao=Conhe%C3%A7a%20a%20Anatel%26nomeCanal=Sobre%20a%20Anatel%26nomeItemCanal=Miss%C3%A3o,%20atribui%C3%A7%C3%B5es%20e%20caracter%C3%ADsticas%26codigoVisao=8> Acesso em: 1 mai. 2012.

ANDRSS, Jason. Advanced Persistent Threat, ISSA Journal, 2011. <http://www.issa.org/images/upload/files/Andress-Advanced%20Persistent%20Threat.pdf> Acesso em: 20 abr. 2012.

ARRUDA, Felipe. Engenharia Social: o malware mais antigo do mundo, 2011. <http://www.tecmundo.com.br/8445-engenharia-social-o-malware-mais-antigo-do-mundo.htm#ixzz1uOJWlFfN> Acesso em: 9 mai. 2012

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.

BERSON, Tom. Skype Security Evaluation, Anagram Laboratories , 2005

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.

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.

BRASIL. Projeto de Lei nº 3.272, apresentado em 16 de abril de 2008. Congresso Nacional. Brasília. 2008.

BRASIL, Lei nº 9.034, de 3 de maio de 1995. Presidência da República. Brasília. 1995.

CAMPOS, Alessandro de Souza. A Convergência de Voz em Dados, 2007. TELECO. Seção: Tutoriais Telefonia Fixa – Telefonia. Disponivel em: <www.teleco.com.br/tutoriais/tutorialconvdados/Default.asp>. Acesso em: 11 abr. 2012.

CARMONA, Tadeu. Universo H4CK3R, 2ª Edição. São Paulo: Digerati Books, 2006. 128 p.

CIRIACO, Douglas. 20% dos brasileiros devem abandonar a telefonia fixa em 2012, Tecmundo, 2012. <http://www.tecmundo.com.br/telefonia/17887-20-dos-brasileiros-devem-abandonar-a-telefonia-fixa-em-2012-enquete-.htm#ixzz1sPlUDbsn> Acesso em: 18 abr. 2012.

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

CNJ. Sobre o CNJ, Brasília, 2004. <http://www.cnj.jus.br/sobre-o-cnj> Acesso em: 01 mai. 2012.

COLERIDGE, Robert. The Cryptography API, or How to Keep a Secret, MICROSOFT, 1996. <http://msdn.microsoft.com/en-us/library/ms867086.aspx> Acesso em: 11 jul. 2012.

CRYPTOSYS, Cryptography software tools for Visual Basic and C/C++/C# developers, 2011 <http://www.cryptosys.net/> Acesso em: 11 jul. 2012.

DELL, Quatro etapas para a segurança total, 2011. <http://content.dell.com/br/pt/empresa/d/sb360/sb-newsletter-6-2011-2.aspx?&ST= phishing &dgc=ST&cid=69631&lid=1765417> Acesso em: 9 mai. 2012.

DÍGITRO, s.d. Ensinare. Treinamento online Básico de Redes Convergentes. <http://moodle.digitro.com.br/cursos/redes_conv/topico1/html/t1l2.htm> Acesso em: 11 abr. 2012.

DUNM, *John.* Criminals using Skype, say Italian police. Techworld, publicado em 16/02/2009.<http://news.techworld.com/security/110902/criminals-using-skype-say-italian-police/> Acesso em: 21 abr. 2012.

FERNANDES FILHO, Dario Simões, AFONSO, Vitor Monte, MARTINS, Victor Furuse Martins, GRÉGIO, André Ricardo Abed, GEUS, Paulo Lício de, JINO, Mario, SANTOS, Rafael Duarte Coelho dos. Técnicas para Análise Dinâmica de Malware , Instituto de Computação, UNICAMP, Campinas, São Paulo, 2011. <http://www.las.ic.unicamp.br/~paulo/papers/2011-SBSEG-Minicurso-dario.fernandes-vitor.afonso-victor.martins-andre.gregio-mario.jino-rafael.santos.pdf> Acesso em: 13 mai. 2012.

GRINOVER, Ada Pellegrini Grinover, O regime brasileiro das interceptações telefônicas, Brasília, 1997, Revista CEJ - v. 1 n. 3, Biblioteca do Conselho da Justiça Federal, Periódicos – Artigo – Artigos on-line. <http://daleth.cjf.jus.br/revista/numero3/artigo16.htm> Acesso em: 27 abr. 2012.

GUERRA FILHO, Willis Santiago. O princípio constitucional da proporcionalidade. Revista do Tribunal Regional do Trabalho da 15ª Região, Campinas, n. 20, 2002. Disponível em: <http://trt15.gov.br/escola_da_magistratura/Rev20Art6.pdf>. Acesso em: 10 mai. 2012.

