INAPLICABILIDADE DA LEI 12.965/14 EM RELAÇÃO AOS CRIMES VIRTUAIS

Mayron da Costa Amaral[1]

Lyzia Menna Barreto Ferreira[2]

RESUMO

Este artigo tem como finalidade abordar as circunstancia históricas da internet no Brasil, seu surgimento e o processo de mudança, com analise da evolução em que a tecnologia se instala no país, focando no estudo da lei que regulamenta o acesso da internet no território nacional, Lei 12.965/14 e Lei 12.737/2012 que foi o ponta pé inicial para a necessidade de uma regulamentação da web em solo brasileiro, além de analisar seus avanços e suas dificuldades em ser aplicada no caso concreto, ao longo dos meios que esses crimes são praticados e, refletir sobre a aplicação do Código Penal Brasileiro havendo necessidade ou não de uma lei especifica para casos de crimes cibernéticos e quais as possíveis soluções para este problema.

Palavras-chave: Crimes-virtuais; Internet; Bitcoin; Marco Civil.

INTRODUÇÃO

O elemento criminológico virtual amplia-se de forma a fazer surgirem novos crimes diariamente, além de fomentar os já existentes. A grande maioria desses crimes é cometida por meio da internet por meio de um computador ou smartphone, nesse passo, é criada uma linha de atuação delituosa, a saber, os chamados crimes virtuais ou cibercrimes (como são chamados os crimes praticados com o uso de qualquer meio eletrônico ou crimes praticados pela internet).

De certa forma, a globalização cibernética nos proporciona uma fácil conexão entre as pessoas e, caso não utilizada de forma correta, acaba por ser um amplo meio eficaz nas práticas dos crimes.

Conforme o avanço da tecnologia e seus meios de interligarem o mundo e as pessoas, surgem, também, mecanismos de ações diversas das que são propostas pelo que se entende de

[1] UNIVAG – Centro Universitário. Área do Conhecimento de Ciências Sociais Aplicadas. Curso de Direito. Aluno da disciplina TCC II, turma DIR 132 AM. E-mail – mynamaral@outlook.com

[2] UNIVAG – Centro Universitário. Área do Conhecimento de Ciências Sociais Aplicadas. Curso de Direito. Orientadora Especialista em Direito Civil e Direito do Consumidor. E-mail – lyziaadv@gmail.com

avanço tecnológico, hoje, são comuns os termos “cyber ataques”, “cibercrimes” e, os crimes virtuais, que são os crimes cibernéticos que envolvem qualquer pratica ilícita na web, podendo ser uma invasão de um sistema, de um site, roubo de dados, falsificação ideológica, vazamento de informações, acesso às informações pessoais, entre outras.

O presente estudo tem como meta, analisar a ausência de amparo legal em relação aos crimes virtuais no Brasil, pois para resolver os conflitos decorrentes das relações virtuais, é necessário utilizar a analogia com os tipos penais existentes, o que muitas vezes não acarreta como a melhor punição, visto que dependendo do crime, é grandioso o impacto causado na vida das pessoas.

Esses crimes vão desde um ataque de e-mail a uma transação bancária não permitida, por exemplo. No Brasil, temos a Lei 12.965/14 que regulamenta a internet no país, contudo, ao mesmo tempo em que os meios de comunicação avançam os crimes cibernéticos seguem o mesmo caminho, fazendo com que diversas pessoas sejam atingidas por essas ações.

Cabendo assim, ao Estado inibir as ações nocivas às pessoas, sendo necessária a criação de nova legislação ainda não prevista que envolve os crimes virtuais, uma vez que não é permitido no Direito Penal analisar questões por analogia em relação às tipificações já existente. E é nesse ponto em que o presente artigo visa analisar, se essa seria a maneira mais eficiente de combater as ações dos criminosos virtuais.

