UNIVERSIDADE FEDERAL DE JUIZ DE FORA
FACULDADE DE DIREITO

LÍVIA FONSECA BARBOSA

CRIMES CIBERNÉTICOS: UMA ABORDAGEM SOBRE O PROCEDIMENTO INVESTIGATÓRIO ADOTADO PELOS ÓRGÃOS ENCARREGADOS DA PERSECUÇÃO PENAL NO BRASIL

Juiz de Fora

2019

LÍVIA FONSECA BARBOSA

CRIMES CIBERNÉTICOS: UMA ABORDAGEM SOBRE O PROCEDIMENTO INVESTIGATÓRIO ADOTADO PELOS ÓRGÃOS ENCARREGADOS DA PERSECUÇÃO PENAL NO BRASIL

Artigo apresentado à Faculdade de Direito da Universidade Federal de Juiz de Fora como requisito parcial para a obtenção do título de Bacharel em Direito, sob a orientação do Prof. Ms. Felipe Fayer Mansoldo.

Juiz de Fora

2019

LÍVIA FONSECA BARBOSA

CRIMES CIBERNÉTICOS: UMA ABORDAGEM SOBRE O PROCEDIMENTO INVESTIGATÓRIO ADOTADO PELOS ÓRGÃOS ENCARREGADOS DA PERSECUÇÃO PENAL NO BRASIL

Artigo apresentado à Faculdade de Direito da Universidade Federal de Juiz de Fora, como requisito parcial para a obtenção do título de Bacharel em Direito, submetido à avaliação da Banca Examinadora composta pelos membros:

Prof. Ms. Felipe Fayer Mansoldo (Orientador)

Universidade Federal de Juiz de Fora

Prof. Dr. Cleverson Raymundo Sbarzi Guedes

Universidade Federal de Juiz de Fora

Prof. Dr. Cristiano Álvares Valladares do Lago

Universidade Federal de Juiz de Fora

PARECER DA BANCA

( ) APROVADO

( ) REPROVADO

Juiz de fora, de de 2019

CRIMES CIBERNÉTICOS: UMA ABORDAGEM SOBRE O PROCEDIMENTO INVESTIGATÓRIO ADOTADO PELOS ÓRGÃOS ENCARREGADOS DA PERSECUÇÃO PENAL NO BRASIL

Lívia Fonseca Barbosa[1]

RESUMO

O presente artigo tem como objetivo tratar sobre o modelo investigatório adotado pelos órgãos de persecução penal brasileiros para o enfrentamento aos crimes cibernéticos, com base nas normas que tratam da matéria, convenções internacionais e a aplicação adaptada nas figuras penais típicas do Decreto-Lei nº 2.848/40 (Código Penal). Para este fim, a pesquisa foi realizada utilizando-se do método qualitativo-intervencionista, a partir de estudo doutrinário, através de artigos científicos, livros que versam sobre o tema e manuais confeccionados pelas instituições encarregadas da administração da justiça. Quanto à estrutura de organização do artigo, primeiramente será feita uma breve explanação histórica e conceitual dos delitos informáticos, seguido das modalidades e do *modus operandi*, para em seguida dissertar sobre as tentativas de regulamentação legal e as espécies de ilícitos mais cometidos no Brasil. Após, será abordado o tema central do trabalho, com a análise de todo o procedimento desempenhado pelos organismos encarregados da persecução para apuração dos delitos, concluindo com a exposição crítica da necessidade de aprimoramento do atual sistema e de maior estímulo à prevenção contra crimes desta natureza.

PALAVRAS-CHAVE: Crimes Cibernéticos; Internet; Procedimento Investigatório; Marco Civil da Internet; Dispositivos Eletrônicos.

ABSTRACT

The purpose of this article is to talk about the investigated model adopted by brazilian criminal prosecution bodies to combat cybercrime, based on the rules governing the matter, international conventions and the application adapted to typical criminal figures of Law nº 2.848/40 (Penal Code). To this end, the research was conducted using the qualitative-interventionist method, based on doctrinal study, through scientific articles, books on the subject and manuals made by the justice administration institutions. Regarding the organizational structure of the article, first will be made a brief historical and conceptual explanation of computer offenses, followed by modalities and modus operandi, and then discuss the attempts of legal regulation and the most committed species in Brazil. Afterwards, the main theme of the work will be approached, with the analysis of the whole procedure performed by the prosecution bodies to investigate the crimes, concluding with the critical exposure of the need for improvement of the current system and to stimulate the prevention of crimes of this nature.

[1] Graduanda em Direito na Universidade Federal de Juiz de Fora.

KEYWORDS: Cybercrime; Internet; Investigative Procedure; Internet Milestone; Eletronic Devices.

SUMÁRIO: 1. INTRODUÇÃO. 2. CRIMES CIBERNÉTICOS: CONCEITO E CLASSIFICAÇÃO. 2.1. Análise do *modus operandi* dos crimes cibernéticos e o perfil do agente. 2.2 Tentativas de regulamentação no plano internacional. 2.3 Tentativas de regulamentação no Brasil. 2.4 Crimes cibernéticos mais comuns no Brasil. 3. OS MÉTODOS DE INVESTIGAÇÃO DOS CRIMES CIBERNÉTICOS 4. A NECESSIDADE DE APRIMORAMENTO DO PROCEDIMENTO INVESTIGATÓRIO E DE ESTÍMULO À PREVENÇÃO DOS DELITOS CIBERNÉTICOS. 5. CONSIDERAÇÕES FINAIS. REFERÊNCIAS.

1. INTRODUÇÃO

Com as mudanças trazidas pela Terceira Revolução Industrial (Revolução Informacional) e a globalização, houve a proliferação do acesso à internet. Ergueu-se a Era Digital, sendo este o movimento de inserção da sociedade às novas tecnologias e serviços que modificaram substancialmente o cotidiano dos cidadãos em âmbito mundial.

Uma vez que a conexão à rede mundial de computadores foi se tornando mais acessível aos consumidores, seja porque os preços ficaram mais atrativos ou porque grande parte dos afazeres diários passaram a serem resolvidos através da internet, as pessoas começaram a utilizá-la para as mais diversas funções, não mais como apenas objeto para estudo e pesquisa, mas como uma ferramenta facilitadora das tarefas domésticas e laborativas. Agora os indivíduos podem realizar transações bancárias sem ter que se deslocar à agência, pedir refeições através de aplicativos, solicitar transporte de um lugar para o outro, trocar mensagens instantâneas, fazer chamada de vídeo com amigos e parentes distantes, dentre todas as possibilidades que a internet proporciona.

Ao passo que a tecnologia vai invadindo a vida em sociedade, os usuários precisam estar preparados para poder lidar com as consequências da modernidade. É certo que grandes evoluções trazem consigo novas responsabilidades e riscos, surgindo a necessidade de se ter profissionais qualificados para operarem os modernos equipamentos, além de arcar com os altos custos para manutenções.

Sendo a internet uma aliada, ela também poderá se tornar a vilã quando é utilizada por criminosos para a prática de delitos, virando um ambiente propício para a proliferação do que há de pior na humanidade. Agentes criminosos a manipulam como um novo meio de

perpetração de delitos já tipificados. Buscam também atacar a própria rede, desafiando as autoridades a reconhecer a relevância de novos bens jurídicos surgidos com a nova Era Digital, como a segurança dos equipamentos e a proteção dos dados, passando a prever a punição para a violação de tais bens.

Nesse sentido, ocorreram alguns avanços legislativos de grande importância para o enfrentamento dos crimes cibernéticos. Todavia, a regulamentação do tema no Brasil ainda está muito aquém de ser considerada satisfatória.

O presente artigo possui o objetivo de demostrar as tentativas de regulamentação em âmbito mundial e dentro do território brasileiro. Utilizando-se dessas bases, pretende-se examinar o procedimento investigatório perpetrado pelos órgãos encarregados da persecução penal, divididos nas fases de colheita, armazenamento, análise e apresentação das provas produzidas no curso da investigação e do processo. Neste escopo, busca-se o avanço nas técnicas de apuração, visando a promoção de um ambiente mais seguro para os internautas com o incentivo a uma postura mais cautelosa no momento de utilização da rede.

2. CRIMES CIBERNÉTICOS: CONCEITO E CLASSIFICAÇÃO

Com o avanço tecnológico e a chegada da "Era da Informação[2]", o acesso à Internet[3] tornou-se cada vez mais facilitado, o que possibilitou com que a sociedade passasse a utilizar os dispositivos eletrônicos para resolver grande parte de suas funções rotineiras, como acessar aplicativos de bancos para realizar transações financeiras, fazer reuniões à distância através de vídeo-chamadas, trocar mensagens instantâneas através de programas como o *Whatsapp*[4], dentre outras diversas possibilidades oferecidas pela *web*[5].

Além disso, as grandes empresas, os sistemas de transporte, os serviços de saúde, a veiculação de informação, todos estes dependem do fluxo da rede mundial de computadores, que interliga pessoas e faz diminuir as barreiras impostas pela distância.

---

[2] Termo utilizado para designar os avanços tecnológicos advindos após as revoluções industriais e que reverberou na difusão de um *ciberespaço*, ou seja, um meio de comunicação instrumentalizado pela informática e pela internet.

[3] Sistema global de redes interligadas que permitem a conexão descentralizada de computadores através de um conjunto de protocolos denominado *Internet Protocol* (IP), que será abordado no tópico 3.

[4] Aplicativo utilizado para troca de mensagens instantâneas e comunicação em áudio e vídeo.

[5] Sistema de informações ligadas por uma hipermídia (ligações em forma de texto, vídeo, som, etc) que possibilita ao usuário acessar à internet.

Uma vez existente essa dependência, a internet vira um constante alvo de ataques, com o propósito de atingir seu funcionamento para prejudicar uma pessoa, uma empresa, uma rede, ou até uma nação[6].

O ambiente do ciberespaço, por ser algo intangível e imensurável, costuma ser representado por uma figura que se assemelha ao formato de um *iceberg*, dividido em três camadas[7]. A primeira seria a Internet Pública ou *Web*, sendo esta a ponta do *iceberg*, acima da superfície do mar. Já a *Deep Web* seria a fração já dentro da água, porém mais próxima da superfície, enquanto a *Dark Web* ou *Darknet* é o final do bloco, a parte do gelo mais profunda.

