Sala de Visitas

Crimes cibernéticos: desafios da investigação

Silvio Castro Cerqueira
Claudionor Rocha

Claudionor Rocha
Consultor Legislativo da Área Área XVII – Segurança Pública e Defesa Nacional, da Câmara dos Deputados.
Sílvio Castro Cerqueira
Delegado de Polícia, ex-Diretor da Divisão de Repressão aos Crimes de Alta Tecnologia (Dicat) da Polícia Civil do Distrito Federal, pesquisador e especialista em crimes cibernéticos.

Crimes cibernéticos: desafios da investigação

Resumo

O presente estudo objetiva abordar os crimes cibernéticos sob o ponto de vista da dificuldade de sua apuração. Considera os desafios impostos pelo avanço tecnológico, assim como a transnacionalidade dessa espécie de crime, além de apontar os empecilhos que a própria estrutura do sistema de repressão criminal, incluindo o ordenamento jurídico, impõem à investigação.

Palavras-chave

Internet, crimes cibernéticos, investigação criminal.

Abstract

This study aims to address cybercrimes from the point of view of the difficulty of resolving criminal offenses. It considers the challenges posed by technological advancement, as well as the transnationality of this kind of crime, as well as pointing out the obstacles that the structure of the criminal prosecution system, including the legal system, impose to criminal investigations.

Keywords

Internet, cybercrimes, criminal investigation.

1 Introdução

Segundo Moreira (2012), de acordo com a Polícia Federal, de cada dez hackers ativos no mundo, oito vivem no Brasil, além do que dois terços dos responsáveis pela criação de páginas de pedofilia na internet têm origem brasileira. Fraudes financeiras que utilizam internet e correios eletrônicos já superariam, em valores financeiros, os prejuízos de assaltos a banco e caixas automáticos, ao passo que a criminalidade via internet seria a terceira grande ameaça às potências, após as armas químicas, bacteriológicas e nucleares (MOREIRA, 2012). Basta uma simples pesquisa na grande rede para nos apontar que há uma infinidade de sites que pregam o racismo, a violência e o terrorismo, além daqueles que ensinam a fabricar bombas, abrir fechaduras e armar uma fraude bancária. Teve também o caso, amplamente noticiado, dos arquivos disponíveis na grande rede para se imprimir uma arma de fogo em impressora 3D. Inclusive, essas armas, em não sendo metálicas, seriam facilmente transportadas para qualquer local, fugindo ao controle de aparelhos de raios X em aeroportos e entradas de locais protegi-dos. Sem dúvida a internet traz uma série de inseguranças e novos desafios e os crimes ciberné-ticos proliferam na grande rede.

Este trabalho será direcionado às indagações e respostas possíveis sobre o que é cibernética, o que é crime cibernético, quais crimes são passíveis de ser cometidos com emprego da alta tecnologia da informação, o que se pode fazer diante da transnacionalidade do delito, o que deveria estar previsto na legislação nacional e internacional para a efetividade na repressão ao delito cibernético. Ademais, aborda a necessidade do constante estudo das evoluções e novidades tecnológicas e sociais para se possibilitar prevenir, investigar e coligir provas de materialidade e indícios de autoria sobre tais delitos.

A importância do tema é intuitiva diante da presença cada vez mais comum dos aparatos cibernéticos no cotidiano das pessoas, o que gera novas oportunidades delinquenciais favorecidas pelo anonimato e impessoalidade que a rede mundial proporciona ao autor do delito.

Foge ao escopo do presente estudo a abordagem de técnicas investigativas, o qual apontará tão somente as dificuldades de caráter legal e operacional para a investigação.

Não será abordado analiticamente o conteúdo das normas existentes, tampouco das proposições tendentes a alterá-las. Vários conceitos no tocante à investigação foram baseadas no trabalho de Cerqueira (2008), sendo o texto correspondente incorporado ao presente estudo.

2 Contextualização

A lei de regência no Brasil no tocante à exploração, gestão e uso dos serviços de internet é o Marco Civil da Internet, aprovado pela Lei n. 12.965, de 23 de abril de 2014[1], que "estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil". É, portanto, legislação recente, que carece ainda de avaliação segura acerca de sua efetiva aplicabilidade e adequação. Entretanto, essa lei não trata de maneira fundamental cibercrimes, estabelecendo, principalmente, parâmetros para as relações jurídicas e de consumo entre provedores e usuários de internet. No entanto, a lei determina a guarda de registro de conexões e de navegação dos usuários por aplicativo/sítio de internet. Essa disposição de não permitir que uma única entidade guarde todo o registro de navegação do usuário, na verdade, dificulta a investigação criminal, pois, ao mesmo tempo que representa um avanço na proteção das garantias individuais, representa também uma dificuldade adicional para o processo investigativo.

Artese (2013) vislumbrou a que a aprovação da lei traria reflexos em diversas áreas do Direito, tais como: o direito autoral (disponibilização de músicas, vídeos e textos); a propriedade industrial (venda de produtos falsificados); os direitos de imagem (publicação de material de conteúdo pessoal); a liberdade de expressão (e sua contrapartida, como, por exemplo, material de conteúdo ofensivo); e questões tuteladas também pelo Direito Penal (incluindo hacking, malware e conteúdo pedófilo). Tais reflexos seriam sentidos, ainda que aprovada a norma segundo o proposto tripé de sustentação da nova lei, pelo Projeto de Lei (PL) n. 2.126/2011, qual seja: a neutralidade de rede; a responsabilidade civil na internet; e a privacidade de dados pessoais e comunicações.[2]

Os pontos mais polêmicos do PL 2.126/2011, que gerou a Lei n. 12.965/2014, segundo Nazareno (2013) dizem respeito à neutralidade de redes, ao monitoramento dos usuários, à guarda dos registros e à guarda dos dados no país. Para o presente estudo a guarda dos registros avulta em importância, uma vez que pressupõe a preservação dos registros pelos provedores de conexão (vedada a dos dados dos aplicativos acessados), devendo os provedores de aplicação guardar os dados por mais de seis meses, apenas quando houver determinação judicial, garantida a privacidade do registro das atividades dos internautas. A guarda de dados no país também possui relevância uma vez que apenas nessa condição as empresas

1 Toda a legislação citada pode ser obtida por meio do site governamental <www.planalto.gov.br>.

2 As informações sobre os projetos de lei podem ser obtidas no site governamental <www2.camara.leg.br>.

sediadas em outros países são obrigadas a fornecer tais dados, por exemplo, segundo a lei brasileira.

Outro ponto de destaque é a responsabilidade por material infringente, disciplinando a prática da 'notificação e retirada do ar' (do inglês *notice and take down*) para conteúdos protegidos ou que afetem a honra. A nova lei trouxe garantia da liberdade de expressão, privacidade, intimidade dos usuários e inviolabilidade das comunicações; vedação de divulgação de dados pessoais; obrigatoriedade de guarda dos registros de conexão por um ano e proibição de guarda dos registros de navegação; obrigação de retirada dos conteúdos infringentes; e garantia de neutralidade.

Havia a perspectiva dos provedores de aplicação (as empresas pontocom), fundadas na defesa da liberdade de expressão, assim como a dos provedores de conexão (as chamadas teles), pressupondo o controle, especialmente no tocante à privacidade. A garantia do princípio da privacidade supõe a preservação da intimidade, vida privada, honra e imagem das partes direta ou indiretamente envolvidas, cuja restrição deve atender aos princípios da necessidade (ou minimização), finalidade e consentimento do titular.

No dizer de Andrade (2014) havia três grupos declaradamente contrários ao Marco Civil da internet tal como foi aprovado. O primeiro composto pelas teles, que eram contra "o conceito de neutralidade da internet, que garante igualdade a todos, para limitar o poder de filtrar a rede, controlar o tráfego, e moldar a navegação dos usuários". O segundo grupo era a indústria do copyright, principalmente as associações de cinema e música, que consideravam desnecessário ordem judicial para a retirada de conteúdos de sites e portais, por suposta violação do direito do autor. O terceiro grupo integrava setores ligados à segurança e inteligência, que pressionavam pela inclusão de mecanismos de vigilância em massa. A partir do caso Snowden[3] acelerou-se a tramitação do projeto.

O ponto crítico desse última questão era o art. 15, o qual determinava que:

> 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

3 Escândalo de espionagem revelado pelo ex-funcionário da agência americana de inteligência, CIA (*Central Intelligence Agency*), Edward Snowden. O fato de que as agências de inteligência interceptaram mensagens e dados inclusive da presidente Dilma Rousseff e da Petrobras teve como consequência a imposição de regime de urgência na tramitação do Projeto de Lei do Marco Civil da internet na Câmara dos Deputados, trancando inclusive, a partir de outubro, a votação de qualquer outro projeto na casa legislativa (ANDRADE, 2014).

> sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.

Embora alguns autores considerem a medida excessiva, o fato é que para o segmento policial esse prazo ainda é restrito, sendo ideal o de três anos, como constava do projeto original. De se ressaltar, ainda, que não constituiu objeto do marco civil a proteção do direito autoral, não obstante o lóbi a favor dessa inclusão.

Segundo Silveira (2014) a aprovação do marco civil da internet no Brasil rompe com uma lógica de criminalização da rede seguida por diversos países, principalmente após a destruição das torres gêmeas do *World Trade Center* de Nova York, em 11 de setembro de 2001. Para o autor, até o início do século XXI, a chamada indústria do *copyright* era a principal defensora de medidas restritivas do uso da internet e de criminalização de práticas cotidianas dos cidadãos conectados. Prosseguindo, o autor revela que

> Nos primeiros anos deste século, a ideia de que a rede seria fundamentalmente o território do terrorismo, da preparação e execução de crimes gravíssimos tornou-se o centro das práticas de controle político da internet. Jacob Appelbaum, no livro *Cypherpunks*, publicado por Julian Assange com a colaboração de outros autores, denominou de "Os Quatro Cavaleiros do Infoapocalipse: pornografia infantil, terrorismo, lavagem de dinheiro e a guerra contra certas drogas" (Assange *et al*., p. 64). Para combater tais males, seria necessário reduzir as liberdades e ampliar o vigilantismo na internet. Uma grande pressão internacional foi liderada pelos Estados Unidos para que os países criassem leis de vigilância e controle dos seus cidadãos no uso da comunicação digital.

Ainda segundo o mesmo autor, apesar de o marco civil ser das normas mais avançadas do mundo na garantia dos direitos individuais na rede, teve que incorporar dispositivos nocivos à defesa da privacidade, como a chamada guarda de *logs* de aplicação.[4]

O problema, segundo o autor, é que existe um mercado de *logs* de aplicação ou, dito de outro modo, do rastro digital de quem navega pela rede, baseado na microeconomia da vigilância ou da interceptação de dados pessoais, da qual a economia informacional fica cada vez mais dependente.

4 O marco civil trata de três tipos de guarda de registros de *logs*: de conexão (art. 13), de acesso a aplicações de internet na provisão de conexão (art.14) e na provisão de aplicações (art.15). Um site, uma rede social, um mecanismo de busca, um blog, um portal de notícias, um serviço de *streaming*, são exemplos de aplicação da internet (SILVEIRA, 2014).

Assim, os dados de navegação dos usuários são analisados visando a descobrir seus "perfis de comportamento, de consumo e ideológicos para vender possibilidades de modulação de práticas, gostos e vontades para empresas ávidas por ampliar seus mercados". Eis aí o âmago da microeconomia da vigilância, praticada pelos grandes e médios provedores de aplicações da rede. Para o autor, o marco civil deveria restringir, mas não obrigar a guarda de tais logs de aplicação, os quais, mesmo sendo mantidos "sob sigilo, em ambiente controlado e de segurança" por seis meses, após esse prazo poderiam ser trocados entre empresas. Acrescenta que é equivocada a alegação de agentes dos órgãos de vigilância de que a guarda de registros de conexão e de aplicação são fundamentais para esclarecer crimes e punir os criminosos, vez que criminosos de grande potencial agressivo não usam IP fixo, mas *proxies* anônimos e técnicas de invisibilidade na rede.

Silveira repudia, ainda, a necessidade de guarda de logs em oposição à garantia de privacidade, especialmente num cenário de implantação universal do novo protocolo de internet IPv6, quando cada indivíduo conectado poderá possuir inúmeros IP vinculados. O fato é que, se por um lado a guarda restringe a liberdade, por outro, acrescentamos, favorece a identificação de delinquentes no ciberespaço.

A instantaneidade das ações e a possibilidade de assincronia no uso da internet atenua os graus de segurança e certeza nas transações nela realizadas, o que gera a brecha (*breach*) para a atuação dos delinquentes. Cabe à norma de natureza penal, portanto, dispor a respeito dessas vulnerabilidades, de sorte a proteger os objetos jurídicos que o Estado considera sujeitos à tutela legal.

3. Base legal

Existem tipos penais específicos que incluem o uso de recursos de alta tecnologia no núcleo das condutas como elementar do tipo, isto é, só cabem quando é usado o recurso de alta tecnologia, ou o recepcionam diretamente como meio propiciador da conduta.

Recente norma editada a respeito no tema é a Lei n. 12.737, de 30 de novembro de 2012, que "dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências". Essa norma, conhecida como Lei Carolina Dieckmann, foi aprovada em contexto de invasão da privacidade de conhecida atriz brasileira. O núcleo do tipo principal é 'invadir' dispositivo informático alheio, o que gerou críticas pois a invasão pressuporia alguma ação agressiva, ao contrário de 'acessar', por exemplo. A lei,

contudo, estabelece penas simbólicas, a serem estabelecidas pelos juizados especiais criminais.

Antes dessa norma houve a edição da Lei n. 9.983, de 14 de julho de 2000, que alterou o Código Penal, acrescentando os arts. 313-A e 313-B, acerca de crimes previdenciários cometidos por computador (inserção de dados falsos em sistema de informações; modificação ou alteração não autorizada de sistema de informações). Já a Lei n. 9.609, de 19 de fevereiro de 1998, dispusera sobre a proteção da propriedade intelectual de programa de computador e sua comercialização no País (contra a pirataria de softwares).

Há também os tipos penais que recepcionam diretamente o recurso de alta tecnologia como meio propiciador da conduta, como nos artigos 241-A e 241-B do Estatuto da Criança e do Adolescente (ECA), Lei n. 8.069, de 13 de julho de 1990, na redação dada pela Lei n. 11.829, de 25 de novembro de 2008, que criminalizam condutas relacionadas à pornografia envolvendo crianças e adolescentes.

Em termos de facilitação da investigação de crimes cibernéticos, a Lei n. 12.735, de 30 de novembro de 2012 (Lei Azeredo), alterou o Código Penal, o Decreto-Lei n. 1.001, de 21 de outubro de 1969 – Código Penal Militar, e a Lei n. 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares. Seu art. 4º dispõe que "os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado". Entretanto o dispositivo é propositivo, não obrigando os entes federados a cumpri-lo. O próprio decreto regulamentar nele previsto sequer foi editado. Mesmo o Departamento de Polícia Federal (DPF) dispõe apenas de um Serviço de Repressão a Crimes Cibernéticos.

Tal lei é oriunda do PL 84/1999, do deputado Luiz Piauhylino, do PSDB de Pernambuco, cuja ementa original era "dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências". O projeto, relatado no Senado pelo Senador Eduardo Azeredo (PSDB), tipificava os crimes digitais e previa, por exemplo, que os dados dos usuários deveriam ser guardados por três anos para investigação criminal. Em um de seus pontos polêmicos, o projeto previa "detenção de um a dois anos e multa" àqueles que utilizassem de forma não autorizada senhas de computadores. Segundo Andrade (2014), a sociedade reagiu negativamente ao projeto, que ficou conhecido como 'AI-5 digital'.

Em termos de mera repressão o art. 5º do PL alterava o inciso II do § 3º do art. 20 da Lei n. 7.716, de 5 de janeiro de 1989 (Lei Anti-Racismo),

facultando ao juiz determinar, nos crimes cometidos por intermédio dos meios de comunicação social (§ 2º), a cessação das transmissões eletrônicas (inciso II). O inciso III já havia sido incluído pela Lei n. 12.288, de 20 de julho de 2010 (Estatuto da Igualdade Racial), facultando ao juiz interditar as respectivas mensagens ou páginas de informação na rede mundial de computadores (inciso III).

Já a Lei n. 12.894, de 17 de dezembro de 2013, acrescenta inciso V ao art. 1º da Lei n. 10.446, de 8 de maio de 2002, prevendo a atribuição da polícia federal para apurar os crimes de falsificação, corrupção e adulteração de medicamentos, assim como sua venda, inclusive pela internet, quando houver repercussão interestadual ou internacional.

No âmbito das Unidades da Federação, a Lei n. 15.026, de 20 de junho de 2013, de Pernambuco, cria a Delegacia de Polícia de Repressão aos Crimes Cibernéticos – DPCRICI (art. 7º), com competência para:

> prevenir e reprimir, com exclusividade no Município do Recife, a prática de crimes tecnológicos, virtuais e eletrônicos, que envolvam delitos praticados com o uso da tecnologia, sobretudo através da internet; e apurar com uniformidade de ação ou maior especialização, concorrentemente com a Delegacia da Circunscrição do local do fato, no Estado de Pernambuco, a prática de crimes de que trata a alínea 'a' deste inciso.