SURGIMENTO E CRESCIMENTO DO USO DA INTERNET NO BRASIL

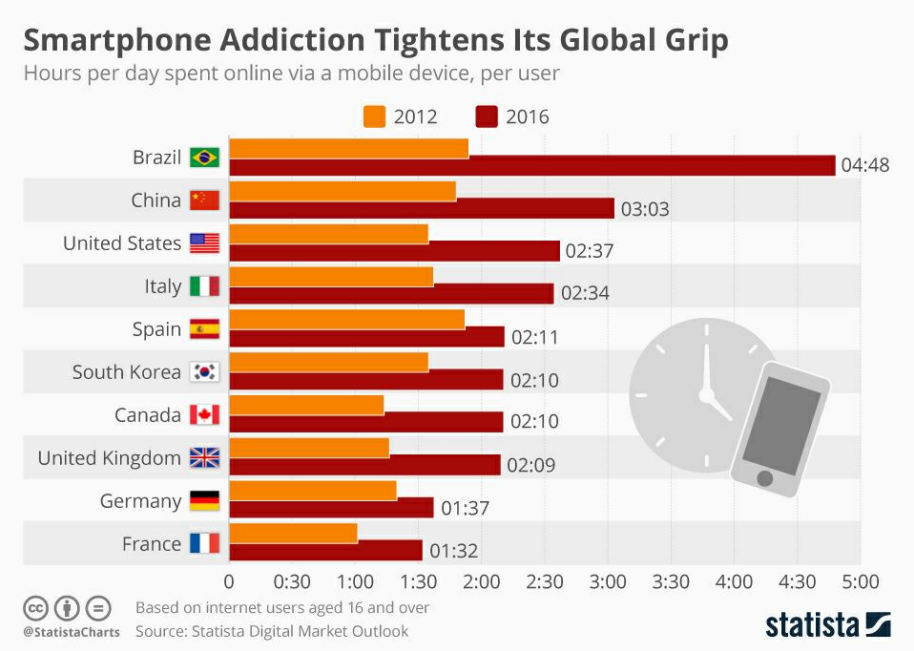
A internet surgiu no Brasil no mesmo ano em que se criou a Constituição Federal Brasileira, em 1988, nessa época a internet era apenas para fins acadêmicos, surgindo no Brasil através da LNCC (Laboratório Nacional de Computação Científica) que acessou ao Bitnet, uma processadora de rede criada pela Universidade de Nova York (CUNY) e a Universidade Yale, de Connecticut.

Posteriormente, foi à vez da FAPESP (Fundação de Amparo à Pesquisa do Estado de São Paulo) ter acesso a rede de computadores, para, também, fins acadêmicos. Após esse período, outros Estados implantaram a rede para comunicação entre as universidades e então em 1994, com o surgimento da World Wide Web (WWW – 1990) a internet no Brasil passa de fins acadêmicos para ser comercializada para o público em geral.

Nos dias atuais com a popularização da internet e o acesso da população a smartphones, surgem a cada momento novos sites e aplicativos, pessoas gerenciando empresas na palma da mão, comunicação intercontinental, nossas vidas sendo gerenciada por meio de um celular.

Entre os 10 países que mais usam o smartphone por hora, o Brasil está no topo, com a média de 04 (quatro) horas e 48 (quarenta e oito) minutos por dia, conforme estudo publicado pela empresa Alemã STATISTA, foram coletado dados de 2016 para a realização da pesquisa, mostrando como o Brasileiro está conectado, é o que expõe o gráfico abaixo[3]:

Gráfico 1: Ranking dos países que mais usam o smartphone por horas no mundo, ano de 2016.



Fonte: (STATISTA, 2016)

ANÁLISE DA APLICABILIDADE DA LEI 12.965/2014

Após a transição da utilização da internet por meios acadêmicos e passando para o uso comum e geral pelas pessoas e, hoje, é quase que impossível pensar no futuro sem a internet, e consequentemente essa utilização de forma ampliada já nos dias atuais, a comodidade em que a internet nos proporciona como exemplo, é realidade as transmissoras de TV tanto livres quanto por assinatura disponibilizarem seus serviços por meio de sites e aplicativos,

[3] Disponivel em: Statista – The Statistics Portal: https://www.statista.com/chart/9539/smartphone-addiction-tightens-its-global-grip/. Acesso em 11.06.2018.

plataformas de streaming de vídeos e músicas, possibilidade das pessoas em conseguir renda por meio de criação de conteúdo para a internet e até o trabalho de transporte por meio de aplicativos conectados a internet, com toda essa conexão também surgem novos meios de crime.

