ISSN 2447-1097

Direito & TI–Porto Alegre / RS www.direitoeti.com.br

APLICAÇÃO DE MODERNAS TÉCNICAS DE INVESTIGAÇÃO DIGITAL PELA POLÍCIA JUDICIÁRIA E SUA EFETIVIDADE

Guilherme Caselli[1]
Alesandro Gonçalves Barreto[2]
Andressa Gaudencio[3]

RESUMO

Frente ao aperfeiçoamento das metodologias empregadas pelos criminosos que veem no cenário virtual um nicho de atuação e a frequente perspectiva de impunidade, objetiva-se, através deste artigo, apresentar ferramentas alternativas para avanços investigativos, trazendo resultado eficaz e oportuno. Como metodologia, utilizou-se o estudo de casos de crimes de extorsão investigados pela Polícia Civil do Estado do Rio de Janeiro, no ano de 2015, cujo meio de execução deu-se pela aplicação *Skype*. Nos casos analisados, foram utilizadas três ferramentas: a primeira trata-se de uma solução específica de análise de tráfego de rede; a segunda, via prompt de comando; e a terceira, uma técnica utilizada por servidores de website para coleta de informações. Todas se apresentaram eficientes para a resolução dos crimes investigados, atingindo, conclusivamente, o objetivo proposto.

Palavras-chave: Crimes Cibernéticos. Investigação Digital. Polícia Judiciária. *Skype*.

INTRODUÇÃO

O uso da internet tem crescido exponencialmente nos últimos anos. Como consequência imediata, os criminosos têm utilizado ferramentas acessíveis na Internet para potencializar suas ações. Antes, a extorsão era utilizada via telefone, período em que as informações disponíveis para cometer o delito eram inexpressivas. Hoje, potenciais vítimas disponibilizam seus hábitos e ciclo de amigos em redes sociais, facilitando o levantamento de informações por parte dos criminosos e, via de conseqüência, a prática da infração, principalmente delitos de extorsão.

É cediço que, ao utilizar a Internet para facilitar a prática de um delito, o malfeitor tenta, a todo custo, furtar-se à ação policial. Para isso, utiliza-se de várias ferramentas, desde aplicativos de troca de mensagens até serviços de telefonia que usam tecnologia VOIP – voz sobre IP. Essa última

[1] Policial Civil do Estado do Rio de Janeiro –DRCI/RJ. caselli.guilherme@gmail.com
[2] Delegado de Polícia Civil do Estado do Piauí e co-autor do livro Inteligência Digital da Editora Brasport. delbarreto@gmail.com.
[3] Mestra, Pesquisadora e Especialista em Gestão. andressagaumor@gmail.com

tem trazido muitos benefícios, dentre os quais a redução dos custos de telefonia e a flexibilidade das chamadas. De outro lado, os criminosos utilizam-na para potencializar suas condutas.

O sistema normativo jurídico brasileiro impõe aos prestadores de serviços de internet, que executam suas atividades em solo pátrio, o dever de fornecimento de dados e informações quando determinado por uma Autoridade Judiciária Brasileira, entrementes, os grandes servidores alegam que não são submissos às leis locais e sim à lei de seus países de origem[i] [ii], disponibilizando como único meio de cooperação o tratado de assistência mútua MLAT – *Mutual Legal Assistance Treaty*[iii] – constando como partes o Brasil e Estados Unidos.

Surge, então, um problema a ser enfrentado: a morosidade e burocracia dos meios investigativos tradicionalmente acessíveis pelas autoridades públicas, frente à urgência que muitas investigações na rotina de polícia judiciária impõem. Tendo em vista os aspectos observados, torna-se necessária a reflexão sobre utilização de meios alternativos, específicos sob o ponto de vista da tecnologia da informação, eficientes e ágeis, capazes de identificar um usuário do serviço *Skype*.

