DOI: 10.5769/C2015015 or http://dx.doi.org/10.5769/C2015015

Perícia Computacional em Artefatos Digitais de Interceptações Telefônicas

Wilson Leite da Silva Filho

***Resumo*—Este artigo apresenta o trabalho pericial realizado em três casos de interceptações telefônicas. São discutidos os aspectos operacionais e técnicos das interceptações telefônicas automatizadas pelos Sistemas Vigia e Guardião. Esses sistemas geram uma grande quantidade de artefatos digitais, que foram questionados quanto a sua integridade e integralidade. A defesa também trouxe à discussão o princípio da igualdade de armas, alegando que não possui os mesmos recursos de análise que a parte acusatória. Desses questionamentos, que envolvem uma grande quantidade de dados, surgiu a necessidade de desenvolvimento de um software pericial específico para atender a essas demandas. Tal software foi utilizado nas três perícias e está pronto para ser usado e/ou adaptado para outros casos semelhantes que demandem os mesmos tipos de análise nos artefatos digitais produzidos pelos sistemas de interceptação telefônica.**

Palavras-Chave*—*Interceptações telefônicas, Sistema Guardião, Sistema Vigia, Software Pericial.

***Abstract*—This article presents the forensics work done in three cases involving phone calls interceptions. It´s discussed the operational and technical aspects of the interception, done by the Vigia and Guardiao systems. These systems produce a huge amount of digital artifacts that has been questioned regarding their integrity and integrality. The defense also discuss the principle of weapons parity, claiming that they don´t have the same analysis resources that the accusatory part. From these questionings, involving a great amount of data, comes the necessity to develop a forensics software specially designed for this task. This software was used in the three cases and is available to be used or adapted for other cases where there is similar digital artifacts generated by phone call interception systems.**

Keywords— Phone Calls Interceptions, Guardião System, Vigia System, Forensic Expert Software.

I. INTRODUÇÃO

A interceptação de comunicação telefônica é uma operação que se constitui na interferência de um terceiro na captação de uma comunicação entre duas ou mais pessoas, sem o conhecimento dos interlocutores. É a modalidade específica de interceptação legal realizada por órgãos policiais na investigação criminal, com autorização judicial e de acordo com os dispositivos legais das leis 9.296/96 e 10.217/01, devendo ser conduzida por autoridade policial a quem cabe a responsabilidade das operações técnicas, a integridade da prova colhida e a análise de seu conteúdo [1].

Os processos de interceptações são realizados por procedimentos amplamente apoiados por sistemas de informação automatizados, que fornecem aos órgãos de persecução criminal ferramentas para a gravação, análise e geração de relatórios com os resultados das interceptações. Os áudios e os relatórios resultantes das operações são adicionados aos processos criminais e seguem para análise das partes interessadas.

Ao serem anexados aos autos, a defesa tem acesso ao conjunto de provas geradas nas interceptações telefônicas. Esse conjunto é formado por artefatos digitais, tais como arquivos de áudio e registros que relacionam alvos interceptados, datas e horas das chamadas. Foi dos questionamentos sobre a integridade das provas geradas pelos sistemas de interceptação que surgiu a necessidade da perícia computacional abordada nesse artigo.

II. OBJETIVO

O objetivo principal do trabalho é apresentar os procedimentos que foram realizados nas análises de três casos de perícia em artefatos digitais de interceptações telefônicas.

Serão discutidas as dificuldades encontradas devido à necessidade de análise da grande quantidade de dados oriundos de fontes diversas. Será apresentado um software desenvolvido pelo autor, específico para esse tipo de perícia.

Por fim, serão apresentados os resultados dos processamentos dos dados realizados pelo software desenvolvido.

III. SISTEMAS DE INTERCEPTAÇÃO TELEFÔNICA

Dois sistemas que são comumente utilizados nos Estados e na União para a automatização e viabilização das interceptações telefônicas são os Sistemas Vigia, da empresa Suntech, e o sistema Guardião, da empresa Digitro.