Outro exemplo é o Decreto n. 44.453, de 25 de maio de 2006, do Rio Grande do Sul, o qual estabelece que "a Delegacia de Polícia de Repressão aos Crimes Informáticos – DRCI, do DEIC, compete investigar os crimes cometidos por meios eletrônicos, telemáticos ou através da Internet, cuja abrangência, incidência ou repercussão exijam investigação especializada" (art. 247).

No tocante a proposições pertinentes ao tema e ainda em fase de tramitação (em 2015), ressalta o PL 1.404/2011 aprovado na Câmara dos Deputados e enviado ao Senado Fe-deral em 22/04/2015. De autoria do Senado Federal-COMISSÃO-CPI-Pedofilia-2008 (PLS[5] 100/2010 na origem), aguarda apreciação por aquela Casa de Leis. O projeto "altera a Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), para prever a infiltração de agentes da polícia na internet com o fim de investigar crimes contra a liberdade sexual de criança ou adolescente". O projeto estabelece regras para a atividade investigativa pretendida, fixando o prazo inicial de 90 dias e o máximo de 720, definindo, ainda o

5 Projeto de Lei do Senado, isto é, o apresentado no Senado Federal. Informações sobre proposições em tramitação no Senado podem ser obtidas no site governamental <www.senado.leg.br>.

que são 'dados de conexão' e 'dados cadastrais'. Isenta de crime o policial que oculta a sua identidade para, por meio da internet, colher indícios de autoria e materialidade dos crimes sob investigação, sujeitando-o, porém, a responsabilidade pelos excessos praticados. Contanto que bem intencionado e apresentando algumas regras básicas, considero o projeto não ser ambicioso. Deixa a dever no tocante às garantias oferecidas ao agente a ser infiltrado, merecendo, no meu entendimento, aperfeiçoamento.

No âmbito dos atos internacionais, os mais conhecidos que tratam da temática em apreço são a Convenção sobre o Cibercrime, também conhecida como Convenção de Budapeste, a Convenção Universal sobre o Direito do Autor, revista em Paris, em 24 de julho de 1971, a Convenção de Berna para a Proteção das Obras Literárias e Artísticas, o Acordo sobre os Aspectos dos Direitos de Propriedade Intelectual relacionadas ao Comércio, e o Tratado da OMPI[6] sobre o Direito do Autor. Segundo Silveira (2014) a Convenção de Budapeste, um tratado internacional de direito penal, elaborado pelo Conselho da Europa, sob forte influência norte-americana, teve sua formulação apressada após o 11 de setembro e foi aberta para assinaturas em novembro de 2001. Ela inspirou diversas proposições legislativas nacionais, de medidas contra as violações do direito autoral, pornografia infantil e garantia da segurança das redes. No Brasil, a Convenção de Budapeste influenciou decisivamente o projeto de lei conhecido como 'AI-5 Digital'. Foi precisamente o combate a esse projeto sobre crimes na internet que gerou o Marco Civil da Internet (MCI) discutido anteriormente. O MCI visou, por esse motivo, garantir os direitos fundamentais dos cidadãos na rede e evitar que a internet tivesse sua dinâmica alterada por medidas de segurança exageradas.

Passando pontualmente para a questão dos direitos autorais, ou *copyright*, a criação intelectual, da qual nasce a obra audiovisual, por exemplo, é tutelada pelos direitos autorais através da Lei n. 9610/1998, sendo que internacionalmente, é regida pela Convenção de Berna, em seu Artigo 25, alínea 1, 3 e 6. A Convenção Universal que foi internalizada pelo Decreto n. 76.905, de 24 de dezembro de 1975, em seu artigo III, também dispõe sobre a tutela, não o gênero audiovisual, mas à espécie de obra cinematográfica.[7]

6 Organização Mundial da Propriedade Intelectual.

7 De maneira geral, a obra audiovisual submete-se a um dos dois sistemas de proteção aos direitos autorais. O sistema anglo-saxônico, denominado *copyright* tem início em 1710 na Inglaterra com a primeira lei a reconhecer o direito exclusivo dos autores a imprimir ou dispor de cópias de qualquer livro seu. E o sistema francês, denominado *droit d'auteur*. Este último norteia o Direito brasileiro (FERNANDES, 2013, p. 171, nota de rodapé n. 63, adaptada).

4. Cibernética e direito penal

Vejamos as relações do Direito Penal com a cibernética, em especial no que pertine às investigações dos crimes cibernéticos no tocante às garantias que envolvem a persecução criminal.

Segundo Sieber (2008), "as atuais mudanças sociais podem ser descritas de maneira emblemática com a expressão 'sociedade global de risco'.[8] Por trás desse conceito, estão os desenvolvimentos da 'sociedade mundial', da 'sociedade de informação' e da 'sociedade de risco' (SIEBER, 2008, p. 270).

Prosseguindo, diz o autor mencionado que "as novas possibilidades de execução transnacional de delitos" – criminalidade transnacional – "decorrem das crescentes 'oportunidades de ultrapassagem de fronteiras' por pessoas e no intercâmbio internacional de mercadorias, serviços e dados na sociedade global. Essas possibilidades têm causas técnicas, econômicas e políticas e efeitos correspondentes". Nessa perspectiva a atuação do direito penal leva em conta os limites da soberania territorial *versus* ampliações transnacionais, isto é, "para o resultante desenvolvimento de um 'direito penal com eficácia transnacional', há duas abordagens distintas na esfera da atividade legislativa penal, entre os quais se encontram, ainda, numerosas formas mistas". O autor menciona modelos de cooperação estatal em assuntos penais, de um lado, fundado nos princípios da confiança mútua e da 'disponibilidade' dos dados existentes em outros ordenamentos jurídicos e, por outro, a construção de um 'direito penal supranacional', de que é exemplo a Comunidade Europeia. Esses dois modelos seriam perpassados por formas mistas, como "uniões federativas e supranacionais, caracterizadas pela coexistência de ordenamentos jurídicos, centralizados e descentralizados (como no direito norte-americano) ou pela diferenciada divisão das atividades legislativa, judicial e executiva entre instituições centralizadas e descentralizadas".

Estudioso do assunto, Sieber destaca um confronto assimétrico, quase bélico, entre a expansão do direito transnacional e a manutenção das soberanias nacionais, com objetivos primariamente políticos, como a retirada de Estados ocidentais de determinados territórios ou a desestabilização de governos moderados. Assim, também surgem riscos políticos,

> quando – por exemplo, na América Latina – traficantes de drogas concorrentes ou outros grupos de criminosos, relacionados a *war lords* locais e paramilitares, colocam em xeque o monopólio estatal da força, quando freqüentemente há uma

8 Deixou-se propositadamente de mencionar, neste estudo, para fins de simplificação, as referências utilizadas por Sieber, as quais poderão ser consultadas em seu trabalho.

> ligação entre terrorismo e criminalidade organizada. Um desenvolvimento similar existe em países – principalmente, africanos – na exploração violenta de recursos naturais do solo por meio de empresas criminosas e líderes de conflitos armados locais. Os riscos políticos criados dessa forma adquirem importância quando um país torna-se, por causa deles, um risco de segurança global, o que pode se dar em decorrência de falhas na sua função local de proteção, seja de fato (como *failed state*) ou normativamente (como 'Estado de não-direito') e, assim, transforme-se, mundialmente, em crime *heavens* (ou *safe harbours*) para grupos organizados de criminosos (por exemplo, na antiga Iugoslávia) ou para terroristas (como no Iêmen ou na Somália) (SIEBER, 2008, p. 281).[9]

Prosseguindo, o autor considera que os limites do direito penal não se resumem às alternativas entre 'direito penal do inimigo' e 'direito penal de cidadão', mas pressupõem a adoção de uma política criminal que considere a desfronteirização do direito penal e o novo direito de segurança, buscando o preparo às antecipações da criminalidade diante dos riscos aumentados pela tecnologia, incluindo o uso de técnicas de vigilância e de conservação de dados.

O autor indica conceitos alternativos para superação das dificuldades de aplicação do direito penal, como 'medidas de proteção alternativas de efeito pró-ativo' e 'sistemas de controle alternativos'. No primeiro grupo inclui a proteção da própria vítima em potencial por meio da técnica (como no campo do cibercrime), as regras processuais de direito administrativo (como em medidas de combate à corrupção), a eliminação de problemas sociais (por exemplo, causas de terrorismo) e na chamada prevenção de estrutura (a exemplo do crime organizado). No segundo grupo contempla as pretensões de indenização de direito civil e as estratégias de solução diferenciadas (mediação, acordo entre criminoso e vítima ou comissões de verdade no campo de crimes contra as pessoas), assim como a auto-regulação e co-regulação de Estado e particulares (destaque para o campo da internet e da imprensa). Sieber sugere que a aplicação de princípios de controle alternativos ou complementares é possível ultrapassar os limites funcionais e territoriais do direito penal clássico, especialmente quanto a medidas de prevenção 'privadas' de empresas e associações de

9 Lembre-se, a propósito, a atuação em curso do auto designado Estado Islâmico (*Islamic State of Iraq and the Levant – Isil, Islamic State of Iraq and Syria ou Islamic State of Iraq and ash-Sham* – Isis).

atuação internacional, por exemplo, quando se obrigam, por meio da autovinculação, ao bloqueio de conteúdos ilegais na internet.