Assim expõe João Araújo Monteiro Neto:

> As condutas ilícitas praticadas através do ambiente informático prejudicam a manutenção dos níveis mínimos de segurança e credibilidade necessários a qualquer negócio jurídico. Mais do que isso: interferem no cotidiano de muitas pessoas, de modo que esse novo ambiente se torna inapto para a mantença de relações sociais. (MONTEIRO NETO, 2008, p. 10)[4]

Existem diversas formas de crimes cibernéticos e tipos diferentes de criminosos e os mais comuns nas estatísticas são os hackers e crackers, define Vicente Lentini Plantullo, (Estelionato eletrônico e seus agentes, 2011) os hackers e crackers como:

É uma pessoa física que detém, como objeto, a investigação da integridade e da segurança de um sistema qualquer de computador. Utilizasse de técnicas avançadas para invadir sistemas e detectar suas respectivas falhas. Todavia, não os destrói ou prejudica. [5]

E respectivamente crackers como:

> Por sua vez, o termo cracker se refere às pessoas que possuem um grande conhecimento de programação e de segurança em sistemas de computação. Tais pessoas utilizam esse conhecimento para tirar vantagens pessoais, como destruição de sistemas por mero vandalismo ou aplicação de condutas para diversos fins ilícitos, como o estelionato eletrônico.

Já os crimes mais comuns no Brasil são aqueles presentes no nosso dia-dia e que acostumamos apenas em ignora-los, justamente por não se sentir amparados legalmente contra esse tipo de delito, que, aparentemente simples, mas que podem gerar transtornos inimagináveis na vida de uma pessoa. Em se tratando dos crimes em espécie podemos classifica-los em: pirataria, roubo de identidade, pedofilia, calúnia e difamação, discriminação e preconceito, ameaça e etc.

Além dos crimes acima mencionados, também podem ocorrer na web outras ações delituosas como, expõe Emanuel Alberto Sperandio Garcia Gimenes:

> Lavagem de dinheiro e de invasão de privacidade, pichações em sites oficiais do governo, vandalismo, sabotagem, crimes contra a paz pública, espionagem, lesões a

[4] Disponível em: <http://dominiopublico.mec.gov.br/download/teste/arqs/cp055676.pdf>.

[5] Disponível em: Portal de e-governo, inclusão digital e sociedade do conhecimento: <http://www.egov.ufsc.br:8080/portal/conteudo/estelionato-eletr%C3%B4nico-e-seus-agentes>. Acesso em 19.06.2018.

> direitos humanos (terrorismo, crimes de ódio, racismo, etc.), destruição de informações, jogos ilegais, falsificação do selo ou sinal público, falsidade ideológica, modificação ou alteração não autorizada de sistema de informação, violação de sigilo funcional, fraude em concorrência pública, dentre inúmeros outros.

Outro crime muito comum é o envio de e-mail simulando ser uma instituição conhecida ou algum órgão público para que, a pessoa que recebe o e-mail, informe dados privados e bancários para um recadastramento ou para que seja sanada alguma pendencia com a instituição, nota-se que, para isso, o criminoso possua um conhecimento sobre a vítima, que pode ser tanto por meio de uma pessoa próxima ou que o criminoso tenha previamente conseguido informações por meio de um crime virtual anterior, como a invasão do computador da vítima.

É nítido que estamos interligados à rede, os avanços tecnológicos e como a economia está interligada a esse sistema, contudo, é necessário visualizar todos os caminhos que essa facilidade (internet) toma, assim feito, em 2014 foi inserida no ordenamento jurídico brasileiro a lei 12.965/14, que regulamenta o uso da internet no Brasil.

Não foi de forma espontânea que a lei surgiu, pelo contrário, se observou a necessidade da criação de uma legislação após vários precedentes de divergências advindas da internet, como o caso midiático que protagonizou a atriz brasileira Carolina Dieckmann em que teve suas fotos intimas publicadas sem autorização na web.

O ocorrido tomou grandes proporções que até mesmo o Congresso Nacional em um curto tempo e que, posteriormente, foi sancionada pela presidente da república, a lei 12.737/2012, apelidada como lei Carolina Dieckmann que, acrescentava ao Código Penal Brasileiro os Arts. 154 – A e 154 – B, tipificando os delitos informáticos, quais sejam:

> **Art. 154-A**. Invadir 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:
> **Art. 154-B**. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

Nesse passo a legislação brasileira já se encaminhava para a tentativa de proteção dos interesses dos internautas que, após o mencionado caso, percebiam que o ambiente virtual não é um lugar sem lei, porém, os dispositivos acima visavam poucos delitos e que mais tarde

notaria que não era suficiente para garantir os direitos de quem acessa a rede de computadores.

A Lei 12.737 de 30 de novembro de 2012, criada para ser um avanço, foi modificada para apenas alterar os dispositivos legais que já existiam. Possuindo a ementa a seguir:

> Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei no 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei no 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências.