IBOPE. Número de brasileiros com acesso a internet chega a 79,9 milhões, 2012. <http://www.ibope.com.br/calandraWeb/servlet/CalandraRedirect?temp=6&proj=Portal IBOPE&pub=T&db=caldb&comp=pesquisa_leitura&nivel=null&docid=9725B59E0CD6FC43832579DC005A03D9> Acesso em: 17 abr. 2012

IDGNOW, Skype licencia gratuitamente codec Silk para áudio de alta qualidade, 2009. <http://idgnow.uol.com.br/mobilidade/2009/03/04/skype-licencia-gratuitamente-codec-silk-para-audio-de-alta-qualidade/> Acesso em: 10 jul. 2012.

ITAGIBA, Marcelo. Você está sendo grampeado? Revista Época, 20/06/2009. <http://revistaepoca.globo.com/Revista/Epoca/0,,EMI58781-15223,00.html> Acesso em: 19 abr. 2012.

JUCE, Raw Material Software, 2010. <http://www.rawmaterialsoftware.com/ juce.php> Acessado em 09 jul 2012.

KISTENMACHER, Deivid, VANDRESEN, Thaís, A Interceptação Telefônica e a Garantia Constitucional da Inadmissibilidade das Provas Ilícitas, 2009, Revista da Unifebe.

KUTWAK, André Bernardo. Análise da Codificação LPC para Sinais de Fala, 1999. <https://www.lps.ufrj.br/arquivos/0909090c772f.pdf> Acesso em: 01 jun. 2012.

LEITE, Leonardo Henrique de Melo. Interceptação Autorizada de Chamadas Telefônicas, 2006. TELECO. Seção: Tutoriais Telefonia Celular. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialinterceptacao/default.asp>. Acesso em: 17 abr. 2012.

MARCELO, Antônio, PEREIRA, Marcos Antônio de Azevedo. A Arte de Hackerar Pessoas, Rio de Janeiro, 2005.

MEDEIROS, Dênis Raphael Alves de Medeiros, LUZ, José Eduardo de Araújo, BATISTA, João, COSTA, Francielly Peixoto, BRITO, Maykon Alves de, PIO, Ricardo Divino, Estudo de constitucionalidade da lei 9296/96, Artigonal, 2011. <http://www.artigonal.com/direito-artigos/estudo-de-constitucionalidade-da-lei-929696-4354859.html> Acesso em 22 abr. 2012.

MICROSOFT, O que é um Driver Assinado? <http://windows.microsoft.com/pt-BR/windows-vista/What-is-a-signed-driver> Acesso em: 15 mai. 2012.

MICROSOFT, What's New in DirectSound <http://msdn.microsoft.com/en-us/library/windows/desktop/ee419022%28v=vs.85%29.aspx> Acesso em: 31 mai 2012.

MICROSOFT. The Power of DirectSound. <http://msdn.microsoft.com/en-us/library/windows/desktop/ee418868%28v=vs.85%29.aspx> Acesso em: 31 mai 2012.

MIYANO NETO, Roberto . A Evolução dos Mecanismos de Segurança para Redes sem fio 802.11 , 2004.<http://www-di.inf.puc-rio.br/~endler/courses/Mobile/Monografias/04/Miyano -Mono.pdf> Acesso em: 01 jun 2012.

MOLLMAN, Tatiane, COLL, Maciel, A interceptação telefônica como meio de obtenção de provas e a (in)validade da prova obtida fortuitamente, Joaçaba, 2011 <http://editora.unoesc.edu.br/index.php/acsa/article/view/587/pdf_156> Acesso em: 20 mar 2012.

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.

MORENO, João Brunelli. Microsoft quer levar Skype para a web, iMasters, 2012. <http://imasters.com.br/noticia/24176/desenvolvimento/microsoft-quer-levar-skype-para-a-web> Acesso em: 18 abr. 2012.

OLIVIO, Cleber Kiel. Avaliação de características para detecção de phishing de e-mail. Curitiba, 2010, xi. 65. <http://www.inf.ufpr.br/lesoliveira/download/Cleber OlivoMSC.pdf> Acesso em: 08 mai 2012.

OPENAL, OpenAL® and Windows Vista, 2008 <http://connect.creativelabs.com/openal /OpenAL%20Wiki/OpenAL%C2%AE%20and %20Windows%20Vista%E2%84%A2.aspx> Acesso em: 31 mai 2012.

OPENAL, Welcome. <http://connect.creativelabs.com/openal/default.aspx> Acesso em: 09 jul 2012.

