

CRIMES CIBERNÉTICOS: UM DESAFIO PARA O DIREITO PENAL NA ERA DA GLOBALIZAÇÃO

Blidônio Rodrigues de Carvalho Neto¹

Sandresson de Menezes Lopes²

RESUMO

Este trabalho busca analisar as mais diversas alterações jurídicas promovidas no ordenamento jurídico brasileiro quanto aos crimes cibernéticos. Para tanto, faz-se uma perspectiva histórica da evolução da tecnologia e da internet no Brasil e no mundo, e, paralelamente a isso, a evolução das ameaças cibernéticas. Assim, mostra-se que o ordenamento jurídico brasileiro ainda é carente de uma lei específica que regule tais delitos, impossibilitando assim que alguns crimes cibernéticos sejam punidos. Porém, percebe-se um esforço quanto a tipificação penal sobre o tema, no momento em que são editadas algumas leis específicas e a utilização da legislação existente para amparar legalmente os delitos no ambiente virtual.

Palavras chave: Crimes cibernéticos. Globalização. Internet. Falta de leis específicas que tipifiquem criminalmente os delitos.

CYBERCRIMES: A CHALLENGE TO CRIMINAL LAW IN THE GLOBALIZATION ERA

ABSTRACT

This study seeks to analyze the diverse legal changes implemented in the Brazilian legal system concerning the cybercrimes. Therefore, the historical perspective of the evolution of technology and the internet in Brazil and in the world is studied and, parallel to this, the evolution of cyber threats is also analyzed. Thus, it is shown that the Brazilian legal system is still lacking a specific law governing such offenses, thus making it impossible for some cyber criminals to be properly punished. However, an effort towards regularization on the subject is perceived, as specific laws are being edited and the existing legislation is already used to legally punish some crimes committed in the virtual environment.

Keywords: Cyber Crimes. Globalization. Internet. Lack of specific laws that criminalize cyber crimes.

¹ Acadêmico do Curso de Direito do Centro Universitário do Rio Grande do Norte – UNI-RN. E-mail: blidonio@hotmail.com

² Professor Orientador do Curso de Direito do Centro Universitário do Rio Grande do Norte – UNI-RN. E-mail: sandresson1@hotmail.com

1. INTRODUÇÃO

Hodiernamente, a utilização dos recursos tecnológicos e da internet está cada vez mais presente no dia a dia da sociedade contemporânea, seja para realização de compras, transações comerciais, fazer amizades nas redes sociais, busca pelo conhecimento, entre outros.

De fato, a internet trouxe à humanidade grandes benefícios. Porém, também trouxe consigo diversos problemas, gerando transtornos e danos as suas vítimas. É daí surgem os crimes cibernéticos, que se caracterizam como a prática de delitos por meio ou no ambiente virtual, ou seja, da internet. Esses delitos tem se intensificado no decorrer dos anos, seja pelo aumento no número de usuários, seja pelas vulnerabilidades descobertas paralelamente à sua evolução.

Isto posto, no segundo capítulo discute-se o que é a globalização e as consequências dessa globalização no direito penal, como a tão falada “expansão do direito penal”, bem como desencadear uma reflexão sobre essa expansão indesejada.

O capítulo três tratará dos crimes cibernéticos. Primeiramente será abordado o aspecto histórico do desenvolvimento tecnológico, desde o surgimento do primeiro computador, a criação das primeiras redes, o surgimento da internet, e sua evolução no mundo e, principalmente, no Brasil. Por fim, abordado todo o exposto anteriormente, será demonstrado como surgiram os crimes cibernéticos.

No capítulo quatro, se discutirá os principais desafios investigativos com relação aos crimes cibernéticos, que causam aos agentes investigadores uma grande preocupação, frente ao avanço tecnológico diário, acarretando uma dificuldade para se localizar os autores dos delitos cibernéticos. Também serão expostas as principais modalidades de crimes cibernéticos e suas peculiaridades.

O capítulo cinco trará as principais soluções trazidas por nosso ordenamento jurídico com a finalidade de prevenir a prática dos crimes cibernéticos, demonstrando ainda que há uma lacuna em nossa legislação quanto à tipificação de algumas condutas, e a utilização por analogia de outras condutas do “crime real”, tipificadas no Código penal, para o “crime virtual”.

E, finalmente, será feita a conclusão do trabalho, partindo dos principais aspectos que envolvem os crimes cibernéticos, os problemas que decorreram dele, a partir de uma análise crítica a respeito da legislação, e sugestões para a uma maior eficiência na busca pela proteção total das vítimas desses delitos.

2. O DIREITO PENAL NA ERA DA GLOBALIZAÇÃO

2.1 O QUE É GLOBALIZAÇÃO?

Não há, hodiernamente, uma conceituação padrão para o que conhecemos como globalização. A globalização pode ser definida como um processo social, econômico, político e cultural de integração entre os povos que compõem o planeta. Para Milton Santos (2007; pág. 23), a globalização é “o ápice do processo de internacionalização do mundo capitalista”. Dessa forma, a globalização permitiu uma grande circulação de informações entre as pessoas, integrando-as, facilitando assim suas relações.

De forma brilhante, Paulo Silva Fernandes (2001; p. 41-42) conceitua o termo globalização como

um estreitamento (e aprofundamento) espacio-temporal de toda uma estrutura econômica, social, política e cultural, suportado por uma densa, complexa e interligada rede de comunicações que, possibilitando-o, acelera todo um processo de diluição do uno no múltiplo, do ser-aí-diferente no ser-em-todo-o-lado-igual, de caldeirão onde se fundem diversidades culturais, econômicas, políticas e sociais, em consequência do qual cada vez menos se encontra um eu “genuíno”.