No mesmo ano da promulgação da lei, sites do governo Brasileiro sofreram com ataques de hackers, que é definido por Marcelo Barreto de Araújo como: “aquele que invade sistemas e computadores, mediante senhas, propagação de vírus e ações similares”, Araújo, Marcelo Barreto de, (Comércio Eletrônico, Marco Civil da Internet e Direito Digital, ed. CNC, pag.74)

Com isso, verificou-se que o país necessitava de uma legislação mais ampla em relação à internet e os crimes advindos desta. Assim, surge em 2014, à lei popularmente conhecida como “Marco Civil da Internet”, lei 12.965/2014.

Os principais pontos que o Marco Civil propõe é em relação a Neutralidade, Privacidade e Registros dos acessos. A primeira atinge principalmente as grandes empresas e provedoras de internet no país, assim, uma provedora não pode oferecer serviços de forma diferenciada em relação ao acesso.

Não pode colocar ao mercado pacotes para um determinado produto, e não permitindo ao usuário acessar conteúdo diverso. O cesso deve ser livre e o usuário tem que possuir a liberdade de utilizar todo o seu pacote como desejar.

Já os registros dos acessos, diz respeito o armazenamento de forma provisória do acesso dos usuários na rede, assim, as provedoras devem guardar a linha de acesso que um usuário fez para acessar um determinado site, por exemplo.

Em relação à privacidade, tange no direito ao sigilo e inviolabilidade nos dados dos usuários, podendo ser quebrado a inviolabilidade quando solicitado por ação judicial ou para identificação em caso de ação ilícita de usuário.

O marco civil da internet muito se fala sobre privacidade e proteção, mas e quando essas garantias são violadas? A lei 12.965/2014, não tem tipificação de ato ilícito contra os direitos que ali são expostos, para isso, o usuário que teve seu amparo legal violado deverá recorrer ao código penal brasileiro.

Mas, nem sempre buscar o código penal é certeza de solucionar a violação de um direito, existe uma legislação de regulamentação (Marco Civil), apenas, o código penal brasileiro não está preparado para amparar os crimes virtuais, uma vez que, para isso seria necessário equipar e preparar os profissionais da justiça e da policia para essa realidade.

É visível os investimentos que governantes implantam em diversas áreas no país, mas, não é comum investimentos em segurança digital, como explica o delegado Emerson Wendt que atua na Delegacia de Repressão aos Crimes de Informática (DRCI) do Rio Grande do Sul, onde os policiais carecem de treinamento, equipamentos e ferramentas adequadas, precisando utilizar softwares gratuitos e que já são conhecidos dos criminosos.[6]

Um exemplo do desamparo legal em relação aos crimes virtuais, e de acordo com Central Nacional de Denúncias de Crimes Cibernéticos (SaferNet), em 2017, 63% dos crimes virtuais estão relacionados ao discurso de ódio na internet. Um crime que dependendo do caso pode ser relativamente fácil de identificar o autor, caso esse não use um perfil fake na internet.

E nesses casos em específico, com base no Marco Civil da Internet, o usuário que comete um crime tem seus dados protegidos pela provedora ou empresa em que disponibiliza o ambiente virtual, sendo necessária uma ação judicial que dependendo do caso, até isso ocorrer, poderá haver a prescrição do crime.

Existe uma tendência no Brasil na criação das delegacias especializadas de crimes virtuais, o que é um grande avanço, entretanto, com a legislação atual predomina-se em uma grande demora na identificação do sujeito ativo do ato criminoso, visto que esse pode estar munido de anonimato no ambiente virtual, o que dificulta o serviço dos investigadores, e quando identificado, o autor ser processado, que depende de representação da vítima, há uma grande demora nesse procedimento.

Um grande atraso da legislação é que caso uma pessoa sofra um crime cibernético essa precisará das informações fornecidas pelas empresas, no caso da Google, Facebook e WhatsApp, por exemplo, essas só fornecem informações de usuários por meio de ação judicial, e somente é fornecido o endereço IP, que é o endereço de uma máquina.

Nessa mesma ação a vitima terá que solicitar aos provedores de internet as informações do usuário desse endereço IP, contudo, nem todos os juízes aceitam os provedores como parte no processo, tendo a vítima que interpor nova ação contra o provedor

[6] Disponível em: G1:< http://g1.globo.com/tecnologia/noticia/2011/01/trabalho-contra-crimes-virtuais-ainda-esta-longe-do-ideal-diz-delegado.html>.

de internet, É o que explica para uma entrevista ao portal Olhar Digital, o Advogado especializado em TI (Tecnologia da Informação) José Milagre.

