CRIMES VIRTUAIS: ANÁLISE DO PROCESSO INVESTIGATÓRIO E DESAFIOS ENFRENTADOS

LESSA, Isabella Maria Baldissera.[1]
VIEIRA, Tiago Vidal.[2]

RESUMO

O presente artigo tem por finalidade mostrar os desafios enfrentados pelas diferentes autoridades no processo investigatório dos crimes praticados por meio eletrônico. Com o avanço tecnológico da internet, a comunicação entre as pessoas se difundiu drasticamente, movimentando a vida de forma positiva nos aspectos social, profissional e pessoal. Contudo, as inovações tecnológicas trouxeram grandes desafios também, dentre eles, os crimes praticados virtualmente. Mesmo diante da constante evolução da tecnologia, as autoridades encontram dificuldades para investigar e solucionar os crimes virtuais, seja pela falta legislação específica, seja pela carência de delegacias e profissionais especializados. Assim, a investigação acaba sendo lenta e complexa, o que gera a impunidade, pois, muitas vezes, ao identificar o autor de um crime, constata-se a ocorrência da prescrição. Isso facilita e explica o surgimento de vários novos golpes a cada dia. Para mostrar como ocorrem essas dificuldades foram analisadas doutrinas nacionais, manuais de atuação do Ministério Público Federal e estaduais, artigos científicos, bem como reportagens televisivas envolvendo casos reais. Um dos caminhos possivelmente eficazes para ajudar nas investigações de forma efetiva seria um investimento por parte da Administração Pública, tanto em pessoal quanto em treinamento, uma vez que restou comprovado que nas cidades onde há delegacia especializada os resultados são bastante satisfatórios. Não menos importante se faz a assinatura do Brasil em tratados de cooperação internacional, como é o exemplo da Convenção de Budapeste, bem como a aprovação de novas leis que propõem uma quebra de sigilo independente de ordem judicial, sendo o primeiro passo para impulsionar o procedimento investigativo dos crimes virtuais, o que fará com que a apuração da autoria seja realizada de maneira mais célere e eficaz, restando tão somente aos provedores de internet o dever de fornecer informações sobre os investigados e manter usuários informados acerca dos perigos que a internet pode oferecer.

PALAVRAS-CHAVE: Crimes virtuais, processo investigatório, possibilidades jurídicas, internet.

1. INTRODUÇÃO

É indiscutível o grande impacto que a internet tem gerado no mundo e, principalmente, na rotina das pessoas. Conforme informações divulgadas pelo Instituto Brasileiro de Geografia e Estatística (IBGE), mais da metade dos domicílios brasileiros passou a ter acesso à internet em 2014. Tal fato sugere que, em decorrência do grande fluxo de pessoas utilizando a rede mundial, as denúncias de crimes virtuais cresceram em 197% no Brasil em 2014, conforme apontam estatísticas do Centro de Estudos, Respostas e Tratamento de Segurança (CERT.br, 2015). No mesmo ano, a Central Nacional de Denúncias de Crimes Cibernéticos (CND) recebeu cerca de 189.211 denúncias anônimas, envolvendo 58.717 páginas da internet, das quais 7.092 foram removidas, conforme demonstra estatísticas da SaferNet Brasil (anexos 1 e 2). Dentre os crimes praticados virtualmente

[1]Acadêmica do curso de Direito da FAG - Faculdade Assis Gurgacz. E-mail: isabellamblessa@live.com
[2]Professor orientador do curso de Direito da FAG – Faculdade Assis Gurgacz. E-mail: tiago.vidal.vieira@gmail.com

ISSN 2318-0633

se encontram: pornografia infantil, ameaça, calúnia, injúria, roubo de dados, falsa identidade, racismo e xenofobia (SAFERNET,2016). Observa-se que o número de denúncias de crimes virtuais sobe cada vez mais no Brasil atualmente, ficando em evidência casos emblemáticos como o de Carolina Dieckmann, que inclusive ensejou a criação da Lei nº 12.737/12.

Esses dados demonstram o impacto do avanço tecnológico na vida das pessoas e que a tendência quanto a utilização da internet aumente cada vez mais, tendo em vista a grande velocidade que fluem as informações e, como consequência, a facilidade na comunicação entre pessoas, o que não traz somente aspectos positivos, mas também aspectos negativos devido à prática de crimes no meio virtual, cuja autoria deve ser investigada.

Contudo, é evidente que existem dificuldades no processo investigatório desses crimes virtuais, como por exemplo, a resistência dos provedores em fornecer dados de usuário e local de acesso, alegando que essas informações são sigilosas (CARVALHO, 2013). Outro problema muito frequente que deve ser citado é a incompatibilidade entre sistemas IPs usados pelas empresas de telecomunicações do Brasil (IPv4) e pelos provedores de conteúdo sediados no exterior (IPv6), pois o primeiro permite o acesso de até 132 pessoas em um mesmo IP simultaneamente, o que acaba por embaraçar a investigação criminal (OLIVEIRA, 2015).

Várias outras dificuldades também acabam impedindo um processo investigatório célere e satisfatório, como por exemplo, a falta de legislação, delegacias especializadas e profissionais capacitados.

O presente trabalho busca trazer à luz os desafios enfrentados pelas autoridades no processo investigatório dos crimes virtuais no Brasil e busca apontar possíveis caminhos para os problemas técnicos presentes durante as investigações, visando auxiliar na obtenção de informações que, consequentemente, levem à autoria do crime de maneira mais rápida e eficiente, evitando, assim, a impunidade.

Tendo em vista a falta de uma legislação específica que facilite as investigações e considerando todas as demais dificuldades que as autoridades policiais e judiciais terão, eis que novas modalidades de crimes virtuais continuarão surgindo, faz-se necessário a adoção de uma nova visão para a aplicação do direito nos casos de crimes virtuais, por meio de uma postura interdisciplinar. Isto é, os profissionais envolvidos precisam, além do conhecimento técnico, analisar cada caso concreto a partir de uma interação com a realidade, o texto legal e as demais

ISSN 2318-0633

áreas do saber que se fizerem necessárias ao caso, ou seja, eles precisam atuar por meio da interdisciplinaridade, pois assim conseguirão um resultado mais efetivo e eficaz.

2. FUNDAMENTAÇÃO TEÓRICA

2.1 BREVES APONTAMENTOS SOBRE A EVOLUÇÃO DA INTERNET

A internet foi criada por um grupo de pesquisadores norte-americanos em meados de 1962, durante a Guerra Fria. Foi construída para objetivos militares, como um meio de comunicação que fosse capaz de resistir a bombardeios e que permitisse o compartilhamento de dados com vários computadores, interligados entre si. Dessa forma, ainda que um ou mais computadores fossem destruídos, os equipamentos ligados ao sistema continuariam funcionando normalmente (BRASIL, 2006).

Inicialmente, foi nomeada ARPAnet (nome derivado de *Advanced Research Projects Agency*), enquanto o termo atual internet começou a ser utilizado décadas depois, para designar uma especificação completa do protocolo TCP/IP. Ao final dos anos 80, surgiram alguns serviços de e-mail (correio eletrônico) e também provedores que se conectavam à rede por meio do método dial-up. Na década de 90, a internet chegou ao seu ápice, quando foi criada a expressão *World Wide Web*, e daí em diante, a internet passou apenas a evoluir (BARROS, 2013).