Porém, a globalização não trouxe apenas benefícios em prol da comunidade global. Também surgiram problemas decorrentes dessa integração em larga escala, criando assim um sentimento de insegurança social. Essa insegurança se traduz no fato da velocidade do avanço tecnológico mundial frente ao encurtamento das distancias existentes entre os países, devido, principalmente, à internet.

Paulo Silva Fernandes (2001; p. 39) destaca que

a internet é que realmente deu o passo em relação ao agora mundial. [...] Transformou o globo em aldeia, possibilitando que se esteja, virtualmente, em todo o lado e ao mesmo tempo desde o momento em que se tem acesso à ‘rede’.

O termo globalização não possui qualquer significado jurídico. Porém o seu alcance é estudado pelas mais diversas ciências sociais e econômicas, por razão de sua abrangência cotidiana. Devido a sua revolução no modelo de interação global, a globalização tem, portanto, gerado efeitos positivos e negativos, como a evolução das formas de delinquir, surgindo assim novos conceitos de criminalidade, diferentes da criminalidade “comum”.

2.2 DIREITO PENAL GLOBALIZADO E SUAS CONSEQUÊNCIAS (EXPANSÃO DO DIREITO PENAL)

A globalização trouxe, portanto, um estreitamento nas relações entre os Estados, redefinindo os conceitos de espaço e tempo, que assim afetaram vários campos sociais, dentre eles o direito penal, com o surgimento de novos modelos de criminalidade. Também trouxe consigo efeitos nunca antes vistos na história da humanidade, gerando crises internas e externas dos Estados.

A sociedade passa por evoluções e revoluções. A criminalidade está crescendo cada vez mais e com novas problemáticas. O Estado, em confronto com esses novos efeitos, passa a utilizar-se do direito penal com o objetivo de tutelar esses novos modos de criminalidade. O direito penal é posto em prova, já que existe uma necessidade, mas ao mesmo tempo uma dificuldade para a utilização dos institutos da persecução penal “tradicional”, no combate a essas novas criminalidades.

Com a utilização do direito penal para prevenção dessas novas problemáticas, o Estado cria uma expansão deste direito, alargando assim seu campo de atuação. Essa expansão, por muitas vezes, é criticada pela doutrina, já que desprestigia o direito penal, posto que ele deve ser apenas utilizado em *ultima ratio*, devido ao seu caráter subsidiário.

MarcoAntonio Marques da Silva (2006; p. 409), sobre a expansão da tutela penal, aduz que o direito penal

não pode apresentar-se como um instrumento além de seus limites de controle social, na sociedade de risco, ou sociedade complexa. O essencial, na técnica legislativa, é limitar a expansão, tendo em vista o risco que efetivamente ocorre para as pessoas, a fim de transformar uma conduta em conduta típica punível.

A criminalidade moderna trouxe uma sensação de insegurança coletiva, já que hoje, o acesso às informações é amplamente facilitado pela internet. Com isso, surgem correntes jurídicas que defendem a restrição da liberdade, dos direitos e das garantias fundamentais, amplamente inserida na nossa Constituição Federal. Essa corrente intervencionista de direitos e garantias fundamentais acaba por restringindo o desenvolvimento de novas técnicas para o combate à criminalidade moderna.

Claro, a expansão por muitas vezes é indevida, mas também não se pode, por qualquer motivo, ignorar a criminalidade globalizada moderna. Ela possui como características a

organização, a internacionalização e por ser uma *criminalidade dos poderosos (crimes of the powerful)*, segundo Anabela Miranda Rodrigues (2006; p. 282-283).

Portanto, com essa expansão, o direito penal deparou-se com alguns problemas, já que a criminalidade moderna necessita de uma atuação diferenciada dos instrumentos jurídicos tradicionais, bem como dos conceitos clássicos, que não se encaixam nas novas condutas existentes, o que acaba por gerar conflitos doutrinários, acarretando a expansão indevida do direito penal, na busca incessante pela proteção aos crimes modernos.

Marco Antonio Marques da Silva (2001; p. 137-138) afirma que

o direito penal da era da globalização tem um objetivo eminentemente prático, deve buscar uma uniformidade de respostas no campo jurídico penal entre os Estados no tocante ao tratamento da delinquência internacional.

3. CRIMES CIBERNÉTICOS

3.1 EVOLUÇÃO HISTÓRICA DOS RECURSOS TECNOLÓGICOS E DA INTERNET

Em 1946 surgiu o primeiro computador digital, denominado ENIAC, criado para automatizar o cálculo das tabelas balísticas. Até a década de 50, vários outros foram construídos, seguindo o avanço tecnológico da época.

No ano de 1957, no período da Guerra Fria, a URSS lançou seu primeiro satélite espacial, o famoso Sputnik. Em contrapartida, os Estados Unidos, por meio de seu presidente John Kennedy prometeu enviar um americano à Lua e criar um sistema de defesa de informações sigilosas que fosse à prova de destruição. Assim, surgiu a ARPA – *Advanced Research Project Agency*, uma agência com a finalidade de acelerar o desenvolvimento tecnológico e coordenar atividades relacionadas com o espaço e satélites.

No ano seguinte, foi criada a NASA – *National Aeronautics & Space Administration*, com a mesma finalidade da ARPA, o que ocasionou o seu enfraquecimento. Ocorreu também o redirecionamento de vários projetos militares para outros setores militares, que originalmente eram tratados pela ARPA.

Devido à esse enfraquecimento, a ARPA passou a realizar novos projetos, porém seguindo outra linha de pesquisa, não mais militar, como a computação interativa e os sistemas de tempo compartilhado, realizando parcerias com instituições de ensino, tornando sua atuação mais técnica e científica. Em 1961, a Universidade da Califórnia (UCLA) recebeu

da Força Aérea Americana um computador que ajudou na inserção da informática no seio da ARPA.

