Vertentes do Direito

ISSN nº 2359-0106 Vol. 4, n. 2, 2017.

CONSIDERAÇÕES SOBRE A APLICABILIDADE DO DIREITO PENAL ACERCA DOS CRIMES VIRTUAIS

CONSIDERATIONS ON THE APPLICABILITY OF CRIMINAL LAW ON VIRTUAL CRIMES

Mariah Dourado de Andrade[1]
Dorinethe dos Santos Bentes[2]
David Franklin da Silva Guimarães[3]

RESUMO

O presente artigo busca compreender os fatos que levaram à atualização tardia e inadequada do Código Penal Brasileiro acerca dos crimes cibernéticos no âmbito da Internet, e a carência de novas Leis Penais regulando esse crime. Para alcançar tais objetivos, pretende-se analisar o contexto histórico desde o surgimento do cibercrime até os dias atuais, avaliar-se-á também as leis já criadas que abrangem essa temática, além de entender a necessidade de uma união universal para o combate desse crime, com foco nos objetivos e resultados da Convenção sobre o Cibercrime, de 2001, e sua importância inovadora para o mundo moderno. Para isso, baseia-se no método indutivo, realizada por bases teóricas, com levantamento bibliográfico de livros, artigos e sites especializados, e na jurisprudência e análise legislativa da Constituição Federal Brasileira de 1988. Com abordagem qualitativa, explicando o porquê é necessário que haja uma extensão do Direito Penal para a tipificação e regulamentação dos crimes virtuais, de forma a compreender o motivo desta urgência e de como um acordo internacional para o combate do crime virtual seria benéfico para a sociedade moderna. Concluindo-se que para assegurar aos internautas segurança neste novo meio de comunicação é necessária uma intervenção estatal no âmbito virtual.

PALAVRAS-CHAVE: Novas Tecnologias de Informação; Direito penal; Hacker; Convenção sobre o Cibercrime; Crimes Cibernéticos.

[1]Acadêmica do curso de Direito da Universidade Federal do Amazonas. E-mail: mariahandrade__@hotmail.com

[2] Professora Mestra, da Universidade Federal do Amazonas . Graduada em Direito e História. Mestra em História do Amazonas pela Universidade Federal do Amazonas (UFAM). E-mail: dorinethebentes@gmail.com

[3] Mestrando do Programa de Pós-Graduação em Ciências do Ambiente e Sustentabilidade na Amazônia da Universidade Federal do Amazonas. E-mail:davidguimaraes2009@hotmail.com

ISSN nº 2359-0106 Vol. 4, n. 2, 2017.

ABSTRACT

This article seeks to understand the facts that led to the late and inadequate updating of the Brazilian Penal Code when dealing with Internet cybercrimes and the lack of ne Criminal Laws regulating this crime. To reach these objectives, we intend to analyze the historical context of the cybercrimes, from the beginning to the present days, which we will also appreciate the current legislation that cover this subject, in addition to understanding the need for an universal union to combat those types of crimes, basing on the objectives and results of the 2001 Cybercrimes Convention and it's innovative importance to the modern world. To reach those objectives, the present article is based on the inductive method, carried out by theoretical bases, with a bibliographical survey of books, articles and specialized websites, and in the jurisprudence and legislative analysis of the Brazilian Federal Constitution of 1988.With a qualitative approach, trying to explain why it is necessary for society to have an extension of criminal law for the criminalization and regulation of virtual crimes in order to understand the reason for this urgency and how an international agreement to combat virtual crime would be beneficial to the modern society. It is concluded that to assure Internet users security in this new way of communication, it is necessary the State intervention in the virtual technologic.

KEYWORD: New Information Technologies; Criminal Law; Hacker; Convention on Cybercrime; Cyber Crimes.

1. INTRODUÇÃO

O crime virtual foi influenciado pela facilidade de anonimato que surgiu quando houve a criação da Internet. Esses crimes são bem variados e vão desde injúria – podendo ser classificado com crime de ódio quando sendo injúria racial – e calúnia até crimes de *software*, conhecidos popularmente como uma forma de pirataria moderna. Dessa forma, esses crimes acabam por sair da esfera virtual e passam a afetar a esfera social, causando danos muitas vezes irreversíveis à moral pessoal.