Adriana Shimabukuro[8] explicita como seria esta classificação:

> Como o próprio nome sugere, a Internet Pública é de fácil acesso e não requer senhas ou softwares específicos para a navegação, ao contrário da Deep Web, que é composta de dados não indexados, isto é, não pode ser detectada por motores de busca como o Google ou Bing. Na Deep Web também encontramos sites dinâmicos, criados como resultado de uma busca ou até páginas que requerem acesso via login e senha, como, por exemplo, sua conta no Gmail.
> Diferente da Deep Web, a Dark Web ou Darknet é uma rede fechada, usada para compartilhar conteúdo de forma anônima. Seu acesso é permitido mediante o uso de softwares específicos, como o TOR Project, o Freenet e a rede I2P (2017) ou outras dezenas de redes secretas e criptografadas. Conforme MERCÊS (2014), a Darknet é majoritariamente composta de sites de venda de produtos ilícitos, como armamento e drogas, além de sites que compartilham pornografia infantil.

No chamado crime cibernético, o computador ou o dispositivo eletrônico pode ser o agente facilitador do crime, mas também pode ser o alvo dos ataques, nos casos de delitos praticados contra sistemas operacionais.

Deste modo, os estudiosos cuidaram de separar os crimes cibernéticos ou virtuais em três modalidades: os próprios, os impróprios, os mistos e os mediatos[9]. Os crimes cibernéticos próprios seriam os que possuem o fim de atacar exclusivamente o campo da tecnologia da

---

[6] Muitas vezes as próprias nações se valem deste mesmo método. É possível lembrar os célebres casos de espionagem pela NSA (Agência Nacional de Segurança dos EUA) envolvendo autoridades do mundo inteiro, inclusive do Brasil. Disponível em: <https://exame.abril.com.br/mundo/grampo-da-nsa-foi-muito-alem-do-celular-de-merkel/>; <http://g1.globo.com/politica/noticia/2015/07/lista-revela-29-integrantes-do-governo-dilma-espionados-pelos-eua.html>; <https://operamundi.uol.com.br/politica-e-economia/43303/wikileaks-revela-espionagem-dos-eua-a-netanyahu-berlusconi-e-ban-ki-moon>.Acesso em: 19 out. 2016.

[7] É possível incluir diversas outras camadas, que estariam nas profundezas do ciberespaço, mas esta representação é a mais comum.

[8] SHIMABUKURO, Adriana. Cibercrime: quando a tecnologia é aliada da lei. In: BRASIL. Tribunal Regional Federal da 3ª Região. Escola de Magistrados. **Investigação e prova nos crimes cibernéticos**. São Paulo: EMAG, 2017, págs. 20 a 21.

[9] JESUS, Damásio de; MILAGRE, José Antônio. **Manual de crimes informáticos.** São Paulo: Saraiva, 2016.

informação ou seja, buscam danificar os próprios elementos do computador, como seus dados, softwares[10], ou até a própria internet, ou podem ainda causar prejuízos externos ao sistema, depredando a máquina.

Já os impróprios podem ser definidos como aqueles que usam a *web* como instrumento para a prática de um delito já tipificado penalmente, que se voltam contra os bens jurídicos que não sejam os tecnológicos, servindo apenas como mais um meio de execução, não alterando o funcionamento do sistema informático da vítima. Temos como exemplo a ameaça (art.147 do Código Penal), os crimes contra a honra (arts. 138, 139 e 140 do Código Penal), o estelionato (art. 171 do Código Penal) e a violação de direito autoral (art. 184 do Código Penal).

No que tange aos crimes virtuais mistos, estes serão crimes complexos, em que além da proteção do bem jurídico informático – inviolabilidade dos dados –, existirá a proteção de outro bem jurídico, ou seja, existirão dois tipos penais distintos, cada um protegendo seu bem jurídico. Derivam do acesso não autorizado a sistemas informáticos, porém se exige uma tipificação mais apurada por ser a segunda conduta mais grave que o mero acesso não autorizado. Exemplo é o crime do art. 72, I, da Lei nº 9.504/97, que prevê que a obtenção de acesso a sistemas de tratamento de dados do serviço eleitoral a fim de alterar a apuração ou contagem de votos é crime punível com pena de reclusão de cinco a dez anos.

Por fim, os crimes mediatos se utilizam da rede como condição necessária para consumação do ilícito, ou seja, para conseguir chegar ao objetivo final é indispensável o acesso à internet, como nos casos em que o agente capta dados bancários e os utiliza para fazer transferências de fundo de uma conta para outra sem a ciência do titular da conta bancária. Neste caso, conforme entendimento do STJ em julgamento de conflito de competência[11] e pelo princípio da consunção, o infrator responderia somente pelo crime-fim,

---

[10] Sequência de comandos escritos em uma linguagem de programação a seres seguidos ou executados pelo computador, de modo que criarão ações dentro de um programa.

[11] Verifica-se a ementa do julgado: CONFLITO NEGATIVO DE COMPETÊNCIA. PENAL E PROCESSUAL PENAL. FURTO MEDIANTE FRAUDE. TRANSFERÊNCIA BANCÁRIA VIA INTERNET SEM O CONSENTIMENTO DA VÍTIMA. CONSUMAÇÃO NO LOCAL DA AGÊNCIA ONDE O CORRENTISTA POSSUI A CONTA FRAUDADA. COMPETÊNCIA DO JUÍZO SUSCITADO. 1. A Terceira Seção desta Corte Superior firmou o entendimento no sentido de que a subtração de valores de conta corrente, mediante transferência fraudulenta, utilizada para ludibriar o sistema informatizado de proteção de valores, mantidos sob guarda bancária, sem consentimento da vítima, configura crime de furto mediante fraude, previsto no art. 155, § 4º, inciso II, do Código Penal - CP. 2. O delito em questão consuma-se no local da agência bancária onde o correntista fraudado possui a conta, nos termos do art. 70 do Código de Processo Penal - CPP; no caso, na Comarca de Barueri/SP. Conflito de competência conhecido para declarar competente o Juízo de Direito da 1ª Vara Criminal de Barueri/SP, o suscitado.
STJ. CONFLITO DE COMPETÊNCIA: CC 145576. Relator: Ministro Joel Ilan Paciornik. DJ: 13/04/2016. STJ, 2009. Disponível em: <

qual seja, o crime de furto, do art. 155, §4°, II, do Código Penal. Contudo, não se confunde com a modalidade dos impróprios, pois, neste exemplo, além do crime de furto houve também a violação direta de dados informáticos. Todavia, o delito patrimonial é de maior gravidade frente à invasão cibernética, que acaba sendo absorvida.

2.1 Análise do *modus operandi* dos crimes cibernéticos e o perfil do agente

Conforme classificação proposta por Romano[12], os crimes cibernéticos estariam divididos em dois grandes grupos. O primeiro se resumiria em um delito com evento único, ou seja, ocorreria o ato somente uma vez com a vítima, sendo exemplos a manipulação de dados através de pirataria ou vírus, fraudes no setor bancário, e um dos mais conhecidos, o *phishing*, que será melhor abordado adiante.

Essa forma de delito é facilitada pelo uso de *malwares* para a prática de atividades ilícitas, como os Cavalos de Tróia[13], e, dispositivos vulneráveis, que não possuem proteção contra esses ataques – como os programas antivírus –, são os alvos mais comuns.

O segundo grupo seria composto por crimes como o assédio, pornografia envolvendo crianças, extorsão, espionagem e planejamento de atividades terroristas. Estes possuem as características da continuidade delitiva, em que o cibercriminoso pratica os eventos ilícitos repetidas vezes, em alguns casos ganhando a confiança da vítima para chegar ao seu objetivo final.

A ferramenta delitiva neste caso não é identificada como ilegal, uma vez que o transgressor se utiliza de salas de bate-papo, redes sociais, aplicativos de mensagens instantâneas, dentre outros meios para o cometimento do crime.

Uma famosa tática fraudulenta utilizada pelos criminosos é o *Phishing Scam*, termo utilizado para um tipo de armadilha onde estes enviam e-mails ou disparam mensagens em massa para dispositivos eletrônicos conectados à internet, contendo *links*[14] falsos que, ao acessá-los, os agentes poderão capturar informações sigilosas dos destinatários, como senhas e dados bancários[15].

---

https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ATC&sequencial=59818480&num_registro=201600556041&data=20160420&tipo=5&formato=PDF>. Acesso em: 10 out. 2019.

[12] ROMANO, Rogério Tadeu. **Convenção de Budapeste e Cibercrimes**. Revista Jus Navigandi, 2019 <https://jus.com.br/artigos/72969/convencao-de-budapeste-e-cibercrimes>. Acesso em: 02 out. 2019

[13] Disfarçados de software confiável, os Cavalos de Tróia são malwares (programas maliciosos) que permitem aos criminosos acessarem o sistema digital dos usuários, permitindo que estes espionem seus atos e roubem dados confidenciais.

[14] Elemento que quando é clicado pelo usuário, o encaminha para uma página na internet.

[15] BRASIL. Ministério Público Federal. 2ª Câmara de Coordenação e Revisão. **Roteiro de atuação: crimes cibernéticos**. 3.ed. Brasília: MPF, 2016. Série Roteiros de atuação, vol. 5.

Oriunda do inglês, a expressão se assemelha à *fishing*, que significa pesca. Os conteúdos das mensagens espalhadas costumam aguçar a curiosidade do destinatário, como oportunidades de sorteios, cursos, prêmios, dentre outros, que o levam a clicar no endereço. O transgressor costuma solicitar o preenchimento de algum documento em um sítio da internet, de modo que a vítima dê informações pessoais. Normalmente esse local possui aparência idêntica ao do sítio legítimo, artifício que permite a obtenção dos dados sem que a vítima desconfie do ilícito. Além disso, também é comum que se peça a instalação de um programa *malware,* que irá coletar dados que poderão ser usados em um golpe, como acessar contas bancárias, realizar compras e até retirar o rastreio de GPS de smartphones.