Segundo Manuel Castells (2001; p. 14), a Força Aérea americana, preocupada em proteger-se de uma eventual guerra contra a URSS, queria uma rede descentralizada de comunicação, que não dependesse somente de um núcleo central, ou seja, uma rede de comunicações totalmente independente que fosse invulnerável a qualquer tentativa de destruição ou controle.

E assim, surgiu a ARPANET, uma rede capaz de integrar computadores que estivessem distantes, possibilitando a comunicação de dados entre eles. Inicialmente, somente estavam interligados na ARPANET a Universidade da Califórnia (UCLA), a Universidade de Stanford e a Universidade de Utah. Com o tempo, alguns organismos militares e outras grandes universidades aderiram à ARPANET, o que consolidou a rede e, futuramente, seria a base para o que chamamos de Internet.

A ARPANET crescia rapidamente. Em 1973 realizou-se sua primeira conexão internacional, interligando a Inglaterra e a Noruega. Na década seguinte, a ARPANET se expandiu pelos Estados Unidos, interligando as universidades, órgãos militares e o governo.

3.2 A INTERNET NO BRASIL

No Brasil, o Instituto Brasileiro de Geografia e Estatística (IBGE) foi o primeiro a utilizar-se de um computador, no ano de 1964. No ano seguinte, foi criado o Serviço Federal de Processamento de Dados. Ainda em 1965, o Brasil se associou ao consórcio internacional de telecomunicações por satélite (INTELSAT). Além disso, também foi criada a Empresa Brasileira de Telecomunicações.

Em 1988 surgiram as primeiras redes brasileiras que ligavam as universidades brasileiras com universidades americanas. No mesmo ano, aconteceu a conexão à Bitnet da Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), do Laboratório Nacional de Computação Científica (LNCC) e da Universidade Federal do Rio de Janeiro (UFRJ), o que consolidou a internet no Brasil.

No ano de 1992, implementou-se a primeira rede conectada à internet, interligando as principais universidades brasileiras. Porém, a internet ainda não possuía uma interface gráfica, observada atualmente. Só era permitida a troca de *e-mails* entre os usuários.

Finalmente, após anos de sua implementação, o governo disponibilizou o uso comercial da internet, no ano de 1995. Porém, comparada com os dias atuais, a velocidade de

conexão daquela época era muito baixa. Nesse mesmo ano, foi criado o Comitê Gestor da Internet no Brasil (CGI.br), que tinha como finalidade “coordenar e integrar todas as iniciativas de serviços de internet no país, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados”.

Atualmente, a internet está consolidada em solo brasileiro. O usuário brasileiro tem como média de tempo online durante um mês 24 horas e 42 minutos, média esta superior à países como França, Estados Unidos, Austrália e Japão. Segundo o Ministério da Ciência e Tecnologia, são 60 milhões de computadores em uso no Brasil, com 80,7% destes com acesso à internet.

3.3 CONCEITO

Hodiernamente existe uma ampla gama de utilizações para a internet. Podem-se trocar mensagens, baixar arquivos, pagar contas, comprar produtos, acessar sites e etc. Em todas essas utilizações, há a possibilidade da existência de um usuário malicioso tentando se aproveitar, de qualquer modo que seja.

O termo “crimes cibernéticos” é utilizado para definir os delitos praticados contra ou por intermédio de computadores. Ou seja, é qualquer tipo de atividade ilegal que se utilize da internet ou de dispositivos tecnológicos e que tragam danos a outrem. Existe uma subdivisão dos crimes cibernéticos em “crimes cibernéticos abertos” e “crimes exclusivamente cibernéticos”.

Os “crimes cibernéticos abertos” são aqueles que podem ser praticados por intermédio de computadores ou pela forma clássica, ou seja, o computador é apenas um meio para sua prática, já que também poderia ser cometido por outros meios.

Já os “crimes exclusivamente cibernéticos”, como seu nome já diz, são aqueles que somente podem ser praticados com o uso de computadores ou de qualquer tecnologia que permita o acesso à internet.

Primeiramente, devemos compreender que existem as chamadas “condutas indevidas praticadas por computador”. Essas condutas são divididas em “crimes cibernéticos” e “ações prejudiciais atípicas”.

As “ações prejudiciais atípicas” são as condutas praticadas através da internet, que causam transtorno ou qualquer prejuízo para a vítima. Porém, essa conduta não possui previsão penal, o que impossibilita o indivíduo de ser punido pela mesma. Contudo, nada impede que ele seja responsabilizado no âmbito civil.

3.4 SURGIMENTO DOS CRIMES CIBERNÉTICOS

Os primeiros indícios de ameaças cibernéticas remontam à década de 50, mas somente na década de 60 que essa ameaça tomou forma, quando *“um grupo de programadores desenvolveu um jogo chamado Core Wars, capaz de se reproduzir cada vez que era executado, sobrecarregando a memória da máquina do outro jogador”*. Dessa primeira ameaça, também surgiu o primeiro antivírus, criado pelo mesmogrupo de programadores, e que era capaz de desativá-lo.

Na década seguinte, surgiram outras formas de ameaças cibernéticas, porém, nenhuma de grande porte, já que até a década de 80 os computadores eram utilizados por poucas empresas. Em 1982, Richard Skrenta, com apenas 15 anos, criou o que muitos consideram como o primeiro vírus desenvolvido para infectar computadores.

Importante ressaltar que nessa época, ainda não se conhecia o termo “vírus de computador”, que só foi difundido em 1984, quando Fred Cohen publicou o seu trabalho *“Experiments with Computer Viruses”* (Experimentos com vírus de computador).

Na década de 90, a oferta de produtos de informática ficou mais acessível, o que possibilitou a difusão da utilização do computador pelas empresas e, principalmente, pelos usuários domésticos. Com isso, as ameaças aumentaram e se aperfeiçoaram.