Esses crimes causam uma insegurança nada saudável nesse novo serviço de comunicação que é a internet, que não apenas funciona como forma de lazer, como também possui finalidades comercias, como os negócios de compra e venda e de fechamento de contratos empresariais. A insegurança nesse serviço causada por tais crimes pode afetar a economia mundial, tendo em vista que a internet, diferentemente de países, não possui fronteiras. Sendo assim, vê-se de extrema importância, não apenas social, mas também econômica, a garantia de segurança por lei aos usuários

ISSN nº 2359-0106 Vol. 4, n. 2, 2017.

desses serviços, pois cada vez mais o mundo tende a se deslocar para o âmbito virtual, em busca de maior facilidade e rapidez nos trabalhos.

Diante do exposto, chega-se à seguinte reflexão: por que, apesar de toda a importância social e jurídica que a Internet tem sobre nossas vidas, as leis ainda não foram atualizadas adequadamente para garantir segurança aos seus usuários? A resposta para essa pergunta não poderia ser outra a não ser o fato de os legisladores serem conservadores demais para aceitar a relevância de tal processo à sociedade.

A tentativa de se atualizar o código se deu apenas através de um conjunto reduzido de normas que tipificam somente algumas condutas no mundo virtual, não sendo abrangente ou mesmo eficaz, e que obrigam a utilização do método de analogia para que os crimes não saiam impunes, o que entra em conflito com Nélson Hungria (1954), que veta a utilização de analogia para a solução de crimes penais.

A importância desse trabalho justifica-se pela necessidade de preencher as lacunas do Direito Penal, conforme defendido por Norberto Bobbio (1992), culminando na sanção de leis para tipificação dessas condutas, com o intuito de findar esse novo tipo de crime moderno e trazer novamente segurança à população para que não se tema utilizar a internet. E ainda avaliar um possível acordo universal para tipificação dos crimes extraterritoriais, que são de difícil combate por não se saber a qual legislação eles devem ser aplicados.

Portanto, o presente artigo visa avaliar as possíveis soluções para a falta de leis especificas, utilizando-se de referências teóricas e mecanismos legais utilizados pelo Direito Penal, buscando garantir o direito dos indivíduos de acesso à informação e privacidade asseguradas pela Constituição Federal (BRASIL, 1988).

O primeiro tópico faz uma breve apresentação sobre o surgimento da internet e, consequentemente, as primeiras evidências de um novo tipo de crime no âmbito virtual ainda na década de 70 com o surgimento dos *hackers* e dos diversos tipos de vírus cibernéticos. Em seguida, o próximo tópico divide os crimes virtuais em dois tipos: os crimes cibernéticos puros e os crimes cibernéticos impuros, classificando cada um deles e dando exemplos. No terceiro tópico analisou-se a *Deep Web* e as consequências desse mundo sem leis, analisando ainda os ciberataques em massa

ISSN nº 2359-0106 Vol. 4, n. 2, 2017.

ocorridos em 2017 em diversos locais do mundo. O quarto tópico avaliou a Convenção de Budapeste sobre o Cibercrime de 2001 e a sua importância para o combate ao crime virtual na modernidade, além de sua eficiência. Por fim, o último tópico considerará a necessidade de novas leis penais na atualidade e qual a real importância da atualização frequente do Código Penal Brasileiro para que este acompanhe as mudanças sociais.

2. SURGIMENTO DOS CRIMES VIRTUAIS

A internet surgiu em meados do século XX, no auge da Guerra Fria, quando as duas grandes potências mundiais da época disputavam uma corrida bélica, armamentista e espacial. Nesse contexto histórico, o primeiro computador digital foi construído em 1946 com a denominação de *Electronic Numerical Integrator and Computer*, mas o marco inicial propriamente dito da criação da internet, considerado assim por muitos autores, foi em 1957 quando o então presidente dos Estados Unidos, John F. Kennedy, lançou o programa que futuramente levaria o homem à Lua (WENDT; JORGE, 2012, p.5). A primeira conexão internacional, no entanto, só foi realizada em 1973 pela Agência de Pesquisas em Projetos Avançados na Rede (ARPANET), que interligou a Inglaterra e a Noruega (Ibidem, p.7).

