ISSN 1808-6136

ISSN on-line 2674-7499

ANÁLISE DA APLICAÇÃO DO DIREITO PENAL NOS CRIMES VIRTUAIS

CLÁUDIO RODRIGUES ARAUJO[1]

[1] Mestre em Teologia e Ciências Sociais pela Pontifícia Universidade Católica do RJ, Bacharel em Direito pela Universidade de Vila Velha, Pós graduando em Ciências Penais e Segurança Pública pela Universidade de Vila Velha; Pós graduando Direito Constitucional e Direito do Consumidor pela Faculdade Legale. Delegado de Polícia Civil do Espírito Santo. Email: claudio.araujo2020@hotmail.com.

RESUMO

A Internet vem tendo cada vez mais expansão, bem como o número dos seus usuários. A procura por informações, entretenimento, diversão, relacionamento, dentre outras, tais como pesquisas e atualidades são algumas das principais atividades que são advindas por ela. No entanto, certos usufruidores fazem seu emprego de maneira prejudicial, realizando a prática dos crimes virtuais. O Brasil não é possuinte de uma legislação específica acerca da temática, têm-se alguns artigos e leis que terão abordagem no decorrer do trabalho, mas, de antemão, não possuem suficiência para punir os agentes que cometem os crimes virtuais. Dessa forma, o presente trabalho tem como objetivo identificar como é feita a aplicação do Direito Penal aos crimes virtuais, evidenciando as insuficiências de uma legislação em especificidade acerca da temática, por meio de uma pesquisa bibliográfica comparativa em diversas legislações em vigor. Conclui-se que o Código Penal do país faz a tipificação de várias atuações que possuem enquadramento no ambiente web, entretanto, possui penas brandas e sem suficiência para a coibição da prática desses atos. Com isso, a ausência de uma legislação em especificidade ao cybercrime faz a intensificação da ideia de que a internet é uma terra sem leis. Por fim, é fundamental produzir uma legislação que venha a versar acerca dos crimes cometidos na internet, sendo que, são comuns e trazem para suas vítimas prejuízos reais. Com isso, tendo conhecimento dos resultados advindos dos crimes virtuais, é preciso fazer a criação de uma lei que não mais permita que a internet tenha utilização de maneira que prejudique seus usuários.

Palavras-chave: Crimes Virtuais; Direito Penal; Internet.

ANALYSIS OF THE APPLICATION OF CRIMINAL LAW IN VIRTUAL CRIMES

ABSTRACT

The Internet is increasingly expanding, as well as the number of its users. The search for information, entertainment, fun, relationship, among others, are some of the main activities that are welcomed by it. However, certain connoisseurs do their job in a harmful way, making the practice of virtual crimes. The country does not have legislation in specificity on the subject, there are some articles and laws that will have an approach in the course of the work, but beforehand, do not have the sufficiency to punish the agents who commit the virtual crimes. Thus, the present work aims to identify how criminal law is used to virtual crimes, evidencing the shortcomings of legislation in specificity on the subject. It is concluded that the Penal Code of the country makes the typification of several actions that have framing in the web environment, however, has mild penalties and without sufficiency for the inhibition of agents who commit cybercrimes. Thus, the present work aims to identify how criminal law is used to virtual crimes, evidencing the shortcomings of legislation in specificity on the subject. It

Recebido em 20/01/2021 e aprovado para publicação em 10/02/2021.

is concluded that the Penal Code of the country makes the typification of several actions that have a framework in the web environment, however, has mild penalties and without sufficiency for the inhibition of the practice of these acts. With this, the absence of legislation specific to cybercrime intensifies the idea that the internet is a land without laws. Finally, it is essential to produce legislation that will deal with the crimes committed on the Internet, and are common and bring to their victims real damages. With this, knowing the results arising from virtual crimes, it is necessary to make the creation of a law that no longer allows the Internet to have use in a way that harms its users.

Keywords: Virtual Crimes; Criminal Law; Internet.

1 INTRODUÇÃO

A Internet vem tendo cada vez mais expansão, bem como o número dos seus usuários. Os prováveis fatores que acabam impulsionando esse aumento são a evolução da tecnologia e a acessibilidade dos computadores e dispositivos móveis para acessar a internet.

Essa rede tem conceituação como sendo o maior sistema de comunicação do mundo, por causa dos diversos recursos que acabam apresentando para a facilitação da vida dos seus adeptos. A procura por informações, entretenimento, diversão, relacionamento são algumas das principais atividades que são advindas por ela. No entanto, certos usufruidores fazem seu emprego de maneira prejudicial, fazendo a prática dos crimes virtuais.

Diversas alterações foram tendo ocorrência na sociedade no aspecto tecnológico e, na mesma medida, o número de vítimas dos crimes virtuais só tem aumento no mundo todo. Percebe-se, com isso, que existe uma enorme dificuldade para o ordenamento jurídico fazer a resolução desses conflitos por causa da vasta proporção que a internet tornou pelo mundo, o que ocasionou diversas alterações, que não foram acompanhadas de forma devida pela legislação do país, fazendo com que o jurista, dentro do possível, fizesse o enquadramento das novas condutas lesivas nos tipos penais que já existiam, sendo que as legislações existentes e o controle das autoridades não têm tanta eficiência quanto parece ter.

O país não é possuinte de uma legislação em especificidade acerca da temática, tem-se alguns artigos e leis que terão abordagem no decorrer do trabalho; mas, de antemão, não possuem suficiência para punir os agentes que cometem os crimes virtuais.

Assim, o presente trabalho tem a seguinte questão-problema: como é feita a aplicação do Direito Penal aos crimes virtuais, evidenciando as insuficiências de uma legislação em especificidade acerca da temática?