Nota-se que para os crimes gerais cometidos em ambiente virtual não há uma tipificação específica na legislação, mas sim uma adaptação dessa conduta ao código penal, gerando certa confusão em relação aos delitos, como exemplo, o envio de e-mails falsos para um determinado usuário com o intuito da captação de seus dados bancários, por meio de instalação de programa malicioso, como um vírus, por exemplo.

Esse sujeito comete furto de dados (art. 155 do CP) ou estelionato (art. 171 do CP)? O STJ possui decisões divergentes quanto a isso, há casos em que o tribunal adota a postura de furto e em outros como estelionato para práticas criminosas semelhante, nítida a carência de legislação específica para a tipificação de crimes oriundos do meio virtual. Mesmo que o judiciário adapte o crime com a legislação existente, os casos que possuem peculiaridades ficam na margem da inaplicabilidade.

A respeito da atuação jurisdicional contra os crimes virtuais, o site do Jornal Folha de São Paulo noticiou em 24.11.2008 o seguinte:

> Os crimes praticados por meio da Internet, que em 2002 motivaram apenas 400 sentenças, crescem vertiginosamente no país. Seis anos depois, o número chega a 17 mil sentenças tratando dos chamados crimes virtuais, informa o blog do Josias de Souza. A notícia vem do STJ (Superior Tribunal de Justiça) e serve para desmistificar a ideia de que a Internet seria uma espécie de território sem lei.
> A Justiça vem enquadrando os novíssimos crimes cibernéticos no velhíssimo Código Penal brasileiro, editado em 1940, ainda sob o governo Getúlio Vargas.
> Segundo o STJ, cerca de 95% dos delitos cometidos pela Internet já estão previstos no Código Penal e apenas são cometidos em um ambiente novo: a Internet.

Com analise da jurisprudência, o que se refere aos 95% dos delitos cometidos pela internet já previstos por adaptação ao código penal, são os crimes comuns que se denotam de pouca complexidade, os crimes que estão “em alta” atualmente são justamente os 5% não previstos na legislação, sendo assim, devem continuar sem legislação específica?

Não é dessa maneira que devemos enxergar o ambiente virtual, como já mencionado aqui, um ataque virtual pode afetar de forma instantânea a vida de milhares de pessoas, trazendo prejuízos psicológicos quanto financeiros.

É nesse sentido que a empresa mundial especializada em segurança informática, McAfee publicou um relatório em que o Brasil perde por ano 32,4 (bilhões de reais) em decorrência de ataques criminosos contra empresas.[7]

Nesse ponto que grande parte da impunidade em relação aos crimes virtuais surge, uma vez que conforme o art. art.5º, XXXIX, da Constituição Federal expõe: "não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal". Podemos então concluir que como não há pena anterior que tipifique os crimes cibernéticos não há como ter punição à aqueles que cometem.

Contudo, os crimes comuns foram adaptados ao código penal e em até certo ponto e desde que não possua complexidades, funcionam muito bem, disserta Ivette Senise Ferreira, o seguinte:

> (...) em crime informático impróprio e crime informático próprio. Os primeiros não seriam crimes informáticos, seriam crimes comuns nos quais o computador é usado como instrumento para sua execução. Exemplos de crimes informáticos impróprios pode ser a calúnia (art.138 CP), difamação (art. 139 CP), injúria (art. 140 CP), todos podendo ser cometidos, por exemplo, com o envio de um e-mail, correio eletrônico através do qual os usuários trocam mensagens. (2000, p. 220).

Outrossim, os casos dos contratos que são celebrados pela esfera digital que, embora a cada dia mais possui contratos sendo celebrados pela internet para contratação de diversos serviços e produtos, são mais um exemplo de que o Brasil não possui legislação específica sobre os ilícitos cometidos através desse meio.

Muitas vezes, é utilizado o princípio da analogia como única via para não deixar o criminoso cibernético sem punição. Entretanto, tal princípio não é aplicável no Direito Penal, por ferir do princípio da taxatividade, sendo importante a criação de leis mais específicas.

São exemplos de normas aplicadas, com a utilização da analogia, aos crimes virtuais: Calúnia (art. 138 do Código Penal); Difamação (art. 139 do Código Penal); Injúria (art. 140 do Código Penal); Ameaça (art. 147 do Código Penal); Furto (art. 155 do Código Penal); Dano (art. 163 do Código Penal); Apropriação indébita (art. 168 do Código Penal); Estelionato (art. 171 do Código Penal); Violação ao direito autoral (art. 184 do Código Penal); Pedofilia (art. 247 da Lei nº 8.069/90 - Estatuto da Criança e do Adolescente); Crime contra a propriedade industrial (art. 183 e ss. da Lei nº 9.279/96); Interceptação de comunicações de informática (art. 10 da Lei nº 9.296/96); Interceptação de E-mail Comercial ou Pessoal (art.