Seu principal objetivo seria possuir um alcance universal de comunicações e uma via vasta para acesso as informações. Em tese, todos que a usassem seriam anônimos e iguais entre si, sem distinção de condição social ou aparência, trazendo velocidade aos relacionamentos do mundo moderno, tanto interpessoais quanto de comércios, negócios, tanto locais quanto internacionais, eliminando as fronteiras físicas dos países e alcançando certa liberdade para os seus usuários. No entanto, de acordo com Renato Nunes Bittencourt (2010), com o acesso à internet, também houve o surgimento novos meios para a difusão de ameaças:

> Se por um lado a tecnologia dá aos usuários ampla liberdade e máxima igualdade individual, por outro lado ela lhes retira a habilidade de distinguir as pessoas com as quais se relacionavam virtualmente, além de lhes restringir a

ISSN nº 2359-0106 Vol. 4, n. 2, 2017.

> capacidade de diferenciar a sensação de segurança da ideia de segurança como realidade.

Em 1960 foram relatados os primeiros casos de crime virtuais, com maior destaque a casos de manipulação e sabotagem de sistemas de computadores, mas foi apenas na década de 70 que surgiu a figura do *Hacker*, conhecido por invasão de sistemas e furto de *softwares* (CARNEIRO, 2012). Em 1980, houve uma maior propagação de outros tipos de crimes não apenas envolvendo vírus e *softwares*, como o da pirataria e pedofilia online, gerando certa preocupação com a segurança virtual. Com a criação da Teia Mundial *(World Wide Web* – WWW) em 1986, a ARPANET[4] passou a ser chamada de internet e com certas melhorias em sua interface gráfica ficou mais acessível ao público em geral, tornando esse novo meio de comunicação popular na década de 90 (Ibidem).

Não se sabe ao certo quando surgiu o primeiro vírus de computador. Sabe-se apenas que em 1986 surgiu o primeiro "Cavalo de Tróia", ou seja, um vírus embutido dentro de um arquivo que aparenta ser pacifico, mas que ao ser instalado em um computador torna-se prejudicial à máquina. Neste caso do *PC Write*, ele aparentava ser um editor de texto, mas ao ser executado ele corrompia os arquivos do disco rígido do computador (MONTEIRO NETO, 2008, p.14). Hoje existem vários tipos de vírus diferentes, cada um com um resultado diferente. Uma das ações mais efetivas são os *spams,* mensagens não solicitadas enviadas em massa para e-mails, pessoas, sites, etc, sendo utilizados por muitos criminosos para difundir códigos maliciosos.

O *hacker* é um indivíduo que se dedica a pesquisar e estudar os códigos de programação de *softwares*, buscando falhas de sistema que não deveriam existir, e buscam acesso a certos dados. Alguns *hackers* fazem isso para o bem, para informar às empresas que seu sistema está falho ou ainda são pagos para tal serviço, outros, entretanto, usam essas falhas para seu proveito, seja para ter acesso a banco de dados ou para subornar empresas. De acordo com Marco Aurélio Rodrigues da Costa (1997), os crimes virtuais na atualidade são crimes afeitos à oportunidade (*special*

[4]Agência de Pesquisa Avançada e Rede, em inglês Advanced Research Projects Agency Network.

ISSN nº 2359-0106 Vol. 4, n. 2, 2017.

opportunity crimes), tendo suas condutas delituosas dividas em estágios de objetivos. De acordo com o autor, esses crimes são realizados por jovens movidos pelo interesse de vencer a máquina apenas, mas ao perceberem que conseguiram ganhar uma quantidade considerada de dinheiro com esse serviço, continuam a realizar tais atividades ilegais para sustentar seus altos gastos na aparência pessoal e em equipamentos de ponta.

