REVISTA JURÍDICA DA
LIBERTAS FACULDADES INTEGRADAS – Número 1 – Ano 5

CRIMES CIBERNÉTICOS: EVOLUÇÃO DO DIREITO PENAL ELETRÔNICO FRENTE ÀS NOVAS DEMANDAS DA VIDA ATUAL

Luís Antonio da Paixão
Graduando em Direito

Marliza Núbia Caetano
Graduanda em Direito

Fabiana Cristina da Silveira Alvarenga
Mestranda (aluna especial) em Políticas Públicas e Desenvolvimento Regional

RESUMO

O uso abrangente dos meios digitais de comunicação aproximou pessoas e proporcionou a troca de informações e conhecimento de maneira global e imediata. Por outro lado, com a mesma velocidade, criou possibilidades de se disseminar ataques criminosos que tanto causam danos materiais quanto ferem intimamente a dignidade humana, causando danos morais irreparáveis. O presente artigo tem como problema de pesquisa os crimes cibernéticos e seu tratamento dentro do Direito Penal Eletrônico e pretende, no primeiro momento, qualificar o que é crime ou delito cibernético e, sem seguida, responder as seguintes perguntas: quais são seus principais agentes, sujeitos ativos e meios? Quais são as possibilidades de defesa que as vítimas de crimes cibernéticos encontram junto ao Direito Penal Eletrônico, campo que tem evoluído consideravelmente na última década? O objetivo geral é, portanto, identificar a relevância do debate sobre o tema e as possibilidades de defesa das vítimas. Abordando como metodologia a pesquisa bibliográfica, imprescindível em função do aproveitamento de idéias já expostas sobre o tema, o artigo não tem a pretensão de esgotar o debate acerca de tema tão controverso e novo, esse trabalho enfatiza, a título de consideração final não conclusiva, que para além de uma criminalização específica, o esclarecimento técnico aos operadores do Direito, à autoridade policial, aos administradores de sistemas informáticos, aos magistrados e membros do Ministério Público é altamente recomendável.

Palavras-chave: Crimes Virtuais, Internet, Informática**.**

INTRODUÇÃO

É inegável que no mundo atual sofremos muita influência das tecnologias, sobretudo da internet que, por sua vez, afeta os relacionamentos e a maneira como obtemos conhecimento e trocamos informação. Além das questões comportamentais, o uso crescente de tecnologia conectada á internet, trouxe à tona outro problema: a invasão ilegal de informações e de privacidade por pessoas que possuem conhecimento específico e que podem, com isso prejudicar a vida dos envolvidos.

Tratam-se de danos materiais como fraude, espionagem, sabotagem e ataques a contas bancárias; crimes contra a honra e a liberdade individual, bem como crimes de pedofilia e divulgação de imagens pornográficas. Nesse ensejo, a Lei 12737/2012, intitulada pela imprensa de "Lei Carolina Dieckmann" por ter sido aprovada na época em que a atriz global foi vítima da divulgação indevida de fotos íntimas obtidas pela invasão de seu computador, dispõe sobre a tipificação criminal de delitos informáticos, acrescendo ao Código Penal artigos que criam um novo tipo penal para tutelar os crimes cibernéticos.

Em um artigo nomeado "Tem Boi na Linha", em alusão à expressão usada para designar invasões por *hackers*, Heitor Shimizu e Ricardo B. Setti advertem que o destaque do Brasil no crescente uso da grande rede mundial de internet tem animado os interessados em invadir sistemas. Segundo eles:

> A rede, que liga mais de 35 milhões de computadores em todo o mundo, é um dos caminhos prediletos para as invasões. Até agora, só tinham acesso a ela instituições acadêmicas e governamentais. E muitas já foram alvo dos hackers. Só nos cinco primeiros meses desse ano, a Empresa Brasileira de Pesquisas Agropecuárias, a Universidade de São Paulo, a Universidade Estadual de Campinas, a Universidade Federal de Pernambuco e até o governador desse Estado tiveram seus computadores invadidos. Em agosto, foi a vez do Jockey Clube, no Rio de Janeiro. Seu sistema travou exatamente na hora das apostas do Grande Prêmio Brasil, prova tradicional do turfe. O saldo das brincadeiras inclui a destruição de pesquisas e

arquivos importantes[1].