Mais tarde surgiram as tecnologias de banda larga, como redes cabeadas e ADSL, e atualmente são diversas as opções de conexão, podendo ser via satélite, telefonia celular e via rádio (BRASIL, 2013).

Conforme dados do IBGE, 54,4% da população brasileira já possuía acesso à internet em 2014. Isso significa que cerca de 95,4 milhões dos brasileiros passaram a ter acesso à internet. Acesso esse, que pode ser feito por diferentes dispositivos, como computadores, celulares, tablets e até mesmo televisão. Sabemos que um pouco mais da metade da população brasileira utiliza a internet em sua rotina diária e para diversas finalidades. Logo, não é de se espantar que vários indivíduos estejam fazendo uso dessa ferramenta para cometer crimes também (BRASIL, 2006).

ISSN 2318-0633

2.2 O MARCO CIVIL DA INTERNET

A Lei nº 12.965/2014, em vigência desde 23 de junho de 2014, trouxe diversos dispositivos que, apesar do seu cunho "civil", também influenciam na investigação dos crimes virtuais. A referida lei dispõe acerca da preservação de dados de provedores de acesso à internet, que possuem o dever de manter armazenados os registros de conexão de seus usuários, ou seja, data e hora do acesso, a duração e o endereço IP, pelo período de um ano, sob sigilo (GIACCHETTA, FREITAS e MENEGUETTI, 2014). A proteção de dados de acesso dos internautas é justificada pelo princípio da privacidade, que garante aos usuários o direito de não fornecimento desses dados, sem que haja prévio consentimento ou fora dos casos indicados na lei (COSTA, 2016).

Pode ocorrer que em determinada investigação de um crime virtual seja necessária a quebra do sigilo desses dados, obrigando provedores a fornecerem essas informações mediante ordem judicial. Entretanto, tal norma acaba por deixar o processo lento, principalmente quando o provedor não possui sede no Brasil. Como observa Burg (*apud* ROVER, 2017), um significativo período de tempo já teria se passado até que a autoridade policial remeta o inquérito ao fórum e haja representação judicial.

Além disso, o Marco Civil não impõe aos provedores de internet o dever de manter sob sua guarda as comunicações privadas dos usuários. Tanto que o WhatsApp, por exemplo, utiliza criptografia para proteger ainda mais o sigilo dos dados dos usuários. Só há responsabilização do provedor nos casos em que eles guardem comunicações privadas e que não haja técnicas para impedir esse acesso ao conteúdo das conversas, porém há negativa da parte do provedor em fornecê-las. Portanto, caso ficar verificado que o provedor utilize criptografia para manter os dados de seus usuários sigilosos ou não realize a guarda das conversas, a sanção aplicada em razão da negativa da prestação de informações estaria afrontando a Lei nº 12.965/2014 e a Constituição Federal (LOPES, 2016).

2.3 CRIMES VIRTUAIS

ISSN 2318-0633

Crimes virtuais são condutas tipificadas em lei como crime, tendo como característica essencial o emprego da internet como meio de serem praticadas.

Exemplos de crimes virtuais tipificados em lei seriam os praticados por crackers, como invasão de sistemas e ataques por meio de vírus como *trojan horses* (cavalos de Tróia) e as *logic bombs*, a fim de causar prejuízos a grandes provedores, impossibilitando usuários de acessarem os sites. Ainda, é correto chamar de crimes virtuais, aquelas condutas praticadas visando um bem jurídico tutelado pelo Direito Penal, quando o sistema é utilizado apenas como um meio para atingir bem jurídico diverso do computador, como por exemplo, atingir o patrimônio (crimes de fraude e estelionato) ou imagem, honra e intimidade (crimes de calúnia, difamação, injúria e racismo) (ARAS, 2001).

Muito se discutia a respeito da falta de dispositivos legais específicos a respeito dos crimes virtuais. Entretanto, não importa se existe ou não tais dispositivos, pois quando o computador é utilizado como um meio para a prática do crime, esse será caracterizado independentemente de existir uma lei que pune especificamente aquela conduta cometida em meio virtual. Portanto, a lei é aplicada de qualquer forma e os acusados serão devidamente processados (ABPERITOS, 2016).

2.4 PROCEDIMENTO INVESTIGATÓRIO

Para a análise das etapas da investigação dos crimes virtuais é necessário, primeiramente, haver uma denúncia de crime virtual. É preciso identificar o meio utilizado para a prática do delito (e-mail, website, salas de bate-papo, etc), pois para cada meio há um caminho diferente a ser seguido. É importante para o investigador proteger o computador que utiliza para obtenção de dados, no intuito de evitar um ataque digital, capaz de obter e destruir dados ou até mesmo permitir que um terceiro o utilize remotamente (BRASIL, 2006).

2.4.1 Evidências no mundo virtual

Evidências virtuais são consideradas provas da ocorrência de um crime e são associadas com o lugar onde o crime teria sido praticado (nesse caso, na internet). São exemplos de evidências

ISSN 2318-0633

digitais os logs (registros de login), amostras de registros de sessões e registros de navegação da internet (WENDT e JORGE, 2013).

Conforme Santos e Fraga (2010), as provas obtidas da investigação dos crimes virtuais são extremamente voláteis, significando que sempre há o risco da perda dessas informações a qualquer momento. Por isso da necessidade de preservar as provas desses crimes, no intuito de evitar que sejam perdidas ou até mesmo modificadas.

Em virtude disso, existem procedimentos específicos para aquisição, preservação, análise e apresentação, que precisam ser cumpridos para dar devida validade jurídica às evidências digitais (BRASIL, 2013).

Imprimir e salvar arquivos, imagens de tela (apertando tecla *PrintScreen* do computador, ou no caso de smartphones, apertar o botão de desligar junto com o botão central) e páginas de internet relacionadas ao crime é algo muito importante, devido à volatilidade dessas provas, as quais podem ser retiradas do ar com extrema facilidade, ou até mesmo editadas, para parecer que o crime nunca tivesse ocorrido.

Em seguida, recomenda-se ir ao cartório registrar ata notarial das evidências, instrumento público realizado e assinado por tabelião que relata e comprova as informações contidas nos documentos apresentados para dar a devida fé pública, sendo, assim, possível apresentá-las em juízo (CASSANTI, 2014).

Existem programas gratuitos que auxiliam na aquisição e armazenamento de provas, como por exemplo: o *HTTrack Website Copier*, responsável por realizar cópias completas de sites para um diretório local do computador do investigador. Através dele é também possível navegar por cada umas das páginas do site sem levantar suspeitas que podem levar o autor da página a modificar informações. Já o *MD5summer* auxilia na verificação da integridade de arquivos, gerando assinaturas digitais (*hashes*) nesses arquivos, responsáveis por determinar se um arquivo é original ou se houve alguma modificação (WENDT e JORGE, 2013).

2.4.2 Investigação em sites brasileiros

Todo o procedimento se inicia quando o fato criminoso chega aos ouvidos da autoridade policial por denúncia da vítima ou outro interessado. Se for denúncia de algo publicado em website

ISSN 2318-0633

deve-se proceder a três importantes fases: coleta do conteúdo do website, aquisição de informações referentes ao domínio do website e do endereço IP do servidor que hospeda o website. (BRASIL, 2013).