Ao todo, as condutas indevidas no âmbito virtual podem ser divididas em duas: ações prejudiciais atípicas e crimes virtuais. A primeira não possui previsão legal, podendo o causador ser responsabilizado apenas no âmbito civil, um exemplo disso é o acesso não autorizado a redes de computadores (WENDT; JORGE, 2012, p. 18). Já no segundo caso, esses crimes podem ser realizados de forma tradicional, ou seja, aberta, por meio de computadores como é o caso dos crimes contra a honra, ou podem ser praticados com o uso do computador ou alguma outra fonte com acesso à internet, como no caso de clonagem de cartões por meio da internet (Ibidem, p. 19).

3. TIPOS DE CRIMES VIRTUAIS

Os crimes virtuais são todas as condutas típicas, antijurídicas e culpáveis praticadas com a utilização de computadores ou qualquer outro sistema de informática, sendo estes diversos e tendo como classificação mais aceita a distinção entre crimes cibernéticos puros/próprios ou impuros/impróprios, tendo o autor do crime como o agente ativo, popularmente conhecido como *hacker* ou *cracker*, e qualquer pessoa física ou jurídica ou uma entidade titular, pública ou privada, que sofra a ação ou sobre quem recaiu tal ação é o agente passivo do crime (WENDT; JORGE, 2012, p.18-20).

Crimes cibernéticos puros ou próprios são mais raros, eles consistem obrigatoriamente que o agente ativo utilize o sistema informático do agente passivo para poder realizá-lo, tendo o sistema tecnológico sendo o objeto e o meio para execução do crime, de forma que se atinja diretamente o software ou hardware do computador, podendo ter acesso de dados não autorizados e possibilitando alteração

ISSN nº 2359-0106 Vol. 4, n. 2, 2017.

de senhas, modificação e alteração de documentos e permitindo a implantação de dados falsos. De acordo com Damásio de Jesus (2003):

> Crimes eletrônicos puros ou próprios são aqueles que sejam praticados por computador e se realizem ou se consumem também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado.

É árduo o dever de tipificar esses crimes, como por exemplo, invasão de sistemas, proliferação de vírus, divulgação de conteúdos não autorizados, etc. Nesse sentido, Carneiro (2012), ainda classifica os *spams* como crimes cibernéticos próprios, ao afirmar que eles geram danos morais pelo transtorno causado às vítimas, atentando contra sua dignidade e invasão de privacidade, e danos materiais, pois de acordo com a empresa de segurança de rede e soluções de disponibilidade, McAfee, para ler e apagar os cerca de 62 trilhões de *spams* consome 33 *terawatts*/hora de energia por ano, o que contribui para a poluição do meio-ambiente.

A maioria dos crimes virtuais praticados na internet é impuro ou impróprio, consistem em realizar práticas ilícitas com a utilização de um computador ou qualquer outro instrumento tecnológico, atingindo todo o meio jurídico já tipificado, mas que agora foram realizados com a utilização do computador e da rede informática, mas que não permanecem necessariamente apenas no âmbito virtual. Um exemplo disso é o tráfico de drogas online e a promoção da pedofilia. Ainda de acordo com Damásio de Jesus (2003):

> (...) Já os crimes eletrônicos impuros ou impróprios são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço 'real', ameaçando ou lesando outros bens, não-computacionais ou diversos da informática.

Alguns crimes classificados como crimes cibernéticos puros são: crimes contra a honra, no caso de calúnia, difamação e injúria (respectivamente, artigos 138, 139 e 140 da Lei n. 2.848/40, do Código Penal), pedofilia e pornografia infantil (artigo 247 da Lei n. 8.069/90, o Estatuto da Criança e do Adolescente – ECA), crimes contra a

Vertentes do Direito

ISSN nº 2359-0106 Vol. 4, n. 2, 2017.

propriedade, crimes contra o Estado e a incolumidade pública, falsa identidade, infrações a direitos de autor, incitação ao ódio, discriminação, racismo, xenofobia, escárnio religioso, *bullying*, terrorismo, etc.

