ETIC 2015 - Encontro de Iniciação Científica
ISSN 21-76-8498

CRIME CIBERNÉTICO A LUZ DOS ARTIGOS 154-A E 154-B DO CÓDIGO PENAL BRASILEIRO

Thatiana Dal Fabbro Costa LIMA[1]
Marina Barroquelo Viana LOPES[2]

RESUMO: O presente trabalho apresentará os conceitos de crime cibernético suas penas, identificando sua autoria delitiva e como foi o surgimento desse tipo de crime através da evolução do mundo virtual.

PALAVRAS-CHAVE: Internet. Crime cibernético. Cracker. Pena.

1. INTRODUÇÃO

A internet evoluiu de tal maneira que sua utilização passou a ser em massa e fazer parte da vida de toda a humanidade. Com ela, não só os meios de comunicação foram aprimorados, mas também a incidência de crimes, haja vista que com ela vieram a facilidade e a praticidade dos criminosos em encontrar suas vítimas e consumarem os delitos. Foi com o advento da Lei 12.737/2012 que o legislativo passou a regular as ações de criminosos que utilizam desse meio para a prática de delitos. No entanto, por se tratar de um meio de acesso mundial e de difícil descobrimento de autoria, além de possuir uma sanção muito branda, ainda é difícil processar e julgar esses tipos de sujeitos e delitos.

2. EVOLUÇÃO DA INTERNET

Em meados dos anos 70, o surgimento da internet veio basicamente para fins de pesquisas acadêmicas e científicas. A internet também passou a ser uma forma de propagação da liberdade de expressão, já que o número de pessoas atingidas pelos meios eletrônicos era considerável.

[1]Discente do 6º termo do curso de direito do Centro Universitário "Antônio Eufrásio de Toledo" de Presidente Prudente. thati.dfcl@hotmail.com
[2]Discente do 6º termo do curso de direito do Centro Universitário "Antônio Eufrásio de Toledo" de Presidente Prudente. ma-bviana@hotmail.com

ISSN 21-76-8498

Com o passar dos anos, os livros começaram a ser substituídos pelos *bits* para fins de pesquisas e leituras. A globalização foi evoluindo e com ela novos ideais foram trazidos, novas formas de pensar e de se expressar, novo modo de ver o mundo afora.

A evolução da internet foi e continua sendo surpreendente. O acesso das pessoas ao mundo virtual vem evoluindo a cada dia devido as grandes alterações econômicas, políticas, sociais e até culturais que vem propiciando uma melhora na qualidade de vida em geral.

Além disso, a tecnologia vem se manifestando na vida das pessoas de maneira muito incisiva, até mesmo na população economicamente menos favorecida.

O uso da internet se expandiu de modo inimaginável, seja para fins de pesquisas, comércio, bate-papo, diversão, localização, até mesmo para transações bancárias. Tudo isso podendo ser feito nos mais variados lugares, como em bares, no sofá de casa, na academia, em restaurantes, no trabalho, na faculdade etc.

Além dos meios de comunicação em geral, os meios de acesso a internet trouxeram uma grande melhora para sua utilização. Hoje os computadores foram substituídos por muitos usuários pelos notebooks e estes pelos *smartphones*. Tudo isso para o auxílio e a facilidade para as atividades rotineiras.

Atualmente, a internet tem sido utilizada para diversas finalidades, devido o barateamento dos meios de acesso à rede mundial. Porém o demasiado acesso aos meios eletrônicos trouxe consigo um aumento significativo da criminalidade.

São inúmeros tipos de infrações que podem ser cometidas através da internet, como a falsificação de dados, transmissão e posse de fotografias, “estelionatos eletrônicos”, racismo, injúria etc.

Com o aumento da incidência de tais delitos e com cada vez mais constância, o poder legislativo tomou iniciativas para criar medidas protetivas para combater esses crimes.