Essa modalidade de crime tem se alastrado no Brasil. Para designar as formas de comportamentos ilegais ou, de outro modo, prejudiciais à sociedade, que se realizam pela utilização de um computador, são usadas várias expressões, tais como: criminalidade de informática, infrações cometidas por meio de computador, crimes de computador, *cybercrimes*, *computer* crimes, computing crimes, delito informático, crimes virtuais, crimes eletrônicos ou, ainda, crimes digitais, crimes cibernéticos, infocrimes, crimes perpetrados pela Internet, entre outras nomenclaturas que devem surgir dia após dia no universo da informática.

Ante a ampla possibilidade de ataques digitais, os instrumentos do crime podem ser dos mais variados, tais como computadores de mesa (*Desktops*), computadores portáteis (*notebooks* e *netbooks*), telefones celulares com funções integradas (*smartphones*), ou dispositivos mais singelos tecnologicamente, tais como circuitos integrados (processadores ou chips), dispositivos de armazenamento de dados (pendrives ou hard disks) ou outros dispositivos similares que processem dados, além dos recursos empregados por meio de engenharia social.

Para penetrar nesse universo, é preciso antes conhecer seus agentes, seus sujeitos ativos. Embora comumente todos sejam tratados pelo termo hacker, há uma forte distinção de comportamentos e objetivos que difere os hackers dos crackers.

1. AGENTES DE CRIMES CIBERNÉTICOS: HACKERS, CRACKERS E ENGENHEIROS SOCIAIS

1.1 Hackers

O termo hacker foi introduzido à informática aproximadamente na década de 1960, para designar pessoas que conseguiam resolver problemas comuns de formas incomuns. Por essa característica criativa, o termo “hacker” pode ser traduzido para “fuçador”, segundo defende Assunção, em *Segredos do Hacker Ético*. O autor pondera que devemos abolir o estereótipo de criminoso digital, já que ser curioso não necessariamente significa ser bandido. Nenhum outro termo (fuçador) traduz melhor

[1] SHIMIZU, Heitor; Ricardo B. SETTI. "Tem boi na linha." *Revista Super Interessante, São Paulo* 10 (1995): 26-33.

alguém que vai a fundo em alguma questão, revirando-a até resolver o problema. “Einstein foi um fuçador. Newton foi um fuçador também. Foram pessoas que pensaram à frente do seu tempo”[2].

É preciso entender que há uma diferença entre hackers e crackers:

> Alguns hackers destroem os arquivos ou unidades de disco inteiras das pessoas. Eles são chamados de *Crackers* ou *vândalos.* Alguns hackers novatos não se preocupam em aprender a tecnologia; eles apenas querem baixar as ferramentas dos hackers para entrar nos sistemas de computadores, Esses são chamados de *script kiddies.* Os hackers mais experientes, com habilidades em programação, desenvolvem programas para hackers e os postam na Web e nos sistemas de bulletin board. Em seguida, temos os indivíduos que não têm nenhum interesse em tecnologia, mas que usam o computador apenas como uma ferramenta que os ajuda a roubar dinheiro bens ou serviços[3].

De acordo com Mitnick, em geral os *hackers* detém, assim como os *crackers*, um vasto conhecimento de informática, sabem encontrar com facilidade qualquer brecha de segurança nos sistemas, porém, não altera nem danifica nada. Os *hackers* muitas vezes são contratados por empresas que pretendem testar os seus sistemas de segurança, de modo a procurar por eventuais falhas que comprometam seus dados sigilosos ou o próprio funcionamento da empresa[4].

Sandro D'Amato Nogueira discorre sobre o conceito de hacker:

> Este indivíduo em geral domina a informática e é muito inteligente, adora invadir sites, mas na maioria das vezes não com a finalidade de cometer crimes, costumam se desafiar entre si, para ver que consegue invadir tal sistema ou página na internet, isto apenas para mostrar como estamos vulneráveis no mundo virtual. Várias empresas estão contratando há tempos os Hacker's para proteção de seus sistemas, banco de dados, seus segredos profissionais, fraudes eletrônicas etc[5].

Outro termo comumente associado aos hackers é o "White Hat". Esse termo é designado para aqueles que apesar do conhecimento das brechas e falhas dos sistemas não cometem, em tese, nenhum crime.

De acordo com Assunção, os "White Hat" são os "hackers do bem", como descreve:

> Hacker White-Hat seria o "hacker do bem", chamado de "hacker chapéu branco". É aquela pessoa que se destaca nas empresas e instituições por ter um conhecimento mais elevado que seus colegas, devido ao autodidatismo

[2] ASSUNÇÃO, 2008, p. 7.
[3] MITNICK;SIMON, 2003, p. 12.
[4] Idem.
[5] NOGUEIRA, 2008. p. 61.