Para início da análise do *modus operandi* e das características do agente, é necessário traçar o perfil do cibercriminoso. Todavia, isso não é algo fácil de ser feito.

Grande parte dos crimes digitais hoje, se deve à sensação de anonimato, aumento das técnicas de práticas dos crimes e o despreparo das autoridades investigativas. Muitas vezes, os delitos de invasão são praticados por agentes que possuem forte ligação com o mundo da informática, seja porque trabalha na área, ou por *hobby*[16]. Este transgressor é conhecido popularmente por *hacker*. Contudo, esta nomenclatura não se refere ao criminoso digital, mas a alguém com grande conhecimento de computação, habilidade de programação, podendo ser um pesquisador ou profissional de tecnologia da informação que, de fato, possa fazer invasões, mas sem o *animus* de cometer um crime.

A denominação correta para o agente que possui a intenção de comer delitos cibernéticos é o *cracker*. Segundo Emanuel Alberto S. G. Gimenes[17]:

> Por sua vez, o termo cracker se refere às pessoas que possuem um grande conhecimento de programação e de segurança em sistemas de computação. Tais pessoas utilizam esse conhecimento para tirar vantagens pessoais, como destruição de sistemas por mero vandalismo ou aplicação de condutas para diversos fins ilícitos, como o estelionato eletrônico.

Considerando a expertise dos infratores e as características da rede, verificou-se a insuficiência de uma legislação que tratasse do tema apenas sob o plano interno dos países. Isso porque inevitavelmente haveria a possibilidade do agente explorar as fragilidades legais existentes em determinada nação, com o objetivo de assegurar sua impunidade. Diante dessa situação, se fez necessário o contato entre as autoridades a fim de que criassem normas

---

[16] Atividade praticada por prazer. Passatempo.

[17] GIMENES, Emanuel Alberto Sperandio Garcia. **Crimes virtuais**. Revista de Doutrina da 4ª Região, Porto Alegre, 2013.

internacionais que regulamentassem e garantissem a cooperação entre as nações no que tange a matéria.

2.2 Tentativas de regulamentação no plano internacional

Em âmbito internacional, é importante pontuar considerações sobre a "*Convention on Cybercrime".* Popular no português como Convenção sobre o Cibercrime ou Convenção de Budapeste (2001), foi celebrada no ano de 2001 e entrou em vigor três anos depois (2004), após cumprida a exigência de ter, no mínimo, cinco ratificações, sendo três de países integrantes do Conselho Europeu. Trata-se do primeiro tratado que abordou a temática em âmbito internacional.

O encontro na capital húngara possuía como principais objetivos o estabelecimento de regras e a intensificação da cooperação entre os Estados signatários do tratado, que buscariam uma política criminal comum e harmônica através da adoção de uma legislação internacional para combater a cibercriminalidade.

Segundo trecho da Convenção, retirado de seu preâmbulo (tradução livre)[18]:

> Convictos de que a presente Convenção é necessária para impedir os actos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta de desses sistemas, redes e dados, assegurando a incriminação desses comportamentos tal como descritos na presente Convenção, e da adopção de poderes suficientes para combater eficazmente essas infracções, facilitando a detecção, a investigação e o procedimento criminal relativamente às referidas infracções, tanto ao nível nacional como internacional, e estabelecendo disposições materiais com vista a uma cooperação internacional rápida e fiável.

Dividida em quarenta e oito artigos de fácil compreensão, a Convenção contém normas de direito material, direito processual e vários tópicos relacionados à cooperação internacional, que deverá ser desenvolvida em conformidade com as disposições apresentadas e demais acordos e instrumentos pertinentes, de forma a possibilitar uma busca de solução frutífera para os conflitos relacionados aos sistemas informáticos. Prevê a determinação da competência para investigação e punição de infrações penais, em que a escolha da jurisdição apropriada é facultada à escolha das partes. Aponta como basilar o auxílio mútuo entre as partes signatárias da convenção na apuração de crimes, podendo uma requerer à outra permissão para o acesso a dados que se encontram no sistema informático oposto.

[18] Traduzida para o português. Disponível em: <http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf> Acesso em: 01 out. 2019.

Há uma série de definições importantes em seu art. 1º, dentre as quais se destacam: sistema informático (que seria qualquer dispositivo, isolado ou em grupo, que desenvolve, executando um programa, o tratamento automatizado dos dados); dados informáticos (que pode ser qualquer representação de fatos, informações ou conceitos que são processados num sistema de computadores); fornecedor de serviços (que é qualquer entidade pública ou privada que possibilite a comunicação através de um sistema informático ou qualquer entidade que processe ou armazene dados em nome de um serviço de comunicação ou dos utilizadores deste) e dados de tráfego (que são todos os registros que são gerados através de navegações realizadas na rede).

O acordo foi firmado no âmbito do Conselho da Europa, possuindo adesão de mais vinte países como Ucrânia, Noruega, França, Lituânia, Croácia, além dos Estados Unidos da América, Japão e Austrália.

Contudo, o Brasil não aderiu à Convenção. Segundo declaração do Secretário Geral do Ministério das Relações Exteriores/Itamaraty do governo Lula, Samuel Pinheiro Guimarães Neto, o Brasil não poderia simplesmente aderir à convenção, pois dependeria de convite feito pelo Comitê de Ministros do Conselho da Europa. Ademais, como o país não participou das negociações, não foi possível incluir as percepções brasileiras no tratado que, por sua vez, foi elaborado em conformidade com as leis dos países signatários (SOUZA e PEREIRA; BRASIL, 2016). Nesse sentido, o art. 37 da convenção reforça:

> Após a entrada em vigor da presente Convenção, o Comité de Ministros do Conselho da Europa pode, depois de ter consultado os Estados contratantes da Convenção e de ter obtido o acordo unânime, convidar qualquer Estado não membro do Conselho e que não tenha participado na sua elaboração, a aderir à presente Convenção. [...]

A despeito desta previsão, a adesão é vista com bons olhos pelas demais autoridades brasileiras, que defendem a atuação diplomática junto ao Conselho da Europa para que o país possa fazer parte da Convenção. A CPI da Pedofilia no Senado abordou sobre a temática (CPI da Pedofilia, 2010, *apud* BRASIL, 2016):

> A Polícia Federal tem participado de encontros internacionais, mas o Ministério das Relações Exteriores, não. Eu já, por mais de uma vez, já provoquei o Ministério das Relações Exteriores nesse sentido, no sentido de que o Brasil faça adesão à Convenção de Budapeste, que trata desse assunto cibernético como um todo, como eles chamam, os países da Europa todos já assinaram, os Estados Unidos, o Canadá, o Japão; na América Latina o México e a Costa Rica também já se pronunciaram e o Brasil, não. (p.15, pronunciamento do Senador Eduardo Azeredo, em sessão de abertura da CPI)

> [...]
>
> Sobre a possibilidade de o Brasil se vincular à Convenção, lembramos o seguinte: (i) o Brasil não é membro do Conselho da Europa, não participou da produção do texto convencional e não goza do status de observador perante o Conselho; (ii) a Convenção está aberta à assinatura dos Estados-membros do Conselho, bem assim dos não membros que participaram da sua elaboração (África do Sul, Canadá, Japão, Montenegro e Estados Unidos da América); e (iii) a Convenção dispõe sobre a possibilidade de o Comitê de Ministros do Conselho da Europa (órgão de decisão política mais elevada que congrega os chanceleres dos países membros) convidar qualquer outro Estado para se vincular ao tratado, após obtenção do consentimento unânime dos Estados contratantes da Convenção (art. 37) 157. (p. 306 do relatório final).

O problema encontrado é que em um possível cometimento de um crime por um brasileiro em um sítio estrangeiro é que, sendo o servidor de internet de outro país, está fora do alcance da jurisdição brasileira[19], e, se o Brasil tivesse optado por ser membro da Convenção, devido à previsão de cooperação internacional entre seus signatários, aceleraria a investigação e possível punição dos agentes envolvidos.

É o que problematizam Fernanda Domingos e Priscila Röder[20]:

> [...] os operadores do Direito depararam-se com a perplexidade de não saber qual local teria jurisdição para decidir acerca do fornecimento de tais dados. Além disso, cada país possui uma percepção peculiar acerca da proteção da privacidade, o que se reflete nas diferenças legislativas sobre requisitos para fornecimento de dados e conteúdo.

Apesar do país ainda não ter aderido ao documento, é perceptível que suas disposições influenciaram diretamente em debates ocorridos no Congresso Nacional, que resultaram em projetos de lei que acabaram sancionados (caso da Lei nº 12.737/2012). A regulamentação da temática no plano interno, entretanto, ainda merece ser aprofundada. É, portanto, importante que ocorram avanços locais para que o país possa caminhar em direção a uma futura situação de conformidade com a Convenção.

---

[19] Insta frisar a regra da extraterritorialidade, prevista no Código Penal, que indica ficarem sujeitos à lei brasileira, embora cometidos no estrangeiro, os crimes praticados por brasileiro (art. 7º, II, b, do CP), e os praticados por estrangeiro contra brasileiro, fora do Brasil (art. 7º, §3º, do CP), se reunidas as condições do art. 7º, II, §2º, do CP. Todavia, no caso de crimes cometidos por brasileiros em sites estrangeiros, em que o provedor também seja estrangeiro, o problema reside no acesso das autoridades do Brasil aos dados constantes no sítio, uma vez que este não estará sujeito a jurisdição brasileira e poderá impor dificuldades no fornecimento das informações para fins de investigação.

[20] DOMINGOS, Fernanda Teixeira Souza; RÖDER, Priscila Costa Schreiner. Obtenção de provas digitais e jurisdição na internet**.** In: BRASIL. Tribunal Regional Federal da 3ª Região. Escola de Magistrados. **Investigação e prova nos crimes cibernéticos**. São Paulo: EMAG, 2017, p.63

2.3 Tentativas de regulamentação no Brasil

O Brasil, apesar das diversas tentativas de regulamentação que já propostas no Congresso Nacional, não foi capaz de produzir uma legislação que abarcasse satisfatoriamente essa nova modalidade delitiva, especialmente em relação aos crimes cibernéticos próprios. É certo que, quanto aos impróprios, o Código Penal cumpre essa função, pois o meio virtual seria apenas mais um meio de execução. Também se reconhece que as recentes alterações legislativas buscaram estabelecer a tipificação de algumas condutas.