Primeiramente, deve a autoridade copiar o conteúdo desse site por meio do *HTTrack Website Copier*, já mencionado (WENDT e JORGE, 2013). A necessidade da análise de todo o conteúdo de um website é justificada, pois pode haver dados dentro de documentos que sejam capazes de encontrar e-mails que identifiquem o criminoso (BRASIL, 2013). Em seguida, deve-se observar a terminação do site.

Para os websites com terminação ".br" busca-se os dados cadastrais através do Registro.br (http://registro.br), selecionando o Serviço de diretório *whois*. Isso é feito para obter informações sobre o proprietário do domínio, o contato administrativo e o contato técnico e servidores DNS (WENDT e JORGE, 2013). Para identificar o endereço IP do servidor que hospeda o website é possível utilizar o software *Dig* (*domain information groper*), que cumpre com o seu papel de consultar nomes de domínios associados a endereços IP e detectar a quantidade de servidores DNS que estão vinculados ao site (BRASIL, 2013).

Caso um usuário cadastrado ao site tenha sido o responsável pelo crime, é necessário acionar o provedor de serviços por meio de uma ordem judicial, para que forneça os dados de conexão exatos (IP, data, hora, GMT) que partiram de um determinado computador ou smartphone, pois serão necessários para, posteriormente, requerer ao provedor de acesso as informações físicas da pessoa que realizou essa conexão (CASSANTI, 2014).

Dependendo do caso, existirá a necessidade de requisição de ordem judicial direcionada ao provedor de acesso à internet, ordenando a quebra de sigilo dos dados físicos do usuário ou do administrador do site (caso esse tenha realizado o crime), para que seja localizado (WENDT e JORGE, 2013).

Ao final da investigação, pode-se chegar à origem do acesso, que pode ter partido de uma residência, empresa ou órgão público. Há também a possibilidade de o serviço de conexão à internet estar vinculado à telefonia móvel (3G ou 4G). Logo, o próximo passo, nesse caso, seria requerer ao juízo que fosse expedida ordem judicial para o fornecimento de dados pela empresa responsável, referentes à geolocalização do sinal de celular (ERB ou estação rádio base), em que foi utilizada para a conexão (BRASIL 2013).

ISSN 2318-0633

Em um caso real, o pai de santo Tata Ricardo recebeu comentários de intolerância religiosa pela internet. A pessoa intolerante se referiu ao local de evento do Candomblé como "casa do diabo" em sua publicação no Facebook. Durante a investigação do crime houve pedido de quebra de sigilo de dados e a equipe do Facebook encaminhou as informações necessárias (e-mail e logs), para auxiliar na localização do autor do crime. Verificou-se qual foi o provedor de conexão que deu o IP à pessoa, e por meio dessa investigação foi possível identificar o endereço do autor do crime de ódio (GLOBO, 2015).

2.4.3 Investigação em sites estrangeiros

Não difere muito do procedimento empregado em sites brasileiros, mas há a opção de pesquisar no site do órgão responsável pelo registro de sites do respectivo país ou, caso o site tenha um domínio genérico (.net, .emp, entre outros), fazer a pesquisa no site responsável pelo registro desses.

Para achar o site responsável pelo registro desses domínios, pode-se acessar o site da IANA (www.iana.org/domains/root/db), mas também há a opção de utilizar uma ferramenta chamada "whois" disponível na internet, as mesmas que servem para pesquisar os domínios genéricos, que não fazem referência a nenhum país. (WENDT e JORGE, 2013). Nessa hipótese, quando o provedor está localizado em outro país e não possui filial, agência ou sucursal no Brasil há a necessidade de pedido de cooperação internacional, que pode ser feito junto ao Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional (DRCI) do Ministério da Justiça. Quando o provedor possui escritório no Brasil, a cooperação não é necessária, nos termos do parágrafo único do artigo 21, do Código de Processo Civil de 2015 (WENDT e JORGE, 2013). Esse dispositivo facilita muito o processo de investigação, uma vez que um pedido de cooperação internacional pode demorar muito tempo para receber a resposta, dependendo do país envolvido (BRASIL 2013).

O Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional (DRCI), do Ministério da Justiça presta informações sobre como fazer o pedido de cooperação internacional, e existe um roteiro que deve ser seguido para solicitar interceptação telemática de e-mails e conversas instantâneas (IMS), perante empresa provedora de acesso que esteja localizada nos Estados Unidos.

ISSN 2318-0633

Primeiramente, é necessário obter ordem judicial do governo norte-americano, nos termos da legislação do país, o chamado *Eletronic Communications Privacy Act of 1986*. Isso é possível, pois o Brasil é signatário do *Mutual Legal Assistence Treaty* – MLAT, que é um tratado para cooperação judicial entre países. Para tanto, deve ser feita a minuta de solicitação de assistência jurídica em matéria penal, enviada para o e-mail cooperacaopenal@mj.gov.br, a fim de que seja analisada pelo DRCI (WENDT e JORGE, 2013).

Há também a possibilidade de cooperação internacional policial, que é regulamentada por meio de um tratado chamado *Network for Computer Crime Matters* (Rede para Assuntos de Crime de Informática), tendo como responsável por tal rede no Brasil o Setor de Crimes de Informática da Polícia Federal (BRASIL, 2017).

O principal objetivo dessa rede é encaminhar pedidos de preservação de evidências virtuais e retirada de conteúdo relacionado a crimes virtuais, além de também tirar dúvidas sobre a legislação jurídica internacional de forma muito menos burocrática. O e-mail de contato da rede é cybercrime_brazil_24x7@dpf.gov.br (WENDT e JORGE, 2013).

2.4.4 Investigação de fraudes eletrônicas

O número de fraudes com cartões de crédito tem aumentado consideravelmente no Brasil devido à comodidade que a utilização do internet banking proporciona, facilitando ainda as compras virtuais. Existem sites e programas mal-intencionados responsáveis pelo roubo de informações do computador da vítima, como número do cartão, data de validade e também o código de segurança (CASSANTI, 2014).

Geralmente o criminoso envia um e-mail à vítima com um link de site fraudulento, que tem por objetivo roubar informações ao simular ser um site governamental, site de bancos conhecidos ou empresas. Muitas vezes os e-mails chegam a mostrar mensagens com notícias falsas, prêmios, fotos de pessoas famosas, avisos ou ameaças de órgãos governamentais, induzindo a vítima a clicar no link que acessa o site e solicita o preenchimento de formulários com dados pessoais ou instala programas maliciosos, capazes de enviar informações do computador do alvo para o criminoso virtual (WENDT e JORGE, 2013).

ISSN 2318-0633

O nome desse tipo de golpe é denominado *phishing scam* e sua investigação é bem mais criteriosa do que as anteriormente abordadas. Isso porque é necessário preparar o ambiente para o procedimento investigatório, instalando no computador um programa chamado máquina virtual (*Virtual Machine* ou VM), que possibilita ao investigador a instalação de um sistema operacional que executa programas, como um computador que trabalha de forma independente, enquanto o sistema hospedeiro se mantém isolado e livre de danos. Além disso, todas as informações da VM estarão salvas em um disco rígido no computador vetor, tornando assim, mais fácil a rotina da investigação, sendo necessárias as duplicações, backups e transferência desses dados (BRASIL 2013).

O primeiro passo da investigação em caso de fraude com cartões de crédito é oficiar a instituição bancária para obtenção do número IP, data, hora e padrão GMT, e ouvir a explicação da vítima de como ocorreu a compra indevida, a fim de identificar o método utilizado pelo criminoso para fraudar o cartão de crédito (WENDT e JORGE, 2013).