Uma das medidas foi a criação da Lei 12.737/2012 apelidada por “Lei Carolina Dieckmann”, isto porque a lei se inspirou no caso da atriz que teve seus dados pessoais e fotos íntimas copiados de seu computador no momento em que

ISSN 21-76-8498

este esteve em conserto e tais dados foram divulgados na internet pelos sujeitos que arrumavam o computador.

Essa lei trouxe algumas inovações ao Código Penal, como, por exemplo, os artigos 266 e 298, que tiveram seu texto alterado para se adequarem a época em que estamos incluindo o mundo virtual.

No entanto, essas penas ainda são muito brandas e há uma grande dificuldade em descobrir a autoria desses crimes virtuais em muitos casos concretos, já que são grandes os obstáculos para encontrar dados dos computadores, onde praticaram o delito e quem os pratica.

A internet evoluiu com o homem para o bem de todos, possibilitando os mais variados conhecimentos, diversão, inclusão de culturas etc. Hoje distância deixa de existir quando se encontra online. Porém, a internet, assim como o homem, também evoluiu para o mal em alguns aspectos, haja vista que é através dela que muitos atos ilícitos são praticados.

Foi pensando nesse crescimento do mundo virtual que o legislador não se deixou omisso, passando a regulamentar leis e sanções para que haja o controle desses delitos cibernéticos.

2.1. ACESSO À INTERNET

O acesso à internet vem crescendo a cada dia. Segundo pesquisas esse crescimento se dá muito em razão dos celulares. O celular vem sendo o meio mais fácil de conectar na internet, e através dele que os números de acessos cresceram excessivamente. Não só o uso do celular, mas como venda de computadores, e ainda da própria internet também cresce aceleradamente.

Diz site do G1 com base na pesquisa feita pelo IBGE:

> Em 2013, as regiões Sudeste (57,7%), Sul (54,8%) e Centro-Oeste (54,3%) tiveram proporções de internautas superiores à media nacional de 50,1%. O Norte, com 38,6% do total da população, e o Nordeste, com 37,8%, ficaram abaixo. Todas as regiões brasileiras registraram crescimento de internautas

ISSN 21-76-8498

> em 2013, com destaque para o Nordeste (4,9%) e o Sul (4,5%). O Sudeste (2,2%), e o Centro-Oeste (1,3%) e o Norte (0,4%) aparecem em seguida.

Segundo tais pesquisas, em 2013 mais de 50% da população brasileira estiveram conectadas à internet. De acordo com dados específicos, a proporção de internautas brasileiros passou de 49,2% em 2012, para mais da metade em um ano.

3. O CRIME CIBERNÉTICO

Crime informático, crime cibernético, e-crime, crimes eletrônicos, *cybercrime* são termos utilizados para se referir a toda atividade cujo computador é utilizado como ferramenta, como meio para prática de determinado delito.

Segundo Guilherme Guimarães Feliciano (2001, p. 31):

> por criminalidade informática o recente fenômeno histórico-sócio-cultural caracterizado pela elevada incidência de ilícitos penais (delitos, crimes e contravenções) que tem por objeto material ou meio de execução o objeto tecnológico informático (*hardware, software,* redes e etc)

O crime cibernético é distinguido pelos doutrinadores penais de duas formas: crime cibernético puro e crime cibernético impuro. Estes são crimes “comuns” que utilizam a internet como meio de cometer o delito, é usado como instrumento para cometerem condutas maiores, como é o caso do estelionato, por exemplo. Já os puros são aqueles cujo bem jurídico é a informática. A internet é não só o instrumento, mas também onde o crime se consuma.

Esse crime aqui estudado deriva da internet e se consuma por elas, mas também é através dela que os criminosos vêm praticando outros delitos, não só os puros. Através do uso de um computador ou ainda de uma rede de computadores que os crimes podem ser praticados.