O uso da analogia do Código Penal foi necessário para enquadrar a grande maioria desses crimes já previstos pela lei no âmbito virtual, por esse motivo torna-se mais fácil a identificação e punição desses crimes em contrapartida com os demais, por estes se tratarem de crimes comuns e os demais de delitos que só existem no mundo virtual. Mas apenas sua tipificação não significa o fim ou o combate efetivo a esses crimes, a promoção da pedofilia e pornografia infantil ainda é altamente realizada via internet através de outros meios não convencionais onde a legislação brasileira dificilmente alcança: a *Deep Web.*

4. *DEEP WEB*: consequências de um mundo sem leis

A internet a qual nós temos acesso se chama *Surface Web*, ela pode ser acessada através dos mecanismos de busca padrão, e apesar de contar mais de 15 bilhões de páginas, ela é apenas aproximadamente 10% do que a internet realmente é. A parte da internet criptografada, que se chama *Deep Web*, é muito mais vasta do que a internet padrão, e contém diversos conteúdos ilegais. É por ela que ocorrem ilícitos, como: tráfico de drogas, de órgãos, de pessoas, pedofilia, entre outros via internet, de forma que não sejam identificados pelas autoridades. A *Deep Web* é um mundo sem leis assegurado pelo anonimato, que influencia a prática de atividades ilegais, já que este ambiente está criptografado, o que impossibilita o rastreamento dessas atividades.

> A internet é o espaço por excelência da liberdade, o que não significa dizer que seja um universo sem lei e infenso à responsabilidade pelos abusos que lá venham a ocorrer (STJ, REsp 1117633/RO, Rel. Ministro Herman Benjamin, Segunda Turma, julgado por unanimidade em 09/03/2010, DJe 26/03/2010).

ISSN nº 2359-0106 Vol. 4, n. 2, 2017.

Por esses motivos, é tão árduo o controle de certos crimes. De acordo com Lima (2014), há a necessidade do aumento da intervenção estatal no âmbito virtual e tecnológico, de forma a proteger a difusão de informações, como garantido na Constituição, tendo foco numa maior fiscalização para pôr fim às práticas nocivas e delitos virtuais.

Em 2017, uma onda de ataques cibernéticos se iniciou, atingindo dezenas de milhares de computadores de uma centena de países, entre eles Rússia, Espanha, México, Brasil, Itália, e ainda diversas empresas e organizações ao redor do mundo, incluindo hospitais britânicos e a empresa francesa Renault (PRESSE, 2017). O vírus de computador de resgate "*ransonware",* explorando uma falha nos sistemas Windows, criptografou vários arquivos de computador e seus criadores exigiram das empresas pagamento em "*bitcoins"*, uma espécie moeda virtual volátil possível de se converter para qualquer outro tipo de moeda no mundo e não rastreável, com o pagamento as empresas receberiam a devolução dos documentos, alguns fundamentais para o funcionamento delas. As empresas que não possuíam cópias de segurança na "*nuvem*" ou em um HD externo viram-se obrigadas a pagar o resgate, o que incentivou a continuação do golpe.

Este infortúnio acontecimento prova uma vez mais o quanto a nossa sociedade atual encontra-se tão dependente do computador e da internet, e quão desprotegidos e vulneráveis estamos frentes a eles. É dever do Estado garantir o direito à informação e a segurança para alcançar este direito, já que foi estabelecido pela Organização das Nações Unidas (ONU) em 2011 que o acesso à internet é um direito humano fundamental. Os crimes virtuais ocorrem no mundo inteiro, e por não respeitarem fronteiras físicas e a internet atuar no ciberespaço, além da legislação específica é necessária a criação de tratados internacionais que abordem esse tema.