[7] Disponível em: Revista Veja: https://veja.abril.com.br/economia/brasil-perde-us-10-bilhoes-por-ano-com-cibercrime-diz-mcafee/. Acesso em 11.06.2018.

10 da Lei nº 9.296/96); Crimes contra software - “Pirataria” (art. 12 da Lei nº 9.609/98). (CARNEIRO, 2012, p. 1)

Ante o exposto, fica claro que mesmo utilizando o Código Penal Brasileiro não se verifica uma forma eficiente para o combate aos crimes digitais, carecendo o país de uma legislação penal específica aos crimes cibernéticos.

Furlaneto Neto e Guimarães (2003, s/p) destacam ainda que:

> Além das condutas descritas como crime, existem ainda aquelas consideradas ilícitos prejudiciais, as quais não são consideradas crime e não possuem legislação específica, não sendo possível, igualmente, a aplicação da analogia.[8]

São exemplos os danos praticados contra informações, os programas contidos em computador, as propagações de vírus informáticos entre outros.

Não o bastante, existem leis específicas que tratam do assunto, contudo, de forma a não abranger todo o meio de atuação dos cybers criminosos. Assim, ainda não é suficiente o eixo de tipos incriminadores no ordenamento jurídico pátrio.

No entendimento de Alexandre Atheniense:

> Entendo que as soluções legais a serem buscadas deverão objetivar a circulação de dados pela internet, controlando a privacidade do indivíduo sem cercear o acesso a informação. Neste sentido é necessário aprimorar nossas leis de proteção de dados, inclusive com a regulamentação da atividade dos provedores que controlam a identificação do infrator, bem como um maior aparelhamento das delegacias especializadas. (ATHENIENSE, 2004, p. 1)

Um crime cibernético diverge do crime real e comum, que é contra uma ou algumas pessoas, o crime cometido em ambiente virtual pode ser propagado para centenas de pessoas em questão de minutos. Nossa justiça está preparada para uma ação dessa magnitude? Enquadrando os crimes com o código penal, provavelmente não estaria.

Além de toda a questão jurídica temos também as barreiras que a internet proporciona. É comum corrente em aplicativos de mensagens de promoções atrativas, mas que na verdade é mais um ataque criminoso, onde o usuário acessando o link fornecido pelo agente criminoso tem seus dados subtraídos.

Entretanto, enquanto a justiça enfrenta barreiras para uma punição à criminosos virtuais, estes não possuem barreiras, uma vez que é possível que uma pessoa de Nova York utilize por meio de uma alteração em seu sistema um servidor de Londres para fazer uma vítima aqui no Brasil.

> No que tange à conduta transnacional dos infratores cibernéticos, os mesmos utilizam-se de tecnologia de ponta para encobrirem aspectos relacionados à

[8] Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/crimes_na_internet.pdf>

> materialidade dos delitos. Assim, eles se mantêm no anonimato de forma fácil, sendo indispensável uma colaboração internacional, proposta, inclusive, na Convenção de Budapeste, não ratificada pelo Brasil, a qual prioriza uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no meio digital através da cooperação internacional. (WANDERLEI, 2012, p. 45-46; HAJE, 2011, s/p; SOUZA; PEREIRA, 2009, p. 5)

Hackers possuem tecnologia de ponta tanto para cometer crimes quanto para se esconderem da lei, assim, enquanto criminosos se aperfeiçoam, nossos Estados ficam a mercê das condições que possuem para o combate dos crimes digitais, enfatizando assim, a total discrepância em que o país está em relação à tecnologia.

Em uma entrevista ao site UOL, Fábio Assolini, analista de segurança da empresa Kaspersky, empresa especializada em segurança digital, explica:

> A investigação demora, principalmente quando há solicitação de dados de servidores em outros países. Nesse tempo, o criminoso já eliminou as evidências que podem ser usadas nessa investigação e está fazendo outro golpe.[9]

Outra questão é falta de preparo das polícias, são poucos os Estados que possuem divisões especializadas em crimes cibernéticos e os que têm tendem o foco no crime comum, como o de estelionato, por exemplo.

Já no que se diz respeito a Policia Federal essa apenas investiga crimes que relacione a União e seus interesses ou crimes que ultrapassam a fronteira, os demais ficam a cargo das policias Estaduais, contudo, a polícia de São Paulo, por exemplo, não atua em relação a crimes gerais, mas apenas em específicos.