Junto a isso, o desenvolvimento e a popularização da internet também contribuíram para a proliferação das ameaças cibernéticas, já que antes os vírus eram disseminados por meio de discos removíveis, e agora, com o aumento do uso de e-mail, essa contaminação é difundida com uma velocidade nunca antes vista.

4. DESAFIOS INVESTIGATIVOS E ALGUMAS MODALIDADES DE DELITOS CIBERNÉTICOS

Diferentemente do que se imagina, o processo investigativo em crimes cibernéticos não possui grandes peculiaridades, frente à investigação criminal clássica. Existem duas fases na investigação dos crimes cibernéticos: a fase inicial, chamada de fase técnica, e a consequencial, que é a fase da investigação policial.

Na fase técnica são realizadas atividades para que seja identificado o meio utilizado (website, e-mail, programas de mensagens instantâneas e etc.) pelo criminoso e qual a

localização de seu computador. Para que isso ocorra, são analisadas as informações passadas pela vítima.

É importante ressaltar que as evidências dos crimes cibernéticos são voláteis, ou seja, podem ser apagadas, alteradas ou perdidas num simples “clique”. A fim de evitar que isso aconteça, a vítima deve ser orientada para que preserve o material comprobatório do crime. Além disso, é de suma importância o registro do boletim de ocorrência, para que seja instaurado o feito.

Ainda na fase técnica, há a coleta das provas no ambiente virtual, para obtenção de prováveis autores do delito. Essas provas possuem um formato complexo (podem ser arquivos, fotos e etc.) e na maioria das vezes estão misturadas a dados legítimos, sendo necessária uma profunda análise pelos peritos que participam da investigação.

Caso haja necessidade para complementação do conjunto de provas já coletado, poderá ser requerido ao Poder Judiciário uma autorização para a quebra do sigilo dos dados, acesso e conexões às operadoras de telefonia ou provedores de conteúdo.

A maior evidência, no âmbito dos crimes cibernéticos, é, sem dúvida, o endereço de IP (*Internet Protocol*). O IP é um tipo de identificação que existe em todos os computadores que acessam à Internet. Essa identificação é única, ou seja, não existe a possibilidade de que dois computadores possuam o mesmo endereço de IP.

Após a identificação do meio utilizado e a localização do computador do agente delituoso, passa-se para a fase de campo. Como já dito anteriormente, essa fase é a investigação policial propriamente dita, onde são necessárias diligências para o reconhecimento do local em que se encontra o criminoso. Importante ressaltar que, como já exposto, as evidências dos crimes cibernéticos são voláteis, portanto, essas diligências devem ocorrer da maneira mais prudente possível, com o intuito de não ocorrer a perda das informações.

4.1 PEDOFILIA

A falsa ideia de anonimato que a Internet propicia aos seus usuários favoreceu a ampla divulgação de fotos e vídeos de crianças e adolescentes em cenas de sexo explícito. Além disso, o anonimato também possibilitou que esses criminosos assediem crianças e adolescentes no ambiente virtual, já que hoje a Internet é uma ferramenta livre e comum para todas as idades. Há também, aqueles que buscam as comunidades de pedofilia, afim de compartilhar conteúdos entre si.

O número de sites com conteúdo de pornografia infantil tem crescido assustadoramente no Brasil e no mundo nos últimos anos. Segundo ASACP – *Association of Sites Advocating Child Protection*, o número de denúncias reportadas sobre crimes de pedofilia passou de 800 no ano 2000 para 8342 no ano de 2013. É um número que assusta e que nos mostra o quanto essa modalidade de crime se propagou nos últimos anos.

O grande problema dessa modalidade é que o criminoso dificilmente deixará de praticar novamente esse crime, após o cumprimento de sua pena. Assim concorda o psiquiatra forense Guido Palomba que, em entrevista para o site G1, afirma que

é impossível curar um psicopata. O melhor é mantê-lo afastado da sociedade. O erro mais comum é condenar um criminoso com esse diagnóstico a penas corporais, como a detenção. O mais sensato é a medida de segurança, que permite tratamento e estabilização do quadro diagnosticado.

Além disso, Palomba afirma ainda que

a diferença é que a pena de reclusão permite a progressão da pena e o sentenciado vai para a rua, volta para a casa e ao convívio social. A medida de segurança pode ser para a vida toda do criminoso. Por não haver cura para a psicopatia, ele não deixará a Casa de Custódia e Tratamento.

O modo mais fácil de identificar o indivíduo que praticou o crime de pedofilia na internet é obter as informações do usuário que postou o conteúdo pornográfico no ambiente virtual. Para isso, como dito anteriormente, às vezes é necessária a quebra do sigilo dos dados e a colaboração dos provedores de internet.

Importante também que, após a identificação do criminoso e do local de sua atuação, seja localizado e apreendido qualquer tipo de equipamento que possa armazenar conteúdos com essa finalidade, como computadores pessoais, celulares, pendrives, HD, CD/DVD e etc. O e-mail, apesar de sua baixa utilização em comparação com outros tempos, também é uma fonte de comprovação que aquele indivíduo pratica o crime de pedofilia.

4.2 RACISMO

Do mesmo modo que no crime de pedofilia, o racismo na internet vem sendo disseminado devido ao falso anonimato oferecido aos usuários da rede mundial de computadores. Além disso, devido à proporção e o alcance que a internet dá ao seu conteúdo,

potencializando-o, uma manifestação racista que fora da dela não teria tanta força, dentro dela se torna muito repercutida, tomando proporções não imaginadas.

O crime de racismo foi tipificado no Código Penal com a edição da Lei 9.459/1997, onde serão punidas as manifestações discriminatórias de raça, cor, etnia, religião ou procedência nacional. É um dos crimes penais definido como inafiançável, imprescritível e sujeito a pena de reclusão.