O índice do uso da internet aumentou tanto que os sujeitos ativos dos delitos encontraram um meio fácil e rápido de chegarem aos seus objetivos e em muitas vezes sem que sejam descobertos.

Por exemplo, é através da invasão de dados de um computador que se pode furtar todo dinheiro de uma conta bancária, copiar fotos pessoais para ameaçar a vítima em troca de dinheiro ou manchar sua imagem perante a sociedade com isso. O crime ainda pode ser cometido com a utilização de e-mail, grupos de debate, redes sociais, sites de venda etc.

Victor Eduardo Rios Gonçalves (2013, p. 316) dispõe que não há a necessidade da conexão com a internet para que haja a consumação do delito:

> O próprio tipo penal salienta que o computador violado pode estar ou não conectado à internet, posto que, embora menos comum, é possível instalar pessoalmente programas em computadores não conectados à rede, que fazem cópias dos arquivos da vítima (imagens, textos etc.) e que, posteriormente, são retirados, também, pessoalmente, pelo agente.

Não resta dúvida quanto ao conceito do crime cibernético. Doutrinadores entendem unificadamente que são crimes cometidos através da internet e que nela se consumam, ou até mesmo que não seja através dela, mas que seja necessário o seu uso para que os vírus ou instalações obtenham o resultado esperado. E foi buscando soluções e sanções para os criminosos e que estas sejam eficazes e justas, que o legislativo trouxe a vigência da Lei 12.737/12.

3.1. MEIOS UTILIZADOS PARA COMETER OS CRIMES

Os agentes dos delitos cibernéticos se utilizam de vários meios para conseguirem a consumação do crime. Basta que haja a utilização de um hardware para que invadam o sistema de milhares de pessoas.

A invasão a um sistema pessoal normalmente é feita através de vírus instalados nos computadores das vítimas para que assim consigam buscar os dados e informações necessárias dentro do software de cada sujeito.

O mais comum é a utilização de vírus “silenciosos”, que são aqueles que invadem o sistema através de um simples e-mail enviado pelo agente do crime para a vítima que quer alcançar. Com esse e-mail aberto, o vírus se instala facilmente em

instantes e a partir daí começam a copiar os dados gravados nos computadores, celulares, e-mails, contas bancárias online etc. das vítimas.

Os agentes ofensores se utilizam de programas de registro de digitação, Cavalos de Tróia, vírus e rootkits, que são os meios mais comuns para a invasão de sistemas de computadores ou outras localizações com a finalidade de cópia de dados, informações pessoais, fotos etc., como afirma o programa de segurança da internet Norton Secured em seu website (acesso em 24/08/2015).

A vulnerabilidade que a internet traz para as pessoas do mundo inteiro causa uma grande facilitação para os ofensores cometerem esse tipo de delito, que foi introduzido no Código Penal através lei 12.737/12.

Os vírus, segundo Guilherme Guimarães Feliciano (2001, p. 73) “são criados por pessoas detentoras de conhecimento técnico, para emulação ou sabotagem; todo programa contaminado é portador de transmissor potencial do vírus”.

A cada instante o número de incidência desse tipo de crime aumenta, haja vista que o número de usurários da internet cresceu desde os últimos tempos, elevando junto com isto o número de ofensores criadores de websites e vírus contaminados, prontos para atacar uma nova vítima a cada “click”.

Com a evolução internet, houve uma grande facilidade não só ao próprio usuário para acessar seus dados particulares, como também para os sujeitos do delito, que se valem tanto de simples vírus de um link de e-mail clicado inocentemente, quanto ao mais temido Cavalo de Troia instalado a partir de sites da web com grande acesso.