Segundo a Suntech, o Sistema Vigia é uma solução completa para gerenciar todo o processo de interceptação legal e retenção de dados para qualquer serviço ou subsistema de comunicação de qualquer tecnologia ou fornecedor [2]. No contexto das interceptações telefônicas analisadas nas perícias, o Sistema Vigia foi utilizado pelas operadoras de telefonia para programar as centrais telefônicas e realizar os desvios dos telefones alvos das interceptações.

Segundo a Digitro, o Sistema Guardião realiza monitoração de voz e dados e oferece recursos avançados de análise de áudio e identificação de locutores. É uma solução feita

especialmente para as operações de investigação legal [3]. No contexto das interceptações telefônicas analisadas, o Guardião foi usado para receber as ligações telefônicas desviadas pelas operadoras. Era, portanto, o sistema instalado no Órgão Policial com as funções de realizar a coleta de áudio e gerar os relatórios resultantes das interceptações.

Cabe salientar que neste trabalho foram analisadas apenas as características dos sistemas relacionadas às perícias em questão e a forma de utilização que os sistemas foram submetidos para a geração dos dados. Não é objetivo do trabalho qualquer forma de auditoria ou análise crítica sobre os recursos e capacidades que cada sistema oferece.

A. Processo de Interceptação Telefônica

O processo de interceptação telefônica realizado pelo Órgão Policial por meio do Sistema Guardião segue várias etapas que envolvem o Poder Judiciário, o Ministério Público, os membros das forças de segurança pública e as operadoras de telefonia móvel e fixa.

A primeira etapa do processo é a solicitação ao Poder Judiciário de autorização para realizar interceptação telefônica. A Autoridade Policial prepara um documento com tal solicitação, elencando quais os números de telefones que precisam ser interceptados e as respectivas operadoras às quais eles pertencem.

Após receber a autorização judicial, é feita a programação do Sistema Guardião, por um técnico operador do sistema. Nesta configuração, é estabelecido um canal de desvio (canais DDR – PABX) para cada número de telefone a ser monitorado. Nesse momento, o Sistema Guardião está pronto para registrar passivamente os áudios desviados pela operadora por meio do Sistema Vigia.

Na etapa seguinte, envia-se uma solicitação juntamente com o mandado judicial para a operadora de telefonia. Nela, são informados quais telefones deverão ser interceptados e em quais canais de desvio os respectivos áudios deverão ser enviados. Geralmente, é dado um prazo judicial de 24 horas para que a operadora configure os desvios de canal.

Somente a partir daí o Guardião passa a receber as interceptações. Durante as gravações, as conversas podem ser acompanhadas em tempo real pelas equipes de investigação.

Expirado o prazo da interceptação solicitada, a operadora encerra o desvio dos números alvos para as linhas monitoradas pelo Sistema Guardião.

A figura 1 apresenta os agentes envolvidos nos procedimentos de interceptação descritos anteriormente.

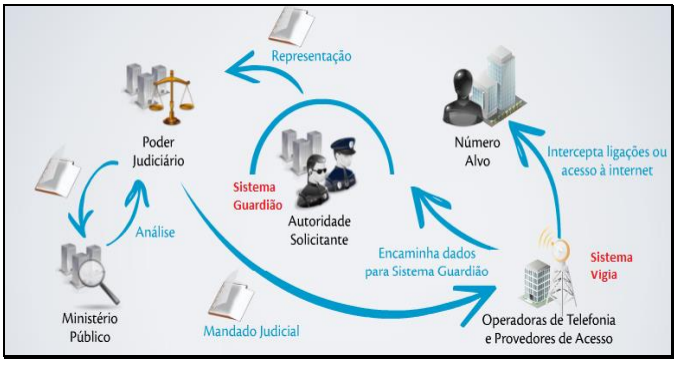

Figura 1 – Agentes envolvidos nas interceptações telefônicas (compilação do passo a passo disponível no site do Guardião [3])

IV. DOS QUESTIONAMENTOS DA DEFESA

As principais indagações feitas pela defesa, por meio de seus assistentes técnicos, e aceitas pelos Juízes, correspondem aos seguintes quesitos: a) se o conjunto dos artefatos digitais anexados aos autos correspondem à completude das interceptações telefônicas; b) se os registros e áudios estão íntegros, ou seja, não foram apagados ou editados; c) se há algum registro de interceptação que esteja fora da data de autorização judicial; d) que seja feito um cotejamento entre os registros do Sistema Vigia, usado pelas operadoras de telefonia, e os registros do Sistema Guardião, usado pelo Órgão Policial.