Dessa forma, o presente trabalho tem como objetivo identificar a resposta a essa questão-problema.

Para tanto, foi utilizada a pesquisa bibliográfica, na qual se buscou investigar o maior número de conhecimento técnico à disposição nessa área e em posicionamento sobre o tema. A pesquisa bibliográfica consiste no exame da bibliografia, para o levantamento e análise do que já foi produzido sobre o assunto que foi assumido como tema de pesquisa científica (RUIZ, 1992).

2 OS PERIGOS DA INTERNET

O modo em que as pessoas começaram a se comunicar e buscar informações mudou muito, principalmente ao que diz respeito à velocidade dessa comunicação. Existe certa facilidade em invadir a segurança da internet e volta em meio nos deparamos com problemas causados por este tipo de fraudes em sistemas como de empresas, bancos e órgãos públicos (MITNICK; KEVIN, 2006).

> [...] grosso modo, a segurança na web pode ser dividida em três partes. Primeiro como os objetos e os recursos são nomeados com segurança? Em segundo lugar, como é possível estabelecer conexões seguranças e autenticas? Terceiro o que acontece quando a *Web* site envia a um cliente um fragmento de código executável? (MITNIK; KEVIN, 2006, p.82).

Todos os dias, tem-se acesso a notícias praticamente em tempo real e o mesmo acontece com conversas on-line, seja através somente de textos como também com o auxílio da *webcam*. Na internet, temos acesso a praticamente tudo: informação imediata, você tem a liberdade de percorrer caminhos diferenciados na internet; a princípio, com segurança realizam-se pesquisas, exploram-se conteúdos, acessam-se sites de relacionamentos a trabalho, entre outras tantas atividades que a internet oferece (MITNICK; KEVIN, 2006).

O aumento de uso da internet e de suas facilidades pelas empresas é uma prática constante que traz benefícios para o desempenho de suas atividades diárias, em que se destacam o acesso imediato a informação e a rapidez na comunicação e umas dessas facilidades que se destaca é a utilização do e-mail e navegação da internet, mais com a utilização inadequada dessas facilidades pode-se deixar as organizações vulneráveis (SHEMA, 2003).

Organizações com acesso corporativo a internet sempre se vem com situações de riscos pela falta de limites nos percursos web. O uso da Internet e de suas facilidades para

esses fins pode gerar significativo impacto sobre os negócios e a reputação das empresas, com reflexo direto sobre os clientes e os resultados financeiros (SHEMA, 2003).

Adicionalmente, a utilização indevida ou inadequada da Internet e de suas facilidades poder trazer problemas jurídicos para as empresas. Aos usuários que possuem computadores em sua residência podemos dizer que correm riscos ainda maiores. Encontram-se vários tipos de vírus, nenhum computador está a salvo do novo método de ameaça de vírus que são *softwares* maliciosos com objetivo de destruir ou obter informação (STARLINGS, 2003).

As grandes organizações estão trabalhando muito para tornar o acesso à internet mais segura, mais esse termo não existe 100% de segurança, o que existe é a possibilidade de aumentar a segurança contratando profissionais capacitados e investindo na segurança (STARLINGS, 2003).

3 OS CRIMES VIRTUAIS

Em primeiro momento, é fundamental ter conhecimento da diferença entre hackers e cracker. Hacker possui um conhecimento avançado em computação e internet, utilizado este conhecimento em favor da justiça, trabalhando juntamente com a polícia no combate dessa rede de criminosos virtuais. Já os crackers, estes sim são as pessoas com responsabilidade pelos crimes com prática na rede partindo da internet. Os repórteres de emissoras de televisão noticiam estes fatos errados, pontuam que o hacker é o causador do dano, assim fica como se o hacker fosse a pessoa malvada da história (VIANA; MACHADO, 2013).

Com a grande disseminação dos computadores e do acesso à internet, acabaram surgindo crimes e criminosos com especialização na linguagem da informática, com proliferação por todo o mundo. Esses crimes são denominados crimes virtuais, digitais, informáticos, telemáticos, dentre outros (CRUZ; RODRIGUES, 2018).

Para definição do crime virtual, apresenta-se alguns conceitos de grandes estudiosos.

Damásio e Milagre (2016, p. 48) explicam que “crime informático é um fenômeno inerente às transformações tecnológicas que a sociedade experimenta e que influenciaram diretamente no direito penal”. Logo, considera-se, neste estudo, crime virtual ou informático, aquele perpetrado por via eletrônica seja por invasão através de rede ou extração de dados de equipamentos telemáticos ou fonográficos sem autorização ou consentimento da vítima.

Para Vicente Greco Filho (2000), os crimes virtuais se subdividem em condutas criminosas que utilizam a rede mundial de computadores como um meio, para a prática desses crimes e os atos ilícitos que atentam contra a Internet, como um bem jurídico:

> Focalizando-se a Internet, há dois pontos de vista a considerar: crimes ou ações que merecem incriminação praticados por meio da internet e crimes ou ações que merecem incriminação praticados contra a Internet, enquanto bem jurídico autônomo. Quanto ao primeiro, cabe observar que os tipos penais, no que concerne à sua estrutura, podem ser crimes de resultado de conduta livre, crimes de resultado de conduta vinculada, crimes de mera conduta ou formais (sem querer discutir se existe distinção entre estes) e crimes de conduta com fim específico, sem prejuízo da inclusão eventual de elementos normativos. Nos crimes de resultado de conduta livre, à lei importa apenas o evento modificador da natureza, com, por exemplo, o homicídio. O crime, no caso, é provocador o resultado morte, qualquer que tenha sido o meio ou a ação que o causou. (GRECO FILHO, 2000, p. 95).