Nesse sentido, registre-se importante avanço ocorrido no ordenamento brasileiro relacionado aos julgamentos dos crimes virtuais. Apesar de não versar sobre matéria penal, a aprovação do Marco Civil da Internet (MCI), disciplinado pela Lei nº 12.964/2014 vem regulando o uso do meio cibernético, preservando seu aspecto de ser um espaço acessível a todos, com autonomia na circulação de conteúdo, sem a ocorrência de censuras. A legislação é salutar na sistematização do abuso dessa independência, garantindo a individualidade e o respeito entre os internautas, retirando a ideia oriunda do senso comum de que a internet é um lugar "sem lei".

Em sua disciplina, o MCI prevê regras importantes como o dever de guarda dos registros de conexão[21], de acesso e de aplicações[22] gerados pelo usuário quando acessa a internet, indicando os prazos em que eles deverão ser mantidos salvos antes de serem descartados pelo provedor[23]

Quanto à provisão de conexão, o MCI estabelece que o provedor deverá armazenar os *logs*[24] pelo período de 01 (um) ano[25]. Por sua vez, determina que na provisão de aplicação, o armazenamento deverá ser de 06 (seis) meses[26].

Peritos em informática e especialistas em direito digital fazem críticas à exiguidade de tais prazos legais, pois o desaparecimento desses dados comprometeria uma possível investigação. Isso porque esses registros são fundamentais para a identificação do usuário que estava vinculado ao dispositivo eletrônico origem de um suposto crime[27].

---

[21] São dados informativos que ficam registrados de todas as conexões do usuário à rede.
[22] Registros de locais específicos que foram acessados pelo usuário.
[23] BRASIL. Ministério Público Federal. 2ª Câmara de Coordenação e Revisão. **Roteiro de atuação: crimes cibernéticos**. 3.ed. Brasília: MPF, 2016. Série Roteiros de atuação, vol. 5.
[24] Logs são registros de eventos dentro do sistema computacional, ou seja, tudo que foi acessado, navegado, baixado, está gravado em Log.
[25] Art. 13, *caput*, Lei nº 12.965/14.
[26] Art.15, *caput*, Lei nº 12.965/14.
[27] CAIADO, Felipe B.; CAIADO, Marcelo. Combate à pornografia infantojuvenil com aperfeiçoamento na identificação de suspeitos e na detecção de arquivos de interesse. In: BRASIL. Ministério Público Federal. 2ª Câmara de Coordenação e Revisão. **Crimes cibernéticos**. Brasília: MPF, 2018.

Além disso, apesar da inegável importância da inovação legislativa, o MCI carecia de regulamentação via decreto para o detalhamento de alguns pontos específicos. Deste modo, a presidenta da República à época editou o Decreto nº 8.771/16, que regulamentou a Lei nº 12.965/2014.

Todavia, a regulamentação acarretou em uma piora no cenário investigativo. O §1º do art. 11 do referido Decreto estabeleceu que "o provedor que não coletar dados cadastrais deverá informar tal fato à autoridade solicitante, ficando desobrigado de fornecer tais dados" (BRASIL, 2016). Ou seja, embora o MCI tenha estabelecido previsões importantes, seu Decreto regulamentador as relativiza, complicando ainda mais o procedimento de apuração dos crimes e deixando uma impressão de que fica a cargo do provedor cumprir ou não as previsões legais.

Noutro quadrante, importante salientar a previsão trazida sobre o alcance da responsabilidade civil por danos decorrentes de atividades realizadas por terceiros. O provedor de acesso é resguardado pelo art. 18 do MCI, que prevê a hipótese de exclusão de sua responsabilidade diante da prática perpetuada por estranhos. Todavia, o art. 19 do MCI apresenta exceção à regra: o provedor passará a ter responsabilização civil, ou seja, responder pela prática de um ato, acaso tome ciência de algum fato ilícito ocorrido por meio de exposição de algum material criminoso. Neste momento, após o recebimento de ordem judicial, ficará obrigado a retirar o conteúdo delituoso da rede.

Poderá, ainda, responder subsidiariamente, em casos de exposição de material de caráter privado sem autorização dos participantes – como vídeos com cenas de nudez –, por violação da intimidade se, após a percepção da notificação emitida pelo sujeito lesionado, deixar de promover a indisponibilização destes materiais.

Outra conquista respeitável foi a sanção da Lei nº 12.737/2012, conhecida na mídia como "Lei Carolina Dieckmann" – neste caso, avanço penal quanto à matéria. A normativa veio tipificar o crime de "invasão de dispositivo informático", acrescentando dois novos artigos ao Decreto-Lei nº 2.848/1940 – Código Penal, quais sejam, art. 154-A e art. 154-B, e alterando o texto dos arts. 266 e 298, a saber:

> **Invasão de dispositivo informático** (Incluído pela Lei nº 12.737, de 2012)
>
> **Art. 154-A**. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: (Incluído pela Lei nº 12.737, de 2012)

> [...]
>
> **Ação penal** (Incluído pela Lei nº 12.737, de 2012)
>
> **Art. 154-B**. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos. (Incluído pela Lei nº 12.737, de 2012)
>
> **Art. 266.** Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:
> Pena - detenção, de um a três anos, e multa.
>
> § 1 º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento. (Incluído pela Lei nº 12.737, de 2012)
> § 2 º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública. (Incluído pela Lei nº 12.737, de 2012)
>
> **Falsificação de documento particular**
>
> **Art. 298.** Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro:
> Pena - reclusão, de um a cinco anos, e multa.
>
> **Falsificação de cartão** (Incluído pela Lei nº 12.737, de 2012)
> Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito. (Incluído pela Lei nº 12.737, de 2012)

Porém, conforme acertada crítica trazida pelos autores Felipe Caiado e Marcelo Caiado[28] (2018):

> [...] não está pacificado nos tribunais o que é necessário que ocorra para caracterizar a violação indevida de mecanismo de segurança, conforme é definido no dispositivo legal, visto que nem sempre o usuário possui qualquer nível de segurança implementado ou que talvez seja inviável comprovar tal violação.

Até então, os delitos cometidos através da internet não possuíam previsão legislativa, e, com isso, não eram considerados crimes autônomos, exceto caso se assemelhassem a fatos comuns, já tipificados. Com a promulgação desta lei, foi dado o primeiro passo para a inibição de ações criminosas.

Todavia, com sua tramitação ocorrida em velocidade estranha ao habitual[29], a Lei se demonstrou atécnica por ter se valido de tipos penais abertos. Com isso, condutas que não

[28] CAIADO, Felipe B.; CAIADO, Marcelo. Combate à pornografia infantojuvenil com aperfeiçoamento na identificação de suspeitos e na detecção de arquivos de interesse. In: BRASIL. Ministério Público Federal. 2ª Câmara de Coordenação e Revisão. **Crimes cibernéticos**. Brasília: MPF, 2018, p. 14.

mereceriam reprimenda penal poderão ser enquadradas como crimes e, em contrapartida, diversas outras que deveriam ser criminalizadas não foram abrangidas pelas tipificações.

Sobre os tipos penais abertos, os eminentes juristas Damásio de Jesus e José Antônio Milagre corroboram[30]:

> [...] nota-se que grande parte dos tipos penais ali propostos apresenta redação significativamente aberta, e muitas vezes sob a forma de tipos de mera conduta, cuja simples prática – independentemente do resultado obtido ou mesmo da específica caracterização da intenção do agente – já corresponderia à consecução da atividade criminosa. Tal estratégia redacional, típica de uma sociedade de risco e de uma lógica de direito penal do inimigo, busca uma antecipação da tutela penal a esferas anteriores ao dano, envolvendo a flexibilização das regras de causalidade, a tipificação de condutas tidas como irrelevantes, a ampliação e a desproporcionalidade das penas e a criação de delitos de perigo abstrato, dentre outras características. Exemplo disso é a criação de um capítulo com o objetivo de tutelar juridicamente, como bem jurídico protegido, a "segurança dos sistemas informatizados". Tal estratégia, como já apontado, resulta na possibilidade de punição gravosa a meras condutas que, por sua natureza ou intenção, não mereceriam ensejar a repressão penal – como o acesso não autorizado a sistemas informáticos decorrentes de testes de segurança efetuados sem a prévia anuência dos titulares de sistemas informatizados.

Por outro lado, com relação à insuficiência dos tipos penais, em depoimento à Comissão Parlamentar de Inquérito dos Crimes Cibernéticos, delegados e membros do Ministério Público enfatizaram:

> [...] essas autoridades informaram que o simples uso de dispositivos por terceiros, mesmo que sem autorização, não caracterizaria crime, na visão dos juízes. Ademais, a simples quebra de sistemas de segurança ou, ainda, a alteração de páginas de internet – a chamada pichação virtual – ou de perfis nas redes sociais não configurariam automaticamente crime, de acordo com a redação dada.

Mesmo assim, apesar de ser uma legislação incompleta, carente de previsões, nascida de uma forte comoção social e pressão midiática, pode-se afirmar que o Brasil já possui tipificações penais específicas sobre crimes cibernéticos, que abarcam detalhes importantes e próprios desta modalidade delituosa.

---

[29] O Projeto de Lei 2793/2011 foi apresentado pela Câmara dos Deputados em 29 novembro de 2011 e sancionado pela ex-presidenta Dilma Rousseff em 30 de novembro de 2012, se transformando na Lei Ordinária nº 12737/2012. Ganhou impulso especial a partir do mês de maio de 2012, com o vazamento das fotos da atriz Carolina Dieckmann, obtidas por meio da atuação de um hacker. Os dados sobre a tramitação estão disponíveis em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=529011>. Acesso em: 21 out. 2019.

[30] JESUS, Damásio de; MILAGRE, José Antônio. **Manual de crimes informáticos.** São Paulo: Saraiva, 2016, p. 74.