A defesa também questiona, baseada no princípio da paridade de armas, o direito de ter as mesmas condições de análise que a parte acusatória. Tal princípio, segundo Ferrajoli, diz que para que a disputa se desenvolva lealmente e com paridade de armas, é necessária a perfeita igualdade entre as partes: em primeiro lugar, que a defesa seja dotada das mesmas capacidades e dos mesmos poderes da acusação; em segundo lugar, que o seu papel contraditor seja admitido em todo estado e grau do procedimento e em relação a cada ato probatório singular, das averiguações judiciárias e das perícias ao interrogatório do imputado, dos reconhecimentos aos testemunhos e às acareações [4].

A defesa argumenta que a parte acusatória possui acesso total ao Sistema Guardião, que possibilita várias ferramentas para a análise dos dados. À defesa restariam apenas os registros digitais das interceptações, gravados em mídia ótica e acessados por um leitor específico. Não haveria ferramentas para fazer um cruzamento dos dados. Dessa necessidade, os defensores formularam mais um quesito: e) que os dados sejam importados para algum Sistema de Banco de Dados para que possam ser analisados, ou que, não sendo possível a importação, que se aponte no laudo as dificuldades do cruzamento da grande quantidade de dados provenientes das interceptações telefônicas.

Por fim, para dirimir eventuais dúvidas em relação à prova, a Autoridade Judicial determinou que os peritos extraíssem na íntegra e com verificação de integridade todos os registros referentes às interceptações telefônicas.

V. OS PROCEDIMENTOS PERICIAIS

Durante o processo de interceptação, os dados desviados pela operadora para o Sistema Guardião foram armazenados em disco rígido. Ao fim da operação policial, esses dados foram gravados em mídias óticas e as mídias anexadas aos autos correspondentes. O volume de dados gerado por uma operação de interceptação telefônica, que geralmente envolve vários alvos, por períodos de meses ou até anos é muito grande. Um dos casos envolveu aproximadamente 7.000 horas de áudio, volume que precisou ser gravado em 18 DVDs, ou seja, cerca de 80GB.

Devido à capacidade de armazenamento limitada do Sistema Guardião que foi periciado e ao número de operações de interceptação telefônicas simultâneas em andamento, não era possível manter por muito tempo os dados de uma operação de interceptação, ou faltaria espaço para operações subsequentes. Em razão disso, os discos rígidos do Sistema foram usados de forma rotativa, ou seja, os áudios de interceptações de operações já finalizadas eram apagados para liberar espaço para novas interceptações.

Cumpre frisar que as informações gravadas pelo Sistema Guardião correspondem a registros de dados em que constam, por exemplo, o número de telefone alvo e o período de interceptação, e arquivos de áudio associados a cada um desses registros. No processo de liberação de espaço de forma rotativa para novas operações, apenas os arquivos de áudio são sobrescritos. Já os registros de dados permanecem no Sistema indefinidamente. No início das análises periciais, o processo de liberação rotativa de espaço já tinha atingido as operações foco da perícia. Dentro do Sistema Guardião existiam, portanto, apenas os registros de dados da operação, sem os áudios correspondentes.

Os arquivos de áudio, além de anexados aos autos em mídias óticas, haviam sido também guardados em disco rígido externo ao Sistema Guardião. Esses arquivos são armazenados com criptografia, e somente podem ser lidos pelo Guardião Reader. Esse software, além de reproduzir o áudio das interceptações, é capaz de verificar sua integridade por meio de algoritmo proprietário, que atesta unicamente a ocorrência ou não de adulteração nos arquivos, e não que eles correspondem à totalidade das gravações coletadas durante o período de interceptação.