OPENAL, Platforms, 2008 <http://connect.creativelabs.com/openal/OpenAL %20Wiki/Platforms.aspx> Acesso em: 09 jul 2012.

PENTEADO, Luiz Fernando Wowk, 2011. TRF4, ACR 0014752-96.2008.404.7000, Oitava Turma, Relator, D.E. 14/04/2011

PERON, A.; DEUS, F. E. G. D.; SOUSA JUNIOR, R. T. D. Ferramentas e Metodologia para Simplificar Investigações Criminais Utilizando Interceptação Telemática, Florianópolis, 05 out 2011, IcoFCS 2011. p 30. ISBN 978-85-65069-07-6 - Online ISBN 978-85-65069-05-2, pp 30-42 DOI: 10.5769/C2011003 e http://dx.doi.org/10.5769/C2011003.

PESSOA, Leonardo Ribeiro. Os Princípios da Proporcionalidade e da Razoabilidade na Jurisprudência Tributária Norte-Americana e Brasileira, 2006. <http://sisnet.aduaneiras.com.br/lex/doutrinas/arquivos/norte.pdf> Acesso em: 10 mai 2012.

PORTAUDIO, s.d. <http://www.portaudio.com/apps.html> Acessado em 09 jul 2012.

REZENDE, Pedro Antonio Dourado de. Combatendo os Trojans, Troianos e similares, Brasília, 2007. <http://www.cic.unb.br/~pedro/trabs/entrevistaCB2.html> Acesso em: 08 mai 2012.

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.

SCHIAVONI, Flávio. APIs para desenvolvimento de software com áudio, 2012 <http://flavioschiavoni.blogspot.com.br/2012/01/apis-para-desenvolvimento-de-software> Acesso em: 09 jul 2012.

SECVOICE Proteção contra escuta telefônica <http://cms.secvoice.com.br/cms/pt/index.php?page=secvoice-3g-para-windows> Acesso em: 17 abr. 2012

SECURSTAR <http://www.securstar.com/products_phonecrypt.php#volta3> Acesso em: 17 abr. 2012

SILVA, Cleber Demetrio Oliveira da. Fundamentos jurídicos e tecnológicos do comércio eletrônico no Brasil. Jus Navigandi, Teresina, ano 11, n. 1190, 4 out. 2006 . Disponível em: <http://jus.com.br/revista/texto/9002>. Acesso em: 19 abr. 2012.

SILVA, Gleydson Mazioli da. Guia Foca GNU/Linux Versão 6.10, 2002 <http://www.mtm.ufsc.br/~krukoski/pub/linux/focalinux3/ch-d-cripto.htm> Acesso em: 17 abr. 2012.

SINGHAL, Nidhi, RAINA, J.P.S. Comparative Analysis of AES and RC4 Algorithms for Better Utilization , Índia, 2011. International Journal of Computer Trends and Technology. <http://www.ijcttjournal.org/volume-1/Issue-3/IJCTT-V1I3P107.pdf> Acesso em: 01 jun 2012.

SIQUEIRA FILHO, Élio Wanderley de. Escuta telefônica: comentários à Lei 9.296/96. Revista do Instituto de Pesquisas e Estudos, Bauru, n. 18, p. 333-349, ago./nov. 1997. <http://bdjur.stj.gov.br/xmlui/handle/2011/20379> Acesso em: 28 abr. 2012.

TELEBRASIL. Brasil fecha trimestre com 68 milhões de acessos em banda larga TELEBRASIL Online, 2012. Disponivel em: <http://www.telebrasil.org.br/artigos/artigos.asp>. Acesso em: 01 mai. 2012.

TELECO. Seção: Tutoriais VoIP. FILHO, Huber Bernal. Telefonia IP, 2008. Disponivel em: <http://www.teleco.com.br/tutoriais/tutorialtelip/default.asp>. Acesso em: 14 abr. 2012.

ULBRICH, Henrique Cesar. Universidade Hacker, 5ª edição, Universo dos Livros Editora LTDA, 2004. p.348.

VIEIRA, Tina, AZEVEDO, Solange. Você está sendo grampeado? Revista Época, 20/06/2009. <http://revistaepoca.globo.com/Revista/Epoca/0,,EMI58781-15223,00.html> Acesso em: 19 abr. 2012.

WEBRTC, iLBC Freeware. <http://www.webrtc.org/ilbc-freeware> Acessado em 10 jul 2012.

ZORZ, Zeljka. Downloads Drive-by Oferecidos com Malware para Usuários Android, Net-security, 2012. <http://www.net-security.org/malware_news.php?id=2095> Acesso em: 15 mai 2012.