Para Colli (2010), os crimes cometidos nesse ambiente possuem caracterização pela falta física de agente ativo, por esse motivo, acabaram ficando de forma usual com definição como crimes virtuais, isto é, os delitos com prática partindo da internet possuem denominação de crimes virtuais, por causa da falta física dos seus autores e asseclas.

Para Viana e Machado (2014), a conceituação de delito informático pode ter tralhado como uma conduta típica e ilícita, que constitui crime ou contravenção, doloso ou de culpa, comissiva ou de omissão, por prática por pessoa física ou jurídica, com a utilização da informática no ambiente de rede ou fora dele, ofendendo de forma direita ou não a segurança informática, que possui por elementos a integridade, a disponibilidade e a confidencialidade.

Os chamados delitos informáticos, de acordo com Viana e Machado (2014), abordam crimes e contravenções penais, o que alcança não apenas as condutas com prática no contexto da internet, mas total conduta na qual existe relacionamento com sistemas informáticos. Isto é, uma fraude na qual o computador tem utilização como ferramenta de crime, fora da internet, também seria alcançada pelo que teve denominação delitos informáticos. Mas, delito informático é gênero, de onde delito telemático é espécie, dada a peculiaridade de ocorrência no e partindo inter-relacionamento perante os computadores em rede telemática utilizados na prática delitiva.

Cruz e Rodrigues (2018) faz apresentação de um conceito bem amplo da criminalidade informática, pontuando que tem conhecimento por criminalidade informática o recente fenômeno histórico-sócio-cultural com caracterização devido à alta incidência dos ilícitos penais, que possuem como objeto material ou meio de execução o objeto tecnológico informático.

Já Cassanti (2014) faz descrição do crime informático como um ato de lesão cometido partindo de um computador ou de um periférico na intenção de obtenção de uma vantagem indevida.

Segundo o autor, crimes ou ação praticados por meio da internet ou contra a internet merecem ser observados e distinguidos para não haver aplicação de sanções majoradas ou diminuídas quando imputadas ao agente causador do ilícito penal.

De acordo com Santaella (2013) e Moreira (2009), a nanotecnologia empregada em certos dispositivos informáticos reduz cada vez mais o seu tamanho, tornando-os cada vez mais portáteis e fáceis de utilizar em qualquer ambiente; com isso, facilitando o acesso a redes de internet, muitas vezes não seguras, aumentando os riscos de ataques cibernéticos. Com isso, o objeto que veio para nos auxiliar, tornar o nosso dia a dia mais simplificado, acaba significativamente, trazendo problemas imensuráveis para a vida das pessoas.

4 CARACTERÍSTICAS E CLASSIFICAÇÃO DOS CRIMES VIRTUAIS

Os crimes de informática são aqueles perpetrados através dos computadores, contra eles, ou através deles. A maioria dos crimes praticados através da internet é por meio de computador ou similares conectados a grande rede (JESUS; MILAGRE, 2016).

Leonardi (2012) e Soares (2012) evidenciam que os crimes digitais podem ser conceituados como as condutas de acesso não autorizado a sistemas informáticos ou não, ações destrutivas nesses sistemas, a interceptação de comunicações, modificações de dados, infrações a direito autorais, incitação ao ódio e discriminação, escárnio religioso, divulgação de pornografia infantil, terrorismo, entre outros.

As denominações quanto aos crimes praticados em ambiente virtual são diversas, não há um consenso sobre a melhor denominação para os delitos que se relacionam com a tecnologia, crimes de computação, delitos de informática, abuso de computador, fraude informática, enfim, os conceitos ainda não abarcam todos os crimes ligados à tecnologia, e, portanto, deve-se ficar atento quando se conceitua determinado crime, tendo em vista que existem muitas situações complexas no ambiente virtual, até porque o Código Penal Brasileiro só tipifica dois crimes virtuais que são invasão de dispositivos informáticos e interrupção de serviço telemático, os demais são considerados crimes comuns cometidos com auxílio da web (LEONARDI, 202).

Entende-se que as denominações dos delitos devem ser feitas de acordo com o bem jurídico protegido, conforme diz Leonardi (2012), o autor deixa claro que somente através da ação humana é que é possível o acometimento de crime.

Ao analisar um crime como sendo de informática, faz-se necessária uma análise inicial, primeiramente, para verificar se é um cybercrime ou não, depois aplicar o tipo penal correspondente, tendo em vista o bem jurídico tutelado, que é a prática de delitos cometida através da internet que pode ser enquadrada no Código Penal Brasileiro (SANCHES E ANGELO, 2017).

Tratando-se de crime de invasão de dispositivo informático como delito permanente, o art. 158 do Código de Processo Penal evidencia e explicita sua formatação, não obstante, esclarece que realmente é: "[...] indispensável o exame de corpo de delito, direto ou indireto, não podendo suprimi-lo a confissão do acusado".

Mediante representação da vítima, instaura-se inquérito policial para averiguação dos fatos narrados. Havendo provas concretas e, após identificação do autor do delito, procede-se representação em juízo para punições cabíveis (SANCHES; ANGELO, 2017).

5 APLICAÇÃO DO DIREITO PENAL AOS CRIMES VIRTUAIS

As expansões das novas tecnologias fizeram ganhar importância a criação de legislação relacionada em coibir os atos ilícitos com prática partindo do meio virtual. Essa legislação não é bem vista por diversos, por ter representação como acúmulo sem utilidade à tipificação penal. Entretanto, foi percebido que havia a necessidade de atualização da norma penal para que os crimes virtuais não fugissem do controle (OLIVEIRA, 2013).