Desse cenário, constata-se a existência de dois conjuntos de informações, armazenadas em locais distintos. Para que se cumpra o requisitado pela Autoridade Judicial é necessário que se integre estes dois conjuntos de dados, formando um todo válido. O primeiro conjunto de informações são os arquivos de áudio, armazenados no disco rígido externo. Este conjunto de áudio é tecnicamente íntegro, ou seja, os áudios que ali estão não foram adulterados, conforme atestado pelo algoritmo de verificação de integridade. O segundo conjunto de informações são os registros de dados (sem os áudios) relativos a toda operação, que está armazenado dentro do Sistema Guardião. Para determinar se os áudios do disco rígido externo e dos DVDs correspondem aos áudios da operação de interceptação, deve-se relacionar esses arquivos de áudio com os registros de dados presentes dentro do Sistema Guardião.

Tais registros de dados armazenados no Guardião, correspondentes às três interceptações telefônicas periciadas, compreendem aproximadamente 600.000 linhas de informação organizadas em aproximadamente 12.000 páginas de relatório. Como pode-se notar, o processo de comparação de dados é custoso e exige um esforço que só pode ser realizado em tempo razoável com o auxilio de recursos computacionais. Desta forma, desenvolveu-se um software específico para esta tarefa. Em linhas gerais, o software deve ler o relatório emitido pelo Sistema Guardião na presença do perito, e interpretar cada linha deste relatório, extraindo informações que serão usadas para procurar o arquivo correspondente nas mídias anexas aos autos e no disco rígido de *backup*. O sucesso desta comparação é similar ao processo de extração dos áudios de dentro do Sistema Guardião, caso eles ainda estivessem lá. Os módulos e o fluxo dos dados envolvidos nessa operação estão demonstrados nos diagramas das figuras 2, 3 e 4.

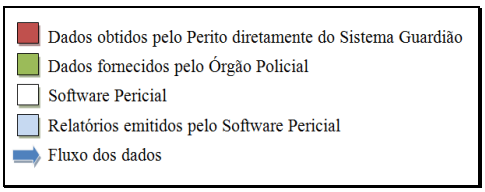

Figura 2 – Legenda dos fluxogramas

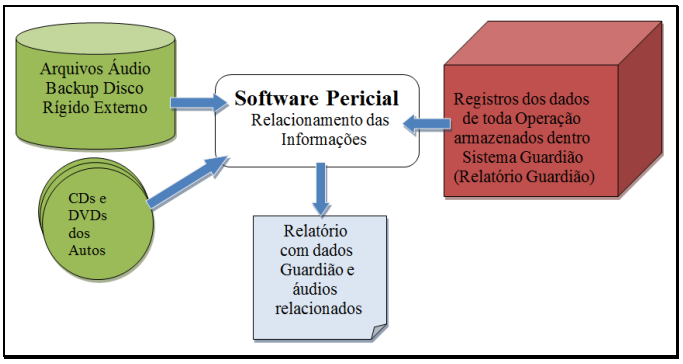

Figura 3 – Fluxograma do software pericial

Com esse módulo do software foi possível responder aos quesitos: a) se o conjunto dos artefatos digitais anexados aos autos correspondem a completude das interceptações telefônicas; b) se os registros e áudios estão íntegros, ou seja, não foram apagados ou editados.

O próximo quesito a ser respondido foi: c) se há algum registro de interceptação que esteja fora da data de autorização judicial. Para isso foi desenvolvido um módulo que verifica os prazos judiciais autorizados e compara com cada registro, dizendo se a interceptação correspondente está ou não autorizada.