Sieber questiona se os objetivos clássicos do direito penal podem ser contrapostos a uma desfronteirização do direito penal, para utilização de novas medidas de investigação baseadas na tecnologia da informação, por exemplo, afetando até inclusão de particulares no controle da criminalidade (SIEBER, 2008, p. 293). Vislumbra, então, a dificuldade de coexistência de medidas preventivas de interferência intensa com as garantias do direito penal, preconizando sua 'exportação' para o direito policial ou outros ramos do 'direito de segurança'.

Avaliando as alternativas postas, Sieber conclui que

> As atuais pesquisas – principalmente sobre a criminalidade organizada – mostram que medidas de prevenção pró-ativas e extrajurídicas (como para a eliminação de causas de mercados ilegais da criminalidade organizada) podem ser não apenas muito mais efetivas do que medidas de direito penal, policial ou mesmo militares, mas também são freqüentemente menos agressivas em relação aos direitos de liberdade do indivíduo do que poderes de coação jurídicos (SIEBER, 2008, p. 296).

5. Os tipos de crimes digitais

A criminalidade digital é potencializada, segundo Cavalcante (2013), em razão do aumento do número de usuários da rede, pelas falhas de segurança desta ou por inabilidade ou negligência no seu uso.

O dado primário para a investigação de crimes cibernéticos é o protocolo TCP/IP ou simplesmente o endereço IP da máquina ligada à rede, a qual recebe um número fixo (estático) ou variável (dinâmico), composto por uma série de algarismos que conferem a identidade única no mundo a determinado computador em determinado dia, horário e fuso horário No entanto, como todos os dispositivos conectados à internet não cabem no formato IP (pois este possui o seguinte formato 255.255.255.255), os computadores conectados se escondem atrás de um número geral que identifica cada rede (dessa forma apenas um número IP é necessário para cada domínio registrado na internet).

A apuração dos cibercrimes passa pelos logs, que são os registros das ações realizadas durante a conexão por determinado IP. Os endereços IP são passíveis de identificação em alguns casos, noutros só o provedor de acesso pode informá-lo. Mediante consulta a sites como <registro.br> (Comitê Gestor da Internet) é possível identificar seus responsáveis. Indi-

cação dos gestores dos registros de nomes de domínio de cada país pode ser obtido no site da *Internet Assigned Numbers Autority* (Iana): <www.iana.org/domains/root/db>. Já os logs estão disponíveis apenas nos arquivos do provedor.

Dentre as principais ameaças cibernéticas, é sabido que mensagens de correio eletrônico (*e-mail*) são muito utilizadas para o cometimento de crimes contra a honra (injúria, difamação, calúnia), além de pornografia infantil, fraude amorosa e instalação de programas maliciosos (*phishing*, mediante as técnicas de *scam* e *spam*). Os dados do destinatário e do remetente da correspondência estão no chamado cabeçalho do e-mail, cuja expansão às vezes é de fácil execução, noutras exige ferramentas especiais. No cabeçalho de uma mensagem de *e-mail* geralmente constam o endereço IP do servidor de e-mail e do usuário, a data, hora e o fuso horário (*timezone*) pela referência GMT[10], dados que não podem ser burlados. Sites de leitura de IP completam a tarefa. Provedores do serviço de correio eletrônico geralmente fornecem uma 'conta espelho' que facilitar a gestão do fluxo de mensagens.

No caso da interceptação telemática, a obtenção do trânsito de dados de internet do investigado pode ser buscada no local de trabalho, residência, instituição de ensino, no smartphone ou outro meio. Entretanto, apenas mediante técnicas de intrusão se poderia reproduzir todo o movimento de navegação.

Outro instrumento para cometimento de crimes cibernéticos são as redes sociais *on line*, que propiciam a criação e compartilhamento de páginas, com troca de documentos, figuras, fotografias, vídeos e mensagens sobre qualquer assunto, incluindo relacionamentos amorosos falsamente engendrados, espionagem, terrorismo, guerra e protestos, sendo muito utilizado pelo crime organizado transnacional. Usuários comuns dessas redes são as crianças e adolescentes, que facilmente se tornam vítimas de pedofilia e tráfico humano para prostituição forçada, por exemplo. Trabalho escravo e tráfico de órgãos igualmente fazem vítimas de todas as idades na rede.

Não obstante, para assegurar o sucesso das investigações soluções incrementais são essenciais, como as novas legislações, treinamento para agências policiais e a cooperação policial e jurídica internacional.

Uma das maiores dificuldades na investigação de crimes cibernéticos é descobrir o IP da origem de uma conexão, que pode ser burlado com o uso de recursos técnicos de mascaramento, de *proxies* (que facilitam a navega-

10 *Greenwich Mean Time* (hora média de Greenwich), conhecido como o marcador oficial de tempo. Greenwich é um bairro de Londres onde está localizado o Observatório Real de mesmo nome, cujo meridiano foi adotado como o inicial para a contagem dos fusos horários: para oeste, o fuso é negativo; para leste, positivo.

ção em redes privadas), de *hotspots* (pontos de acesso à internet) como redes *wifi* abertas (aeroportos, por exemplo), cyber cafés e *lan houses*. Dificuldades adicionais ocorrem com a inserção de dados falsos no cadastro da conta do usuário, além do uso de documento falso nesse cadastro.

Uma dificuldade moderna que restringe o rastreamento de dados é o sistema de computação nas nuvens (*cloud computing*), que permite o armazenamento de dados na rede (na nuvem, *cloud storage*) mediante o uso de aplicativos específicos, como iCloud, Dropbox, Google Drive e outros.

Inúmeras pessoas devotam suas potencialidades ao aprendizado de tecnologias de ponta em sistemas de comunicação e desenvolvimento de *softwares*, objetivando aplicação em atividades que, dolosamente, prejudicam terceiros que conquistaram o direito de uso dessas mesmas tecnologias para a evolução pessoal ou empresarial: são os criminosos do mundo moderno, os vilões do ciberespaço.

Segundo Cavalcante (2013), os principais riscos da internet são a engenharia social (isto é o desenvolvimento compartilhado por grupos), os vírus de *boot, time bomb, worm* e cavalo de troia (*trojan horse*), os *botnets*, o *deface*, o *keylogger*, o *hijacker*, os *sniffers*, a *backdoor* (ou porta dos fundos, ou portas de acesso ao sistema do usuário ao qual ele não tem conhecimento), e os *phishing scam*. Os atores do crime no mundo virtual são divididos ou classificados em clãs ou tribos, segundo suas ações e o direcionamento de suas vontades. Dentre outros tantos, os *hackers*, os *crackers*, os *phreakers* e mais recentemente os *scammers* são considerados os que exigem mais cuidados dos usuários de tecnologia da informação e os que efetivamente demandam atenção dos órgãos voltados ao combate do crime em meio cibernético. Nem todos, porém, estão diretamente associados ao crime.[11]

Os *hackers* são os personagens mais conhecidos, tornados famosos pela mídia e muito tematizados por Hollywood, a quem genericamente se atribuem a autoria dos crimes e outras violações no mundo cibernético. São, pela definição dominante, especialistas em segurança informática que possuem alto conhecimento tanto em sistemas operacionais como em linguagens de programação e ferramentas lógicas. Em geral o *hacker* busca notoriedade e difusão do conhecimento adquirido.[12] Não é incomum que alguns deles sejam

11 Skibell (2003) usa apenas três categorias: *script-kiddies* ('programadores infantis'), *hackers* e *crackers*. Exemplo do prestígio que gozam os hackers são os eventos denominados Hackaton, Hack Day ou Codefest, maratonas de programação que visam congregar os hackers em atividades afins. A própria Câmara dos Deputados promove eventos dessa natureza, como o Laboratório Hacker.

12 Exemplo do prestígio que gozam os *hackers* são os eventos denominados *Hackaton*, *Hack Day* ou *Codefest*, maratonas de programação que visam congregar os *hackers* em atividades afins. A própria Câmara dos Deputados promove eventos dessa natureza, como o Laboratório Hacker.

contratados pelos próprios entes ou empresas que atacaram para o mesmo fim de fortalecerem seus sistemas e evitarem outros ataques. Quando o *hacker* explora seus conhecimentos e habilidades para obtenção de benefício financeiro próprio ou prejuízo alheio, passa a ser chamado de *cracker*.