Na falta de legislações específicas para esses crimes, os tribunais do país enfrentam e punem internautas que fazem o uso da internet como instrumento da prática de crimes. A maior parte dos magistrados considera que aproximadamente 95% dos delitos cometidos de forma eletrônica já possuem tipificação no Código Penal, por caracterizar crimes comuns com prática partindo da internet (OLIVEIRA et al. 2017).

Para esses 5%, a internet não é uma área nova de atuação, mas somente um novo caminho para realizar delitos já com prática no mundo real e basta somente que as leis tenham adaptação para os crimes virtuais. E é isso que a justiça vem fazendo, adaptando e empregando diversos dispositivos no Código Penal para combater o crime digital (OLIVEIRA et al. 2017).

A listagem é enorme: insultar a honra de uma pessoa; espalhar boatos na internet sobre pessoas; insultar pessoas levando em consideração suas características ou fazer a utilização de apelidos grosseiros; fazer a ameaça a alguém; fazer o uso de dados da conta bancária de outra pessoa para desviar ou sacar dinheiro; fazer comentários em chats, e-mails e outros de maneira negativa acerca de raças, religiões e etnias; realizar o envio, troca de fotos de crianças nuas (LIMA, 2014).

Em relação a legislações em especificidade, as que possuem mais aplicação são: utilizar logomarca da empresa sem autorização do titular, no todo ou em parte, ou imitá-la de maneira que seja possível a indução à confusão (crime contra a propriedade industrial art. 195 da Lei nº 9279/1996), monitoração sem aviso de forma prévia (interceptação de comunicações de informática art. 10 da Lei nº 9.296/1996) e fazer o uso de cópia de software sem licença (crimes contra software pirataria art. 12 da Lei nº 9.609/1998) (OLIVEIRA et al. 2017).

O Supremo Tribunal de Justiça (STJ), como guardião e agente de uniformização da legislação infraconstitucional, vem fazendo a consolidação da aplicação desses dispositivos em vários julgados. Nos casos voltados a pedofilia, por exemplo, o STJ já acabou firmando o entendimento que esses crimes e a divulgação de pornografia infantil partindo da internet possuem descrição no art. 241 da Lei nº 8.069/1990, e com previsão em convenção internacional da qual o país é signatário. Além do mais, a corte chegou à conclusão, por si só, que enviar fotos de pornografia partindo da internet já é constituinte de crime. Baseado no art. 241 do Estatuto da Criança e do Adolescente (ECA), os ministros da 5ª Turma do STJ acabaram cassando um habeas-corpus com concessão partindo do Tribunal de Justiça do Estado do Rio de Janeiro (TJ-RJ), que fazia a determinação do trancamento de uma ação penal perante argumentação de que o ECA faria a definição como crime somente a "publicação" e não apenas "divulgação" de imagens de sexo explícito ou pornografias de crianças ou adolescentes (FERREIRA, 2005).

No ano de 2011, uma onda de ataques de crackers a sites oficiais do governo e empresas públicas fizeram diversos sites ficar fora do ar de forma temporário. Esse acontecimento realizou influências para a criação da Lei 12.737/2012.

De acordo com Wendt e Jorge (2012), esse tipo de ação poderá possuir conotações de emulação, apresentando destaque ao grupo a que pertence, ou de ciberativista, no objetivo de defesa de convicções religiosas, filosóficas ou políticas.

Independentemente das conotações, fato é de que essas ações delitivas reinflamaram as discussões sobre a necessidade de imposição de limites penais às condutas com prática pelo

ambiente virtual. Nesse contexto, o PL 84/1999 (Lei 12.737/2012) teve denominação de AI-5 digital pela acusação de promoção da censura e obrigação de reter logs ou IP's (endereço do computador na internet) por 3 anos pelos provedores. Por oportuno, um projeto de lei opcional acabou sendo trazido pela bancada governista, a saber, o PL 2.793/2011, no intuito da não criminalização do acesso à internet (OLIVEIRA, 2013).

Entretanto, o que acabou determinando a aprovação desses institutos foi a publicação das fotos íntimas da atriz Carolina Dieckmann. De acordo com Oliveira (2013) e Sanches e Angelo (2017), a conta de e-mail da vítima foi hackeada, de maneira que os invasores tiveram acesso aos seus dados. As imagens tiveram publicação nos sites de pornografia. A atriz, bem como na Lei Maria da Penha, acabou cedendo seu nome à lei nº 12.737/2012, trazendo modificações ao Código Penal do país, ordenando sobre a tipificação criminal dos crimes informáticos (SANCHES E ANGELO, 2017).

A Lei Carolina Dieckman acabou trazendo modificações no Código Penal, fazendo o acréscimo dos arts. 154-A e 154-B, originando o tipo penal "Invasão de dispositivo informático". O bem jurídico, com amparo por esses artigos, é a inviolabilidade dos dados informáticos. É buscada a preservação da privacidade e da intimidade, constadas no art. 5º da Constituição. O sujeito ativo é qualquer pessoa que não tem licença para acessar as informações. Já o passivo é qualquer indivíduo, podendo esse ser físico ou jurídico, proprietário dos dados computacionais (SANCHES E ANGELO, 2017).

A Lei 12.735/2012, de forma inicial, com projeção para ser extravagante, teve alteração somente para modificar os diplomas legais que já existiam. É possuinte da seguinte emenda: "Altera o Decreto-Lei nº 2.848/1940 - Código Penal, o Decreto-Lei nº 1.001/1969 - Código Penal Militar, e a Lei nº 7.715/1989, para tipificação das condutas com realização partindo utilização de sistema eletrônico, digital ou similares, que tenham prática contra sistemas informatizados e similares; e dá outras providências" (BRASIL, 2012, on-line).