Na máquina virtual, o investigador deve abrir o e-mail e clicar no link que estiver no corpo da mensagem, para simular o comportamento da vítima. Depois deve verificar o comportamento do navegador e para qual site o internauta é direcionado e, caso o site seja enganoso, será necessário verificar o seu funcionamento, inserindo informações falsas nos formulários que aparecem na tela; exibindo o código-fonte das páginas para encontrar possíveis URLs utilizadas; inserindo páginas padrão na barra de endereços para tentar acessar diretórios e arquivos ou até mesmo tentando localizar o console utilizado pelo autor da fraude (BRASIL 2013).

A partir dessas informações, é possível descobrir e-mails, URLs e servidores de banco dados vinculados ao autor do crime. Entretanto, pode ainda haver necessidade de requerer ordem judicial, para que haja a quebra de dados telemáticos perante os provedores de acesso à internet (WENDT e JORGE, 2013).

2.4.5 Investigação em redes sociais e outras mídias

É evidente que as redes sociais, como Facebook, Twitter, Google+ e Orkut são os maiores pontos de encontro de grupos que possuem interesses em comum. O Brasil está em segundo lugar

ISSN 2318-0633

no ranking mundial de perfis cadastrados no Facebook com 65 milhões, perdendo apenas para os Estados Unidos, com o total de aproximadamente 164 milhões de perfis (CASSANTI, 2014).

Os crimes virtuais ocorrem principalmente em redes sociais, sendo que nesse meio as condutas, mais praticadas, tipificadas no Código Penal Brasileiro são as do art.138 (Calúnia), art.139 (Difamação), art.140 (Injúria), art.147 (Ameaça), e art. 307 (Falsa Identidade), cuja autoria pode ser investigada buscando-se o IP de criação da página de perfil falso e o IP de postagem das mensagens ofensivas. A materialidade do delito virtual deve ser preservada mediante a impressão e salvamento das páginas, que contém o conteúdo ofensivo e, ainda, deve requerer ao provedor a retirada do conteúdo em até 24 horas, com sua preservação em dispositivos de armazenamento, para continuar a auxiliar nas investigações do autor do crime (BRASIL 2013).

Entretanto, também é exigida a ordem judicial na quebra de sigilo telemático para aquisição de dados pessoais do criminoso junto ao provedor de acesso, assim como nos outros procedimentos de investigação (WENDT e JORGE, 2013).

2.4.6 Investigação em comunicadores instantâneos

São programas que visam o envio e o recebimento simultâneo de mensagens, em que a comunicação é feita em tempo real (se houver conexão à internet) por meio de textos, voz, imagens, GIFs (animações) ou vídeos. Exemplos de comunicadores instantâneos são: Skype, ICQ, Yahoo Messenger, Google Talk, entre outros (CASSANTI, 2014).

Vale frisar que a principal característica desse tipo de comunicação é o fato de o conteúdo transmitido entre os interlocutores não ser armazenado num host central antes de ser entregue ao destinatário, como ocorre nos serviços de e-mail. Esse aspecto reforça a sensação de anonimato, uma vez que parece não haver terceiros na conversa, o que incentiva a prática de crimes como o aliciamento de menores (BRASIL 2013).

A investigação da autoria de crimes cometidos por essa via geralmente se inicia com a expedição de ofício para a empresa responsável pelo programa, solicitando obter informações sobre dados cadastrais, logs (IP, data e horário, incluindo fuso horário) de criação do e-mail, log (IP, data e horário, incluindo fuso horário) dos últimos acessos, lista de contatos e outras informações sobre o

ISSN 2318-0633

e-mail. Todavia, já como as empresas responsáveis por esses programas são normalmente estrangeiras, há a necessidade de requerer a cooperação internacional (WENDT e JORGE, 2013).

Descoberta a localização geográfica da conexão do criminoso, é possível, juntamente com ordem judicial, solicitar ao provedor responsável pelo acesso à internet a interceptação telemática de dados trafegados, sendo necessária a análise desses dados pelo investigador, por meio de softwares especializados (BRASIL 2013).

2.4.7 Investigação de e-mail

É muito comum que a maioria das pessoas tenham contas cadastradas em serviços de e-mail gratuitos, como Yahoo!, Gmail (Google) e Hotmail (Microsoft). Com essa informação, pode-se ter uma noção do caminho percorrido pela mensagem, uma vez que o usuário deverá estar conectado à internet por um provedor de serviços de internet, para que seja possível acessar o serviço de e-mail. Portanto o investigador pode requerer, por ordem judicial, informações sobre conexões e acessos tanto do provedor de internet, quanto do provedor de e-mail (WENDT e JORGE, 2013).

No entanto, pode-se ainda extrair do cabeçalho do e-mail informações importantes, que são: conteúdo da mensagem (e seus anexos), endereço de e-mail do remetente, endereços de e-mail dos destinatários, IP do computador que enviou a mensagem e número IP dos computadores em que a mensagem transitou até chegar ao destino final (BRASIL 2013).

Para descobrir a origem de um e-mail, deve-se promover uma análise detalhada do cabeçalho, em que existe o campo *Received*, que em certos casos é possível identificar a diretamente o computador de onde se originou a mensagem. Entretanto, há casos em que o provedor serviu apenas de intermediário para envio do e-mail, o que significa que será necessária ordem judicial para conseguir do provedor de internet a identificação do remetente (WENDT e JORGE, 2013).

2.5 COMPETÊNCIA E TERRITORIALIDADE

É o que vai determinar o lugar onde será instaurado o processo, bem como em que âmbito do judiciário será processado o crime virtual, destacando-se, assim, as competências material (*ratione*

ISSN 2318-0633

materiae) e territorial (*ratione loci*). No caso de divulgação ou publicação de fotografia, filmagem ou outro registro com pornografia infantil por meio da internet, a competência material será da Justiça Federal, tendo em vista o teor do inciso V do art. 109 da Constituição, bem como o fato de que o Brasil é signatário da Convenção sobre os Direitos da Criança da Assembleia das Nações Unidas (BRASIL, 2013).

Exemplo claro do emprego da referida regra de competência é o CC 112.616, em que o STJ concluiu que o crime de difamação contra menores em redes sociais é de competência da Justiça Federal, uma vez que afronta os direitos protegidos pela Convenção sobre os Direitos da Criança da Assembleia das Nações Unidas, e o site em que foi praticado o crime pode ser acessado inclusive no exterior, respeitando assim os requisitos do inciso V do art. 109 da Constituição Federal (LOPES JR., 2014).

Entretanto, tal regra de competência material não é utilizada para casos em que há mera troca de e-mails ou fotografias entre pessoas que moram no Brasil. A competência é, portanto, da Justiça Estadual, pois falta aqui o requisito de repercussão internacional, sendo a competência prevista no art. 109 da Constituição Federal como residual (BRASIL 2013).

Além disso, vale ressaltar que as situações do art. 109 da CF não podem ser presumidas e sim devidamente comprovadas no caso concreto, e apenas a presença de internacionalidade não justifica o deslocamento para a Justiça Federal (LOPES JR., 2014).

Os crimes de racismo seguem a mesma regra de competência material dos crimes de pornografia infantil. Ou seja, quando praticado através da troca de e-mails ou mensagens privadas, a competência será da Justiça estadual, enquanto se o crime for praticado com utilização de blogs, sites ou redes sociais, a competência será da Justiça Federal. Os demais crimes seguem a regra do inciso IV do art. 109 da Constituição, portanto serão estes também de competência da Justiça Federal (BRASIL 2013).