Em regra, os hackers usam seus conhecimentos na procura por falhas nos sistemas que 'visitam', empregando técnicas previamente existentes ou por eles desenvolvidas, e não têm o objetivo de causar danos ou roubar informações: são motivados pelo aprimoramento dos conhecimentos, pela pesquisa, pelo teste de habilidades e pelo desafio a ser vencido. Na verdade muitos *hackers* contribuem para a melhoria de sistemas de segurança. Existe uma corrente, conhecida como '*hackers* éticos', que, depois de superar as barreiras encontradas, deixa um alerta para o administrador de rede consertar as falhas que permitiram o acesso, normalmente acompanhado da indicação de uma conta de *e-mail* para que possa ser localizado e preste esclarecimentos adicionais.

Os *crackers* são menos populares por causa do alarde dado aos hackers. Eles têm os mesmos conhecimentos técnicos dos *hackers* e também desenvolvem a maioria das ferramentas que usam; chegam a ser chamados de '*hackers* do mal', ou *Dark Side Hackers*, em alusão aos filmes da saga Guerra nas Estrelas. Diferente dos *hackers*, que buscam falhas nos sistemas e alertam para os reparos, os crackers receberam essa denominação pela capacidade de quebrarem os elementos de segurança que controlam, limitam ou impedem o acesso a sistemas de informação ou programas comerciais.

É dessa forma que eles exploram vulnerabilidades e invadem os sistemas que encontram, provocando danos ou subtraindo dados e arquivos ou ainda subtraindo senhas de acesso a contas bancárias e números de cartão de crédito, realizando espionagem industrial e promovendo a quebra de travas de proteção de *softwares*, por exemplo, sendo motivados pelo lucro pessoal ou pela simples vontade e pelo poder de fazer. Não existe barreira para eles, seja ela física, lógica ou moral.

Passaram, então, a desenvolver programas maliciosos, vírus do tipo 'cavalo de tróia' (*trojan horse*)[13], para serem enviados como anexos a mensagens de *e-mail* ou *links* para downloads e instalação do vírus, que tem o objetivo de capturar comandos de teclado e mouse em busca de números de cartões de crédito, contas bancárias e respectivas senhas, de contas de

13 Alusão ao romance *Odisseia*, de Homero, no qual o autor relata o episódio ocorrido na Guerra de Troia, quando os gregos ingressaram naquela cidade fortificada usando o estratagema de deixar às suas portas um grande cavalo de madeira, dentro do qual os guerreiros gregos se esconderam. Levado o cavalo para dentro da cidade, dele saíram os guerreiros, atacando a defesa troiana. Daí a origem, também, da expressão 'presente de grego'

e-mail, de serviços de internet, enfim, de qualquer informação que possa ser usada para benefício pessoal.

As mensagens usadas para difusão desses programas maliciosos, elaboradas com acuradas técnicas e fundamentos de engenharia social, exploram a curiosidade humana e incitam a vítima a instalar o programa espião disfarçado de fotos de infidelidade, imagens pornográficas, avisos de problemas com a Receita Federal do Brasil (RFB), Tribunal Superior Eleitoral (TSE), serviços de proteção ao crédito, cobranças ou outro qualquer capaz de chamar a atenção de quem recebe a mensagem e atiçar-lhe a curiosidade. A técnica é chamada de *phishing scam*, em alusão à pescaria de senhas por *spam*, já que as mensagens são enviadas concomitantemente para centenas de milhares de destinatários.

Em regra os *crackers* não fazem o envio das mensagens. Eles desenvolvem o programa malicioso e o método de envio de mensagens em massa, vendendo-os na internet para terceiros que encontram seus anúncios em salas eletrônicas de bate-papo. Há códigos que incorporam a função extra de enviar ao desenvolvedor mensagens secretas sobre o usuário ou suas vítimas, oferecendo-lhe vantagens extras.

Os *phreakers* são especialistas em tecnologia da informação com profundos conhecimentos de informática, semelhante aos *hackers*, agregando também grandes conhecimentos de telefonia e eletrônica digital. São fanáticos por telecomunicações e suas ações são, em regra, voltadas ao ataque de computadores de empresas de telefonia que lhes permitam efetuar ligações interurbanas e internacionais de graça ou à alteração de bilhetagem, como é chamado o registro de uso dos serviços de telecomunicações para tarifação.

Em regra desenvolvem seus ataques através de servidores sediados em outros países e sua localização é muito dificultada. Ocorre também de se valerem de seus conhecimentos de tecnologia para obter números e senhas de cartões de crédito e de contas bancárias para benefício próprio.

Os *scammers* são pessoas com pouco ou nenhum conhecimento de tecnologia da informação, e que adquirem o 'pacote', ou *kit*, de programas para *phishing scam*, normalmente composto por um *link* para download do vírus tipo cavalo de tróia, o programa gerador automático de mensagens e um ou mais modelos de texto para mensagem de correio eletrônico ou sites de relacionamento pela internet, e os divulgam na rede, recebendo as informações ilicitamente obtidas para auferir lucro pessoal.

Como não possuem conhecimentos técnicos a serem desafiados ou barreiras a serem quebradas, os scammers atacam indistintamente, chegando a difundir mais de quinhentas mil mensagens simultâneas por um

único acesso à internet, em geral oferecidos por órgãos governamentais ou estabelecimentos comerciais que não efetuam cadastros dos usuários.

A grande frequência de atualização dos programas antivírus tornou os códigos maliciosos em anexo às mensagens inefetivos, levando os scammers à alternativa da hospedagem remota e clandestina dos *trojans* em servidores de rede nacionais ou estrangeiros vulneráveis e a inclusão do *hiperlink* para *download* na mensagem, que inclui 'sofisticadas' instruções para instalação.

A inserção dos programas nos servidores de rede pelos respectivos desenvolvedores, os *crackers*, e a informação dos respectivos *hiperlinks* fazem parte do *'kit scam'*. Não existe alvo específico para o *scammer*. Qualquer internauta desavisado pode se tornar vítima e contaminar toda uma rede local de computadores.

O fato de a difusão do *scam* ser extremamente fácil e barata, tem atraído muitos criminosos, aumentando sensivelmente a sua prática. Isso ocorre porque a tais fatores se alia a sensação de segurança na obtenção do proveito do crime, que pode ocorrer a partir de qualquer computador conectado à internet. Além disso há a facilidade de cooptação, ou recrutamento, de terceiro para movimentação bancária mediante pequena retribuição em pecúnia.

As mesmas facilidades que tornam o *scam* atrativo para o criminoso criam excepcional dificuldade às investigações e à punição dos autores dessa prática, que continuará a apresentar crescimento enquanto a legislação não favorecer sua repressão.

Conforme ataques mais direcionados se tornam populares, aumentam também os casos de *spear phishing*, em que criminosos bombardeiam empresas com spam altamente direcionado que parece vir de dentro da empresa, geralmente dos departamentos de tecnologia da informação e de recursos humanos.

Frequentemente o criminoso oferece uma pequena recompensa em troca de informação privilegiada. Acreditando que as mensagens são legítimas, muitas empresas a acatam e, inconscientemente, acabam revelando informações que permitirão ao criminoso acessar áreas restritas da rede corporativa, o que pode resultar na subtração de propriedade intelectual e outros dados corporativos sensíveis.

Spear phishing, como técnica de engenharia social, também tem sido usado para induzir pessoas a abrir códigos maliciosos, substituindo, em alguns casos, ataques dirigidos de *scam*.

Ainda não há denominação ou classificação própria conhecida para aqueles criminosos que se valem dos recursos de tecnologia para ações simuladas, como adulteração de caixas eletrônicos com instalação de equipamentos co-

nhecidos por 'chupa-cabras', dispositivos para obtenção de números de cartões bancários e câmeras para registro visual das respectivas senhas.

Como tal conduta não exige conhecimentos avançados de eletrônica ou computação, seus autores são normalmente delinquentes comuns que adquirem o equipamento e as instruções de operação dos técnicos que os desenvolvem ou de outros criminosos, que passam a cobrar percentual sobre os lucros estimados.

Com relação à pornografia infantil, por exemplo, com o uso dos programas de computação gráfica é possível combinar duas imagens em uma, ou distorcê-las criando outra totalmente nova (*morphing)*.[14] *Morphing* é um efeito especial em filmes e animações que muda (ou *morphs*) uma imagem para outra através de uma transição sem problemas. Na maioria das vezes ele é usado para descrever uma pessoa se transformar em outra através de meios tecnológicos ou como parte de uma fantasia ou uma sequência surreal. As novas tecnologias modificaram a natureza da pornografia. Câmeras e filmadoras digitais tornaram a produção fácil e barata. Há menos risco de que outra pessoa descubra a operação, haja vista que não é necessário revelar as fotos, qual a fotografia convencional. A reprodução do material não acarreta perda de qualidade. A distribuição tornou-se fácil, barata e rápida com o advento da internet (FERNANDES, 2013, Nota 35, p. 157).