Nessa modalidade de crime cibernético, é importante que o caso seja analisado com muito cuidado, já que a investigação deve demonstrar se o crime foi praticado por apenas um indivíduo ou por um grupo.

4.3 CYBERBULLYING

A violência de um indivíduo sobre outro nem sempre é apenas física, conforme a maioria das pessoas imaginam. O constrangimento, ofensa moral e etc., também são modalidades de violência. E daí veio o termo *bullying*, que nos últimos anos vem sendo amplamente divulgado nos meios de comunicação em massa, que é a agressão física ou psicológica reiterada, que prejudique a vítima de qualquer forma.

O *cyberbullying* possui as mesmas características do *bullying*, entretanto é aquele crime que é praticado por meio dos computadores ou qualquer aparelho tecnológico. Os principais meios de comunicação utilizados na prática do *cyberbullying* são o e-mail, vídeos, fotos, ofensas em site, blogs, redes sociais, mensagens de texto (SMS) e *chats* (bate-papos).

A grande diferença entre os dois crimes é que o *cyberbullying* possui a característica principal da maioria dos crimes cibernéticos: a velocidade na propagação da prática criminosa. E essa velocidade, na maioria das vezes, traz consigo danos irreparáveis, já que a internet é um mundo em que não há limites de espaço e tempo, impossibilitando assim a exclusão de todo rastro deixado por seu cometimento, além de comprometer, por muitas vezes, a identificação do agressor. Segundo Aramis Lopes, especialista em *bullying* e *cyberbullying* e presidente do Departamento Científico de Segurança da Criança e dos Adolescentes da Sociedade Brasileira de Pediatria, em entrevista para a Revista Escola, “o grupo de agressores passa a ter muito mais poder com essa ampliação do público”.

Quando nos deparamos com o termo *cyberbullying* automaticamente já se cria uma ideia de que existe apenas um ofensor (agressor) e um ofendido (vítima). Porém, também existe o terceiro sujeito da relação: o espectador. Esse sujeito é o que não toma partido por nenhum dos lados, nem defende a vítima, nem se junta ao agressor.

Os motivos que levam a prática do *cyberbullying* são os mais diversos possíveis, desde uma simples deficiência física, ou uma religião, orientação sexual e etnias diferentes da maioria. Diversos estudos afirmam que essa modalidade de crime cibernético tem gerado variadas consequências, como traumas, baixo desempenho escolar, depressão, dificuldades de relacionamentos e, inclusive, suicídio.

Resta saber ainda que alguns casos de *cyberbullying* ultrapassam a licitude e se enquadram em previsões penais. É daí que surge essa modalidade de crime cibernético. A calúnia, difamação, injúria, ameaça, constrangimento ilegal, falsa identidade e molestar ou perturbar a tranquilidade são os grandes exemplos disso.

Com isso, fica claro que a prática dessa modalidade de crime cibernético possui diversas formas de punibilidade. Importante destacar ainda que o *bullying* virtual não impede sanções civis, posto que essa prática gera transtornos à vítima e o responsável deve buscar um meio de reparar tais danos, como preceitua a Constituição Federal em seu artigo 5º, Inciso X, e o Código Civil em seus artigos 927 e 953.

Por fim, é um fator determinante para a resolução dos casos de *cyberbullying* que a vítima forneça toda e qualquer informação útil à Polícia, afim de evitar que seja responsabilizada penalmente, no caso em que a ela noticia o fato, mas não consegue prová-la.

4.4 FRAUDES ELETRÔNICAS

A internet, de fato, está introduzida na vida social e profissional dos indivíduos no mundo contemporâneo. A conexão com a internet é imprescindível para vários setores da sociedade. Uma pequena falha, inviabilizando o uso dela, é capaz de trazer grandes prejuízos à quem é dependente da mesma. É com essa dependência da internet que surgem também os problemas decorrentes de sua utilização. A criação do computador e o surgimento da internet intensificou a propagação e a utilização das fraudes no mundo virtual.

Primeiramente, devemos compreender a definição de fraude. Segundo Moisés J. Santos³, Gerente de Prevenção a Fraudes do HSBC, fraude é o

Subterfúgio para alcançar um fim ilícito, ou ainda, o engano dolosamente provado, o malicioso induzimento em erro ou aproveitamento de preexistente erro alheio, para o fim de enriquecimento ilícito.

³SANTOS, Moisés J. **Fraude Eletrônica**. 2008. Disponível em: <<http://www.febraban.org.br/Arquivo/Servicos/Eventoscursos/Palestras/CLAIN2008/PalestraSrMoisesJSantos.pdf>>. Acesso em: 06 nov. 2013.

A fraude eletrônica, segundo Antonio de Loureiro Gil (1991, p. 15), é a utilização de *software* e bancos de dados com finalidade de alcançar algum benefício indevidamente de outrem.

Um dos principais tipos de fraudes eletrônicas é o que ocorre no comércio eletrônico (ou *e-commerce*). Aproveitando-se dos inúmeros usuários que se utilizam desse tipo de comércio para realizar suas compras, o fraudador oferece determinados produtos por valores abaixo do valor real de mercado e ilude o cliente no que diz respeito a credibilidade da loja virtual, sempre com avaliações positivas de outros clientes.

O grande problema no comércio eletrônico é a falta de controle e rigidez no registro de um domínio na internet. Qualquer pessoa pode registrar um domínio no ambiente virtual, bastando utilizar-se do CPF. E é aí que surge o problema. A grande maioria das lojas eletrônicas que se utilizam desse mercado para fraudar, ou sites fraude, utilizam domínios que são registrados em nome de laranjas ou de pessoas que perderam seus documentos, o que dificulta uma posterior investigação da empresa fraudadora, já que na maioria dos casos os dados não se interligam.