Quanto à competência territorial, o art. 69 do CPP prevê os critérios para tanto, sendo o primeiro deles o lugar da infração. Ainda, o art. 6º do CP prevê que o local do crime é onde teria ocorrido os atos de execução do crime ou onde a conduta criminosa surtiu ou deveria surtir efeitos no caso de crime tentado. Quando verificado um conflito de competência territorial, uma vez que, segundo entendimento doutrinário, poderá haver um maior número de juízos competentes em determinadas circunstâncias e a depender da forma que o crime é consumado, utiliza-se o segundo critério de fixação de competência territorial, que é o do domicílio do réu. Entretanto, muitas vezes

ISSN 2318-0633

é incerta a localização do réu no momento em que houve o crime, tendo em vista que o crime poderia ter sido praticado por meio de um dispositivo eletrônico, que poderia estar localizado, por exemplo, em uma *lan house* em cidade diversa do domicílio do autor.

O artigo 70, §3º do CPP, por sua vez, determina a prevenção como forma de fixação da competência nesses casos de incerteza, sendo, portanto o juízo competente o que primeiro atuasse ou determinasse medidas dentro do processo (RAMIRES, 2016). Inclusive, é esse o entendimento adotado pelo STF no HC 106074 PR (STF *apud* RAMIRES, 2016).

3. METODOLOGIA

O presente trabalho caracteriza-se como uma pesquisa explicativa de cunho bibliográfico, cujos recursos utilizados para a exposição de fatos foram: análise de doutrinas nacionais, manuais de atuação do Ministério Público Federal e Estadual, artigos científicos, bem como matérias e reportagens envolvendo casos reais, estando essas disponíveis na internet para acesso e leitura.

4. ANÁLISES E DISCUSSÕES

4.1 DIFICULDADES NO PROCESSO INVESTIGATÓRIO

4.1.1 Desafios na investigação da autoria de crimes praticados por e-mail

Um dos principais problemas na investigação de crimes praticados por e-mails é que certos provedores não possuem registros apropriados, o que pode resultar em um equívoco durante esse processo, recaindo a autoria do crime sobre um usuário que de fato não praticou o delito (BRASIL 2013).

ISSN 2318-0633

Outro problema muito comum é a utilização de esteganografia por internautas, que é uma maneira muito eficaz de mandar mensagens privadas e, por esse motivo, gera muitas dificuldades para os investigadores. As técnicas variam muito de um software para outro, portanto, é necessário que o investigador tenha conhecimento sobre os programas e técnicas mais comuns empregadas nesse sistema de códigos, para que seja possível operar efetivamente em diferentes casos (BRASIL 2013).

Há também o *Cloud Computing* ou computação em nuvem, que permite a disponibilização de um computador para que seja acessado pelo usuário via internet, ficando todo o conteúdo salvo em servidores brasileiros ou estrangeiros. Se os dados do crime se encontrarem em servidor estrangeiro, será muito mais difícil, demorado, ou até mesmo impossível para os peritos conseguirem as informações necessárias para a investigação criminal, considerando que o Brasil não é signatário da Convenção de Budapeste, também conhecida como Convenção sobre o Cibercrime, que trata da cooperação internacional para a persecução de crimes virtuais (WENDT e JORGE, 2013).

4.1.2 Prescrição

Outro desafio encontrado diz respeito ao lapso temporal dispensado na investigação de alguns crimes. A demora na apuração dos crimes virtuais pode gerar impunidade dos infratores. Isso por que no caso de crimes de menor potencial ofensivo, como é o exemplo dos crimes contra a honra e crime de invasão de dispositivo informático, existe grande chance de o crime prescrever antes mesmo de entrar em um efetivo processo contra o praticante do crime. Isso ocorre porque as penas previstas para esses crimes são baixas (até dois anos), o que significa que é muito fácil ocorrer prescrição retroativa pela pena aplicada em concreto (CAVALCANTE, 2012).

4.1.3 Conhecimentos técnicos dos profissionais de polícia

A quantidade de policiais capacitados e treinados na investigação de crimes virtuais ainda é escassa, e isso passa a tornar-se problemático, ao passo que dificulta a persecução penal dos responsáveis e, inevitavelmente, resulta na impunidade (WENDT e JORGE, 2013).

ISSN 2318-0633

É evidente o atraso que o Brasil possui em relação a outros países, estando no 33º lugar no ranking de segurança cibernética, lista que contém outros 219 países (anexo 3). Observa-se que a quantidade de denúncias vem crescendo em volume, enquanto a Polícia Federal e Civil não possui uma estrutura boa o suficiente para atender a todos esses casos de maneira eficaz (CANUTO, 2015).

Além disso, apenas 14 dos 27 estados (incluindo DF) contam ao menos com uma delegacia especializada em crimes virtuais, enquanto dois possuem setores que oferecem orientações, a saber: Mato Grosso e Distrito Federal. Os Estados que possuem delegacias especializadas em crimes virtuais são: Bahia, Espírito Santo, Maranhão, Mato Grosso do Sul, Minas Gerais, Pará, Paraná, Pernambuco, Piauí, Rio Grande do Sul, São Paulo, Sergipe, Rio de Janeiro e Tocantins (SAFERNET, 2017).

Portanto, diferentemente dos criminosos, nota-se que não há uma integração entre os órgãos de investigação de cada Estado, e a maioria das delegacias carecem em profissionais especializados em crimes virtuais, o que revela a importância da capacitação de profissionais da área criminal que poderiam ser trazidos, por meio de políticas públicas nacionais voltadas aos órgãos de segurança pública e estimular o investimento por parte dos Estados nessa área tão importante (WENDT e JORGE, 2013).

Por vezes, a polícia se depara com quadrilhas especializadas na prática de crimes virtuais, sendo que cada membro reside em um Estado diferente. Exemplo disso foi um dos casos apresentados no programa “Profissão Repórter”, em que haviam 20 pessoas envolvidas em diversas práticas criminosas, como transferências fraudulentas de contas, pagamento de boletos e compras na internet com cartões clonados. É evidente que houve nesse caso uma integração de criminosos de diversas localidades, sendo que o líder residia no estado do Pará, enquanto o segundo na linha de comando residia em Goiás (GLOBO, 2015).

Essa interação entre criminosos de Estados ou até países diferentes gera uma dificuldade nas investigações, tendo em vista que a grande maioria se utiliza de recursos tecnológicos com a presença de criptografia ou esteganografia, para que seja impossível determinar o conteúdo das conversas entre os integrantes da quadrilha (WENDT e JORGE, 2013).

4.1.4 Necessidade de conscientização dos usuários da internet

Também outro problema é a falta de conscientização dos usuários sobre como se proteger dos ataques virtuais. Muitas pessoas podem até conhecer a internet e desfrutar de suas mil funcionalidades, porém não entendem a proporção dos riscos que pode estar sofrendo ao receber um simples e-mail ou acessar um link para um site (WENDT e JORGE, 2013).

Atenta-se que as novas gerações estão conectadas à internet cada vez mais cedo, e isso pode deixá-los muito vulneráveis quando não há uma educação específica sobre essas ameaças. Conforme pesquisa realizada pelas empresas Kapersky Lab e B2B International, apenas 39% dos pais conversam com seus filhos sobre segurança na internet e 20% se mantém inerte quanto à proteção de seus filhos contra as ameaças, dados que revelam a falta de conscientização sobre o tema e também a falta controle sobre o conteúdo que seus filhos poderiam estar acessando (CONVERGÊNCIA DIGITAL, 2016).