6. O papel da polícia

As discussões que giraram em torno da tramitação do PL 84/1999 (PLC[15] 89/2003 no Senado) que foi transformado na Lei n. 12.735/2012, nos trazem importantes lições a respeito do tema. Relatado na Câmara pelo Deputado Eduardo Azeredo (PSDB/MG) e no Senado pelo mesmo parlamentar, agora como senador, embora de iniciativa louvável, o projeto, foi aprovado de maneira bastante simplificada. O impasse na aprovação do projeto tal como proposto originalmente revelou importantes pontos a serem considerados.

14 *Morphing* é um efeito especial em filmes e animações que muda (ou *morphs*) uma imagem para outra através de uma transição sem problemas. Na maioria das vezes ele é usado para descrever uma pessoa se transformar em outra através de meios tecnológicos ou como parte de uma fantasia ou uma sequência surreal. As novas tecnologias modificaram a natureza da pornografia. Câmeras e filmadoras digitais tornaram a produção fácil e barata. Há menos risco de que outra pessoa descubra a operação, haja vista que não é necessário revelar as fotos, qual a fotografia convencional. A reprodução do material não acarreta perda de qualidade. A distribuição tornou-se fácil, barata e rápida com o advento da internet. Disponível em: <http://content.worldgroups.com/groups/Custom/P/PortugalCompanhia Onli-ne/naoapedofilia.htm>. Acesso em: 30 dez. 2011. (FERNANDES, 2013, Nota 35, p. 157).

15 Projeto de Lei da Câmara, como são designados no Senado Federal os projetos originários da Câmara dos Deputados.

A elaboração de legislação específica que descreva condutas a serem tratadas como crime e condições para resposta do Estado não poderá apresentar resultado satisfatório à sociedade se não contar com o apoio de especialistas em segurança da informação e dos profissionais de polícia com experiência na repressão ao dito crime cibernético, detentores de conhecimento útil ao subsídio da redação de textos técnica e procedimentalmente corretos e efetivos.

A necessidade de lei federal que regulamente o fornecimento, pelas empresas provedoras de acesso, serviço ou conteúdo na internet, de informações de cadastro e de identificação na rede, é realidade patente. A inexistência do dispositivo legal coercitivo muitas vezes conduz ao fracasso das investigações, normalmente pelo perecimento da informação volátil ou pela alteração das condições que, no início, eram favoráveis ao sucesso, em mera razão do decurso do tempo.

A interceptação de comunicações telefônicas é realizada há vários anos pelas polícias de todo o mundo com consagrados resultados positivos, pelo que evoluiu com o desenvolvimento de novas ferramentas auxiliares que facilitam tanto a execução da medida, naturalmente que com a devida ordem judicial, como a análise do material obtido.

Esta não é a realidade da comunicação telemática. O processo técnico para se realizar uma interceptação telemática é complexo e há situações para as quais ainda não existe solução na tecnologia. Dependendo da provedora de acesso, pode ser possível executar a interceptação do sinal de comunicação remotamente, isto é, em uma dependência policial. Pode haver a necessidade de instalação de computador dedicado e especialmente configurado nas dependências da empresa provedora, com posterior busca e análise dos arquivos gravados referentes ao tráfego. E há casos em que simplesmente não é possível realizar a interceptação por absoluta falta de viabilidade técnica.

Mesmo quando o computador é instalado nas dependências da empresa provedora a confidencialidade do conteúdo interceptado é questionável. Ainda nos casos em que o provedor de acesso dispõe de condições técnicas que possibilitem a interceptação, nem todo o conteúdo pode ser visualizado, a exemplo do tráfego encriptado e algumas soluções de voz sobre IP, ou VoIP.

As soluções comercialmente disponíveis para a interceptação telemática são caras e, muitas vezes, inadequadas, pois a maioria requer conexão à rede local e só funciona quando instalada como integrante da rede que o 'alvo' use para o acesso, excluído o provedor de conteúdo.

Vale dizer que a comunicação telemática é verdadeiro desafio à investigação criminal, em razão da inexistência ou inadequabilidade das ferramentas de tecnologia atualmente disponíveis, principalmente de serviços de comunicações via internet sediados no estrangeiro. A obtenção dos

elementos que indiquem, ou apontem, a autoria normalmente só podem ser encontrados com o provedor do acesso, de serviço ou de conteúdo de internet por meio do qual o crime tenha sido cometido.

As grandes empresas do ramo mantêm registros dos seus eventos de rede, tornando tecnicamente possível identificar o usuário do serviço empregado para cometimento do crime, como o responsável pelo estabelecimento de conexão à internet, a identificação do endereço IP que individualiza a conexão a uma conta de *e-mail* ou página pessoal, por exemplo.

Dificuldade similar ocorre também para a obtenção de registros de eventos e identificação de responsáveis por comunidades de relacionamento virtual, por serviços de correio eletrônico, de comércio eletrônico e outros oferecidos pela internet que possuem sede em outros países

Como atualmente este procedimento apresenta acentuada demora, o recebimento da resposta não apresentaria nenhum valor prático para a persecução penal, pois a volatilidade da prova eletrônica faria desaparecer os indícios ainda existentes no território nacional, que somente poderiam se encontrados com as informações oriundas do estrangeiro, redundando em impunidade ao autor do crime e irreparável prejuízo às vítimas e à sociedade, que se vê desde há muito, desamparada.

A solução para tal empecilho surgirá naturalmente, seja pela celebração de acordos internacionais de cooperação, a exemplo da Convenção de Budapeste, seja pela intervenção participativa de redes como a Interpol ou, no caso extremo, pelo advento de legislação que proíba o acesso a serviços cujos responsáveis não cumpram a lei brasileira, o que se afigura impossível. Corrobora esse posicionamento o fato de que a Comissão Parlamentar de Inquérito (CPI) da Pedofilia, da Câmara dos Deputados, obteve sucesso para que a norte-americana *Google Inc.*, responsável pelo serviço de relacionamento via internet denominada *Orkut*, já desativada, prestasse informações sobre os responsáveis por páginas pessoais que tratassem de pornografia infantil e preservassem o respectivo conteúdo para uso em processos criminais no Brasil, ação realizada com o intermédio da empresa que representa a norte-americana no país, a Google Brasil Internet Ltda, fato amplamente divulgado pela imprensa nacional.

O processo que envolve a persecução penal dos crimes cometidos por meio da tecnologia é, até o momento, exatamente o mesmo aplicado ao crime comum. As mudanças compreendem, efetivamente, somente uma parte da maneira de se investigar, que demanda conhecimentos avançados de internet, computação, engenharia de *software*, eletrônica, redes de comunicações e internet.

Enquanto países como os Estados Unidos da América, contudo, já mantém estrutura departamental para oferecer à sua sociedade a necessária segurança no universo cibernético, pois lá as questões da internet são tratadas também como de segurança nacional, já que o meio é propício para a prática também do terrorismo, outras nações começam a engatinhar, por assim dizer, nos meandros da internet e a enxergar as potenciais ameaças e oportunidades que a rede mundial oferece.

No Brasil, as polícias judiciárias já começam a entender a necessidade de se especializar no combate aos criminosos da era tecnológica moderna, sendo possível encontrar uma ou outra unidade policial no país voltada exclusivamente para investigar sobre autoria e materialidade nesta modalidade delinquencial.

Ocorre que a resposta aos crimes cometidos com emprego da tecnologia exige profissionais de polícia que dominem, no mínimo, essa mesma tecnologia, a ponto de estarem em condições técnicas de cometerem o mesmo crime objeto da investigação. Se não for assim, dificilmente a ação repressora logrará êxito em comprovar materialidade, autoria e circunstâncias do crime que possibilitem ao juiz decidir pela condenação do acusado e sentenciá-lo consoante a gravidade da conduta, a seriedade dos resultados e demais circunstâncias legalmente previstas.

É forçoso concluir que a medida mais razoável e lógica a se adotar é a formação de equipe de especialistas destinada a prestar apoio às unidades policiais nas investigações por elas conduzidas sobre crimes que envolvam os recursos de tecnologia da informação.

Toda delegacia de polícia, seja ela especializada ou não, possui o *expertise* da investigação das condutas descritas pela legislação como crimes, apresenta a estrutura necessária para o ciclo de polícia judiciária e o conhece bem, sendo inerente à sua natureza a investigação preliminar de notícia de crime, a instauração do pertinente inquérito policial, se confirmada a notícia, e o respectivo relatório, ao final.