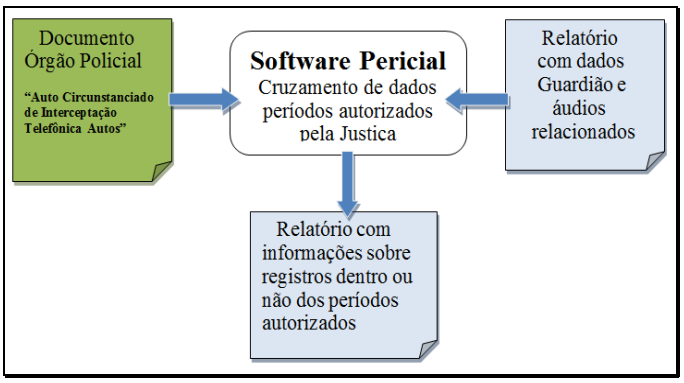

Figura 4 – Fluxograma do software pericial

O próximo quesito a ser respondido, refere-se ao cotejamento dos dados do Sistema Vigia com os dados do Sistema Guardião. Há ressalvas importantes a serem feitas sobre essa tarefa. Os dois sistemas são independentes, foram projetados de formas distintas. Nem todos os eventos de um sistema estão diretamente relacionados com os do outro. Além disso, há diferença de horário em que as chamadas começam a ser registradas e possíveis diferenças de ajuste do relógio dos módulos relacionados ao Sistema Vigia. Por exemplo, o Sistema Vigia registra o início do horário de uma chamada no momento em que a chamada é atendida. Já o Sistema Guardião registra a chamada logo ao término da discagem do número. Outro exemplo que geraria discrepâncias é que os relógios das

centrais telefônicas das operadoras podem não estar precisamente sincronizados com o horário oficial de Brasília. Os relógios podem estar atrasados ou adiantados em relação a ele, ou ainda, em desacordo quanto ao horário de verão. Essa falta de sincronismo causa diferenças nos registros das chamadas entre os Sistemas Vigia e Guardião.

Dessa forma, esse módulo do software deve realizar um trabalho de aproximação entre as datas e horários para tentar relacionar os registros compatíveis entre os dois sistemas e apresentar esses resultados. Em caso de dúvidas não resolvidas pelo algoritmo do software, uma análise pontual deverá ser feita em cada caso de interesse. Em uma das perícias realizadas, do total de aproximadamente 270.000 registros, 180.000 foram relacionados. Nos 90.000 registros restantes, o relacionamento automático não logrou êxito.

O último quesito a ser respondido baseia-se no princípio da paridade de armas, no qual a defesa pede: e) que os dados sejam importados para algum Sistema de Banco de Dados para que possam ser analisados.

Durante todo o processamento, o software pericial fez uso de Banco de Dados Relacional e arquivos de relatório. Foram criadas tabelas que modelam os registros que estão sendo questionados. Essas tabelas podem ser exportadas para que a defesa possa realizar as consultas que achar necessárias.

O modelo relacional das tabelas que modelam os registros envolvidos nas interceptações telefônicas está ilustrado na figura 5.

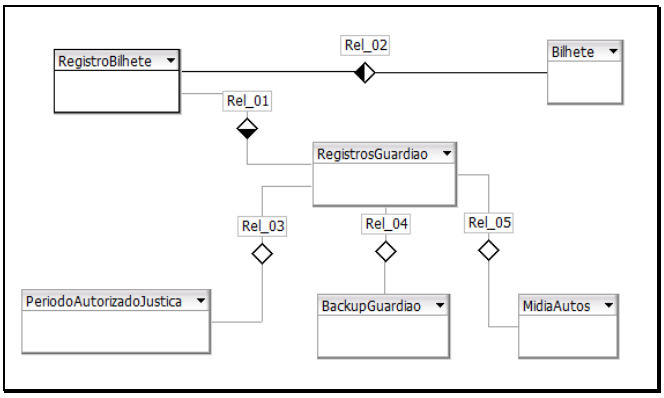

Figura 5 – Modelo relacional dos dados das interceptações

VI. CARACTERÍSTICAS TÉCNICAS DO SOFTWARE PERICIAL

O software pericial citado no artigo foi desenvolvido em Java. Para acesso ao sistema de arquivo e para a listagem e procura de arquivos em discos e mídias óticas optou-se por fazer chamadas aos comandos de busca em disco do sistema operacional Linux. Tal decisão foi baseada no contato prévio que o autor tinha com esses comandos (*locate* e *updatedb)* e em sua confiabilidade. Para realizar as chamadas foi usado o método *exec* do ambiente Java.

Para as análises dos arquivos texto e relatórios fornecidos pelos Sistemas Guardião e Vigia foram desenvolvidos interpretadores dos relatórios. Para o relatório principal do Sistema Guardião foi especificado uma gramática formal, usando-se EBNF[5], e criado um interpretador dessa gramática. EBNF é um código que expressa a gramática de uma língua formal. Uma gramática definida em EBNF consiste em símbolos terminais e regras de produção não-terminais. Restrições relativas, como símbolos terminais, podem ser combinados em uma sequência válida. Exemplos de símbolos terminais incluem caracteres alfanuméricos, sinais de pontuação e caracteres de espaço em branco. EBNF é utilizado na definição de linguagens formais e pode estar envolvida no processo de construção de interpretadores e compiladores [5].