Segundo Oliveira (2013), a criação dessa normativa possui como grande influência a impossibilidade de proteger bens da vida, maculados pelos crimes virtuais, partindo de uma legislação dos anos 40, ano da criação do Código Penal.

Por conseguinte, a Lei 12.737/2012 acabou trazendo a mesma ideia da Lei 12.735, isso é, a legislação penal que já existia teria suficiência para o combate dos crimes virtuais. Traz a seguinte ementa: "Dispõe acerca da tipificação criminal de delitos informáticos; modifica o decreto-lei nº 2.838/1940 - Código Penal; e dá outras providências" (BRASIL, 2012, on-line).

Entretanto, uma das grades críticas sobre a Lei 12.735/2012 apresenta-se no sujeito ativo, sendo que é atípica a conduta do indivíduo que faz a invasão do aparelho computacional próprio para a obtenção de dados de outrem que lá estejam, por exemplo, numa Lan House, o proprietário não cometerá crime caso acesse as informações do locador do computador. Com isso, existe uma falha na lei, sendo que, quem cometeu o crime precisa ter punição, não devendo importar quem que o praticou. Uma outra lacuna é encontrada nos mecanismos de segurança, sendo que um usuário sem experiência que não faz a utilização de aparatos de segurança, como é caso do antivírus ou senhas de acesso, não terá amparos pelos artigos, sendo o crime atípico (SANCHES; ANGELO, 2017).

Num outro caso, a Turma acabou mantendo a condenação de um publicitário que teve participação e filmou cenas eróticas que envolviam crianças e adolescentes. Ele teve denúncia pelo Ministério Público de Rondônia, baseado no art. 241 do ECA, nos arts. 71 e 29 do Código Penal e por corrupção de menores (Lei nº 2.252/1954: é constituinte crime, com punição com pena de reclusão de 1 a 4 anos e multa, corromper ou facilitar a corrupção de indivíduo menor de 18 anos, com ela praticando, infração penal ou induzindo-a a fazer sua prática) (SANCHES; ANGELO, 2018).

Casos relacionados a furto e estelionato virtual também já tiveram enquadramento pela Corte. A 3ª Seção do STJ acabou consolidando o entendimento de que, a apropriação dos valores de conta corrente partindo de transferência bancária com fraude utilizando a internet sem consentimento do correntista tem configuração de furto qualificado por fraude, sendo que, nesses casos, a fraude tem utilização para burlar o sistema de proteção e vigilância do banco perante os valores com mantimento em sua guarda. Também chegou a decisão de que a competência para julgamento deste tipo de crime é do juízo do local da consumação do delito de furto, que é dado no local onde o bem tem subtração da vítima (MAUES et al. 2018).

Numa outra decisão, relatada pelo ministro Felix Fischer, a 5ª Turma do STJ fez definição de forma clara que, mesmo em ambiente virtuais, o furto subtrai para si ou para outro, coisa alheia móvel (art. 155 do Código Penal) partindo de fraude não tem confusão com o estelionato, obter para si ou para outro vantagem ilícita, em prejuízo alheio, com indução ou manter alguém em erro, partindo de artifício, ardil, ou outra forma fraudulenta (art. 171 do Código Penal), sendo que, no furto, a fraude tem utilização para burlar a vigilância da vítima, e, no estelionato, o intuito é a obtenção de consentimento da vítima e iludi-la para que entregue de forma voluntária o bem (SANCHES; ANGELO, 2018).

Numa ação com envolvência, os determinados crimes contra a honra com prática partindo da internet, o desembargador Carlos Fernando Mathias de Souza acabou mantendo a decisão da Justiça do estado do Rio Grande do Sul que fez a condenação de um indivíduo ao pagamento à ex-namorada de indenização por danos morais com o valor de R$ 30 mil, por ter feito a divulgação pela internet de mensagens chamando-a de garota de programa. No caso, a moça fez alegações de que, depois das falsas publicações de e-mails que continham seus dados pessoais juntamente a uma fotografia de mulher em posições eróticas, ficou constrangida ao receber diversos convites para programas sexuais (MAUES et al., 2018).

Ainda relacionado com esses crimes, a 4ª Turma do STJ acabou determinado que o site Yahoo! Brasil fizesse a retirada do ar as páginas com conteúdos inverídicos acerca de uma mulher que ofertava programas sexuais. A empresa fez alegações de que o presente site teve criação partindo de um usuário com o uso de um serviço com oferta pela controladoria americana Yahoo Inc, assim, caberia a essa empresa cumprir a determinação judicial. O ministro Fernando Gonçalves fez sustentação de que a Yahoo! Brasil é pertencente ao mesmo grupo econômico e tem apresentação aos consumidores fazendo o uso do mesmo logotipo da empresa americana e o acesso ao endereço trazido nos motivos do recurso como Yahoo! Inc, é aberto, sendo, na verdade, a página do Yahoo! Brasil. Com isso, chegou à conclusão de que, o consumidor não faz a distinção, de forma nítida, das divisas perante as duas empresas (MAUES et al. 2018).

A 3ª Turma chegou a decisão de que ações indenizatórias por danos morais poderão ter ajuizamento em nome do proprietário da organização vitimada de mensagens de difamação em comunidades do site de relacionamentos Orkut. O tribunal levou em consideração legítima a ação com proposição partindo de um empresário do estado de Minas Gerais contra dois indivíduos que difamaram seu negócio de criar avestruzes, causando-lhe diversos prejuízos. De acordo com a ministra Nancy Andrighi, as mensagens com divulgação não foram apenas consideradas ofensivas ao empresário e seu filho, mas também ao seu comércio de aves (SANCHES E ANGELO, 2018).