Sendo assim, o objetivo deste artigo é apresentar ferramentas alternativas para avanços investigativos, trazendo resultados eficazes e oportunos frente aos delitos cuja execução se dê no cenário virtual. Não se pretende substituir ou questionar a eficácia do MLAT, mas sim a sua efetividade frente à urgência da atuação policial em persecuções penais onde a atividade criminosa se encontra em execução e seus desdobramentos, caso ocorram, tornem-se irreparáveis.

1. MARCO CIVIL DA INTERNET E EFETIVIDADE DAS DECISÕES JUDICIAIS

O Marco Civil da Internet[iv] estabelece que, em qualquer operação de coleta, armazenamento, guarda ou tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e aplicações de internet, em que pelo menos um desses atos ocorra em território nacional, deve haver o respeito à legislação pátria. Nos casos de a empresa ser sediada no exterior, nossa legislação deve ser obedecida desde que haja prestação de serviço ao público brasileiro ou possua representante do mesmo grupo econômico no Brasil[v].

Este mesmo diploma legal[vi] determina o prazo de 01 (um) ano para a guarda dos registros de conexão e 06 (seis) meses para os registros de acesso à aplicações de internet, possibilitando à autoridade policial ou administrativa e ao Ministério Público o requerimento cautelar para a guarda

desses registros até por prazo superior. Após essa solicitação, há o prazo de 60 (sessenta) dias para envio da respectiva ordem judicial determinando o fornecimento desse conteúdo armazenado.

É certo que os grandes grupos econômicos da Internet têm sede nos Estados Unidos e para responder as solicitações judiciais ou requisições por autoridade policial utilizam-se de legislação americana[vii]. De acordo com a respectiva Lei Federal, há a seguinte distinção:

a) Intimação: permite o fornecimento de dados básicos do assinante, podendo incluir nome, duração do serviço, endereço de e-mail vinculado à conta, informações de cartão de crédito e, caso disponível, endereço de IP da última conexão. São informações prestadas diretamente à polícia, existindo apenas a necessidade de investigação policial em andamento.
b) Ordem Judicial: para o fornecimento de outros dados relacionados à conta de determinado usuário, excluindo-se o conteúdo das comunicações, há necessidade de que o juiz expeça um mandado determinando seu fornecimento;
c) Mandado de Busca: é exigido para os casos em que se exige o fornecimento do conteúdo das comunicações.

No caso da intimação, as aplicações de internet têm informado esses dados básicos do assinante através de ofício requisitório expedido por autoridade policial. Para os demais casos, requerem a expedição de ordem judicial, excetuando-se os casos que envolvem fornecimento de conteúdo. Nessa última condição, mesmo a decisão sendo exarada por juiz brasileiro, algumas aplicações têm negado seu cumprimento, alegando que tal solicitação deve ser feita através de cooperação jurídica internacional.

Essa cooperação jurídica internacional é um caminho, entretanto, não é o único[viii]. A jurisprudência pátria tem reiterado decisões nesse sentido, preconizando que a investigação é pautada pelos princípios da oportunidade e celeridade. Ao adotar a via da assistência mútua internacional, em que pese o esforço do governo brasileiro ao tentar encurtar o tempo de resposta via cooperação, o lapso dilatado para que a polícia acessasse esses dados tornaria, na maioria dos casos, inúteis as informações extemporâneas transmitidas.

As empresas não podem se negar a prestar informações sob o pretexto de que não possuem acesso a conteúdo armazenado em outro país. Não há como condicionar o cumprimento de uma decisão judicial à localização do servidor, sob pena do Brasil se tornar um paraíso cibernético, onde os entes abstratos aqui se instalam e só arcam com bônus. A persistir um cenário desses, as aplicações de internet irão situar seus servidores em locais em que não haja nenhum tratado de

cooperação para furtar-se à aplicação da lei. O local físico do servidor da empresa não pode ser regra de delimitação de competência.