Outro tipo de fraude eletrônica são aqueles que oferecem empréstimos de dinheiro facilitados. Uma simples busca na internet nos faz encontrar diversos sites de falsos empréstimos. Na maioria dos casos, infelizmente esses sites fraude só chegam ao conhecimento da Polícia quando algum indivíduo denuncia por ter sido vítima do golpe.

Em ambos os casos descritos acima, a tipificação que incide nessas condutas é, por falta de legislação específica para crimes cometidos no mundo virtual, a prevista no art. 171 do Código Penal Brasileiro, ou seja, o estelionato. Importante ressaltar que é muito comum, no decorrer da investigação policial, observar a ocorrência de outros crimes. Geralmente, nos casos de sites fraude, o crime é realizado por uma quadrilha ou bando, o que faz incidir também o art. 288 do Código Penal Brasileiro. Ainda, a competência para investigar e julgar os crimes de estelionato é do local onde se obteve a vantagem indevida, conforme a jurisprudência do STJ:

PENAL E PROCESSO PENAL. HABEAS CORPUS. NARRATIVA DE CONDUTA QUE, EM TESE, SE SUBSUME AO ARTIGO 171, CAPUT, C/C ARTIGO 71, DO CÓDIGO PENAL. CRIME DE DUPLO RESULTADO MATERIAL. CONSUMAÇÃO DO ESTELIONATO: OBTENÇÃO DA VANTAGEM PATRIMONIAL EM DETRIMENTO DA VÍTIMA. CHEQUES SACADOS DIRETAMENTE NO CAIXA BANCÁRIO. INDICAÇÃO DO ATO CONSUMATIVO QUE SE FAZ INDEPENDENTEMENTE DE SE SABER SE A VANTAGEM ERA “DEVIDA” OU “INDEVIDA”. JUÍZO COMPETENTE: O DO LUGAR

EM QUE SE DERAM OS SAQUES. ORDEM DENEGADA. 1. A doutrina penal ensina que o resultado, no estelionato, é duplo: benefício para o agente e lesão ao patrimônio da vítima. 2. A fraude, no estelionato, é circunstância de meio para a obtenção do resultado. 3. Desacompanhada da obtenção da vantagem, em prejuízo alheio, a fraude não caracteriza a consumação do delito. 4. **Para fixação da competência, basta a indicação do lugar em que se deu a consumação do delito em tese, ou seja, o local onde foi obtida a vantagem patrimonial** – o exame acerca da ilicitude dessa vantagem é objeto da ação penal condenatória. 5. Benefício patrimonial obtido através de saques realizados diretamente no caixa do banco situado na cidade do Rio de Janeiro: lugar da consumação. Ordem denegada. (HC 36760/RJ, STJ, Relator Ministro Paulo Medina, Sexta Turma, DJ 18.04.2005 p. 396) (grifo nosso).

Por fim, percebe-se que o ambiente virtual proporcionado pela internet é amplo, no que diz respeito à prática de delitos virtuais, o que faz com que o usuário tenha cada vez mais cuidado e atenção quando ao seu uso devido e seguro.

5. SOLUÇÕES JURÍDICAS APRESENTADAS PELO BRASIL

Como visto anteriormente, o ambiente virtual a cada dia que passa fica mais visado pelos criminosos para a prática de delitos cibernéticos. Apesar desse fato ser de conhecimento da grande maioria, pouco foi feito para que se proteja puna penalmente os responsáveis pelas práticas dos ditos crimes. No Brasil, ainda não há uma lei específica que regulamente tais práticas criminosas, já existentes em outros países, como Estados Unidos, Inglaterra, Portugal, entre outros.

Porém, apesar do Brasil se mostrar atrasado no que diz respeito a essa matéria, não quer dizer que a prática dos crimes cibernéticos é impune no nosso país. São várias as normas encontradas em nosso ordenamento jurídico que tratam do assunto, como a Lei 11.829/2008, Lei 9.504/97, Lei 9.609/98, Lei 9.296/96, Lei 12.034/09, entre outras que serão demonstradas a seguir. E ainda, a aplicação da legislação já existente, como o Código Penal, enquadrando os crimes cibernéticos dentro dele, já que para vários juristas, alguns crimes praticados no ambiente virtual já estão tipificados no CP, o que mudaria era somente o meio utilizado, nesse caso, o computador ou dispositivos tecnológicos.

5.1 ESTATUTO DA CRIANÇA E DO ADOLESCENTE (LEI 8.069/1990)

Um dos importantes avanços da legislação específica brasileira contra os crimes cibernéticos foi a edição da Lei 11.829/2008 que alterou os artigos 240 e 241 da Lei 8.069/90,

mais conhecida como ECA. Antes da edição dessa lei, havia uma certa lacuna quanto a pedofilia na internet.

Essa alteração trouxe grandes benefícios para a proteção da criança e dos adolescentes contra o crime da pedofilia. A Lei 11.829/2008 aumentou a pena de dois a seis anos para quatro a oito anos, para quem produzir, reproduzir, dirigir, fotografar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente. A novidade incluiu também na tipificação penal para quem filmar ou registrar tais atos.

Além disso, houve acréscimo dos artigos 241-A, que prevê punição para quem divulgar imagens que contenham sexo explícito ou pornografia infantil por meio de sistema de informática ou telemático; 241-B, que prevê punição para quem armazenar imagens que contenham sexo explícito ou pornografia infantil; 241-C, que prevê punição para quem realiza montagens ou modificações, simulando a participação de crianças e adolescentes em cenas que contenham sexo explícito ou pornografia; e, finalmente, o art. 241-D, que prevê a punição para quem alicia, assedia ou constrange criança ou adolescente para a prática de ato libidinoso.