4. LEI 12.737/2012 E A INTRODUÇAO DOS ARTIGOS 154-A E 154-B NO CÓDIGO PENAL

ETIC 2015 - Encontro de Iniciação Científica
ISSN 21-76-8498

A Lei 12.737/12 foi sancionada em novembro de 2012, sem vetos, e entrou em vigor dia 02 de abril de 2013. Foi criada com o fim de punir os crimes praticados através da internet, trazendo para o Código Penal um novo crime disposto nos artigo 154-A e 154-B, que tratam do crime de "Invasão de Dispositivo Informático" e sua ação penal, respectivamente, além de alterar o texto dos artigos 266 e 298 do mesmo Código.

Essa lei foi apelidada por Lei Carolina Dieckmann, nome de uma atriz muito conhecida que teve suas fotos em situação íntima divulgadas na internet. Esse foi o caso fundamental que fez com que houvesse finalmente uma lei com previsão de crimes cibernéticos.

Antes da criação dessa lei, os crimes cometidos via internet eram solucionados através do Código Penal sem as alterações, mas nem sempre de forma perfeita, pois os delitos digitais não deixavam de ter sua característica de crime, conforme o disposto por Omar Kimaniski (2009, p. 21):

> O furto de componentes de computador não deixa de ser furto. A lavagem de dinheiro não deixa de ser um crime. Fraude é fraude. Extorsão é extorsão. Sejam esses crimes cometidos através da Internet, ou de outros mecanismos tradicionais, são eles crimes previstos em lei.

Porém, a partir de abril de 2012, os crimes cometidos através desse objeto material passaram ser solucionados a luz do Código Penal conforme os rtigos 154-A e 154-B com redação dada pela Lei 12.737/2012.

Apesar da criação e alteração desses dispositivos, agora com previsão legal, as penas desses crimes são muito brandas, como a pena no *caput*, que é de detenção de três meses a um ano e multa. Penas assim não intimidam os criminosos e terceiros a não cometerem o crime novamente ou a não passarem a cometer. Esses criminosos deveriam ser punidos de maneira mais severa, já que esse tipo de delito está cada vez mais presente em nossa realidade atual.

Sendo assim, o advento da Lei trouxe uma melhora para a punição específica do delito de invasão de dispositivo informático, mas sua pena não está de acordo com a incidência do delito ou com a quantidade de sujeitos que vem surgindo. Com uma pena maior, melhor seria sua proporcionalidade, evitando o aparecimento de tantos criminosos cibernéticos e o aumento do número de vítimas que surgem a cada dia.

ISSN 21-76-8498

5. AUTORIA DO CRIME

O crime disposto no artigo 154-A do Código Penal, por ser crime comum, pode ser praticado por qualquer pessoa, desde que se valha da internet para atuar no crime. Não basta estar conectado, o crime deve ser próprio da internet, como é o caso de roubos de dados, por exemplo.

O sujeito ativo do delito é o chamado *cracker*, que por sua vez não pode ser confundido com um *hacker*, que segundo Sônia Aguiar do Amaral Vieira (2002, p. 100) é:

> Via de regra, um jovem, fanático por computadores, que adora descobrir senhas e destruir as barreiras de segurança de outros computadores, muito mais pelo prazer de conseguir do que para roubar ou lesar o patrimônio alheio. [...] Através dele, são desenvolvidas as condutas de acesso, de conhecimento, de permanência e de utilização não autorizada em um sistema informático.

Já o *cracker*, é, de acordo com o Dicionário de Informática DICWEB (acesso em 29/08/2015):

> Aficionado por informática, profundo conhecedor de linguagens de programação, que se dedica à compreensão mais íntima do funcionamento de sistemas operacionais e a desvendar códigos de acesso a outros computadores. Ao contrário do *hacker*, utiliza seus conhecimentos para quebrar senhas de acesso a redes, provedores, programas e computadores com fins criminosos.

Assim, o sujeito ativo do tipo é pessoa com conhecimento específico, que possui mais informações sobre o mundo virtual do que as pessoas comuns ao seu redor. Ele se vale dessa característica porque encontra certa facilidade nesse tipo de delito, mas se diferencia do *hacker*, pois este o faz sem o dolo de cometer crimes, atua com o *animus jocandi*.