2. EXTORSÃO COMETIDA ATRAVÉS DE SERVIÇO VOIP

Dentre as várias modalidades de extorsão virtual relatadas no cenário policial, a apontada com maior incidência é a exercida através de chats e serviços VOIP da ferramenta *Skype*. Por *modus operandi*, os criminosos procuram como vítimas mulheres jovens e com características físicas atrativas, aplicando-lhes uma farta engenharia social a fim de que a empreitada criminosa seja bem-sucedida, fazendo-as, por exemplo, acreditar que serão contratadas para prestação de um serviço qualquer. Em alguns casos, identificam-se como produtores de emissoras de televisão, ofertando vagas de atriz.

Este foi o cenário encontrado pela Delegacia de Repressão aos Crimes de Informática da Polícia Civil do Estado do Rio de Janeiro (RJ), no ano de 2015, ao investigar 03 (três) casos de vítimas do sexo feminino com idades entre 20 a 30 anos, moradoras do estado do RJ. As vítimas noticiaram sobre uma mulher, que se identificava como produtora de uma grande emissora de televisão, as adicionou no *Skype* lhes ofertando uma vaga como atriz.

Em todos os casos, potencializando a conduta, os criminosos passaram a interagir com a vítima, encaminhando perfis de artistas e jogadores de futebol, interagindo como se fossem estes, simulando o *stream* de vídeo da *webcam* e levando as vítimas a acreditarem estar vendo uma imagem real quando, na verdade, tratava-se de uma gravação. Após isso, as vítimas foram convencidas a fazer filmagens sem roupas ou mesmo com peças íntimas.

Após a exibição, o interlocutor informou tratar-se de uma farsa, revelando o ardil e passando, por conseguinte, a exigir quantias que variaram de 10 mil a 50 mil reais, via *bitcoins*[ix], cujo pagamento deveria ocorrer no enxuto prazo de até 72h, sob pena de divulgação na internet do vídeo íntimo das vítimas na internet.

Ainda, como forma de coação, o extorsionista encaminhava diversos *prints* dos vídeos gravados, bem como ameaçava as vítimas reiteradamente, seja *via Skype ou Whatsapp*, utilizando números virtualizados[x]. Tal prática torna impossível qualquer tipo de representação por quebra de sigilo de dados cadastrais do titular do número telefônico.

2.1 Análise da Ferramenta Skype

Segundo a *Microsoft*, o *Skype* é uma ferramenta gratuita desenvolvida e disponibilizada por aquela empresa desde maio de 2011. Esta aplicação ganhou notória popularidade por oferecer serviços como ligações VOIP, chats, envio de arquivos de mídia, envio de localização e *chats* de vídeo, dentre outras funcionalidades. Para se ter uma ideia da popularidade desta ferramenta, no ano de 2013, quando completou 10 anos[xi], já haviam mais de 300 milhões de usuários ativos, sendo destes 17,6 milhões de usuários brasileiros[xii]. Atualmente mantem em sua base 600 milhões de usuários[xiii].

Hoje, o serviço está em processo de migração de uma arquitetura ponto a ponto - P2P[xiv] - de chamadas e mensagens para um sistema baseado em nuvem. Conforme ressalta o próprio desenvolvedor, é a maior mudança de arquitetura na história do *Skype*. Essa mudança implica, entre outros fatores, na possibilidade de acessar o histórico das conversas dos últimos 30 dias, independente do dispositivo que acessar a conta.

Outra característica relevante sobre o *Skype* é que, além de preservar nos seus servidores o histórico dos últimos 30 dias de acesso, por padrão, também salva o histórico dos *chats* fisicamente no computador, sendo acessível seu diretório através do comando: [%appdata%\Skype] realizado no *executar*. Em tal diretório, encontra-se um arquivo *data base* intitulado *main.db*[xv] que contém as informações relacionadas aos históricos dos *chats*.