5.2 LEI 12.737/2012 OU LEI CAROLINA DIECKMAN

Em 30 de novembro de 2012 foi sancionada a Lei 12.737 que dispõe acerca da tipificação criminal dos delitos informáticos. Essa lei é, sem dúvidas, o maior avanço da legislação brasileira contra os crimes cibernéticos. Essa lei foi apelidada de “Lei Carolina Dieckman” devido a repercussão do vazamento de fotos íntimas que estavam no celular da atriz no momento em que o projeto, proposto pelo deputado Paulo Teixeira (PT-SP), tramitava na Câmara dos Deputados.

Agora, invadir dispositivo alheio, conectado ou não a rede de computadores, mediante violação de segurança com o fim de obter informações sem autorização é crime, com pena de detenção de três meses a um ano e multa.

Roubar informações em que causem prejuízos econômicos passou também a ser crime, com aumento da pena de detenção de três meses a um ano e quatro meses.

Obter conteúdo de comunicações privadas de forma não autorizada aumenta a pena de detenção de seis meses a dois anos e multa.

A divulgação e comercialização de conteúdo roubado de dispositivo informático também passa a ser crime, com pena de reclusão de oito meses a três anos e quatro meses.

A nova lei também tipifica como crime quando o usuário não autoriza o acesso ao aparelho ou quando o criminoso “instala vulnerabilidades para obter vantagem ilícita”, com pena de detenção de três meses a um ano e multa.

Também há a previsão da pena de reclusão de seis meses a dois anos e multa para quem obtiver dados “de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido”. A pena será majorada de um a dois terços se o crime for cometido contra autoridades do Executivo, Legislativo ou Judiciário. Também será majorada a pena se houver divulgação, comercialização ou transmissão a terceiros dos dados obtidos.

5.3 MARCO CIVIL DA INTERNET BRASILEIRA

O Marco Civil da Internet (PL 2126/11) vem sendo discutido desde o ano de 2009. Esse projeto de lei é uma espécie de Constituição para a internet brasileira, definindo princípios básicos a serem seguidos e criando uma base para as tão esperadas leis específicas. Essa PL ganhou força nos últimos meses devido aos escândalos de espionagem americana no Brasil descobertos recentemente. Os três principais pontos do Marco Civil são: a neutralidade de rede, a privacidade online e a responsabilidade por conteúdo.

Apesar da grande pressão do Poder Executivo brasileiro, o Marco Civil ainda continua em pauta e não há previsão para ser aprovado, devido às diversas opiniões dos deputados brasileiros, que não chegam a um consenso. Isso porque, várias empresas ligadas ao setor de telecomunicações são contra esse projeto de lei, devido às restrições que ela traria às empresas.

Indubitavelmente, se aprovado, será o maior avanço da legislação brasileira contra os crimes praticados no ambiente virtual, proporcionando maior segurança aos seus usuários.

5.4 OUTRAS LEIS ESPECÍFICAS SOBRE CRIMES CIBERNÉTICOS

Além das destacadas acima, temos também em nosso ordenamento jurídicos outras legislações específicas: a Lei 9.609/1998, que trata da proteção da propriedade intelectual do programa de computador; a Lei 9.983/2000, que tipificou os crimes relacionados ao acesso indevido a sistemas informatizados da Administração Pública; a Lei 9.296/1996, que trata da interceptação ilegal de comunicações; a Lei 12.034/2009, que delimita os direitos e deveres dentro da rede mundial, durante as campanhas eleitorais.

Cumprido destacar também o papel que o Código Penal possui frente aos crimes cibernéticos, já que alguns de seus dispositivos tutelam tais condutas, como: o art. 153, que trata da divulgação de segredo; o art. 313-A, que trata da inserção de dados falsos em sistemas de informações; o art. 313-B, que trata da modificação ou alteração não autorizada de sistema de informações; o art. 325, que trata da violação do sigilo funcional; o art. 184, que trata da violação dos direitos autorais; entres outros.

6. CONCLUSÃO

Por todo o exposto, o desenvolvimento tecnológico e o consequente surgimento do computador e da internet, combinado com a globalização mundial, geraram uma facilitação na troca de informações e a redução dos limites das fronteiras entre os Estados. Por outro lado, acarretou também o surgimento de ameaças nesse mundo tão vasto que é a internet.

Finalizada as ponderações acerca da globalização, percebemos que com o aumento das ameaças cibernéticas, a sociedade passa a exigir do Estado uma maior proteção, com o fim de proporcionar a redução desses problemas. Essa maior intervenção estatal gera uma expansão indesejada pela tutela penal.

O avanço tecnológico, de fato, gera uma grande preocupação para aqueles que regulamentam essa área que a cada dia evolui mais e mais. Porém, pouco se tem feito para reverter esse problema, já que as legislações da maioria dos Estados, dentre eles o Brasil, não possui uma legislação específicas tratando sobre o tema.

Dessa forma, é fundamental a criação de tipos penais específicos, garantindo assim que os criminosos sejam punidos por seus atos, já que quanto maior for a impunidade para os autores, maior será o estímulo para que outros indivíduos pratiquem delitos semelhantes.

Entretanto, deve-se propor, além da tão falada tipificação criminal, outros meios que proporcionem uma maior integração entre as normas penais e a desburocratização na obtenção dos dados, na busca pelos autores de crimes cibernéticos, por meio de uma regulamentação geral sobre o todo o ciberespaço.

Portanto, conclui-se que o presente trabalho procurou demonstrar a utilização da tecnologia e da internet pelos agentes delituosos, e o quanto essa prática ainda não possui proteção por parte do ordenamento jurídico brasileiro. Apesar disso, percebe-se algumas evoluções sobre o tema, com o surgimento de algumas legislações específicas, com a finalidade de prevenção dos crimes virtuais.

REFERÊNCIAS

A EPIDEMIA via internet. **PCWORLD**. Disponível em:

<<http://www.cin.ufpe.br/~rdma/documentos/revistaPCWORLDseguranca.pdf>>. Acesso em: 04 set. 2013.