> e à paixão pelo que faz. Não chega a invadir sistemas e causar estragos, exceto ao realizar testes de intrusão. Resumindo: tem um vasto conhecimento, mas não o usa de forma banal e irresponsável[6].

Com base nos conceitos acima transcritos, pode-se afirmar que os *hackers* ou *White hats* não procuram causar danos, porém, isto não significa que não cometem crimes. O fato de invadir, por exemplo, um sistema ou computador sem autorização, ainda que sem alterar ou danificar nada, pode caracterizar um crime.

1.2 Crackers

Os crackers são os criminosos que possuem um vasto conhecimento de informática e utilizam deste conhecimento para encontrar brechas no ciberespaço de modo a causar danos a terceiros ou obter alguma informação confidencial. Ao contrário dos *hackers* que são chamados de "White Hat", os *crackers* tem como sinônimo a expressão em inglês "Black Hat", conforme verificado abaixo:

> Hacker Black-Hat: "Hacker do Mal" ou "chapéu negro". Esse, sim, usa seus conhecimentos para roubar senhas, documentos, causar danos ou mesmo realizar espionagem industrial. Geralmente tem seus alvos bem definidos e podem passar semanas antes de conseguir acesso onde deseja, se o sistema for bem protegido[7].

1.3 Engenheiros sociais

A engenharia social usa a influência e a persuasão para enganar as pessoas. O engenheiro social pode aproveitar-se das fraquezas das pessoas para obter as informações com ou sem o uso da tecnologia. Engenharia Social é, portanto, a ciência que estuda como o conhecimento do comportamento humano pode ser utilizado para induzir uma pessoa a atuar segundo seu desejo. Em outras palavras, é “fazer com que as pessoas façam coisas que normalmente não fariam para um estranho”[8].

Não se trata de hipnose ou controle da mente, as técnicas de Engenharia Social são amplamente utilizadas por detetives (para obter informação) e magistrados (para comprovar se um declarante fala a verdade). Também é utilizada para lograr todo tipo de fraudes, inclusive invasão de sistemas eletrônicos.

---

[6] ASSUNÇÃO, 2008.p. 13.

[7] ASSUNÇÃO, 2008, p. 13.

[8] MITNICK;SIMON, 2003, p.16.

2. EM CASO DE CRIMES DIGITAIS

Tornou-se muito difícil se defender das invasões digitais, mas há algumas medidas se serem tomadas caso haja a ocorrência das mesmas. Por se tratar de uma nova espécie de crime, onde não há um entendimento consolidado a respeito do método probatório e das medidas necessárias à conservação das provas obtidas, é necessário que o profissional de tecnologia de informação, a autoridade policial e os demais operadores do Direito empreguem o maior zelo possível quanto à preservação dos indícios.

Inicialmente, o administrador de sistema ou de redes, ou qualquer profissional de tecnologia de informação pode apresentar delação à autoridade policial quando constatar a ocorrência de crime digital. A *notitia criminis* (notícia do crime), que é o conhecimento pela autoridade, espontâneo ou provocado, de um fato aparentemente criminoso deve ser apresentada na espécie de delação provocada, que é quando qualquer pessoa pode noticiar o fato delituoso à autoridade policial, dando ensejo à instauração de inquérito. É o que faculta o Código de Processo Penal:

> Art. 5º - Nos crimes de ação pública o inquérito policial será iniciado: (...)
> § 3º - Qualquer pessoa do povo que tiver conhecimento da existência de infração penal em que caiba ação pública poderá, verbalmente ou por escrito, comunicá-la à autoridade policial, e esta, verificada a procedência das informações, mandará instaurar inquérito.

Tavares e Reis ponderam que o delator poderá elaborar um documento simples contendo seu nome e dados pessoais, especificando as provas que possui que comprovem o cometimento dos crimes digitais, e, caso identifique, indícios de quem cometeu tal conduta. Após, pode protocolar em delegacia de polícia, endereçado à autoridade policial, no caso, o Delegado de Polícia Civil[9].

No caso da ocorrência de um crime digital, os cuidados para preservar o estado e conservação do aparelho afetado são muito importantes. Em caso de utilização de *malware*, *phishing*, *DOS attack*[10], vários dados podem ser perdidos com o simples desligamento do aparelho que o agente malicioso utilizou para o propósito delitivo. Dessa forma, recomendamos enfaticamente que não se desligue qualquer aparelho que tenha relação com o crime perpetrado, tendo em vista que informações

[9] Tavares e Reis, 2014.
[10] Programas maliciosos que são usados para facilitar invasões.

importantíssimas podem ser perdidas.