Além disso, a internet vem sendo o meio mais utilizado para o cometimento de crimes devido a grande dificuldade encontrada para descobrir a autoria do delito. No entanto, o que muitos *cracker* não percebem é que a mesma

ISSN 21-76-8498

facilidade que eles encontram para cometer crimes com pessoas mais vulneráveis ou com as mais protegidas na internet, pode ser usada pela investigação da polícia judiciária para encontrar a autoria do crime. Isto porque mesmo parecendo ser algo impossível para o mundo virtual, as pessoas sempre deixam rastros quando se trata de crime cibernético.

Mesmo que o autor do delito tome o maior cuidado para que não seja pego, os vestígios largados no caminho do mundo cibernético são muito comuns, tão comuns quanto no mundo real. E é função dos investigadores da polícia especialistas em crime cibernético buscar a autoria do crime para que então o promotor de justiça possa oferecer a denúncia, haja vista que a denúncia só poderá ser oferecida se estiver presente a justa causa.

Ainda assim, a dificuldade de encontrar o sujeito ativo do delito é grande, haja vista que a internet vem se aprimorando a cada minuto e com ela, aprimoram-se também os conhecimentos dos praticantes desses delitos, que muitas vezes passam despercebidos. Além de ser de alcance internacional, que faz com que a busca seja de alcance mundial, podendo dificultar ainda mais a busca pela autoria do delito.

6. PENA E AÇÃO PENAL

Consoante ao disposto no artigo 154-A do Código Penal, a pena para quem comete este crime é de detenção de 03 (três) meses a 01 (um) ano com a cumulação de multa.

Por se tratar de crime de menor potencial ofensivo, há a possibilidade de suspensão condicional do processo, que tem como requisito o mínimo de 2 anos. Portanto, de acordo com a Lei 9.099/95 o sujeito tem a possibilidade de não chegar ao menos a ser processado, trocando sua pena de detenção por restritivas de direito.

Incorre na mesma pena quem oferece, distribui, vende ou difunde dispositivo ou programa de computador, que é o caso disposto no §1º do artigo 154-A do Código Penal.

Quando o autor do delito traz prejuízo econômico para a vítima no momento da invasão ao dispositivo informático, sofrerá uma majoração em sua pena, que, conforme o §2º do artigo 154-A, será de um sexto a um terço.

Já no §3º desta lei, há uma forma qualificada, que passa a ter a pena de reclusão de 06 (seis) meses a 02 (dois) anos e a cumulação com a multa caso a conduta do sujeito, salvo não resulte em um crime mais grave:

> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
>
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave

O §4º traz a possibilidade de aumento de um a dois terços da pena da figura qualificada quando "houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos".

Outra forma de causa de aumento da figura do *caput* é o disposto no §5º:

> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
>
> I - Presidente da República, governadores e prefeitos;
>
> II - Presidente do Supremo Tribunal Federal;
>
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
>
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

A ação penal está descrita no artigo 154-B do Código Penal, que é pública condicionada a representação, portanto, só haverá a denuncia caso a vítima manifeste a sua vontade.

No entanto, quando o crime for cometido contra a Administração Pública Direta ou Indireta, ou ainda contra empresas concessionárias de serviços públicos, a ação penal será pública incondicionada, que quer dizer que a promotoria poderá

oferecer a denuncia assim que tiver provas concretas sobre o cometimento do delito e sua autoria.

Nesse sentido são as palavras do doutrinador Luiz Regis Prado (2014, p. 596):

> A ação penal nos delitos definidos pelo artigo 154-A é pública condicionada, salvo se o crime é cometido contra administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos, hipótese em que a ação é pública incondicionada.

A competência para processar e julgar o crime disposto no artigo 154-A, segundo o artigo 61 da Lei 9.099/95, será dos Juizados Especiais Criminais, conhecido como JECRIM.