2.4 Crimes cibernéticos mais comuns no Brasil

Sendo a internet um paraíso de informações, de conteúdo, e de livre acesso às pessoas, inevitavelmente, será alvo da criminalidade. Com o objetivo de infringir a lei penal, utilizando-se do recurso de anonimato para não serem reconhecidos, os transgressores praticam os mais diversos delitos com o uso da rede.

Em recente sistematização publicada pelo Superior Tribunal de Justiça em seu sítio eletrônico[31], foram apresentados os crimes cibernéticos que mais comumente são julgados pelo tribunal. A Corte alegou estar sendo constantemente procurada para apresentar a correta interpretação das normas infraconstitucionais em relação aos ilícitos praticados por meio da rede. Em sua maioria, a publicação indicou crimes cibernéticos impróprios, em que a internet é utilizada como um meio para a prática do delito.

Foram citados os delitos de extorsão (art. 158 do CP), furto mediante fraude (art. 155, §4º, II, do CP) e ameaça (art. 147 do CP), bem como golpes praticados no comércio online que caracterizam crime contra a economia popular (art. 2º, IV, da Lei 1.521/51).

A extorsão envolve a obtenção de materiais pessoais (fotos e vídeos) por meio da internet e a exigência do pagamento de certa quantia para que o conteúdo não seja revelado.

Já o furto eletrônico se caracteriza em sua modalidade cibernética pela subtração de valores de conta corrente da vítima mediante transferência bancária fraudulenta com dados obtidos pela internet.

Concernente à ameaça, esta se intensificou com a possibilidade de anonimato para intimidar as vítimas, aterrorizadas com a promessa de praticar um mal contra suas vidas, se estendendo até a vida de seus familiares. Uma das formas de seu cometimento é através do *cyberbulling*[32].

---

[31] BRASIL. Superior Tribunal de Justiça. **Crimes pela internet, novos desafios para a jurisprudência**, 2018. Disponível em: < www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias-antigas/2018/2018-06-17_06-57_Crimes-pela-internet-novos-desafios-para-a-jurisprudencia.aspx> Acesso em: 10 out. 2019.

[32] Derivado da conduta denominada "*bullying*", que corresponde à prática de diversas condutas violentas e repetitivas, sejam físicas e/ou psicológicas, com intenção de ofender, magoar e humilhar a vítima, o *cyberbullying* é o cometimento do *bullying* no ambiente digital.
Conforme explica CALHAU (2010, p. 6), "não existe uma tradução exata para a palavra. *Bullyng* é um assédio moral, são atos de desprezar, denegrir, violentar, agredir, destruir a estrutura psíquica de outra pessoa sem motivação alguma e de forma repetida"
O autor registra ainda que o *bullying* pode ser conhecido como assédio moral, *mobbing* (Noruega e Dinamarca), *mobbining* (Suécia e Finlândia), *harassment* (EUA), *acoso* (Espanha), e define *cyberbullying* como aquele que "ocorre com a utilização de meio eletrônico como instrumento de agressão no bullying"[32].
Aproveitando-se da distância física que separa os usuários da internet, os agentes intimidam, menosprezam, divulgam imagens e fazem piadas com o jeito, a aparência, as roupas, o sotaque da pessoa ofendida. Além disso, fazendo uso do recurso do anonimato, a identificação do infrator torna-se dificultosa, pois se furta de perfis falsos, *nicknames*[32] e redes de proteção da *Deep* e *Dark Web*.

Com relação aos golpes praticados no comércio online, pode ser citada uma classificação proposta por Gustavo Corrêa[33]. Segundo ele, as fraudes na rede poderão ser separadas em três espécies: mercadorias físicas, mercadorias digitais, e serviços ou mercadorias publicadas.

As mercadorias físicas envolveriam a compra e venda de produtos físicos através da internet, em que os objetos oferecidos seriam advindos de furtos, descritos no anúncio de maneira adulterada ou ainda oferecido por um vendedor que não possui ligação com a empresa que alega prestar serviço.

No que concerne às mercadorias digitais, elas abarcariam o comércio de bens intangíveis, como jogos de computador, imagens, programas, *softwares*, dentre outros. Neste tipo de fraude, o consumidor paga pelo produto, mas na hora de recebê-lo virtualmente ocorre algum erro na transmissão, ou simplesmente não ocorre o envio.

Já os serviços ou mercadorias publicadas estariam relacionados aos próprios conteúdos da *web*. Quando o usuário quer acessar um site em que este acesso exige pagamento, o criminoso utiliza-se deste requisito para perpetuar crimes. Ou seja, o criminoso prometerá um tipo de conteúdo disponível, porém, o consumidor ao quitar o valor e verificar o site, irá se deparar com um produto diferente do que lhe foi prometido, ou até a inexistência de produto.

A sistematização do STJ está longe de ser considerada exaustiva. Além dos citados pelo Egrégio Tribunal, poderiam ser abordados exemplificativamente muitos outros delitos, a exemplo dos crimes de violação de direitos autorais[34] (art. 184 do Decreto-Lei nº 2.848/40 - Código Penal), crimes contra a honra e lavagem de dinheiro. De todo modo, é importante para conhecermos os delitos mais frequentes com os quais a Justiça se depara e, com isso, buscar técnicas investigativas capazes de promover a identificação dos agentes com a justa repressão ao ilícito.

Em grande parte dos casos, é complicado de se voltar rapidamente ao estado emocional anterior ao oferecimento dos insultos, haja vista que uma vez publicado um conteúdo na rede mundial de computadores, é extremamente difícil que ele não se dissemine, tornando praticamente impossível a total retirada de circulação do material ultrajante, postergando o sofrimento da vítima.

[33] CORRÊA, Gustavo Testa. **Aspectos jurídicos da internet**. 5.ed. rev. e atual. – São Paulo: Saraiva, 2010, p. 70.

[34] Consoante art. 18 da Lei n º 9.610/98, que regulamenta os direitos autorais no Brasil, esse direito é conferido ao autor de uma obra, seja ela científica, artística ou literária, que possuirá a prerrogativa de transmitir e comercializar seu conteúdo. Assim, o delito ocorre quando se disponibiliza o material produzido por alguém sem a devida autorização, não sendo necessário que este possua registro para que se configure a violação.

Já o art. 7º traz que "são obras intelectuais protegidas as criações do espírito, expressas por qualquer meio ou fixadas em qualquer suporte, tangível ou intangível, conhecido ou que se invente no futuro". Neste cenário, presente no texto a proteção a obras em meio imaterial, restarão incluídas as páginas da internet, que são normalmente tratadas como "terra sem lei", com constantes e displicentes reproduções de seu conteúdo.

3. OS MÉTODOS DE INVESTIGAÇÃO DOS CRIMES CIBERNÉTICOS

Acompanhando o desenvolvimento da tecnologia e o vertiginoso crescimento dos crimes cibernéticos, os órgãos encarregados da persecução penal no país devem buscar meios para a implementações de condutas preventivas, a fim de estreitar os caminhos para a consumação do ato ilícito.

Utilizando da divisão feita pelo Ministério Público Federal, em seu Roteiro de Atuação contra crimes cibernéticos[35], dos métodos utilizados pela ciência forense para investigação de crimes cometidos através da internet, podemos concluir que existem quatro passos: o de aquisição, o de preservação, o de análise e o de apresentação das evidências. Obviamente, em cada uma dessas etapas haverá diversos procedimentos, praticados por diversos agentes da persecução penal, como autoridades policiais e o *Parquet*. Além disso, cada uma delas consistirá em um exercício do contraditório, dando a possibilidade ao acusado de se defender da conduta que lhe estiver sendo imputada, o que torna comum a repetição de algumas dessas fases, como a de aquisição e a de análise de provas.

Ainda citando o Roteiro oferecido pelo MPF[36], é importante que as evidências – além do modo como são coletadas e armazenadas – possuam certas características para que possam ser juridicamente válidas e relevantes para a investigação sobre o suposto crime digital.

Inicialmente, deverá ser a prova admissível, ou seja, estar de acordo com a lei, não podendo ser, por exemplo, uma prova adquirida de forma ilícita ou irregular. Além disso, devem ser autênticas, o que quer dizer que deverão possuir clara ligação com o crime investigado. Os documentos devem ser completos, confiáveis e convincentes, ou seja, possuir um arcabouço completo sobre o evento delituoso, desprendida de incertezas acerca de sua autenticidade e também deverá ser documentada, sendo juntada ao processo de forma cristalina e organizada.

Sendo que os crimes digitais são delitos que deixam rastros, estes vestígios poderão ser os *logs* de acesso e de conexão[37] dos usuários da rede e seus endereços IP privados – *logs* estes que deverão ser guardados pelos provedores –, que serão captados através da ferramenta *whois*[38]. Este é um dos principais meios para descobrir a autoria de um delito, pois é após a

---

[35] BRASIL. Ministério Público Federal. 2ª Câmara de Coordenação e Revisão. **Roteiro de atuação: crimes cibernéticos**. 3.ed. Brasília: MPF, 2016. Série Roteiros de atuação, vol. 5, p. 159.
[36] *Ibidem*, p. 159.
[37] O log de conexão consiste em um conjunto de informações gerados com a utilização da internet pelo usuário. Já o log de acesso é o responsável por dados sobre a utilização de um serviço específico pelo navegante.
[38] Base de dados que fornecerá informações do responsável pelo registro de um endereço IP na internet.

análise do registro/*log* e das informações geradas pelo acesso à internet que se poderá chegar ao sujeito praticante. É o que reforçam Fernanda Domingos e Priscila Röder[39]:

> O funcionamento correto dessa rede obedece a critérios organizacionais matemáticos, que permitem a fluidez dessa estrutura. Isto significa que as empresas provedoras de Internet detêm as informações referentes aos passos que os usuários percorrem na rede: acessos, postagens e comunicações.
> São essas informações que em geral permitem, de forma precisa, desvendar um crime cibernético ou obter uma prova digital para elucidar um crime real. O que tem aturdido o mundo jurídico é a obtenção dessas informações, desses dados que consubstanciam a prova digital.