A aplicação guarda alguns inconvenientes investigativos no aspecto atinente à preservação do histórico dos diálogos realizados: ainda que os históricos de mensagens sejam salvos fisicamente no dispositivo utilizado, existe a possibilidade de qualquer um dos interlocutores editar ou até mesmo excluir o conteúdo das mensagens trocadas, repercutindo diretamente em todos os participantes do *chat*.

Com o intuito de preservar essa evidência, tanto a vítima quanto o investigador devem atuar rapidamente. Para tanto, como meio de comprovação do alegado, dois caminhos podem ser seguidos pela vítima: a lavratura de certidão do escrivão de polícia ou a ata notarial exarada por tabelião, em razão de estes serem dotados de fé pública. Ambos os documentos devem contar com a realização de um *printscreen* das conversas realizadas demonstrando a atividade criminosa noticiada.

Quanto à preservação dos dados, deve ainda ser realizada uma cópia do arquivo *main.db* onde ficam armazenados os históricos de todas as conversas, garantindo assim, elementos para subsidiar ações futuras nas esferas cível e criminal.

O outro inconveniente dessa ferramenta é a possibilidade de utilização de aplicações que simulam o *stream* de vídeo da *webcam*, podendo levar o interlocutor a acreditar estar vendo uma imagem real quando, na verdade, trata-se de uma gravação.

2.2 Da Solicitação de Registros ao *Skype*

Não há dúvidas de que a ferramenta *Skype*, quando utilizada por indivíduos em solo brasileiro, faz a coleta desse conteúdo aqui. Além do mais, oferta serviço ao público brasileiro e ainda possui representante do mesmo grupo econômico situada em território nacional. Não há, portanto, nenhum óbice ao cumprimento da legislação pátria.

Com efeito, o Poder Judiciário tem prolatado várias decisões no sentido de que a *Microsoft* forneça dados que venham a interessar em investigações policiais, dentre as quais os dados cadastrais e demais informações sobre um usuário de *Skype*. Ao receber tais determinações emanadas do Poder Judiciário, o representante do mesmo grupo econômico no Brasil tem informado não deter tais dados, atendo-se apenas a gerir o denominado LERM que intermedeia as requisições[xvi].

Ao ser demandado, o Skype responde às solicitações mediante uma requisição por ofício de autoridade judicial ou de ordem judicial, a depender do conteúdo solicitado. Fornece informações obtidas no momento do registro da conta, endereço de cobrança, dados de pagamento, números designados para o usuário, detalhes do histórico de chamadas realizadas e recebidas para a rede de telefonia pública, registros do histórico de mensagens de texto SMS - *Short Message Service*, histórico de registros de *Skype WiFi Hotspots* e histórico de atividade de alteração de e-mail e senha.

Contudo, apesar de aparentemente eficaz, o único meio viável de requisição de informações sobre uma conta *Skype* disposto por seu servidor sofre de nítida síndrome da ineficiência, pois a morosidade e o formalismo exacerbado vão nitidamente de encontro aos princípios que lastreiam a primeira fase da *persecutio criminis (Persecução Penal)*.

Assim, frente a uma atividade ilícita em curso, de nítida gravidade e do premente risco de cometimento de um mal ainda maior, deve a polícia judiciária lançar mão de outros meios lícitos, viáveis e técnicos de avanço nas investigações.

3. CENÁRIO DA INVESTIGAÇÃO

O cometimento de uma infração produz, no local do crime e adjacências, vestígios que contribuirão para a individualização da autoria e materialidade. Caberá, portanto, à polícia judiciária identificá-los. É o caso, por exemplo, de um crime de homicídio em que, para solucionar o fato, os investigadores irão coletar informações sobre o local, meios, motivos, circunstâncias, testemunhas e imagens de circuitos fechados de TV e representarão judicialmente pela quebra de sigilo de dados protegidos e por medidas cautelares diversas como interceptação telefônica, entre outras.