ASSOCIATION OF SITES ADVOCATING CHILD PROTECTION. **Statistics**. Disponível em: <http://www.asacp.org/index.php?content=statistics>>. Acesso em: 04 nov. 2013.

BRASIL. Código Civil (2002). **Código Civil Brasileiro**. Brasília, 2002. Disponível em:

<http://www.planalto.gov.br/ccivil_03/leis/2002/110406.htm>. Acesso em: 18 set. 2013.

BRASIL. Código Penal (1940). **Código Penal Brasileiro**. Brasília, 2002. Disponível em:

<http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 18 set. 2013.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília: Senado Federal, 1988. Disponível em:

<http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 18 set. 2013.

BRASIL. Lei n.º 11.829, de 25 de novembro de 2008. **Altera a Lei nº 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet**. Brasília.

Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/11829.htm>. Acesso em: 06 out. 2013.

BRASIL. Lei n.º 12.034, de 29 setembro de 2009. **Altera as Leis nºs 9.096, de 19 de setembro de 1995 - Lei dos Partidos Políticos, 9.504, de 30 de setembro de 1997, que estabelece normas para as eleições, e 4.737, de 15 de julho de 1965 - Código Eleitoral**.

Brasília. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/lei/112034.htm>. Acesso em: 06 out. 2013.

BRASIL. Lei n.º 12.737, de 30 de novembro de 2012. **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**. Brasília. Disponível em:

<http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/112737.htm>. Acesso em: 06 out. 2013.

BRASIL. Lei n.º 8.069, de 13 de julho de 1990.**Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências.** Brasília. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8069.htm>. Acesso em: 06 out. 2013.

BRASIL. Lei n.º 9.296, de 24 de julho de 1996.**Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal.** Brasília. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9296.htm>. Acesso em: 07 out. 2013.

BRASIL. Lei n.º 9.459, de 13 de maio de 1997.**Altera os arts. 1º e 20 da Lei nº 7.716, de 5 de janeiro de 1989, que define os crimes resultantes de preconceito de raça ou de cor, e acrescenta parágrafo ao art. 140 do Decreto-lei nº 2.848, de 7 de dezembro de 1940.** Brasília. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9459.htm>. Acesso em: 08 out. 2013.

BRASIL. Lei n.º 9.609, de 19 de fevereiro de 1998.**Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências.** Brasília. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9609.htm>. Acesso em: 07 out. 2013.

BRASIL. Lei n.º 9.983, de 14 de julho de 2000.**Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal e dá outras providências.** Brasília. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9983.htm>. Acesso em: 08 out. 2013.

CASTELLS, Manuel. **A Galáxia da Internet:** reflexões sobre internet, os negócios e a sociedade. Rio de Janeiro. Jorge Zahar Editor, 2001.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais.** São Paulo: Saraiva, 2011.

FERNANDES, Paulo Silva. **Globalização, “sociedade de risco” e o futuro do direito penal.** Coimbra: Almedina, 2001.

FOLHA DE SÃO PAULO. **Estudante é responsabilizado por racismo na internet.** Disponível em: <<http://www1.folha.uol.com.br/fol/tec/tx033414.htm>>. Acesso em: 10 nov. 2013.

GIL, Antonio de Loureiro. **Fraudes Informatizadas.** 2ª edição. São Paulo: Atlas, 1991.

O HOMEM no espaço. **Super Interessante.** Editora Abril. Disponível em: <<http://super.abril.com.br/tecnologia/homem-espaco-442035.shtml>>. Acesso em: 03 set. 2013.

PALOMBA, Guido. É impossível curar um psicopata, diz psiquiatra Guido Palomba. **G1**. Disponível em: <<http://g1.globo.com/Noticias/Brasil/0,,MUL1568178-5598,00-E+IMPOSSIVEL+CURAR+UM+PSICOPATA+DIZ+PSIQUIATRA+FORENSE+GUIDO+PALOMBA.html>>. Acesso em: 03 nov. 2013.

REVISTA ESCOLA. **Cyberbullying: a violência virtual**. Disponível em: <<http://revistaescola.abril.com.br/crianca-e-adolescente/comportamento/cyberbullying-violencia-virtual-bullying-agressao-humilhacao-567858.shtml>>. Acesso em: 07 nov. 2013.

SANTOS, Milton. **Por uma outra globalização: do pensamento único à consciência universal**. 14. Ed. Rio de Janeiro: Record, 2007.

SANTOS, Moisés J. **Fraude Eletrônica**. 2008. Disponível em: <<http://www.febraban.org.br/Arquivo/Servicos/Eventoscursos/Palestras/CLAIN2008/PalestraSrMoisesJSantos.pdf>>. Acesso em: 06 nov. 2013.

SILVA, Marco Antonio Marques da. **Globalização e direito penal econômico**. In: COSTA, José de Faria; SILVA, Marco Antonio Marques da. **Direito penal especial, processo penal e direitos fundamentais**. São Paulo: QuartierLatin, 2006.

SILVA, Marco Antonio Marques da. **Acesso à justiça penal e Estado Democrático de Direito**. São Paulo: Juarez Oliveira, 2001.

THE SIDNEY MORNING HERALD. **First vírus hatched as a practical joke**. Disponível em: <<http://www.smh.com.au/articles/2007/09/01/1188671795625.html>>. Acesso em: 06 set. 2013.

WENDT, Emerson; NOGUEIRA JORGE, Higor Vinicius. **Crimes Cibernéticos: ameaças e procedimento de investigação**. Rio de Janeiro: Brasport, 2012.

WIKIPÉDIA. **Crime Informático**. Disponível em: <http://pt.wikipedia.org/wiki/Crime_inform%C3%A1tico>. Acesso em: 1 ago. 2013.