A equipe especializada em crimes cibernéticos participa dos trabalhos com a prestação de apoio, materializado pela realização de procedimentos afetos à tecnologia, entregando à investigação tradicional o conhecimento produzido sobre o crime que a delegacia investiga, subsidiando seus procedimentos de coleta de prova de materialidade e indícios de autoria sempre que tal se fizer necessário.

Assim, todo e qualquer crime que venha a ser praticado com emprego de tecnologias deve ser apurado pela mesma unidade que o apuraria se tivesse sido ele cometido por vias ditas normais, ou sem emprego de

ferramentas da tecnologia, mas com o auxílio do órgão especializado nas tecnologias passíveis de utilização no crime.

Exemplificando, o uso fraudulento de cartões de crédito em compras pela internet, cujos números tenham sido obtidos após invasão em site de comércio eletrônico, deve ser investigado pela mesma unidade que trataria da fraude comum, como o uso fraudulento do cartão de crédito clonado em posto de gasolina ou fisicamente subtraído da vítima desavisada. Na hipótese, a delegacia contaria com o auxílio do órgão especializado, que executaria os procedimentos adequados à identificação da origem da conexão que resultou na invasão do banco de dados e outros elementos úteis, emitindo os respectivos relatórios técnicos das atividades investigativas, que seriam juntados ao inquérito policial da delegacia competente e fariam suas vezes de elementos de convicção do juiz.

Este órgão especializado na investigação cibernética demandaria equipamentos com grande poder de processamento, de conectividade e franco acesso à rede mundial de computadores, além da constante treinamento e intercâmbio de informações com outros especialistas das áreas de tecnologia da informação voltada à polícia judiciária e à segurança de dados.

As instituições responsáveis pelas investigações criminais não podem se dar ao luxo de parar no tempo e esperar que os acontecimentos ditem suas respostas à sociedade. Atendendo aos princípios gerais do Direito Administrativo, elas precisam, sob pena de ingressar na esfera da ineficiência, se adiantar ao crime e construir estruturas que lhes permitam efetivamente cumprir suas missões constitucionais dentro dos preceitos afetos às ações do administrador público.

Deixar de buscar a evolução propiciada pelo mundo da tecnologia equivale a negar o emprego de novos e eficientes instrumentos de combate ao crime moderno, que é executado sem aviso, sem violência, sem contato pessoal, onde o criminoso busca refúgio no anonimato do universo cibernético e restará impune se não houver o devido preparo da força repressora. Assim, a decisão de criar um órgão com equipes especializadas no combate ao delito no mundo da tecnologia deve ser isenta de paixões e norteada pela busca da eficiência máxima.

7. Considerações para reflexão

A crescente incidência de condutas lesivas praticadas pela internet, constantemente divulgadas nos noticiários locais e nacionais, e que deixam a sociedade com sentimento de impotência pela aparente falta de normatização sobre o assunto que a ampare, precisa ser encarada como fato social carecedor de atenção especial do Estado.

A relevância do tema também fica bem evidenciada quando se percebe que os tribunais pátrios, responsáveis pela interpretação do texto legal, ainda não firmaram entendimento pacífico sobre os limites à iniciativa e ação das autoridades policiais nos procedimentos investigativos, chegando a atribuir à interpretação da lei letra que dela não consta, mesma resposta que posições defensivas de provedores de acesso, de serviço e de conteúdo de internet oferecem às investigações criminais, atitude que protela o anonimato do autor e retarda sua punição.

Além disso, a prospecção de informações válidas que possibilitem a identificação de criminosos e o monitoramento de fontes abertas de informação, muitas vezes possibilita a antecipação à ação delitiva pelo poder repressivo do Estado, sendo atividade de inteligência policial ainda pouco explorada no Brasil.

A transnacionalidade dessa modalidade de crime precisa ter suas barreiras bem expostas, como atitude primeira voltada ao rompimento de obstáculos da persecução ao ilícito. Como exemplo já clássico de óbice às investigações, está a prática de *phishing scam*, modalidade preparatória para furtos mediante fraude bancária e estelionato praticado no comércio eletrônico, consistente no envio de mensagem de *e-mail* com 'estória cobertura' que busca convencer a vítima a acessar uma página da internet previamente indicada e instalar no computador programa espião que efetivamente quebra a confidencialidade de acessos às contas bancárias, de cartões de crédito, etc., para usufruto indevido do crédito alheio pelo seu, digamos, controlador. A técnica se vale de vulnerabilidades de páginas de internet hospedadas no exterior para guardar os arquivos de instalação do vírus de computador.

As dificuldades impostas por entidades estrangeiras em fornecer informações essenciais à investigação criminal, ou civil, somadas ao exíguo prazo que a legislação nacional dispõe sobre preservação e disponibilização de registros de eventos de provedores de acesso à internet e serviços de conteúdo, conduzem à triste realidade do insucesso, com consequente impunidade ao autor em muitos casos.

A tecnologia continua avançando e disponibilizando mais conectividade, portabilidade e equipamentos cada vez mais potentes, mais rápidos, reduzindo dia após dia a distância entre estados, países e continentes. Lamentavelmente, contudo, a evolução tecnológica não traz só benefícios. Ao mesmo tempo em que a Era da Informação democratiza o conhecimento, difundindo-o para as nações mais pobres, faz surgir oportunidades de ataques à privacidade e ao patrimônio do cidadão, à segurança do Estado e da sociedade, ameaça representada pela *Information Warfare*,

ou *InfoWar* (guerra da informação), onde o poder do conhecimento e da informação faz frente à segurança tradicional.

A *InfoWar* está disponível para qualquer um que seja possuidor de um computador e tenha um objetivo definido. Nessa guerra o computador pode se transformar em uma arma altamente ofensiva, cujos alvos podem ser dados de pessoas físicas, segredos de empresas, ou invasões de sistemas corporativos ou de serviços essenciais, como abastecimento de água, energia elétrica, telefonia, bancário, hospitalar, etc., modificando registros ou causando interrupções de fornecimentos por sabotagem.

Sites de comércio eletrônico, de *internet banking* e outros tipos de serviços on-line são alvos freqüentes de *crackers* que desejam acesso a grandes bases de dados de informações de crédito, para a venda ou utilização direta em compras via internet. A identificação de ataques dessa natureza resulta no aperfeiçoamento das medidas de segurança, que ficam cada vez mais fortes, e os métodos tradicionais de aplicação da lei vêm se mostrando suficientes, apesar de inadequados, para a persecução de autores desse tipo de crime, embora a investigação policial ainda careça de dispositivos legais que a facilitem e propiciem maior sucesso.

O elemento que motiva diversos dos ataques através da internet se tornou claro a partir das prisões de alta repercussão de criminosos cibernéticos nos Estados Unidos e no mundo inteiro, que apontam para indivíduos ligados ao crime organizado, cujo objetivo é simplesmente o lucro, o dinheiro. Com softwares e redes se tornando cada vez mais seguros, como acontece com os serviços de automação bancária, é de se esperar que grande parte destes criminosos procure atingir o ponto de acesso mais vulnerável dentro da companhia ou organização, os funcionários, para executar o ataque.

A análise de textos especializados indica tendências potenciais de aumento de ataques cibernéticos, como, por exemplo os ataques internos, a exploração das deficiências de regulação nos mercados emergentes, o uso de botnets e mensagens instantâneas – DoS e DDoS, o aproveitamento da vulnerabilidade dos dispositivos móveis, os ataques por mensagens de e-mail direcionadas, o *spear phishing*, os vírus de computador, o esquema de *phishing* e a crescente engenhosidade de códigos maliciosos.

Apesar de os *softwares* tornarem-se mais seguros a cada dia, os usuários de computador continuarão a ser o elo mais fraco de empresas e organizações. Criminosos se esforçarão para convencer usuários finais a executar o ataque, ao invés de perder um tempo longo para descobrir onde o *software* é vulnerável. Recursos globais, funcionários demitidos, fusões e aquisições apresentam desafios para empresas que desejam instruir usuários contra esses ataques.

Criminosos cibernéticos tiram proveito da fraca cooperação internacional contra cibercriminalidade e fazem ataques internacionais com pequeno risco pessoal. Por essa razão, ataques a países emergentes e em desenvolvimento e ataques vindo dos mesmos, estão aumentando. Isso torna ainda mais difícil rastrear os ataques até suas fontes, especialmente quando tendências mostram o crescimento de ataques originados em regiões como o Leste Europeu, Ásia e América do Sul, onde não há a adoção da Convenção de Budapeste, as sanções são mais brandas e o controle é limitado ou inexistente.