Da mesma forma, as infrações cometidas com ou através da internet produzem um local de crime virtual, com informações importantíssimas que auxiliarão no esclarecimento do fato. Vestígios cibernéticos são deixados pelo infrator, devendo a perquirição criminal encontrá-los, como, por exemplo, as informações livremente descritas pelo autor do fato como postagens realizadas na internet aberta ou ainda a coleta dos protocolos de internet utilizados pelo criminoso. Essa atuação não resulta em monitoramento de pacote de dados com o conteúdo das informações trafegadas pelo usuário, ou acesso à base de dados protegido pelo sigilo constitucional. A atividade policial é exercida no sentido em colher e individualizar vestígios e fragmentos deixados pelo criminoso quando da execução da atividade ilícita.

Quanto ao avanço da investigação dos casos praticados via *Skype*, em sua grande maioria, as coletas em fontes abertas, como o *nickname* ou número descrito para SMS, não lograram êxito. Da mesma forma, os perfis utilizados da ferramenta não costumam informar outros elementos que possibilitassem avançar nas investigações.

Mediante tal cenário, não resultaria em real efetividade nos valermos apenas dos meios disponibilizados por aquele servidor para a coleta de elementos informativos na investigação, refém da burocracia e morosidade. Resta, apenas, socorrer-se às técnicas que possibilitem o acesso a elementos individualizadores do criminoso.

Para tanto, utilizar-se-á o mesmo raciocínio empregado por um *website* para captar informações relacionadas aos seus usuários, não implicando em métodos intrusivos ou de acesso à

base de dados protegida por privacidade, que necessitam de ordem judicial. Ressalte-se, por oportuno, que essa coleta de IP é prática comum realizada por aplicações de internet para diversos propósitos, desde estatísticas de acesso até auxílio de diagnósticos de problemas do site.

Em ambos os casos, é possível lançar mão de três técnicas auxiliares, todas *freeware*, quais sejam:

1 – Programas que se propõem a analisar todo o tráfego de rede e a organizar protocolos, cujas funcionalidades são próximas ao *tcpdump*, contudo, com mais informação e possibilidade da utilização de filtros[xvii].

2 - Ferramenta executada via *prompt* de comando do *Windows*, *Unix* e *Linux*, utilizada para se obter informações sobre as conexões de rede (de saída e de entrada). Permite, também acessar tabelas de roteamento e outras informações relacionadas às estatísticas da utilização da interface na rede, capaz de individualizar todas as portas abertas para *Transmission Control Protocol* (TCP) e *User Datagram Protocol* (UDP)[xviii xix].

3 - Técnica utilizada por servidores de *web sites* para verificar e coletar informações disponibilizadas pelos usuários a cada acesso realizado em seu sítio eletrônico: *Page Tag* tem por finalidade precípua traçar um perfil dos usuários que acessam determinado *website*, como exemplo: a localidade, tipos de rotina, a frequência, etc. Assim, a utilização desta sistemática traz em aproveitamento das investigações virtuais dados valiosíssimos sob a ótica da eficiência e efetividade, sendo possível arrecadar informações como: sistema operacional utilizado pelo criminoso; *web browser* (navegador); informação temporal precisa; navegador utilizado; provedor de acesso à internet e, o principal, o IP da conexão utilizada. A junção destes dados obtidos nos permite, a depender do caso, verificar o tipo de conexão usada como 3G, *wifi*, dentre outros[xx].

CONSIDERAÇÕES FINAIS

As técnicas descritas se mostraram eficazes no processo de identificação da conexão utilizada pelo criminoso. Contudo, a última técnica, a *Page Tag*, mostra-se mais eficaz sob o ponto de vista técnico pois, além de individualizar a conexão utilizada pelo criminoso, ainda é capaz de precisar e registrar a conexão usada no exato instante da interação, o horário, o sistema operacional, provedor de acesso e o tipo de navegador.