5. CONVENÇÃO DE BUDAPESTE SOBRE O CIBERCRIME

Com a criação da internet surgiu o ciberespaço, que não é um território físico propriamente dito, mas sim um fluxo constante de informações através de uma rede de

ISSN nº 2359-0106 Vol. 4, n. 2, 2017.

comunicação no espaço virtual, que de acordo com Conte (2008), seria um ambiente global no qual há uma transcendência dos limites territoriais (da vida real), podendo um indivíduo está em diversos espaços na internet ao mesmo tempo. Por esse motivo, os crimes cibernéticos possuem caráter transnacional, por atingirem diversos países através de um mesmo computador pelo ciberespaço, que não possui fronteiras, e devido a essa característica tão especifica desse tipo de crime, deve-se criar um acordo internacional para o combate dos crimes virtuais transnacionais.

> Já se deu a internacionalização da criminalidade informática, devido à mobilidade dos dados nas redes de computadores, facilitando os crimes cometidos à distância. Diante desse quadro, é indispensável que os países do globo harmonizem suas normas penais, para prevenção e repressão eficientes (FERREIRA, 2008).

Foi proposto em 2001, na Convenção sobre o Cibercrime, ou Convenção de Budapeste, um tratado internacional de direito penal e direito processual firmado no âmbito do Conselho da Europa, que tinha como objetivo encontrar formas de persecução aos crimes praticados por meio da internet, propondo-se uma colaboração internacional entre os Estados-membros, dos quais o Brasil faz parte, para deter a ação dos infratores cibernéticos em suas condutas transnacionais com a adoção de uma política criminal comum, além de apresentar normas do direito penal material e normas processuais, de forma a regular a questão das competências (CONTE, 2008). No artigo 22 da Convenção está disposto:

> 1.Cada parte adotará as medidas legislativas e outras que se revelem necessárias para estabelecer à competência relativamente a qualquer infração penal definida em conformidade com os artigos 2º *a* 11º da presente Convenção, sempre que a infração seja cometida:
> a) no seu território;
> b) a bordo de um navio;
> c) a bordo de aeronave matriculada nessa parte e segundo as suas leis; ou
> d) por um dos seus cidadãos nacionais, se a infração for punível criminalmente onde foi cometida ou se a infração não for de competência territorial de nenhum Estado (BUDAPESTE, 2001).

Tal convenção, no entanto, não foi efetiva no combate a esses crimes, tendo em vista que em 2012 foi necessária a criação da lei 12.737/2012, resultante do PL

ISSN nº 2359-0106 Vol. 4, n. 2, 2017.

84/1999 devido uma onda de ataques de *hackers* e *crackers* a sites oficiais do governo e empresas públicas em 2011, que acabaram por ficar fora do ar temporariamente. Ainda assim, devido à volatilidade da Internet, o anonimato e a falta de cuidado por parte de diversas empresas, a ação dos hackers continua a existir, e o combate a eles torna-se mais difícil a cada dia, devido à continuidade dos avanços tecnológicos. Mas ainda há no mundo uma carência por um tratado internacional, efetivo, que regule esse crime e aumente a punição para quem o realize, pois há o risco que esse delito seja julgado em toda e qualquer parte do mundo ou, ainda, não seja julgado em nenhum.

6. NOVAS LEIS PENAIS

Apesar do uso da analogia para classificar os crimes virtuais no Direito Penal, a simples classificação em uma categoria não é eficiente para pôr fim a tal crime, tendo em vista que continua ocorrendo nos dias de hoje e que os culpados muitas vezes saem impunes. Em 2012, a atriz Carolina Dieckmann teve seu computador pessoal *hackeado* e diversas fotos íntimas da atriz foram vazadas *online*. A partir desse caso, foi criado a Lei Brasileira Nº 12.737/2012 que tipifica alguns delitos virtuais.

> Invasão de dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita. Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa (BRASIL, 2012, art. 154- A).

Essa lei, no entanto, sofreu diversas críticas por seus dispositivos amplos, confusos e abertos a mais de uma interpretação, sua amplitude dificulta a tipificação e aplicação de certos crimes não expostos de forma correta nas leis penais. É necessário um maior estudo dos crimes virtuais pela quantidade de usuários da internet, um exemplo claro disso é na famosa rede social *Facebook*, que no ano de 2016 estimou uma média de um bilhão de visualizações em sua página todos os dias, e este número só tende a crescer.