Programas que transformam computadores em robôs, chamados *bots*, permitem o controle de um sistema sem conhecimento do proprietário. *Bots* mais novos, com núcleos menores para melhor se esconder e assinaturas não reconhecidas pelos dispositivos antivírus e *firewall*, chegarão por mensagens instantâneas, scripts em páginas da internet, redes ponto-a-ponto, etc., servindo de instrumento para comandar e controlar os sistemas infectados, contaminar novas máquinas e formar redes de robôs, ou *botnets*.

O número de aparelhos celulares, *smartphones*, dispositivos PDA, acrônimo para a expressão *portable data assistant* – assistente portátil de dados, e outros dispositivos sem fio, ditos *wireless*, afetados por códigos maliciosos cresce ano após ano, mas isso ainda não se transformou em aumento do número de invasões, já tais tipos de vírus ainda não podem se espalhar sozinhos: dependem de ação humana direta que os distribua. A popularização dos telefones celulares chama a atenção dos especialistas em segurança para a nova moda de atacar dispositivos móveis de acesso à internet e subtração de créditos de linhas celulares, transferidos por mensagens de SMS para a conta do autor.

Os casos de vírus enviados como anexos de mensagens por *e-mail* apresentaram diminuição gradual ao longo dos anos. Como os métodos de identificação e detecção de vírus apresenta avanço constante, a técnica de difusão do código malicioso por anexo de *e-mail* apresenta redução progressiva de sucesso, levando os atacantes a optarem pela hospedagem remota com a difusão do *link* para *download* por mensagens tipo *phishing scam*.

Os crimes cometidos com uso de alta tecnologia ainda são fontes de debates pelo mundo e causam muitas divergências de opiniões entre a comunidade jurídica e a comunidade de informática, que não chegaram a um consenso sobre o tratamento a ser dado aos chamados crimes de informática, ou cibercrimes.

Há os que defendem a criação de legislação específica para tratar do assunto, descrevendo tipos penais para cada hipótese de delito praticado por intermédio da informática, e os que entendem serem suficientes as tipificações existentes no Código Penal e leis extravagantes, onde já estão

definidos os crimes de furto mediante fraude, dano, estelionato, peculato, violações da intimidade e de segredo, fraude eleitoral, pornografia infantil, ameaça, calúnia, difamação e injúria, além de outros crimes que podem ser perpetrados por meio do computador, até mesmo homicídio. Mesmo o direito autoral tende a sofrer mudanças significativas, pois os trabalhos intelectuais colocados na rede, tais como artigos, teses, imagens, músicas, etc., ou mesmo ideias, ficam à disposição de qualquer usuário no mundo e, a princípio, podem ser usados ou manipulados livremente, dificultando sobremaneira a aplicação e o exercício dos direitos do autor.

Em verdade o direito positivo já prevê como delito grande maioria das condutas lesivas perpetradas com recursos da alta tecnologia, já que, normalmente, são crimes comuns que utilizam a informática como arma, instrumento ou meio de armazenamento ou difusão, mas há que se entender, contudo, que a tipificação penal envolve elementos nem sempre presentes nos crimes cometidos pelo computador ou com emprego da alta tecnologia.

Como exemplo pode ser citado o furto, que exige a subtração de um bem material, palpável. Programas de computador ou dados armazenados em computador são considerados, na maioria dos países, bens imateriais. Mesmo que equiparado o 'dado' a 'coisa', no furto, para manter o exemplo, há necessidade da subtração, da retirada do bem da esfera de vigilância de quem legitimamente o detém, o que somente ocorreria se, além da cópia dos dados, eles fossem apagados.

Assim, em tese, não se pode falar em furto quando alguém se apodera de um banco de dados, por exemplo, sendo absolutamente necessário definir esse tipo de 'furto' em lei especial ou complementar à legislação penal positiva, conferindo abrangência da tutela do Estado aos bens imateriais quando objetos de crime e equiparando a cópia à subtração.

8. Conclusão

A natureza do crime está mudando. Está deixando a violência das ruas para assumir o anonimato propiciado pelo incremento da capacidade de processamento e de miniaturização de componentes – que se traduz em portabilidade – e pela conectividade entre equipamentos, ao exemplo da rede mundial de computadores. As facilidades que a tecnologia oferece acabam por tornar o crime cometido com auxílio da tecnologia, cujo autor se esconde no manto do anonimato, um negócio rentável e de baixo risco. As polícias precisam investir no acompanhamento dos novos recursos eletrônicos, em novos métodos de produção e difusão do conhe-

cimento, em especialização do seu quadro de pessoal, para fazer frente aos delinquentes da Era da Informação.

Ao contrário do crime comum, aquele de ocorrência cotidiana nas ruas das grandes cidades, cuja investigação está sob controle, o emprego da tecnologia da informação, que hoje tem baixo custo e extrema facilidade de obtenção, já foi descoberto por criminosos mais habilidosos que a usam desde a comunicação para organização de empreitadas ilícitas à obtenção direta do lucro fácil, sendo o principal elemento de preocupação das polícias mais avançadas do mundo.

É preciso que os gestores se conscientizem de que existe largo espectro de crimes que podem ser cometidos com o auxílio da alta tecnologia, crimes que dispensam o uso de armas de fogo e habilidades especiais, que podem ser cometidos no anonimato, no aconchego do lar do criminoso e que atingem vítimas indistintas. São, na grande maioria das vezes, condutas que se amoldam perfeitamente à descrição de tipo penal vigente. Cuida-se que a força repressora precisa investir nesse ramo de investigação para não se tornar obsoleta, pois tanto os batedores de carteira e os ladrões de banco como os policiais que não acompanham as evoluções da tecnologia tendem a receber o mesmo destino dos dinossauros: a extinção.

Referências

ANDRADE, Simone Caixeta de. **Trajetória legal do marco civil.** (2014). Disponível em:

<http://comciencia.scielo.br/scielo.php?script=sci_arttext&pid=S1519-76542014000400004&lng=en&nrm=iso>. Acesso em 19 maio 2015.

ARTESE, Gustavo. *As trancas da Lei de Internet*. Disponível em: <http://convergecom.com. br/tiinside/services/02/12/2013/trancas-da-lei-de-internet/#.VVpgj_lVhBc>. Postado em: 02/12/2013. Acesso em 18 maio 2015.

CAVALCANTE, Waldek Fachinelli. Crimes cibernéticos: investigação e ameaças na inter-net. **Revista Jus Navigandi**, Teresina, ano 18, n. 3782, 8 nov. 2013. Disponível em: <http://jus.com.br/artigos/25743>. Acesso em: 18 maio 2015.

CERQUEIRA, Silvio Castro. **Rrepressão aos crimes cibernéticos - oportunidades e ameaças - práticas da PCDF**. Trabalho de Con-

clusão de Curso apresentado como requisito à obtenção de título Pós-Graduação em Gestão de Segurança Pública com foco em Inteligência, do Centro Universitário do Distrito Federal. Orientador: Prof. Msc Celso Moreira Ferro Júnior. Brasília : 2008.

FERNANDES, David Augusto. Crimes cibernéticos: o descompasso do estado e a realidade. **Rev. Fac. Direito UFMG**, Belo Horizonte, n. 62, pp. 139 - 178, jan./jun. 2013.

MOREIRA, Rômulo de Andrade. **A nova lei sobre a tipificação de delitos informáticos: até que enfim um diploma legal necessário**. Disponível em: <http://www.egov.ufsc.br/portal/ conteudo/nova-lei-sobre-tipifica%C3%A7%C3%A3o-de-delitos-inform%C3%A1ticos-at%C3% A9-que-enfim-um-diploma-legal-necess%C3%A1ri>. Postado em 6 dezembro 2012. Acesso em 18 maio 2015.

NAZARENO, Claudio. **Comentários acerca do Projeto de Lei nº 2.126/11, que "[e]stabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil", o chamado Marco Civil da Internet**. (2013) Disponível em: <http://bd.camara.gov.br/bd/bitstream/handle/bdcamara/15076/comentarios_acerca_nazareno.pdf?sequence=1>. Acesso em 18 maio 2015.

SIEBER, Ulrich. Limites do Direito Penal. **Revista Direito GV**, São Paulo 4(1) | P. 269-330 | jan-jun 2008. Disponível em: <http://www.scielo.br/pdf/rdgv/v4n1/a12v4n1.pdf>. Acesso em 19 maio 2015.

SILVEIRA, Sergio Amadeu da. **Marco civil e a proteção da privacidade**. (2014) Disponível em: <http://comciencia.scielo.br/scielo.php?script=sci_arttext&pid=S1519-76542014000400008&lng=en&nrm=iso> Acesso em 18 maio 2015.

SKIBELL, Reid. Cybercrime & Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act. **Berkeley Technology Law Journal** Volume 18 | Issue 3 Article 4 June 2003. Disponível em: <http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1430&context=btlj> Acesso em 19 maio 2015.