CONCLUSÃO

Por tudo visto, são possíveis algumas conclusões. A evolução da internet trouxe consigo não só a melhoria da comunicação e informação para a humanidade, mas também um aumento na criminalidade. Hoje é possível distinguir o crime comum com o crime cibernético por causa do advento da Lei 12.737/12, que trouxe a possibilidade da punição específica para os sujeitos ativos do disposto no artigo 154-A do Código Penal. No entanto, tais delitos ainda são difíceis de ser processados e julgados por causa da dificuldade que existe para encontrar a autoria, pois a internet é um meio de difíceis rastros, é quase impossível de identificar de onde surgiu aquele ato praticado que levou a consumação do delito naquele dispositivo informático.

REFERÊNCIAS BIBLIOGRÁFICAS

Código Penal Brasileiro de 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Data da consulta: 25 de agosto de 2015

Lei n. 12.737/12. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Data da consulta: 25 de agosto de 2015

FELICIANO, Guilherme Guimarães. **Informática e Criminalidade:** primeiras linhas. Ribeirão Preto: Nacional de Direito, 2001. 137 p. ISBN 85-88289-02-4
GONÇALVES, Victor Eduardo Rios. **Direito Penal Esquematizado:** parte especial. 3.ed. São Paulo: Saraiva, 2013. 874 p. ISBN 9788502184688

KAMINSKI, Omar. **Internet Legal: o direito na tecnologia da informação**: doutrina e jurisprudência. 1. ed. Curitiba: Juruá, 2009. 291 p. ISBN 85-362-0439-7

PRADO, Luiz Regis. **Comentários ao código penal:** jurisprudência, conexões lógicas com os vários ramos do direito. 9. ed., rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2014. 1147 p. ISBN 978-85-203-5177-2

PRADO, Luiz Regis; CARVALHO, Erika Mendes de; CARVALHO, Gisele Mendes de. **Curso de Direito Penal Brasileiro.** 13. ed. rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2014. 1630 p. ISBN 9788520350683.

ROSA, Fabrízio. **Crimes de informática.** 1. ed. Campinas: Bookseller, 2002. 137 p. ISBN 85-7468-167-9

VANCIM, Adriano Roberto. **Direito & internet: contrato eletrônico e responsabilidade civil na web**: jurisprudência selecionada e legislação internacional correlata. Leme: Lemos & Cruz, 2011. 293 p. ISBN 9788599895559

DICWEB. **Dicionário Informática e Negócios**. Disponível em: <http://www.dicweb.com/cc.htm#cracker> Acesso em 29 de agosto de 2015.

CABETTE, Eduardo Luiz Santos. **Primeiras impressões sobre a Lei nº 12.737/12 e o crime de invasão de dispositivo informático**. Disponível em: <http://jus.com.br/artigos/23522/primeiras-impressoes-sobre-a-lei-n-12-737-12-e-o-crime-de-invasao-de-dispositivo-informatico#ixzz3jyb6JPMT>. Acesso em 25 de Agosto de 2015.

CAVALCANTE, Waldek Fachinelli. **Crimes Cibernéticos**. Disponível em: <http://jus.com.br/artigos/25743/crimes-ciberneticos/2#ixzz3jvzxCcLz>. Acesso em 28 de Agosto de 2015.

G1. **Mais de 50% dos brasileiros estão conectados à internet, diz Pnad.** Disponível em: <http://g1.globo.com/tecnologia/noticia/2014/09/mais-de-50-dos-brasileiros-estao-conectados-internet-diz-pnad.html>. Acesso em 28 de agosto de 2015.

MANZEPPI, Eduardo. **A chamada Lei "Carolina Dieckmann" (Lei nº 12.737/2012)**. Disponível em: <http://www.oabmt.org.br/Artigo/Artigo.aspx?id=166> Acesso em 29 de agosto de 2015