ISSN nº 2359-0106 Vol. 4, n. 2, 2017.

O Diretor de Crimes de Alta Tecnologia da OAB, Coriolano Aurélio de Almeida Camargo Santo, em entrevista afirmou que na atualidade os infratores da lei costumam sair impunes, pois o direito penal prevê condutas muito especificas enquanto deveria existir uma legislação clara para a qual os infratores iriam responder com uma maior facilidade do que a atual[5]. Outro fator que dificulta a punibilidade é a precariedade de provas nos casos por terem sido praticados no âmbito virtual.

Em 2011 no Brasil, ataques a computadores brasileiros quase triplicaram em relação ao ano anterior, e no ano seguinte, em 2012, foram registrados 399.515 casos de problemas com vírus, códigos maliciosos ou tentativas de fraude, em contrapartida com os apenas 142.844 casos registrados em 2010 (MACHADO, 2014). É evidente que esse caso de crimes virtuais vem aumentando ao longo dos anos, e qualquer legislação já criada para abordar o caso não está sendo eficaz.

Na era da Globalização, a Internet é usada para mais do que entretenimento e comunicação, atualmente é utilizada como ambiente de compra e venda, perpassando por compras de ações bancarias e fechamento de contratos multimilionários, até pedidos de entrega de comida em casa e compras de roupas *online.* Por haver uma grande movimentação monetária *online*, a possível desconfiança nesse serviço ou o medo de ataques cibernéticos é inviável, podendo prejudicar em milhões de dólares diversos negócios, desde as microempresas, que tem como única forma de venda a plataforma *online*, até multinacionais que tendem a fechar negócios via internet por terem sedes espalhadas pelo mundo.

De acordo com Vedovate (2005), falta uma norma específica que assegure os asseios da comunidade virtual, pois o código apenas sana parte dos conflitos a respeito desse tema. Vários projetos de lei contra crimes virtuais já foram criados, mas hoje viraram lei ordinária, e mesmo essas ações ainda não são suficientes para coibir as práticas do infrator cibernético.

[5] Disponível em: http://egov.ufsc.br:8080/portal/conteudo/crimes-virtuais-elementos-para-uma-reflex%C3%A3o-sobre-o-problema-na-tipifica%C3%A7%C3%A3o. Acessado em: 10 de setembro de 2017.

Vertentes do Direito

ISSN nº 2359-0106 Vol. 4, n. 2, 2017.

CONSIDERAÇÕES FINAIS

Percebe-se, mesmo nos dias atuais, com o acesso à informação facilitada e a grande propagação de meios tecnológicos, ainda não é efetivo no Código Penal Brasileiro o combate aos crimes virtuais, devido a não punição de quem os cumpre. O anonimato gerado pela internet dificulta a atuação jurídica, e a *Deep Web* facilita as atividades ilegais, uma vez que estas são criptografadas, impossibilitando o rastreamento.

O ciberespaço transcende os limites territoriais, e por esse motivo que a necessidade de um tratado internacional é tão grande, propondo uma colaboração internacional efetiva entre os Estados-membros, semelhante ao promovido na Convenção de Budapeste sobre o Cibercrime em 2001, com o intuito de deter a ação dos infratores virtuais para impedir ciberataques em massa como o que ocorreu em 2017.

Tendo em vista o abordado, vê-se de extrema urgência uma mudança drástica no Código Penal Brasileiro para assegurar o direito e a liberdade dos cidadãos nesse novo meio virtual, através do aumento da intervenção estatal no âmbito virtual e tecnológico, de forma a proteger a difusão de informações, como garantido na Constituição, tendo foco numa maior fiscalização e efetividade das leis para pôr fim às práticas nocivas e delitos virtuais, sanando os conflitos acerca desta temática e assegurando a segurança para a comunidade virtual.

REFERÊNCIAS

BITTENCOURT, R. N. A sociedade de transição (Resenha do livro A sociedade de risco: rumo a uma outra modernidade de Ulrich Beck). **Filosofia** (São Paulo), v.53, p.60, 2010.