BITCOIN

Merece grande observação da legislação atual e futura por conta de sua grande influência no mercado financeiro mundial e nacional que nada mais é que uma moeda virtual e, mesmo sendo virtual não é rastreada visto que, possui como sua característica a criptografia.

O bitcoin não é uma moeda governamental e nem atrelada a algum banco, podendo ser identificada sua origem em casos de transações volumosas e apenas com cruzamento de informações, mas para isso é necessário um grande conhecimento tecnológico.

---

[9] Disponível em: <https://tecnologia.uol.com.br/noticias/redacao/2018/02/05/por-que-a-pessoa-que-tenta-te-roubar-pelo-whatsapp-nao-e-presa-no-brasil.htm>

Por outro lado, os armazenamentos dessas informações só acontecem em uma pequena quantidade de transações que ficam em cada computador que realiza a operação, assim, não há um grande servidor central para essas informações, fazendo com que seja quase impossível identificar o autor de um depósito e quem recebeu o mesmo.

A referida criptomoeda pode ser muito vantajosa, pois desde a sua criação em 2008, já cresceu cerca de 900% de lá para cá, aquecendo o mercado financeiro, contudo, por ser uma moeda que possui segurança "anti rastreio" já é usada por criminosos virtuais. Como era o caso do maior site de comercialização de drogas ilícitas do mundo, cuja única forma de pagamento aceito era o bitcoin. [10]

É por esse motivo que o próprio Banco Central do Brasil publicou uma nota em que alerta aos brasileiros para o uso das criptomoedas, dizendo que o BC não emite garantias de conversão para o real brasileiro, por exemplo, assim expõe o comunicado:

> Considerando o crescente interesse dos agentes econômicos (sociedade e instituições) nas denominadas moedas virtuais, o Banco Central do Brasil alerta que estas não são emitidas nem garantidas por qualquer autoridade monetária, por isso não têm garantia de conversão para moedas soberanas, e tampouco são lastreadas em ativo real de qualquer espécie, ficando todo o risco com os detentores. Seu valor decorre exclusivamente da confiança conferida pelos indivíduos ao seu emissor. (BANCO CENTRAL, 2017).

A preocupação do Banco Central é da pelo fato de que a moeda virtual oscila de forma surpreendente, ao mesmo tempo em que a moeda está valorizada em um dia, no dia seguinte pode estar em um índice muito inferior.

Mas também é do conhecimento do Banco Central que a moeda virtual é utilizada como um meio eficaz na pratica de crimes, visto que um crime pode ser "contratado" por meio do ambiente virtual e ser pago através da moeda virtual.

CONSIDERAÇÕES FINAIS

Com cada vez mais a quantidade de usuários existente no mundo virtual aumenta e com a grande facilidade ao acesso a internet, a estatística de crimes cibernéticos vem aumentando, uma vez que a internet é vista por muitos como um lugar em que há plena liberdade.

---

[10] Disponivel em: site terra: Como é criada a moeda virtual Bitcoin?: https://www.terra.com.br/noticias/educacao/voce-sabia/como-e-criada-a-moeda-virtual-bitcoin,f41d30f5bb312410VgnVCM5000009ccceb0aRCRD.html. Acesso em 19.06.2018

Por isso, torna-se necessário a intervenção do Estado, para que ele puna aos que ultrapassem os limites da sua liberdade e adentrem na esfera jurídica alheia. Porém, para que o Estado consiga exercer o seu dever de punir, primeiramente é imprescindível que haja meios adequados para tal ação, ou seja, tornam-se necessários que esses crimes já se encontrem tipificados na legislação, o que atualmente não é a realidade.

Outra questão é a falta de infraestrutura e investimentos nas delegacias especializadas em crimes cibernéticos, visto que algumas ações de criminosos merecem maior atenção do Estado por conta da complexidade em que o ato delituoso é cometido, onde criminosos de um país possa cometer um crime em outro e usando o servidor (caracterizado por ser um controlador de acesso, é o servidor quem faz ponte entre as maquinas) de um terceiro país.

Nossa legislação não acompanhou a evolução tecnológica em relação à utilização da internet tendo essa necessidade de adaptar os crimes com os já tipificados em lei, o que nem sempre é o meio mais eficaz para inibir a ação criminosa, uma vez que o código penal brasileiro é da década de 40, ano esse em que não existia internet no mundo e, onde não se previa algo tão grandioso e presente na vida das pessoas.