Assim, pode-se afirmar que, através das técnicas empregadas, objetivou-se êxito na coleta das informações necessárias para a solução dos crimes investigados. Com isso, venceu-se a

morosidade frequentemente atrelada à burocracia dos meios investigativos tradicionalmente impostos pela rotina de polícia judiciária.

Portanto, conclui-se que, em respeito aos princípios norteadores da administração pública como a legalidade e principalmente da eficiência, devem os órgãos de persecução penal ampliar seu horizonte de percepção do processo penal para uma atuação mais dinâmica e adaptada ao movimento irreversível de uma sociedade cada vez mais conectada e dependente dos ônus e bônus deste ilimitado mundo virtual chamado internet.

---

[i] BRASIL. Superior Tribunal de Justiça. RMS 046685 (Decisão Monocrática) Ministro Leopoldo de Arruda Raposo (Desembargador Convocado do TJ/PE) DJE 06/04/2015. Lex: jurisprudência do STJ. Disponível em: <http://www.stj.jus.br/SCON/decisoes/doc.jsp?livre=mlat+e+google&b=DTXT&p=true&t=JURIDICO&l=10&i=1>. Acesso em: 27 fev. 2016.

[ii] BRASIL. Superior Tribunal de Justiça. RMS 041818 (Decisão Monocrática) Ministra Maria Thereza de Assis Moura DJE 02/05/2014. **Lex:** jurisprudência do STJ. Disponível em: <http://www.stj.jus.br/SCON/decisoes/doc.jsp?livre=mlat+e+google&b=DTXT&p=true&t=JURIDICO&l=10&i=2>. Acesso em: 27 fev. 2016.

[iii] BRASIL. Decreto nº 3.810, de 2 de maio de 2001. **Lex:** promulga o Acordo de Assistência Judiciária em Matéria Penal entre o Governo da República Federativa do Brasil e o Governo dos Estados Unidos da América, celebrado em Brasília, em 14 de outubro de 1997, corrigido em sua versão em português, por troca de Notas, em 15 de fevereiro de 2001. Portal da Legislação. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/2001/D3810.htm>. Acesso em: 27 fev. 2016.

[iv] BRASIL. Lei nº 12.965 de 23 de abril de 2014. **Lex:** estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Portal da Legislação. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 27 fev. 2016.

[v] BARRETO, Alesandro Gonçalves; WENDT, Emerson. Marco Civil da Internet e Acordos de Cooperação Internacional: análise da prevalência pela aplicação da legislação nacional aos provedores de conteúdo internacionais com usuários no Brasil. **Direito e TI**, Porto Alegre, ago. 2015. Disponível em: <http://direitoeti.com.br/artigos/mlat-x-marco-civil-da-internet/>. Acesso em: 01 mai. 2016.

[vi] BARRETO, Alesandro Gonçalves. Efetividade da Ordem Judicial em desfavor de Provedores de Conexão e Aplicações da Internet: sanções do Art. 12 do Marco Civil da Internet. **Direito e TI**, Porto Alegre, set. 2015. Disponível em: <http://direitoeti.com.br/artigos/efetividade-da-ordem-judicial-em-desfavor-de-provedores/>. Acesso em: 24 abr. 2016.

[vii] U.S. GOVERNMENT PUBLISHING OFFICE. The Stored Communications Act. SCA. **Legal Information Institute**, codifie at 18 USC Chapter 121 §§ 2701-2712, jul. 2015. Disponível em: <https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121>. Acesso em: 24 abr. 2016.

[viii] BARRETO, Alesandro Gonçalves; WENDT, Emerson. Marco Civil da Internet e Acordos de Cooperação Internacional: análise da prevalência pela aplicação da legislação nacional aos provedores de conteúdo internacionais com usuários no Brasil. **Direito e TI**, Porto Alegre, ago. 2015. Disponível em: <http://direitoeti.com.br/artigos/mlat-x-marco-civil-da-internet/>. Acesso em: 01 mai. 2016.