Fazendo a aplicação das disposições do Código Penal, o STJ vem fazendo a negação de habeas-corpus para aqueles que possuem acusação e condenação por várias modalidades de crimes eletrônicos. Dentre diversos casos com julgamento, a Corte acabou mantendo a prisão do cracker Otávio Oliveira Bandetini, com condenação a dez anos e onze meses de reclusão pela retirada de forma irregular aproximadamente R$ 2 milhões de contas bancários de terceiros partindo da internet; fez negação do relaxamento da prisão preventiva de um

tatuador com denúncia pela divulgação de fotos de pornografia de crianças e de adolescentes na internet; de uma pessoa acusada presa em operação que envolvia a Polícia Federal pela participação de um esquema para furtar contas bancárias; de um cracker que foi preso por furtar mediante fraude, formar quadrilha, violar sigilo bancários e interceptação telemática ilegal; e de um técnico em informática de Santa Catarina com acusação a manipulação de e-mail para a incriminação dos colegas de trabalho (MAUES et al. 2018).

O Tribunal também acabou enfrentando questões relacionadas com a falta de fronteiras físicas no determinado ciberespaço, no entendimento de que, caso o crime possuísse efeitos em âmbito nacional, seria preciso fazer a aplicação da lei do Brasil. Em um caso, uma pessoa acusada de pedofilia fez alegações de que as fotos pornográficas que envolviam crianças e adolescentes tinham sido obtidas no sítio da internet do Kazaa, um software internacional para armazenar e compartilhar arquivos eletrônicos com sede fora do país e que, por isso, a justiça brasileira não seria a competente. A Corte teve entendimento de que como o resultado e a execução tiveram ocorrência em âmbito nacional, o fato dos arquivos terem tido obtenção no Kazaa, teria irrelevância para a ação (MAUES et al. 2018).

É inegável que o advento da Internet impactou diretamente a maneira em que ocorrem as relações sociais no mundo moderno. Como consequência disso, vimos surgir implicações na esfera do Direito. Foi então constatada a necessidade de se criar um instrumento legislativo, no ordenamento jurídico brasileiro, específico para regular os conflitos ocorridos no ambiente digital pertinentes aos assuntos que interessam as ciências jurídicas. Necessidade essa que tange várias disciplinas encontradas nas subdivisões do estudo do Direito como direito penal, civil, consumerista e constitucional (LEAL, 2015).

São exemplos dessa diversidade de assuntos relevantes as interações na internet temas como a responsabilidade, tanto civil como penal, dos usuários e provedores, proteção e segurança nas relações de consumo, exercícios da liberdade de expressão e direito de informação.

De Lucca et al. (2015) utilizam, na sua obra, de dados e números levantados por pesquisas do governo brasileiro para ressaltar a importância do tema. Segundo dados levantados na Pesquisa Nacional por Amostra de Domicílios (PNAD), que foi promovida pelo Instituto Brasileiro de Geografia e Estatística (IBGE), o Brasil possuía sessenta e oito milhões de usuários conectados na internet no ano de 2009, ano que a lei do Marco Civil teve seu projeto apresentado na Câmara dos Deputados.

Outra pesquisa recente revelou que o Brasil é quarto pais do mundo em número de usuários de internet em 2017, ficando atrás apenas de Estados Unidos, Índia e China. Segundo dados da União Internacional de Telecomunicações (UIT), o país tem 59% de usuários conectados, totalizando o número de aproximadamente cento e vinte milhões de brasileiros que se utilizam desse meio de comunicação e interação (REVISTA EXAME, 2017).

O autor Paulo De Lucca et al. (2015) usam o conceito de "Era da Imagem", referindo-se aos meios de comunicação da sociedade moderna, dizendo que esses são meios de alta potência, invasivos e com destinatários que integram uma sociedade massificada, a qual perdeu a capacidade de abstração e reflexão, estando assim fragilizada por consequência. Situação que torna imperiosa a necessidade da normatização desses meios por parte do Estado, principalmente da internet e de seus efeitos no âmbito individual.

A Origem do texto de lei se deu em um debate público ocorrido no ano de 2009, promovido pelo Ministério da Justiça, juntamente com o Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas. Foram recebidas contribuições da comunidade civil organizada, do setor empresarial, acadêmicos, técnicos especialistas e também de cidadãos comuns engajados a participar da discussão.

De Lucca et al. (2015) citam que justamente por essa participação tão ampla de vários setores da sociedade é que o anteprojeto de Lei foi tão inovador em comparação ao processo legislativo tradicional no Brasil. A colaboração entre governo e sociedade visou buscar a elaboração de um sistema de dispositivos legais que atendesse as demandas que o ambiente digital parecia necessitar.

Leal (2015) cita também que um dos motivos que colocaram o tema em evidência no legislativo brasileiro foi um evento ocorrido em 2013, que foi a revelação de que o governo brasileiro teria sido vítima de espionagem do serviço de inteligência americano, fazendo assim com que as autoridades brasileiras passassem a tratar o assunto com mais relevância, colocando como urgente a necessidade e a criação de dispositivos legais que versassem a respeito do ambiente digital.

Havia também, na época, conforme o site da Câmara Legislativa, um projeto de lei, de autoria do deputado Eduardo Azeredo, que tinha por finalidade criar um rol de condutas específicas na internet sujeitas a sansões penais.