O Marco Civil da Internet veio com o escopo de determinar diretrizes para atuação das autoridades e acaba por dar suporte aos procedimentos de investigação. Com finco de tornar possível o processo de apuração sobre o cometimento de um delito, a normativa prevê que o provedor deverá armazenar os *logs* de conexão pelo período de 1 (um) ano, e os *logs* de acesso à aplicativos por 6 (seis) meses, disponibilizando-os somente quando requeridos por ordem judicial.

Porém, esse prazo se demostra muito curto e ineficaz para fins de uma investigação criminal completa, e, a fim de tentar solucionar possíveis problemas, o MCI faculta ao Ministério Público a possibilidade de requerer cautelarmente ao provedor que os registros sejam guardados por prazos superiores aos previstos nos *caputs* dos artigos 13 e 15 da lei[40].

---

[39] DOMINGOS, Fernanda Texeira Souza; RÖDER, Priscila Costa Schreiner. Obtenção de provas digitais e jurisdição na internet**.** In: BRASIL. Tribunal Regional Federal da 3ª Região. Escola de Magistrados. **Investigação e prova nos crimes cibernéticos**. São Paulo: EMAG, 2017, p.63.

[40] Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
§ 1º. O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.
Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.
[...]
§ 2º. A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no caput.
Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.
[...]
§ 2º. A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no caput, observado o disposto nos §§ 3º e 4º do art. 13.

Conforme preceitua a 2ª Câmara de Coordenação e Revisão do Ministério Público Federal, em seu Roteiro de Atuação de combate aos Crimes Cibernéticos (2016):

> O MCI faculta que o Ministério Público possa requisitar dados cadastrais e que as prestadoras de serviço na Internet tenham a obrigação de guardar dados de conexão por um período razoável, a fim de facilitar o rastreamento do domicílio digital do suspeito.
> Por suposto, essa abertura de informações particulares exigirá uma postura vigilante a respeito da responsabilidade civil na liberação dos dados.
> Eis aqui um ponto crítico. O acesso a dados apenas mediante ordem judicial pode "burocratizar" as investigações, haja vista o lapso entre se pedir algo ao juiz e o tempo da efetiva resposta.

A fim de descobrir a autoria de um delito, a inspeção dos registros de acesso e de conexão iniciará de modo a descobrir de qual computador está sendo realizada a conduta criminosa. Para isso, são necessários os dados de *Internet Protocol*.

Conhecido como endereço IP, *Internet Protocol* é um protocolo que carrega uma base de dados composta de dígitos que representam um dispositivo conectado à uma rede de computadores. Devido à problemática de identificar um usuário por suas identidades ou quaisquer outros documentos pessoais, pelo perigo de um criminoso se utilizar dos dados para se passar por ele e cometer delitos, utilizam-se os endereços IP para identificar o dispositivo e seu utilizador. Para garantir que não exista mais de um endereço IP na rede, eles são distribuídos em uma estrutura organizacional hierárquica de alocação de endereços, fornecendo um IP a cada *host*[41].

Além dos endereços públicos, muitos computadores utilizam-se de endereços privados, os quais são invisíveis e "inalcançáveis" na rede. Isso ocorre porque alguns provedores de conexão[42], utilizando-se de seus endereços públicos, conseguem disponibilizar diversos outros IP's privados aos consumidores.

Esta privacidade traz a redução de possíveis invasões dos computadores por outros internautas e dos custos para os provedores de acesso uma vez que com um endereço público possibilitam diversos endereços privados.

Todavia, essa facilidade para os internautas e para os provedores não é a mesma para as autoridades investigativas. Com a dificuldade de alcance – em um primeiro momento – desses endereços, é necessário requerer a quebra de sigilo do endereço público que está

[41] Dispositivo conectado à rede de internet, que possui seu endereço IP único.
[42] Chamado de provedor de acesso ou provedor de conexão, é pessoa jurídica fornecedora de serviços que possibilita o ingresso dos consumidores à internet.

possibilitando o acesso de diversos endereços privados, o que dificulta a individualização de cada usuário, e, consequentemente, na identificação de um possível cibercriminoso.

Conhecido o objeto primário de uma investigação – podendo ser uma página fraudulenta da internet, ou um perfil de um usuário em uma rede social –, começarão as buscas, inicialmente, pelas informações disponibilizadas em locais públicos. Em muitos casos, somente os dados que são divulgados abertamente já são suficientes para a resolução do problema. Porém, em muitos outros será necessário o uso de técnicas para coleta dos dados privados, que carecerão de autorização judicial, como a infiltração em sistemas, interceptação telemática e telefônica[43], dentre outros. O material arrecadado em um desses acessos poderá aclarar rapidamente elementos fundamentais de uma investigação.

Uma relevante forma de captação de indícios de um crime cibernético – quando praticado através de e-mail – é examinando a correspondência virtual. Além do conteúdo da mensagem, endereço de e-mail do remetente e do destinatário, elas trazem informações como o endereço de IP do computador que disparou a mensagem, e, o mais importante para a finalidade da investigação, é o campo *Received*.

O cabeçalho do correio eletrônico contém dados que instruem os computadores a processá-los, o que possibilita a reconstituição do caminho percorrido pela mensagem de seu envio até o recebimento pelo destinatário. O manual oferecido pelo MPF detalha:

> [...] Em geral a análise dos campos Received possibilita ao investigador conhecer todo o caminho percorrido pela mensagem. Uma mensagem de email pode passar por diversos servidores até chegar ao computador de destino. Toda vez que a mensagem passa por um servidor, este adiciona um novo Received: com informações sobre a origem, data e próximo destino da mensagem. Embora possa conter alterações, o campo Received: usualmente possui o seguinte padrão (geralmente não respeita as quebras de linha abaixo, forçadas aqui para melhor compreensão):
> Received: from <servidor de origem>by <servidor que recebeu esta mensagem> with <protocolo usado na transferência> id <identificador único da mensagem>for <endereço de email do destinatário>;<data/hora em que foi recebida pelo servidor>[44].

No cenário do crime, onde os agentes se aproveitam de todos os recursos para fraudá-los e forjá-los com o escopo de não serem descobertos, estes cabeçalhos podem ser adulterados, possibilitando golpes como o *phishing scam*[45] e a disseminação de vírus. Na hipótese de um e-mail manipulado, o destinatário deverá atentar a erros da língua portuguesa

[43] Consiste em captar o conteúdo ou o teor de uma comunicação feita através de um sistema de informática, como celulares e computadores.
[44] BRASIL. Ministério Público Federal. 2ª Câmara de Coordenação e Revisão. **Roteiro de atuação: crimes cibernéticos**. 3.ed. Brasília: MPF, 2016. Série Roteiros de atuação, vol. 5, págs. 193 e 194.
[45] Vide tópico 2.1

que costumam ser praticados pelos criminosos, ao conteúdo da mensagem que por vez possua alguma obrigação a ser cumprida, incentivando a vítima a clicar num endereço que a levará para um portal, e lá possivelmente terá uma armadilha que captará dados pessoais e bancários. Ademais, é costumeiro recorrerem à impessoalidade, utilizando de pronomes de tratamento como "senhor" e "senhora", já que os e-mails são enviados a um número indeterminado de pessoas para que as chances de êxito do delito sejam maiores.

Após iniciadas as buscas pelo endereço do agente delitivo, diante da suspeita do cometimento de crimes cibernéticos ou com base nas informações angariadas dos provedores de conexão e acesso, podem as autoridades requerer mandados de busca e apreensão no local da infração[46], que serão cumpridos pela Polícia Federal ou pela Polícia Civil – dependerá da repercussão da infração, se será intermunicipal, interestadual ou internacional[47] – para a coleta de provas e vestígios que possam esclarecer os fatos, como computadores, *notebooks*, *tablets*, *smartphones*, entre outros. Recolhido o material, proceder-se-á ao registro no auto de busca ou em documento apartado dos procedimentos realizados para a análise da perícia do conteúdo dos objetos recolhidos[48].

Mas não estará tudo resolvido quando for descoberto o endereço do computador que foi instrumento do fato típico. Isso porque o uso de muitos dispositivos é compartilhado por diversas pessoas, dentro de uma mesma família ou até em locais de acesso público, como *Lan Houses*[49]. Sendo assim, a dificuldade de localização do agente é imposta às autoridades, que deverão precisar a pessoa que efetivamente utilizou o computador para a prática do crime.

Adquiridas as provas, estas deverão ficar guardadas para futura vistoria. Isso porque o domicílio digital é um ambiente de fácil adulteração de dados e de grande facilidade de serem perdidos. Assim, deve ser ressaltada a importância da coleta e preservação das evidências desses delitos, uma vez que são extremamente voláteis.

---

[46] O lugar do crime é um ponto que merece enfoque. O Código Penal prevê em seu art. 6º que é considerado o local do crime onde ocorreu a ação ou omissão, bem como onde se produziu ou deveria se produzir o resultado. Já no que tange a competência para processar e julgar o delito informático, será do juízo do foro do lugar de cometimento da infração, consoante art. 69, inciso I, do Código de Processo Penal. Assim, o juízo de onde foi praticada a conduta será o competente para a causa. Contudo, por vezes essa determinação encontra problemas, uma vez que os delitos virtuais normalmente são praticados de vários locais, o que dificulta a delimitação da competência.

[47] Art. 144, §1º, da Constituição Federal: A polícia federal, instituída por lei como órgão permanente, estruturado em carreira, destina-se a: I - apurar infrações penais contra a ordem política e social ou em detrimento de bens, serviços e interesses da União ou de suas entidades autárquicas e empresas públicas, assim como outras infrações cuja prática tenha repercussão interestadual ou internacional e exija repressão uniforme, segundo se dispuser em lei; [...] §4º. Às polícias civis, dirigidas por delegados de polícia de carreira, incumbem, ressalvada a competência da União, as funções de polícia judiciária e a apuração de infrações penais, exceto as militares.

[48] Insta frisar que as leis que tratam sobre os crimes cibernéticos não preveem a hipótese deste instrumento cautelar, o que, deste modo, impõe-se a aplicação do Código de Processo Penal, em seu art. 240 e seguintes.