Dados recentes também demonstram a amplitude de novos vírus com potencial altamente infeccioso, como o WannaCry, que já fez 200 mil vítimas em 150 países (EUROPOL *apud* JORNAL DO BRASIL, 2017). Outro vírus que ganhou fama graças ao WannaCry é chamado Adylkuzz e ataca também o Windows, porém não é barrado pelas atualizações e correções desenvolvidas pelas empresas de antivírus. A principal função do WannaCry é basicamente a de sequestrar dados pessoais da vítima e exigir um pagamento em Bitcoins em troca do resgate, enquanto o Adylkuzz gera uma moeda parecida com Bitcoin, rouba os dados dos usuários e ainda recebe o pagamento sem o usuário perceber o que ocorreu (ANSA *apud* JORNAL DO BRASIL, 2017).

É evidente que deve haver uma maior conscientização quanto à prevenção de crimes virtuais e uso responsável da internet, visto que as gerações mais jovens estão cada vez mais informatizadas, porém cada vez mais expostas à má índole dos criminosos. Dessa forma, faz-se necessário também que provedores se responsabilizem em deixar seus usuários informados sobre métodos de prevenção contra crimes virtuais que possam eventualmente ocorrer (BRASIL, 2006).

4.1.5 Legislação

ISSN 2318-0633

É importante destacar que a Lei 12.965/2014, conhecida como Marco Civil da Internet, vem sendo vastamente utilizada e aplicada em decisões proferidas pelos tribunais brasileiros, servindo até como incentivo para legislações estrangeiras, como se observa na Declaração de Direitos na Internet Italiana (SOUZA e TEFFÉ, 2017).

Entretanto, a referida lei versa sobre a necessidade de ordem judicial para obtenção de dados relacionados ao crime virtual, o que é muito criticado por vários doutrinadores, por ser algo muito burocrático e demorado e que fatalmente entrava as investigações. Apesar de haver sites e serviços que permitem o fornecimento de informações sem ordem judicial, como é exemplo da Microsoft Brasil e Mercado Livre, muitos não adotam a mesma percepção, prevalecendo assim, a necessidade de ordem judicial para obtenção de dados cadastrais e logs de conexão e acesso (WENDT e JORGE, 2013).

Muito embora o marco civil da internet tenha sido um grande avanço para o Brasil no mundo virtual, se mostra falho e deixa lacunas. Felizmente, há projetos de lei em trâmite que visam autorizar a obtenção de endereços IP em investigações criminais sem a necessidade de ordem judicial, como o Projeto de Lei 730/2015 (CONSULTOR JURÍDICO, 2017). Apesar das fortes críticas recebidas por autores que defendem a privacidade na internet, como consequência da aprovação dessa lei, haveria grande melhoria da atuação policial na busca dos autores do crime com maior rapidez e eficiência. Isso por que, na prática, os maiores problemas decorrem de questões de política criminal e não jurídicas, sendo imprescindível, portanto, a capacitação de profissionais e não a criação de leis.

Considerando o rápido surgimento dos mais diversos crimes virtuais e a dificuldade encontrada pelos profissionais no combate a esses crimes, seja por falta de legislação específica seja pela falta de capacitação de profissionais faz-se necessário uma atuação concomitante de algumas áreas. Isto é, mostra-se imprescindível a interdisciplinaridade entre Direito e Informática.

4.1.6 A importância da interdisciplinaridade no processo investigatório dos crimes virtuais

Embora não haja dificuldade na aplicação das normas de direito penal nos crimes praticados pela internet, sendo esta facilmente identificada como mero meio para a prática do ato, não deixa de ser necessária a tipificação de certas condutas dotadas de juízo de reprovação social e culpabilidade,

ISSN 2318-0633

que merecem ser analisadas e estudadas pelo Direito Penal com maior ênfase, para que futuramente seja possível sua tipificação dentro do ordenamento jurídico penal (NUNES, 2011).

Ainda, ressalta-se que outros países possuem uma legislação mais abrangente que o Brasil e seria de extrema importância tomar essas legislações como exemplo na criação de futuras leis que versem sobre crimes virtuais, pois, assim, haveria uma harmonização da legislação material e processual penal interna dos países, fortalecendo também a cooperação internacional (COLLI e LOPES JR, 2009).

Nesse contexto, os legisladores não podem se manter inertes na criação de normas jurídicas, uma vez que os aspectos sociais e tecnológicos estão em constante desenvolvimento, ao passo que a legislação não acompanha essa evolução. Como qualquer outro ramo do Direito, o Direito Penal deve ater-se à atualização de suas normas, para que seja possível a aplicação efetiva, garantindo sua eficácia e mantendo, assim, a ordem tanto no mundo real quanto no virtual (NUNES, 2011).

5. CONSIDERAÇÕES FINAIS

Em que pese a evolução da internet ter sido de grande importância para a sociedade, trouxe também pontos negativos, como é o exemplo das práticas criminosas. Cumpre às autoridades policiais investigar essas práticas, em um primeiro momento, para apurar a materialidade e autoria do crime, pois surgem muitos desafios quanto ao procedimento investigatório que devem ser superados para alcançar a celeridade e eficácia na identificação do responsável. Ao analisar a Lei 12.965/2014, também conhecida como Marco Civil da Internet, é possível apontar certos problemas no que tange ao sigilo e direito à privacidade, o que entravam as investigações devido à necessidade de obter ordem judicial para buscar as informações necessárias, visando à correta identificação do usuário responsável pelo crime.

Evidencia-se, ainda, a dificuldade em obter cooperação judicial em casos que envolvem outros países, uma vez que o Brasil não é signatário da Convenção de Budapeste que versa exatamente sobre o assunto e, ainda, a falta de previsão legal sobre como os profissionais devem proceder com a investigação deixam lacunas que somente pessoal treinado e capacitado no assunto podem suprir. Nesse contexto, indiscutível se faz a exigência de investimento por parte da Administração Pública na capacitação de profissionais da área criminal, através de políticas

ISSN 2318-0633

públicas nacionais voltadas aos órgãos de segurança pública e a integração entre os órgãos de investigação de cada estado.

Faz-se necessária uma ampla divulgação sobre os riscos e formas de prevenção contra ameaças virtuais, principalmente pelos provedores, tendo como objetivo conscientizar e informar os internautas brasileiros acerca do assunto e evitar que maior número possível de pessoas saiba como proceder no caso de ser vítima de um crime virtual.

Por fim, resta evidente a importância do diálogo do Direito e Informática, buscando sempre realizar um estudo interdisciplinar, uma vez que a criminalidade vem se difundindo rapidamente no ambiente virtual, ao passo que a legislação não acompanha os andamentos da sociedade de maneira eficaz, e por isso clama por meios alternativos de repressão das novas modalidades de crimes virtuais enquanto espera a aprovação de leis mais rígidas e eficazes versando sobre o tema.

Para tanto, uma retomada de consciência se faz necessária, pois diante da realidade atual, ou seja, diante dos novos crimes que estão surgindo e da dificuldade encontrada para solução desses crimes, é imprescindível uma busca constante por um conhecimento maior, que possibilite uma atuação efetiva.