BOBBIO, N. **A era dos direitos.** Trad. Carlos Nelson Coutinho. 10. Ed. Rio de Janeiro: Campus, 1992.

ISSN nº 2359-0106 Vol. 4, n. 2, 2017.

BRASIL. **Constituição Federal**. Brasília: Senado Federal, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 8 de ago. de 2017.

_____. **Código Penal.** Decreto-Lei 2.848de 7 de dez. de 1940.Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm >. Acesso em: 8 de ago. de 2017.

_____.**Código Penal**, artigo 154A. Disponível em: < https://www.jusbrasil.com.br/topicos/28004011/artigo-154a-do-decreto-lei-n-2848-de-07-de-dezembro-de-1940>. Acesso em: 8 de ago. de 2017.

_____. Estatuto da criança e do adolescente: Lei federal nº 8069, de 13 de julho de 1990. Rio de Janeiro: **Imprensa Oficial**, 2002.

_____. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. **Diário Oficial da República Federativa do Brasil**, Brasília, DF, 30 de nov. 2012. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 8 de ago. 2017.

_____. Supremo Tribunal de Justiça. **Recurso especial Nº 1117633/RO,** Relator: Ministro Herman Benjamin. Brasília, 09 de março de 2010. Disponível em: < https://stj.jusbrasil.com.br/jurisprudencia/8569044/recurso-especial-resp-1117633-ro-2009-0026654-2/inteiro-teor-13668131>. Acessado em: 07 de ago. de 2017.

CARNEIRO, A. G. Crimes virtuais**:** elementos para uma reflexão sobre o problema na tipificação**. Âmbito Jurídico**, Rio Grande, XV, n.99, abr. 2012.

CONTE, C. P.; SANTOS, C. A. A. C. Desafios do Direito Penal no Mundo Globalizado: A aplicação da Lei Penal no espaço. **Revista de Direito de Informática e Telecomunicações,** ISSN 1983-392X, 2008.

CONVENÇÃO SOBRE O CIBERCRIME. Budapeste, 2001. Disponível em: < http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf>. Acesso em: 8 de ago. de 2017.

COSTA, M. A. R. Crimes de Informática. **Revista Jus Navingandi**, ISSN 1518-4862; Teresina, ano 2, n.12, 5 maio 1997, disponível em: < https://jus.com.br/artigos/1826/crimes-de-informatica>. Acesso em: 22 jun. 2017.

ISSN nº 2359-0106 Vol. 4, n. 2, 2017.

FERREIRA, I. S. A criminalidade informática. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Co-ord.). **Direito & internet: aspectos jurídicos relevantes**. São Paulo: Quartier Latin, 2008, v.2. p. 213.

HUNGRIA, N. **Comentários ao Código Penal**. Rio de Janeiro: Forense, 1954.

JESUS, D. E**. Direito penal – Parte Geral**. Vol. 1. São Paulo: Saraiva: 2003.

LIMA, S. P. Crimes virtuais: uma análise da eficácia da legislação brasileira e o desafio do direito penal na atualidade. **Âmbito Jurídico**, Rio Grande, XVII, n.128, set. 2014.

MACHADO, L. A. Crimes cibernéticos. In: **DireitoNet**, 20 de nov. 2014, disponível em < https://www.direitonet.com.br/artigos/exibir/8772/Crimes-ciberneticos>. Acesso em: 22 jun. 2017.

MONTEIRO NETO, J. A. **Aspectos Constitucionais e Legais do Crime Eletrônico**. Fortaleza, 2008.

PRESSE, F. **"Ataque de Hackers 'sem precedentes' provoca alerta no mundo".** Disponível em: <https://g1.globo.com/tecnologia/noticia/ataque-de-hackers-sem-precedentes-provoca-alerta-no-mundo.ghtml>. Acesso em: 8 de ago. de 2017.

VEDOVATE, L. L. V. Contratos Eletrônicos. **INTERTEMAS**. V.10, n.10. Presidente Prudente, 2005.

WENDT, E.; JORGE, H. V. N. **Crimes Cibernéticos.** São Paulo: BRASPORT, 2012.