[49] Estabelecimentos comerciais que locam computadores para acesso à internet, devendo o usuário pagar pelo tempo que utilizar a máquina.

Diante da complexidade na inspeção das provas digitais – em que o exame poderá demorar meses –, os *sites* poderão vir a ser modificados ou até excluídos com o tempo, o que ocasionaria a ruína do procedimento investigatório. Desta feita, é necessária a preservação do local.

Uma metodologia eficiente é realizar *snapshots*[50] de seu conteúdo para manter o registro do maior número de informações possíveis. Com essa ferramenta, serão armazenados dados da página investigada, com a data e a hora em que foi feito o registro da imagem, o que torna possível uma futura comparação com modificações que possam vir a ser feitas a fim de adulterar as evidências. Além disso, poderá se obter arquivos que foram lançados por engano no *site* e que foram rapidamente tirados, garantir lastro probatório sem depender do provedor para disponibilizá-los e ainda a otimização no estudo dos indícios por estarem todos catalogados.

Lado outro, em casos que o *site* já estiver sido removido, o investigador terá poucas saídas, seja a de solicitar o conteúdo ao denunciante – imaginando que este tenha realizado um *snapshot* do conteúdo –, ou requerer ao provedor responsável a liberação dos registros, o que é um processo complicado pois demanda a expedição de ordem judicial, e o cenário se agrava quando este provedor for estrangeiro, uma vez que não será regido pelas normas brasileiras.

Para isso, na fase de análise dos documentos, as investigações irão demandar, por excelência, da ajuda de perícia técnica de informática, que realizará uma extração de dados dos computadores aplicando filtros para obter os resultados desejados, que serão evidências do suposto crime e poderão servir de prova da materialidade, além de ajudar na elaboração do convencimento do juízo sobre o conteúdo ilícito e o método empregado para se cometer o crime[51]

Assim, neste momento da investigação, dar-se-á a apresentação de todas as evidências digitais até então colhidas, juntando-as com o fim de preparar um arcabouço probatório capaz de construir um contexto linear e consistente sobre os fatos ocorridos no suposto delito cibernético.

---

[50] Produção de uma imagem através de uma foto instantânea tirada de uma tela de computador ou celular em um determinado instante.

[51] CARNEIRO, Márcio Rodrigo de Freitas. Perícia de informática nos crimes cibernéticos. In: BRASIL. Tribunal Regional Federal da 3ª Região. Escola de Magistrados. **Investigação e prova nos crimes cibernéticos**. São Paulo: EMAG, 2017p. 33-53.

Consoante orientações propostas pelo Roteiro de Atuação do Ministério Público Federal para o exame destes indícios[52], o relatório apresentado deverá conter informações como: a identificação do processo ou do inquérito, o solicitante, quem elaborou, a origem dos dados, como foram coletados, a garantia de sua integridade, a exposição de como ocorreram os procedimentos de análise dos indícios, dizendo qual foi o método empregado pelos peritos, e ainda indicando qualquer possível avaria ou ausência de conteúdo que se demonstraria fundamental no exame da prova, e que por sua vez deveria estar presente nos materiais analisados. Por fim, deverá realizar a explicação da conexão encontrada entre as evidências e as hipóteses levantadas para o crime, fornecendo mídia digital com todos os registros relevantes.

Contudo, consoante as previsões do Marco Civil, é proibida a interceptação das comunicações dos usuários da internet (exceto para fins de investigação), sendo possível somente a guarda dos *logs* que poderão ser fornecidos mediante ordem judicial, para, aí sim, ocorrer a quebra do sigilo das mensagens[53].

A autoridade policial ou administrativa e o Ministério Público, como já mencionado, poderão requerer aos provedores a dilatação do tempo de guarda dos registros – uma vez que o prazo curto de um ano muitas vezes impossibilita a realização de uma investigação processual completa – , porém não podem contactá-los diretamente para adquirir os dados desejados (art. 13, §5º e art. 15, §3º, da Lei nº 12.965/14) . Além da previsão do MCI, verifique-se o rol das atribuições do MPU, constantes na LC nº 75 de 20 de maio de 1993:

> Art. 6º. Compete ao Ministério Público da União:
>
> [...]
>
> XVIII - representar;
>
> a) ao órgão judicial competente para quebra de sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, para fins de investigação criminal ou instrução processual penal, bem como manifestar-se sobre representação a ele dirigida para os mesmos fins;

Como explicita Milagre (2014, p. 1), citado por Damásio de Jesus e José Antônio Milagre (2016, p. 189), "em relação ao requerimento de guarda de dados por mais tempo do

---

[52] BRASIL. Ministério Público Federal. 2ª Câmara de Coordenação e Revisão. **Roteiro de atuação: crimes cibernéticos**. 3.ed. Brasília: MPF, 2016. Série Roteiros de atuação, vol. 5., p. 175.

[53] Impende mencionar que acessar o conteúdo de aparelhos telefônicos, quando seu manuseio foi ocasionado por mandado legítimo de busca e apreensão, não se configura interceptação.

que o legal, a ser feito pelo Delegado ou Ministério Público, a lei complica a vida destas autoridades, exigindo que tal requerimento seja judicial".

Identificado o autor, a autoria do crime deverá constar na narrativa dos autos para que ele possa ser citado e ter conhecimento de que está sendo processado, podendo então apresentar defesa observando sempre o devido processo legal, o contraditório e a ampla defesa.

4. A NECESSIDADE DE APRIMORAMENTO DO PROCEDIMENTO INVESTIGATÓRIO E DE ESTÍMULO À PREVENÇÃO DOS DELITOS CIBERNÉTICOS

O crime virtual, por padecer da volatilidade de suas provas, necessita de atenção e aprimoramento nas técnicas dos procedimentos investigatórios. Com o passar dos anos, os delitos se modernizam e a perícia forense e as autoridades policiais e judiciárias precisam se atualizar em questões de tecnologia para que seja possível, de forma efetiva, a aplicação das normas até então sancionadas e pressionar a atuação da criminalidade para proporcionar uma sociedade da informação mais segura.

Nas provas virtuais, quando de sua colheita e preservação, é indispensável que sejam confiáveis, reproduzíveis e, neste cenário, para serem aceitas juridicamente e serem utilizadas num processo, devem passar por rigorosa perícia técnica.

Consoante as previsões do Código de Processo Civil que tratam da perícia, o trabalho pericial é acionado quando a prova do fato depender de conhecimento específico e técnico (art. 156 do diploma legal mencionado). Assim, conclui-se que este serviço demanda constante estudo e atualização, pois o laudo da busca realizada é fundamental para esclarecimento de fatos dentro de uma investigação.

Conforme conclui Carneiro[54], com a crescente utilização da internet, o número de peritos teve que ser redobrado. Pelo tempo que se gasta na análise das evidências e pela complexidade de seu conteúdo, uma boa estratégia para melhorar a escassez de mão-de-obra é aumentar o número de profissionais. Além destes, a capacitação de policiais de todos os cargos para o conhecimento das normas de informática e dos procedimentos a serem realizados como em buscas e apreensões são essenciais.

---

[54] CARNEIRO, Márcio Rodrigo de Freitas. Perícia de informática nos crimes cibernéticos. In: BRASIL. Ministério Público Federal. 2ª Câmara de Coordenação e Revisão. **Roteiro de atuação: crimes cibernéticos**. 3.ed. Brasília: MPF, 2016. Série Roteiros de atuação, vol. 5, p. 52.

Se demonstra imperativo também a redução do número de aparelhos digitais apreendidos. Isso porque, ao invés de realizar uma busca dirigida aos objetos mais importantes – os que de fato puderem terem sido utilizados na prática do crime – ocorre uma caça coletiva a todos os materiais, se dispersando dos mais específicos e sobrecarregando o trabalho da perícia.

Para abordar outros importantes pontos a serem melhorados pelo procedimento investigatório, valho-me das análises feitas pela Comissão Parlamentar de Inquérito sobre crimes cibernéticos, que se revelam fundamentais para um maior controle da atuação criminosa.

É de observar que, em muitos casos, a postura das vítimas na utilização da internet contribui para os crimes. Há grande desatenção com a segurança dos dispositivos, em que a ausência de uso de programas antivírus e a exposição de informações sigilosas em *sites* não seguros são algumas das causas. Nestes dois casos, abrem-se portas para a entrada de *malwares*, vírus, ocorrências de fraudes bancárias e furtos. Deste modo, congruente ao disposto na CPI, a segurança da internet passa pela educação dos internautas.

Nas investigações da Comissão, restou demonstrada a falta de estrutura das polícias estaduais para tratar do assunto, com a escassez de agentes e de equipamentos, sendo o motivo a conhecida carência de recursos do Estado para o setor.

Ademais, uma falha cometida pelas operadoras de telefone é crucial para os delitos virtuais. Quando se adquire um chip para utilização de créditos pré-pagos, basta colocar um número de CPF. Isto facilita o acesso de criminosos a diversos aparelhos, podendo habilitar uma linha de celular e navegar na internet, abrindo contas e criando perfis em diversos aplicativos sem ser identificado.

Avanço importante ao Brasil seria a adesão às convenções internacionais. Isso porque elas possuem o objetivo de criar uma harmonia entre os governos em busca de solidariedade no enfrentamento aos crimes virtuais. Se o Brasil tivesse participado das negociações como membro da Convenção da Budapeste, tratada anteriormente neste artigo, devido à previsão de cooperação internacional entre seus signatários, tornaria mais fácil a investigação dos delitos.

Apesar de não ser signatário da Convenção Sobre o Cibercrime, importante citar a existência de tratados bilaterais de cooperação. Neste sentido, evidencia-se o acordo existente entre o Brasil e o governo dos Estados Unidos da América. Chamado de Acordo de Assistência Judiciária em Matéria Penal (MLAT), datado de 14 de outubro 1997, o MLAT

estabelece que os países se obrigam a prestar assistência mútua em matérias relacionadas a investigações, inquéritos, ações penais e prevenção de crimes[55].