Segundo Leal (2015), esse momento foi crucial para o surgimento do Marco Civil. Cita o autor que a ideia formulada a época, em 2007, era de que o Brasil precisava, na

verdade, de um Marco Regulatório, e não de uma lei criminal; assim, primeiramente deveriam ser assegurados os direitos fundamentais dentro da rede, através de uma lei civil.

Assim, após uma consulta pública de duas fases, teve ingresso no Congresso Nacional no ano de 2011, o Projeto de Lei nº 2.126/2011. Sua aprovação na Câmara dos Deputados ocorreu em 25 de março de 2014 e no Senado em 22 de abril de 2014. Após 3 anos do início do projeto de lei, em 23 de abril de 2014, foi sancionada pela presidente Dilma Rousseff em 23 de abril de 2014 e publicada no Diário Oficial no dia seguinte a Lei nº 12.965/14, conhecida como o Marco Civil da Internet Brasileira.

Não sendo unanimidade dentro do meio jurídico, foram e são feitas várias críticas até hoje a respeito do Marco Civil da Internet. Alguns autores defendem que era desnecessário e não trouxe inovação para o ordenamento jurídico nacional no sentido prático, além de não ter sido efetivo em encerrar o debate sobre a regulamentação das interações na internet.

É justo também dizer que, possivelmente, a legislação sempre estará defasada em relação ao surgimento de novas tecnologias, tendo em vista a velocidade que essas duas áreas evoluem. Sendo assim, sempre haverá um campo em que o direito deverá avançar quando se tratar de novos métodos de interação social ou avanço tecnológico.

Dito isso, deve-se também atentar que é fato que a Lei nº 12.965/14 trouxe um rol de dispositivos legais que tem profundo impacto nas relações virtuais e no âmbito do Direito Digital brasileiro. A partir de sua vigência, foi delimitada uma série de direitos e deveres referentes a usuários e prestadores de serviços que atuam no ambiente virtual, sendo que, agora, passam a estar sob jurisdição de legislação específica.

A promulgação do Marco Civil da Internet pode ser estabelecida como um grande avanço na postura governamental em busca da regulamentação dos atos da sociedade civil praticados no meio digital. O estabelecimento de direitos e deveres cibernéticos foram tardios, porque levou-se anos para que o Estado reagisse e desse os primeiros passos para normatizar e tipificar tais delitos. É importante conhecer para poder combater dos crimes virtuais, uma vez que, através dessas normas, poderá ser vislumbrado com mais facilidade, o que está sendo violado, estabelecendo assim as condutas ilícitas (SOUZA, 2019).

Dessa forma, há relação deste texto normativo com o direito penal, haja vista que, ao se buscar a proteção dos dados pessoais e cadastrais no meio digital, está automaticamente dificultando a prática de crimes, como, por exemplo, a obtenção e a transferência ilegal de dados. Uma inovação considerável também trazida pelo Marco Civil é a responsabilização

civil, administrativa e criminal dos provedores de Internet, as quais são independentes e cumulativas (SOUZA, 2019).

Há também a previsão da obrigatoriedade de os provedores estabelecerem políticas de adequação, objetivando a proteção dos dados pessoais dos usuários, a liberdade de expressão, a neutralidade da rede e ao cumprimento de determinações dos órgãos estatais (MACHADO, 2014).

A Leis 12.735 e 12.737 tiveram o intuito do preenchimento das lacunas legislativas que impediam tipificar os atos ilícitos com prática pelos meios digitais. Com isso, foi desejado cumprir os princípios norteadores do Direito Penal, o da legalidade e proibição da analogia. Possuíram como foco a proteção da informação. Entretanto, é preciso a criação de mecanismos em especificidade para combater os crimes virtuais. O mundo virtual ainda percebe um vazio de normas, contribuindo para a falta de punição estatal.

6 CONCLUSÃO

Como foi possível ver, a facilidade para acessar a internet, o número de usufruidores do ambiente web tem crescimento de maneira intensiva, consequentemente, as mesmas proporções possuem surgimento aos cybercrimes.

Dentre os crimes que possuem ocorrência com maior frequência no Brasil, apresentam-se os crimes contra a honra, a divulgação de fotos sem autorização e a pedofilia e a pornografia infantil. As pessoas responsáveis por cometerem esses atos ilícitos não acabam sendo responsabilizados a proporção das suas condutas. Os sujeitos passivos que acabam sofrendo consequência além da área virtual, diversas vezes, atingem sua vida íntima, trazendo complicações que podem perdurar por longo tempo.

O Código Penal do país faz a tipificação de várias atuações que possuem enquadramento no ambiente web; entretanto, possui penas brandas e sem suficiência para a coibição da prática desses atos. Existe também a lei Carolina Dickman, que alterou o Código Penal, inserindo artigos em seu corpo. Mas, mesmo da especificação das condutas com prática na web, acaba trazendo dúbias interpretações e punições plácidas para os criminosos. Com isso, a ausência de uma legislação em especificidade ao cybercrime faz a intensificação da ideia de que a internet é uma terra sem lei.

Por fim, é fundamental produzir uma legislação que venha a versar acerca dos crimes cometidos na internet, sendo que esses crimes são comuns e trazem para suas vítimas

prejuízos reais. A punição proporcional é uma maneira de fazer o controle da prática desses delitos, sendo que, ao ter conhecimento que poderá responder de maneira penosa, o cracker, ou ainda um indivíduo comum, acabará se policiando em seus atos. Com isso, tendo conhecimento dos resultados advindos dos crimes virtuais, é preciso fazer a criação de uma lei que não mais permita que a internet tenha utilização de maneira que prejudique seus usuários.