[ix] Moeda online baseada em protocolo de código aberto em que a transação financeira dos usuários da internet não é regulada por autoridade central. BITCOIN Project 2009-2016. Site descritivo do serviço. Disponível em: <https://bitcoin.org/pt_BR/>. Acesso em: 27 fev. 2016.

[x] Números telefônicos virtuais ou VOIP dos mais variados países, confirmados via SMS virtual.

[xi] MOLINA, Violeta. Skype comemora 10 anos em um mercado em constante mudança. **Exame.com**, ago. 2013. Disponível em: <http://exame.abril.com.br/tecnologia/noticias/skype-comemora-10-anos-em-um-mercado-em-constante-mudanca>. Acesso em: 24 abr. 2016.

[xii] ZAMBARDA, Pedro. Skype já conta com quase 18 milhões de usuários brasileiros, diz site. **Techtudo**, abr. 2013. Disponível em: <http://www.techtudo.com.br/noticias/noticia/2013/04/skype-ja-conta-com-quase-18-milhoes-de-usuarios-brasileiros-diz-site.html>. Acesso em: 24 abr. 2016.

[xiii] FAGUNDES, Eduardo. Skype e whatsapp transformaram o modelo de negócios de telecomunicações. **EF.**, fev. 2016. Disponível em: <http://efagundes.com/blog/skype-e-whatsapp-transformaram-o-modelo-de-negocios-de-telecomunicacoes/>. Acesso em: 24 abr. 2016.

[xiv] MICROSOFT Skype 2016. Explicação sobre P2P. Disponível em: <https://support.skype.com/pt/faq/FA10983/o-que-sao-comunicacoes-p2p>. Acesso em: 27 fev. 2016.

[xv] MICROSOFT Skype 2016. **How do I manage my conversation history in Skype for Windows desktop**. Explicação histórico e Db. Disponível em: <https://support.skype.com/en/faq/FA392/where-can-i-find-my-conversation-history-in-skype-for-windows-desktop-and-what-can-i-do-with-it#8>. Acesso em: 27 fev. 2016.

[xvi] Para ter acesso aos logs e dados cadastrais de uma conta, a empresa informa que deverá a Autoridade Policial/Judicial, através do LERM, encaminhar uma requisição para Skype Communications SARL, 23-29 Rives de Clausen, L-2165, Luxemburgo. Não há a necessidade da ordem ser traduzida para o inglês, mas ela deve ser assinada pelo solicitante (juiz, delegado responsável). O Ofício deverá ser encaminhado via e-mail para lerm@skype.net <mailto:lerm@skype.net> (com cópia para lelatam@microsoft.com <mailto:lelatam@microsoft.com>).

[xvii] WIRESHARK FOUNDATION 2016. **About Wireshark.** Explicação da ferramenta wireshark. Disponível em: <https://www.wireshark.org>. Acesso em: 27 fev. 2016.

[xviii] MICROSOFT 2016. Explicação da ferramenta Netstat. Disponível em: <https://technet.microsoft.com/pt-br/library/ff961504(v=ws.10).aspx>. Acesso em: 27 fev. 2016.

[xix] MICROSOFT Skype 2016. **Quais portas precisam estar aberto a usar Skype para Windows desktop**. Explicação sobre TCP e UDP. Disponível em: <https://support.skype.com/pt/faq/FA148/quais-portas-precisam-estar-aberto-a-usar-skype-para-windows-desktop?>. Acesso em: 27 fev. 2016.

[xx] OLSEN, Stefanie. Nearly undetectable tracking device raises concern. **CNET**, jan. 2002. Disponível em: <http://www.cnet.com/news/nearly-undetectable-tracking-device-raises-concern/>. Acesso em: 27 fev. 2016.