No que tange aos crimes cibernéticos, estão presentes no acordo disposições sobre entrega de documentos e busca a apreensão que se aplicam diretamente a aquisição de dados que estejam em posse de particulares ou entes administrativos. Um dos problemas maiores das investigações brasileiras é para a obtenção dos registros/*logs* mantidos por provedores estrangeiros. Com o MLAT, é possível executar contra o Estado Requerido mandado de busca, apreensão e entrega de bens ao Estado Requerente, desde que o pedido contenha informações que justifiquem tal atitude. Isso serve para que o demandado possa verificar se a decisão objeto do pleito de cooperação viola direito de seus cidadãos, o que impõe que qualquer proposta que busque diminuir a burocracia e facilitar os procedimentos de cooperação internacional sejam sempre cautelosas com a explicação da finalidade para que uma prova esteja sendo requerida. Independente dos entraves, os acordos bilaterais se mostram importantes passos para uma futura harmonização entre os países do globo concernente ao combate aos crimes virtuais.

Segundo Fabrízio Roza[56]:

> É imperioso frisar, por derradeiro, que nenhum combate sério aos 'crimes de informática' se esgota no processo tipificador. Sem cooperação internacional, sem a melhoria do aparelhamento policial e sem o aperfeiçoamento profissional dos que operam nessas áreas, a simples existência de uma adequada tipificação não tem o menor significado prático e não basta para tutelar a sociedade contra tão lesiva atividade criminosa.

Dessarte, conclui-se imperioso o investimento estatal na estrutura da polícia e dos órgãos de persecução penal para que obtenham maiores e melhores resultados no desfecho das investigações, contratando também peritos para análise das evidências colhidas, uma vez que são fundamentais para o procedimento. Além disso, deverá ser implementada educação digital para as crianças e também para os adultos, como nas escolas e políticas governamentais de conscientização no uso da internet. Ao fim, sugere-se a correta identificação pelas empresas dos consumidores ao adquirirem telefones pré-pagos, fazendo cadastros com seus dados e

---

[55] GUIDI, Guilherme Berti de Campos; REZEK, Francisco. Crimes na internet e cooperação internacional em matéria penal entre Brasil e Estados Unidos**. Revista Brasileira de Políticas Públicas**. Brasília, v. 8, nº 1, 2018, p. 276-288.

[56]ROZA, Fabrízio. Crimes de informática. 2. ed. Campinas: Bookseller, 2007, p. 73 *apud* JESUS, Damásio de; MILAGRE, José Antônio. **Manual de crimes informáticos.** São Paulo: Saraiva, 2016.

registrando os CPFs para que a Anatel, agência reguladora responsável, fiscalize os procedimentos que estão sendo adotados pelos comércios.

CONSIDERAÇÕES FINAIS

O ordenamento brasileiro se vê diante de um desafio devido aos avanços tecnológicos ocorridos e a consequente difusão do acesso à internet. Com este crescimento, aumenta-se também o índice de criminalidade no âmbito cibernético, uma vez que os agentes se utilizam da vulnerabilidade dos usuários – seja de seus aparelhos que não possuem recursos de segurança ou pela própria inocência na hora de usar aplicativos e fornecer dados sigilosos – verifica-se a necessidade de um aumento no efetivo policial especializado na temática, e, devido as peculiaridades dos delitos, o Brasil se demonstra ainda despreparado no que tange a uma legislação que abarque todos os tipos praticados.

Consoante o que sugere o Superior Tribunal de Justiça no escopo de tentar aumentar a segurança dos internautas enquanto navegam na internet, recomenda-se a utilização de navegação anônima, quando a opção for disponibilizada pelos navegadores, além de sempre manter o antivírus atualizado nos computadores e também nos celulares, atentando quando da entrada em sites de comércio eletrônico para verificar se utilizam de conexão segura – o que garante ao usuário que suas informações serão protegidas.

Outras importantes dicas são de priorizar o uso de *softwares* originais – pois estes possuirão características que resguardam o usuário de fraudes –, e ter cautela ao acessar a internet em locais públicos, uma vez que os dados informados durante a navegação poderão ficar salvos no dispositivo usado.

Isso porque o uso cada vez maior da rede abre brechas para a imaginação dos criminosos, que utilizam da ferramenta como forma de praticar novos delitos ou criar métodos novos de cometimento de crimes já tipificados.

Conforme bem explicitado por Eleutério e Machado[57], "apesar da utilização de computadores não ser nada novo, de fato a legislação brasileira não está preparada e precisa ser revista, de forma a possibilitar a adequada tipificação das diversas modalidades de crimes cibernéticos."

Ao fim deste artigo, constatou-se que além das dificuldades por falta de recurso do governo para aplicar na estrutura investigatória da polícia, outro problema na resposta estatal

[57] ELEUTÉRIO e MACHADO, 2011, *apud* CAIADO, Felipe B.; CAIADO, Marcelo. Combate à pornografia infantojuvenil com aperfeiçoamento na identificação de suspeitos e na detecção de arquivos de interesse.In: BRASIL. Ministério Público Federal. 2ª Câmara de Coordenação e Revisão. **Crimes cibernéticos**. Brasília: MPF, 2018, p. 17)

é a velocidade na qual ocorrem os crimes virtuais, além de que são delitos que deixam poucos vestígios, o que dificulta no procedimento de investigação. Todavia, causam danos à bem jurídicos tutelados, o que, desta sorte, infere-se a importância de uma reforma ampla nas atividades públicas seja por meio de reprimenda policial ou na forma de atuação jurisdicional.

REFERÊNCIAS

BRASIL. Câmara dos Deputados. **CPI – Crimes Cibernéticos**. Relatório Final. Brasília: 2015. Disponível em: <https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos> Acesso em: 06 out. 2019.
BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988.** Brasília, DF: Presidência da República, [2016].

BRASIL. Ministério Público Federal. 2ª Câmara de Coordenação e Revisão. **Roteiro de atuação: crimes cibernéticos**. 3.ed. Brasília: MPF, 2016. Série Roteiros de atuação, vol. 5.

BRASIL. Ministério Público Federal. 2ª Câmara de Coordenação e Revisão. **Crimes cibernéticos**. Brasília: MPF, 2018. Coletânea de Artigos, vol. 3.

BRASIL. Superior Tribunal de Justiça. **Crimes pela internet, novos desafios para a jurisprudência**, 2018. Disponível em: < www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias-antigas/2018/2018-06-17_06-57_Crimes-pela-internet-novos-desafios-para-a-jurisprudencia.aspx> Acesso em: 10 out. 2019.

BRASIL. Tribunal Regional Federal da 3ª Região. Escola de Magistrados. **Investigação e prova nos crimes cibernéticos**. São Paulo: EMAG, 2017, 352p.

CAIADO, Felipe B.; CAIADO, Marcelo. Combate à pornografia infantojuvenil com aperfeiçoamento na identificação de suspeitos e na detecção de arquivos de interesse. In: BRASIL. Ministério Público Federal. 2ª Câmara de Coordenação e Revisão. **Crimes cibernéticos**. Brasília: MPF, 2018. p. 8-24.

CARNEIRO, Márcio Rodrigo de Freitas. Perícia de informática nos crimes cibernéticos. In: BRASIL. Tribunal Regional Federal da 3ª Região. Escola de Magistrados. **Investigação e prova nos crimes cibernéticos**. São Paulo: EMAG, 2017p. 33-53.

CONVENTION ON CYBERCRIME. 23 novembro 2001. Disponível em: <http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf>, *tradução nossa.* No original: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185. Acesso em: 01 out. 2019.

CORRÊA, Gustavo Testa. **Aspectos jurídicos da internet**. 5.ed. rev. e atual. – São Paulo: Saraiva, 2010.

DORIGON, Alessandro; SOARES, Renan Vinicius de Oliveira. Crimes cibernéticos: dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade. **Revista Jus Navigandi**, Teresina, 2018., Disponível em: <https://jus.com.br/artigos/63549>. Acesso em: 17 set. 2019

GIMENES, Emanuel Alberto Sperandio Garcia. Crimes virtuais. **Revista de Doutrina da 4ª Região**, Porto Alegre, 2013. Disponível em: <http://www.revistadoutrina.trf4.jus.br/artigos/edicao055/Emanuel_Gimenes.html> Acesso em: 14 out. 2019.

GUIDI, Guilherme Berti de Campos; REZEK, Francisco. Crimes na internet e cooperação internacional em matéria penal entre Brasil e Estados Unidos**. Revista Brasileira de Políticas Públicas**. Brasília, v. 8, nº 1, 2018, p. 276-288.
JESUS, Damásio de; MILAGRE, José Antônio. **Manual de crimes informáticos.** São Paulo: Saraiva, 2016.

ROMANO, Rogério Tadeu. **Convenção de Budapeste e Cibercrimes**. Revista Jus Navigandi, 2019 <https://jus.com.br/artigos/72969/convencao-de-budapeste-e-cibercrimes>. Acesso em: 02 out. 2019

SHIMABUKURO, Adriana. Cibercrime: quando a tecnologia é aliada da lei. In: BRASIL. Tribunal Regional Federal da 3ª Região. Escola de Magistrados. **Investigação e prova nos crimes cibernéticos**. São Paulo: EMAG, 2017, p. 20-21.

SOUZA, Gills Lopes Macêdo; PEREIRA, Dalliana Vilas. **A Convenção de Budapeste e as Leis Brasileiras.** Disponível em: < http://www.charlieoscartango.com.br/Images/A%20convencao%20de%20Budapeste%20e%20as%20leis%20brasileiras.pdf> Acesso em: 13 out. 2019

STJ. CONFLITO DE COMPETÊNCIA: CC 145576. Relator: Ministro Joel Ilan Paciornik. DJ: 13/04/2016. STJ, 2009. Disponível em: < https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ATC&sequencial=59818480&num_registro=201600556041&data=20160420&tipo=5&formato=PDF>. Acesso em: 10 out. 2019.

TRIKEL, Gustavo Beckert. **Crimes Cibernéticos: Confinando uma conduta de repercussões globais**. Tese de Monografia – Faculdade de Direito, Universidade Federal do Paraná. Curitiba, 2010.