7 REFERÊNCIAS

BRASIL. **Lei 12.735 de 30 de novembro de 2012**. 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. Disponível em: <http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2012/Lei/L12735.htm> Acesso em: 08 Jan. 2021.

BRASIL. **Lei 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 desembro de 1940 - Código** Penal; e dá outras providências. Disponível em: <http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2012/Lei/L12737.htm> Acesso em: 09 Jan. 2021.

CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas reais**. Rio de Janeiro: Brasport, 2014.

COLLI, Maciel. **Cibercrimes:** Limites e Perspectivas à Investigação Policial de Crimes Cibernéticos. Curitiba: Juruá Editora, 2010.

CRUZ, Diego; RODRIGUES, Juliana. Crimes cibernéticos e a falsa sensação de impunidade. **Revista Científica Eletrônica do Curso de Direito**, 13. ed., Janeiro, 2018.

DAMÁSIO, José Antonio. **Manual de Crimes Informáticos**. São Paulo: Saraiva, 2016.

DE LUCCA, Newton. In: DE LUCCA, Newton; SIMÃO, Adalberto; LIMA, Cíntia Rosa Pereira de (coords). **Direito & Internet III –** Marco Civil da Internet (Lei n. 12.965/2014). Tomo I. .São Paulo: Quartier Latin, 2015.

FERREIRA, Ivette Senise. **Direito e internet**: Aspectos Jurídicos Relevantes. 2d. São Paulo: Quartier Latin, 2005.

GRECO, Vicente Filho. **Algumas observações sobre o direito penal e a internet**. Boletim IBCCRIM, v. 8, p. 3, 2000.

JESUS, Damásio de. MILAGRE, José Antonio. **Manual de Crimes Informáticos**. São Paulo: Saraiva, 2016.

LEAL, Luziane de Figueiredo Simão. **Crimes Contra os Direitos de Personalidade Na Internet – Violações e Reparações de Direitos Fundamentais nas Redes Sociais**. Curitiba: Editora Juruá, 2015.

LEONARDI, Marcel. **Tutela e Privacidade na Internet**. São Paulo: Saraiva, 2012.

LIMA, Simão Prado. 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, Felipe. **Marco Civil traz efeitos na apuração criminal, mas pode invadir privacidade**. Disponível em: <https://www.conjur.com.br/2014-jul-14/felipe-machado-marco-civil-traz-efeitos-apuracao-criminal> Acesso em: 06 Jan. 2021.

MAUES, G. B. K.; DUARTE, K. C.; CARDOSO, W. R. S. **Crimes virtuais: uma análise sobre a adequação da legislação penal brasileira**. Revista Científica da FASETE, 2018.

MITNICK, A. D., KEVIN, J. Q. **A Arte de Enganar: Ataques de Hackers:** Controlando o Fator Humano na Segurança da Informação. São Paulo: Pearson Education do Brasil, 2006.

MOREIRA, Danilo dos Reis; Dias, Márcio de Souza. **Web 2.0 – a web social**. Artigo publicado na Revista CEPPG – Nº 20 – 1 – ISSN 1517-8471 – Páginas 196 à 208. 2009.

OLIVEIRA, B. M.; MATTOS, K. R.; SIQUEIRA, M. S. **Crimes virtuais e a legislação brasileira**. (Re)ensando Direito. Ano 7, n. 13, jan./jun., 2017, p. 119-130.

OLIVEIRA, J. C. **O cibercrime e as lei 12.735 e 12.737/2012**. São Cristóvão, 2013.

PINHEIRO, Patrícia Peck. **Direito Digital**. 4. ed. Revista, atualizada e ampliada. São Paulo: Saraiva, 2º tiragem 2011.

REVISTA EXAME. **Brasil é o 4º país em número de usuários de internet**. 2017. Disponível em:: <HTTPS://EXAME.ABRIL.COM.BR/TECNOLOGIA/BRASIL-E-O-4O-PAIS-EM-NUMERO-DE-USUARIOS-DE-INTERNET/>. Acesso em: 03 jan. 2021.

ROSA, Fabrízio. **Crimes de Informática**. Campinas: Bookseller, 2012.

RUIZ, J. A. **Metodologia científica:** guia para eficiência nos estudos. São Paulo (SP): Atlas; 1992.

SANCHES, A. G.; ANGELO, A. E. **Insuficiência das leis em relação aos crimes cibernéticos no Brasil**. Disponível em: <https://jus.com.br/artigos/66527/insuficiencia-das-leis-em-relacao-aos-crimes-ciberneticos-no-brasil/1> Acesso em: 03 jan. 2021.

SANTAELLA, L. **Comunicação ubíqua:** repercussões na cultura e na educação. São Paulo: Paulus, 2013.

SHEMA, M. Hack notes: **Segurança na Web:** referência rápida. Rio de janeiro: Campus, 2003. 182 p

SOARES, Murilo Cesar. **Os Direitos Na Esfera Pública Mediática:** a Imprensa como instrumento da Cidadania. São Paulo: Cultura Acadêmica, 2012.

SOUZA, Ludimila de Freitas. **Marco civil da internet e os crimes virtuais**. Conteúdo Jurídico, Brasília-DF. Disponível em: https://conteudojuridico.com.br/consulta/artigos/51965/marco-civil-da-internet-e-os-crimes-virtuais. Acesso em: 05 Jan. 2021.

STALLINGS, w. **Network Security Essentials:** applications and standards. EUA: Makron Books, 2003. 436 p.

VIANA, Tulio; MACHADO, Felipe. **Crimes informáticos**. Belo Horizonte: Fórum, 2013.

WENDT, E.; JORGE, H. V. N. **Crimes cibernéticos**. São Paulo: Brasport, 2012.