Para as pesquisas e manejo dos dados foi usado o banco de dados relacional. Incialmente, as primeiras versões do software utilizavam arquivos texto e pesquisas diretas em objetos instanciados na memória por meio da linguagem Java. Essa abordagem, entretanto, se mostrou lenta no processamento de uma grande quantidade de dados. Na versão atual, as estruturas de dados alojadas anteriormente em memória e salvas em arquivos texto foram modeladas para tabelas em banco de dados. Foi alcançado um ganho considerável de desempenho com essa abordagem, além de possibilitar recursos mais sofisticados de pesquisa sobre os dados processados. O banco de dados escolhido foi o PostgresSQL [6], acessado via JDBC [7].

A interface do software é toda em linha de comando. É possível usar alguns parâmetros de entrada para escolher determinadas funções. Algumas configurações também podem ser feitas em arquivos texto.

Porém, os recursos foram sendo acrescentados conforme demanda específica. Para se utilizar o software de forma genérica, ainda é necessário um esforço para tornar a interface mais amigável e principalmente para melhorar a documentação, que atualmente se restringe a comentários nos códigos fonte.

VII. CONCLUSÕES

O processo de interceptação de ligações telefônicas é amplamente utilizado pelos Órgãos Policiais em suas investigações. A integridade e confiabilidade das provas geradas pelos sistemas de interceptações telefônicas foram questionadas em três casos distintos. Além desses questionamentos, a defesa argumenta que não possui paridade de armas em relação aos órgãos acusatórios. Este questionamento levou à necessidade de perícia em um ambiente com grande quantidade de dados, que só foi viabilizada com o desenvolvimento de um software específico para este fim. Com o auxílio desse software foi possível responder aos quesitos formulados pelos Juízes e pela defesa, bem como fornecer à defesa dados estruturados para que ela pudesse fazer suas próprias análises.

O software pericial foi utilizado em três perícias distintas e está pronto para ser usado e/ou adaptado para outros casos semelhantes que demandem os mesmos tipos de análise nos artefatos digitais produzidos pelos sistemas de interceptação telefônica.

O cotejamento entre os registros dos dois sistemas envolvidos nas interceptações apresentou dificuldades técnicas devido a diferenças entre seus dados. Foi utilizado um algoritmo que tenta relacioná-los por aproximação. Essa tarefa logrou um sucesso parcial. Como trabalho futuro, haveria espaço para se estudar mais detalhadamente essa relação e com isso propor um aprimoramento desse algoritmo.

REFERÊNCIAS

[1] Ferro Junior, Celso Moreira; Oliveira Filho, Edemundo Dias de; Preto, Hugo César Fraga; "Segurança Pública Inteligente (Sistematização da Doutrina e das Técnicas da Atividade); Editora Kelps: Goiânia, 2008.

[2] Vigia. http://www.suntech.com.br/pt/solucoes/lawful-interception/vigia/, acessado em 18 de abril de 2015.

[3] Guardião. http://www.digitro.com/pt/index.php/component/content/article/89Itemid=1, acessado em 18 de abril de 2015.

[4] Ferrajoli, Luigi. Direito e razão: teoria do garantismo penal. 2. ed. São Paulo: Revista dos Tribunais, 2006, p. 565

[5] Watt, David A.; Brown, Deryck F. Programming Language Processors in Java – Compilers and Interpreters, Prentice Hall, Great Britain: 2000

[6] PostgresSQL. http://www.postgresql.org/, acessado em 12 de junho de 2015.

[7] Silberschatz, Abraham, Korth , Henry F. e Sudarshan, S. - Sistema de Banco de Dados – Tradução da 5ª edição; Editora Elsevier: Rio de Janeiro, 2006.

Wilson Leite da Silva Filho, Perito Criminal - Instituto Geral de Perícias de Santa Catarina; Mestre em Engenharia de Computação - IPT/USP; Especialista em Segurança da Informação – ITA; Graduando em Psicologia – UFSC.