No que se refere às criptomoedas nossa legislação não tem regulação específica, mesmo que no país essa modalidade de moeda esteja a cada dia mais sendo utilizada pelas pessoas e intuições que aceitam a moeda virtual como uma forma de pagamento.

Não podemos negar que o Marco Civil da Internet foi um grande passo para a legislação atual, passo em que os legisladores pretenderam preservar a liberdade de expressão e o direito à privacidade na web, hoje, é possível sentir-se amparado em lei em caso de lesão à direito próprio. Contudo, mesmo com essa proteção a referida lei é civil não se atentando as ações penais praticadas pelos criminosos, que diferente do poder público conta com a mais alta tecnologia a seu favor.

Assim o presente artigo conclui-se que mesmo a legislação adaptando os crimes cibernéticos comuns ao código penal brasileiro é notória a carência de uma legislação específica, visto que os crimes próprios não possuem a mesma facilidade de adaptação que o primeiro.

REFERÊNCIAS

ARAÚJO, Marcelo Barreto de. **Comércio Eletrônico; Marco Civil da Internet e Direito Digital**. Rio de Janeiro: Confederação Nacional do Comércio de Bens, Serviços e Turismo, 2017.

BANCO CENTRAL**. Comunicado nº 31.379**, 2017. Disponível em: <http://www.bcb.gov.br/pre/normativos/busca/normativo.asp?numero=31379&tipo=Comunicado&data=16/11/2017>. Acesso em 21.06.2018.

BRASIL. **Lei 12.737, de 30 de Novembro de 2012**. Tipificação Criminal de Delitos Informáticos, Brasília, DF, nov. 2012.

BRASIL. **Lei 12.965, de 23 de Abril de 2014**. Princípios, Garantias, Direitos e Deveres para o uso da Internet no Brasil, Brasília, DF, abr. 2014.

CARNEIRO, A. G. **Crimes Virtuais: Elementos Para uma Reflexão Sobre o Problema na Tipificação**. In: Âmbito Jurídico, Rio Grande, 15, n. 99, abr. 2012. Disponível em: <http://www.ambitojuridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=11529>. Acesso em: 21.06.2018.

FERREIRA, Ivette Senise. **A criminalidade informática**. In: LUCCA, Newton de, SIMÃO FILHO, Adalberto. Direito e Internet: aspectos jurídicos relevantes. Bauru: EDIPRO, 2000.

GIMENES, Emanuel Alberto Sperandio Garcia. **Crimes virtuais**. Revista de Doutrina da 4ª Região, Porto Alegre, n. 55, ago. 2013. Disponível em: <http://www.revistadoutrina.trf4.jus.br/artigos/edicao055/Emanuel_Gimenes.html>. Acesso em: 21.06.2018

GLOBO NEWS: Crimes Virtuais: **63% de denuncias são relacionadas a discurso de ódio**. Disponível em: <http://g1.globo.com/globo-news/jornal-globo-news/videos/v/crimes-virtuais-63-de-denuncias-sao-relacionadas-a-discursos-de-odio/6479331/>. Acesso em: 25.05.2018.

GHIMARÃES, José Augusto Chaves e NETO, Mário Furlano: **Crimes na Internet**: **elementos para uma reflexão sobre a ética informacional**. Direito da Informática. Brásilia, 2003. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/crimes_na_internet.pdf>. Acesso em: 14.05.2018

OLHAR DIGITAL: **O passo a passo da investigação de um crime digital**, Disponível em: <https://olhardigital.com.br/fique_seguro/noticia/entenda-como-funciona-o-processo-de-investigacao-de-um-crime-digital/35722>. Acesso em: 18.06.2018.

PLANTULLO, V. L. **Estelionato Eletrônico**. Curitiba: Juruá, 2002. Disponível em: < http://www.egov.ufsc.br:8080/portal/conteudo/estelionato-eletr%C3%B4nico-e-seus-agentes>. Acesso em: 18.06.2018.

STATISTA**: The Statistc Portal**, Disponível em:

https://www.statista.com/chart/9539/smartphone-addiction-tightens-its-global-grip/. Acesso em: 25.05.2018.

UOL: **Por que a pessoa que te aplica golpe pelo WhatsApp nunca é presa no Brasil**. Disponível em: <https://tecnologia.uol.com.br/noticias/redacao/2018/02/05/por-que-a-pessoa-que-tenta-te-roubar-pelo-whatsapp-nao-e-presa-no-brasil.htm>. Acesso em: 18.06.2018.