Os profissionais precisam analisar a realidade a partir de uma abordagem crítica acerca dos fatos e das possibilidades para uma efetiva solução. E essa postura precisa ser adotada por toda a sociedade, seja acadêmica, policial ou jurídica.

Adotar uma conduta crítica significa, primeiramente, questionar sobre as possibilidades de solução para o caso concreto, momento em que o profissional estará se utilizando da interdisciplinaridade, pois está interagindo com a realidade, a lei e outras áreas do saber. Assim, o direito conseguirá se aproximar da realidade social atual e garantirá uma efetiva proteção às vítimas dos mais variados crimes praticados virtualmente.

REFERÊNCIAS

ABPERITOS. Instituto Brasileiro de Perícias Forenses. **O que são Crimes Virtuais?** 2016. Disponível em: <http://www.abperitos.com.br/web/2016/10/19/o-que-sao-crimes-virtuais/> Acesso em: 05 nov. 2016.

ISSN 2318-0633

ANSA *apud* JORNAL DO BRASIL. **Novo ataque cibernético está em curso, diz empresa dos EUA**. 2017. Disponível em: <http://www.jb.com.br/ciencia-e-tecnologia/noticias/2017/05/17/novo-ataque-cibernetico-esta-em-curso-diz-empresa-dos-eua/> Acesso em: 22 mai. 2017.

ARAS, Vladimir. **Crimes de informática**. Uma nova criminalidade. 2001. Disponível em: < https://jus.com.br/artigos/2250/crimes-de-informatica>. Acesso em: 01 nov. 2016.

BARROS, Thiago. **Internet completa 44 anos**; relembre a história da web. 2013. Disponível em: <http://www.techtudo.com.br/artigos/noticia/2013/04/internet-completa-44-anos-relembre-historia-da-web.html>. Acesso em: 12 set. 2016.

BRASIL. Ministério Público Federal. **Crimes cibernéticos**: Manual prático de investigação. São Paulo: Procuradoria da República no Estado de SP, 2006.

_____. Ministério Público Federal. **Roteiro de Atuação sobre Crimes Cibernéticos**. Brasília: 2ª Câmara de Coordenação e Revisão do MPF, 2013.

_____. Ministério Público de Santa Catarina. **Manual de Atuação**: Interceptação Telemática. Suporte Tecjurídico. 2017. Disponível em: < https://documentos.mpsc.mp.br/portal/Conteudo/cao/ccr/suporte_tecjuridico/>. Acesso em: 10 abr. 2017.

BURG, Daniel A. *apud* ROVER, Tadeu. **Internet facilita crimes e dificulta investigação, estimulando a impunidade**. 2017. Disponível em: < http://www.conjur.com.br/2017-fev-05/entrevista-daniel-burg-especialista-crimes-virtuais>. Acesso em: 22 set. 2016.

CANUTO, Luiz Cláudio; TRIBOLI, Pierre. **CPI constata dificuldade em rastrear e punir crimes de internet**. 2015. Disponível em: <http://www2.camara.leg.br/camaranoticias/noticias/SEGURANCA/494363-CPI-CONSTATA-DIFICULDADE-EM-RASTREAR-E-PUNIR-CRIMES-DE-INTERNET.html> Acesso em: 22 mai. 2017.

CARVALHO, Mônica S. O. A. **Investigação sobre Crimes Dig**itais. 2013. Disponível em: <http://claudiaseixas.adv.br/investigacao-sobre-crimes-digitais/>. Acesso em: 12 set. 2016.

CASSANTI, Moisés de Oliveira. **Crimes virtuais, vítimas reais**. Rio de Janeiro: BRASPORT, 2014.

CAVALCANTE, Márcio André Lopes. **Primeiros comentários à Lei 12.737/2012, que tipifica a invasão de dispositivo informático**. 2012. Disponível em:

<http://www.dizerodireito.com.br/2012/12/primeiros-comentarios-lei-127372012-que.html>. Acesso em: 10 abr. 2017.

CERT.BR. **Incidentes Reportados ao CERT.br** - janeiro a dezembro de 2014. Análise de alguns fatos de interesse observados neste período. 2015. Disponível em: < http://www.cert.br/stats/incidentes/2014-jan-dec/analise.html>. Acesso em: 12 set. 2016.

COLLI, Maciel; LOPES JR., Aury. **Cibercrimes**: Limites e Perspectivas da Investigação Preliminar Policial Brasileira de Crimes Cibernéticos. 2009. Disponível em: <http://www.pucrs.br/edipucrs/IVmostra/IV_MOSTRA_PDF/Ciencias_Criminais/71527-MACIEL_COLLI.pdf>. Acesso em: 07 jun. 2017.

CONSULTOR JURÍDICO. **Novas leis enfraquecem Marco Civil da Internet, diz pesquisa**. 2017. Disponível em: < http://www.conjur.com.br/2017-abr-23/novas-leis-enfraquecem-marco-civil-internet-pesquisa>. Acesso em: 22 mai. 2017.

CONVERGÊNCIA DIGITAL. **Só 39% dos pais conversam com filhos sobre ameaças online**. 2016. Disponível em: < http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=43883&sid=18>. Acesso em: 22 mai 2017.

COSTA, Thabata F. **A importância de uma Lei Geral de Proteção de Dados Pessoais**. 2016. Disponível em: <https://thabatafc.jusbrasil.com.br/artigos/346208302/a-importancia-de-uma-lei-geral-de-protecao-de-dados-pessoais>. Acesso em: 20 set. 2016.

CYBERDEFCON. **Global Security Map**. 2017. Disponível em: <http://globalsecuritymap.com/#br> Acesso em: 22 mai. 2017.

EUROPOL apud JORNAL DO BRASIL. **Ciberataque afetou mais de 200 mil em 150 países, diz Europol. 2017**. Disponível em: <http://www.jb.com.br/ciencia-e-tecnologia/noticias/2017/05/14/ciberataque-afetou-mais-de-200-mil-em-150-paises-diz-europol/> Acesso em: 22 mai. 2017.

GIACCHETTA, André Z.; FREITAS, Ciro T.; MENEGUETTI, Pamela G. **Marco Civil da Internet põe fim a lacunas na legislação**. 2014. Disponível em: <http://www.conjur.com.br/2014-abr-30/marco-civil-internet-poe-fim-lacunas-existentes-legislacao>. Acesso em: 22 mai. 2017.

GLOBO. **Profissão Repórter 29 09 2015** - Crimes cometidos pela internet no Brasil. 2015. Disponível em: < http://g1.globo.com/profissao-reporter/noticia/2015/09/profissao-reporter-mostra-diferentes-crimes-cometidos-pela-internet.html>. Acesso em: 17 mai. 2017.

ISSN 2318-0633

IBGE. **Pesquisa Nacional por Amostra de Domicílios**: Acesso à Internet e à Televisão e Posse de Telefone Móvel Celular para Uso Pessoal. Rio de Janeiro; 2016.

IOMG. **Polícia Civil mineira é referência nacional em solução de crimes na internet**. 2015. Disponível em: < http://www.iof.mg.gov.br/index.php?/acao-do-governo/acao-do-governo-arquivo/Policia-Civil-mineira-e-referencia-nacional-em-solucao-de-crimes-na-internet.html>. Acesso em: 13 set. 2016.