Atualmente, a maioria dos aparelhos informáticos se utiliza de Memória RAM, a qual pode conter informações essenciais para o deslinde da conduta delituosa, trazendo importantes relevâncias penais. Por se tratar de uma memória volátil, a qual é apagada quando a alimentação elétrica da memória é perdida. Como precaução, o profissional de tecnologia de informação e a autoridade policial devem preservar, portanto, as máquinas ligadas até a chegada do perito.

Não devem, ainda, deixar que o ofendido adultere os dados contidos nos aparelhos por qualquer forma, seja pela modificação do conteúdo pela manipulação da própria máquina, seja pela destruição física do aparelho, a qual pode se dar, inclusive, pela indução magnética (emprego de ímãs próximo ao aparelho), por impactos violentos ou desligamento da fonte de energia.

Recomenda-se, ainda, a identificação do endereço IP local, em intranet, caso a invasão se dê por usuário da própria rede interna, e identificar a sua vinculação ao usuário.Quanto à autoridade policial, caso tenha identificado o endereço IP em rede pública, é possível solicitar informações aos provedores de acesso que garantiram acesso ao agente malicioso através do referido endereço. São essas, em síntese, as medidas que recomendamos em face da constatação de um crime digital.

3. LEGISLAÇÃO PENAL ACERCA DOS CRIMES CIBERNÉTICOS

Entrou em vigor no dia 30/02/2012 a Lei Federal nº 12.737/2012 que trata sobre os crimes de Internet, que foi apelidada de Lei Carolina Dieckmann, que tipifica os crimes informáticos, com a inclusão no Código Penal dos artigos 154-A e 154 - B, dos parágrafos primeiro e segundo no artigo 266 e parágrafo único no artigo 298. Essa legislação traz uma equiparação da clonagem de cartões á falsificações de documentos pessoais. Isso representa um avanço, porque antes havia uma grande dificuldade em criminalizar quem clona cartões e obtém dados, uma vez que só era possível incriminá-lo no momento em que realiza a fraude.

O artigo 154-A versa sobre o crime de invasão de dispositivo informático, no qual o bem protegido é a inviolabilidade dos segredos, ou seja, os dados e informações armazenados no computador, podendo ser de pessoas físicas como de

pessoas jurídicas de direito privado (empresas) e de direito público (estado, órgãos e entidades). Doravante, qualquer pessoa que praticar qualquer conduta ilegal relacionada ao universo cibernético terá cometido crime, sendo que o tipo penal é expresso e claro quando restará configurado o delito, inclusive na forma qualificada[11].

O artigo 154-A especifica que nos casos do crime de invasão de dispositivo informático a ação penal somente poderá ter prosseguimentos e houver representação, com exceção se o delito tiver sido cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviço público.

4. METODOLOGIA

Por se tratar de pesquisa exploratória, o presente artigo científico foi realizado por meio de pesquisa bibliográfica, ou seja, a partir de leituras de livros e artigos relacionados ao tema. Na concepção metodológica de Severino, à qual nos atemos para justificar o empenho em ler material publicado acerca da pesquisa aqui apresentada, temos que:

> A pesquisa bibliográfica é aquela que se realiza a partir do registro disponível, decorrente de pesquisas anteriores, em documentos impressos, como livros, artigos, teses etc. Utiliza-se de dados ou de categorias teóricas já trabalhados por outros pesquisadores e devidamente registrados. Os textos tornam-se fontes dos temas a serem pesquisados. O pesquisador trabalha a partir das contribuições dos autores dos estudos analíticos constantes dos textos[12].

Coaduna-se com essa ideia, a definição empregada por Lakatos e Marconi, na qual o aproveitamento de ideias já expostas e da não repetição de dados é fundamental na escrita científica, uma vez que “uma procura de tais fontes, documentais ou bibliográficas, torna-se imprescindível para a não duplicação de esforços, a não ‘descoberta’ de ideias já expressas, a não inclusão de ‘ lugares-comuns’ no trabalho”[13].