JORGE, Higor Vinicius Nogueira; WENDT, Emerson. **Crimes Cibernéticos**: ameaças e procedimentos de investigação. 2. Ed. Rio de Janeiro: Brasport, 2013.

LOPES JR., Aury. **Crimes cometidos pela internet** - competência. 2014. Disponível em: <https://www.facebook.com/aurylopesjr/posts/634559893297671>. Acesso em: 01 mai. 2017.

NUNES.Valdomiro da Silva. **Direito Cibernético**: Uma abordagem interdisciplinar. 2011. Disponível em: <http://catolicaonline.com.br/revistadacatolica2/artigosv3n5/artigo08.pdf>. Acesso em: 07 jun. 2017.

OLIVEIRA, Déborah. **MP aponta desafios técnicos para investigação de crimes cibernéticos**. 2015. Disponível em: <http://itforum365.com.br/noticias/detalhe/117004/mp-aponta-desafios-tecnicos-para-investigacao-de-crimes-ciberneticos>. Acesso em: 12 set. 2016.

RAMIRES, Bruno. **Conflitos de competência em matéria processual penal**: competência territorial dos crimes cibernéticos. 2016. Disponível em: <https://jus.com.br/artigos/47505/conflitos-de-competencia-em-materia-processual-penal-competencia-territorial-dos-crimes-ciberneticos>. Acesso em: 25 mai. 2017.

SAFERNET. **Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos**. 2016. Disponível em: <http://indicadores.safernet.org.br/>. Acesso em: 12 set. 2016.

SAFERNET. **Delegacias Cibercrimes**. 2016. Disponível em: <http://www.safernet.org.br/site/prevencao/orientacao/delegacias>. Acesso em: 22 mai. 2017.

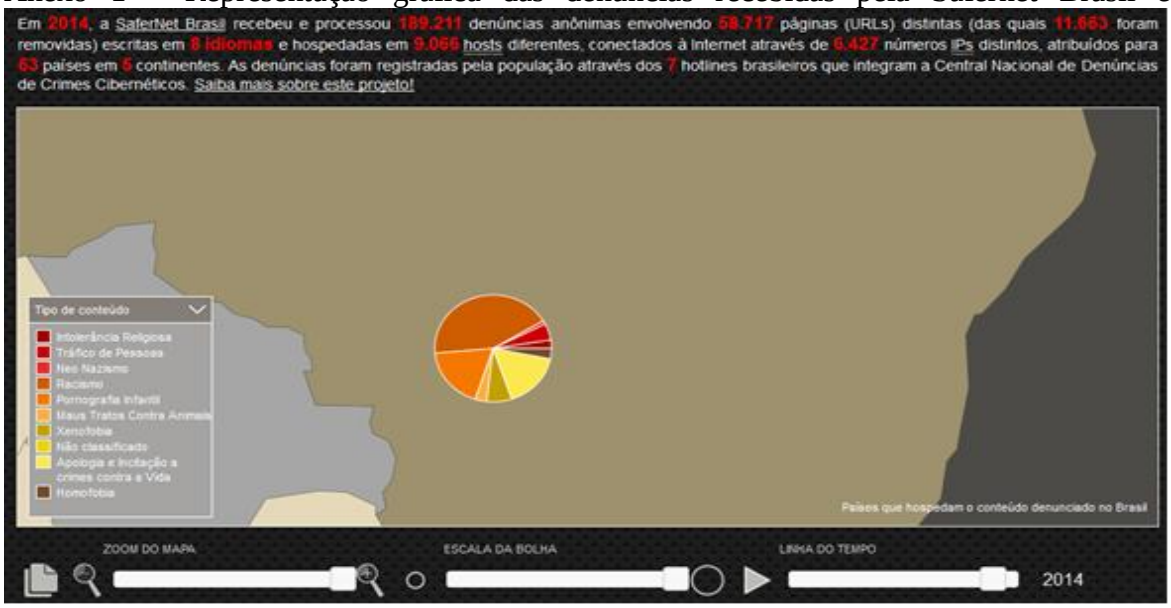
SANTOS, Coriolano A. A. C.; FRAGA, Ewelyn Schots. **As múltiplas faces dos Crimes Eletrônicos e dos Fenômenos Tecnológicos e seus reflexos no universo Jurídico**. 2. Ed. São Paulo: 2010. Disponível em: <https://cidadaovirtual.files.wordpress.com/2010/11/oabsp_livro_crimes_eletronicos_2ed.pdf>. Acesso em 11 set. 2016.

STF *apud* RAMIRES, Bruno. **Conflitos de competência em matéria processual penal**: competência territorial dos crimes cibernéticos. 2016. Disponível em:

<https://jus.com.br/artigos/47505/conflitos-de-competencia-em-materia-processual-penal-competencia-territorial-dos-crimes-ciberneticos>. Acesso em: 25 mai. 2017.

ANEXOS

Anexo 1 – Representação gráfica das denúncias recebidas pela Safernet Brasil em 2014.



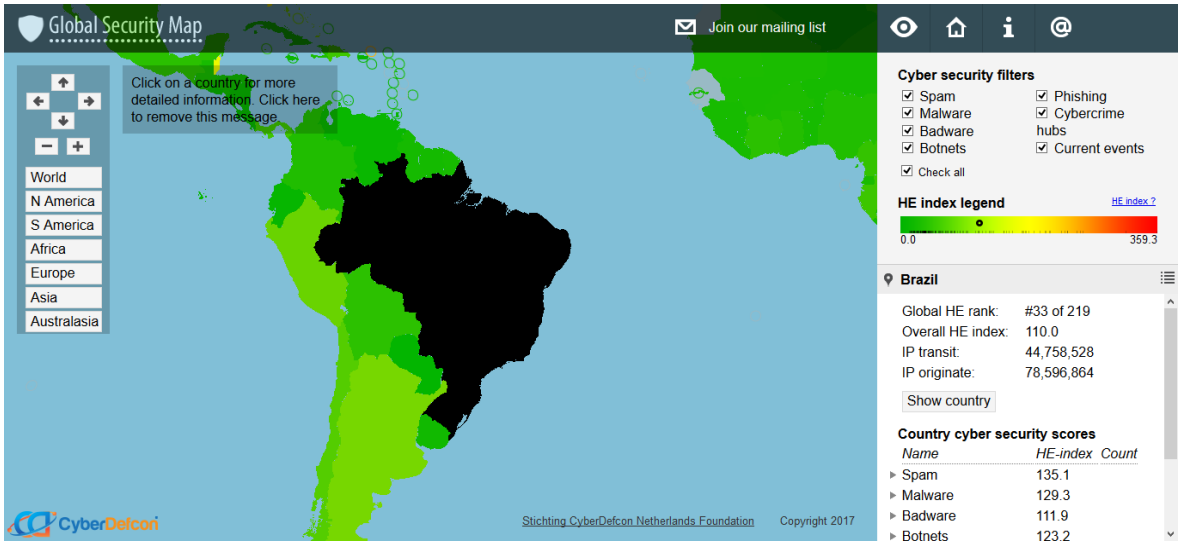
Fonte: SAFERNET (2016)

Anexo 2 – Representação gráfica da relação entre páginas brasileiras denunciadas em 2014.

Fonte: SAFERNET (2016)

ISSN 2318-0633

Anexo 3 – Informações detalhadas sobre o Brasil no Mapa de Segurança Global da empresa CyberDefcon.



Fonte: CYBERDEFCON (2017)

ISSN 2318-0633