A pesquisa bibliográfica pode também ser entendida ser definida como contribuições culturais ou científicas realizadas no passado sobre um determinado assunto, tema ou problema que possa ser estudado. Ainda fazendo uso das definições

[11] TAVARES; REIS, 2015, p.16.
[12] SEVERINO, 2007, p.122.
[13] LAKATOS; MARCONI, 2010, p. 208.

que tomamos emprestadas das referidas autoras, temos que a pesquisa bibliográfica,

> abrange toda bibliografia já tornada pública em relação ao tema estudado, desde publicações avulsas, boletins, jornais, revistas, livros, pesquisas, monografias, teses, materiais cartográficos, etc. [...] e sua finalidade é colocar o pesquisador em contato direto com tudo o que foi escrito, dito ou filmado sobre determinado assunto [...]"[14].

O registro disponível sobre determinado assunto deve ser analisado quando se decide estudar um tema já focado em pesquisas anteriores, por isso nessa pesquisa foi levado em conta artigos publicados sobre o tema. Segundo Antônio Joaquim Severino, trabalhar a partir de contribuições de outros autores, como livros, artigos e teses, é um método de pesquisa científica adequado ao desenvolvimento de estudos temáticos.

Dessas acepções sobre metodologia, é imperativo afirmar que todo trabalho científico, toda pesquisa, deve ter o apoio e o embasamento na pesquisa bibliográfica, para que não se desperdice tempo com um problema que já foi solucionado. Não se trata de mera repetição do que já foi escrito sobre o tema, mas sobretudo, "propicia o exame de um tema sob novo enfoque ou abordagem, chegando a conclusões inovadoras"[15].

Em suma, pode-se dizer que a revisão bibliográfica ou pesquisa bibliográfica oferece ao estudante/pesquisador "reforço paralelo na análise ou manipulação de suas informações"[16].

Em função do exposto, no primeiro momento dessa pesquisa, foi realizado um levantamento bibliográfico de obras relacionadas ao debate sobre crimes cibernéticos, privilegiando artigos disponíveis *on line* por se tratar de assunto relativamente novo.

5. CONSIDERAÇÕES FINAIS

Considerado um efeito da modernidade, o surgimento de crimes cibernéticos merece atenção de legisladores por ser uma seara ainda nova, com algumas controversas e imensa necessidade de debate. Diante do anonimato dos criminosos torna-se impreciso o poder de puni-los, mas é necessário seguir o debate e a difusão de esclarecimentos acerca do tema, até uma maior definição do Congresso Nacional

[14] Idem, p. 183.
[15] LAKATOS; MARCONI, 2010, p. 166.
[16] Idem.

para apurar e punir tais crimes digitais, com base nos tipos penais vigentes.

Contudo, enfatiza-se que é necessário, mais do que a criminalização específica, o esclarecimento técnico aos operadores do Direito, à autoridade policial, aos administradores de sistemas informáticos, aos magistrados e membros do Ministério Público na defesa das vítimas que podem ser afetadas moralmente com a exposição de segredos e imagens, bem como serem lesadas economicamente com a clonagem de cartões de crédito e fraudes eletrônicas.

6. REFERENCIAL BIBLIOGRÁFICO

ASSUNÇÃO, Marcos Flávio Araújo. Segredos do hacker ético. **3ª edição. Florianópolis: Visual**, 2008.

BRASIL. Decreto-Lei no. 2.848 de 7 de setembro de 1940. **Código Penal**. Disponível em <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em: 06 set. 2015, às 17:00.

_____Lei 12.737, de 30 de novembro de 2012. Aprova a tipificação criminal de delitos informáticos. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em 07 set. 2015, às 9:10.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de metodologia científica**. Atlas, 2010.

MITNICK, Kevin D.; SIMON, William L. **A arte de invadir**. São Paulo: Person Prentice Hall, 2005.

NOGUEIRA, Sandro D'Amato. **Crimes de Informática.** São Paulo: BH Editora, 2008.

SEVERINO, Antônio Joaquim. **Metodologia do trabalho científico**. 23º ed. 11º reimpressão. São Paulo: Cortez, 2007.

SHIMIZU, Heitor; SETTI, Ricardo. **Tem boi na linha: hackers os espiões**

cibernéticos. Super Interessante, São Paulo, out. 1995. Disponível em:< http://super.abril.com.br/tecnologia/tem-boi-linha-hackers-espioes-ciberneticos-441127.shtml>. Acesso em: 09 set. 2015, às 15:35.

TAVARES, Adriano Lopes; DOS REIS, Rafael Rocha. **Crimes de Informática**. Revista Jurídica, v. 2, p. 28 a 46, 2015.