A TIPIFICAÇÃO DAS CONDUTAS PRATICADAS EM AMBIENTE VIRTUAL

THE TYPIFICATION OF CONDUCTS PRACTICED IN A VIRTUAL ENVIRONMENT

Fernanda Bílio da Silva
Lizandro Poletto

RESUMO: As novas tecnologias mudaram as formas de manejo de diversas áreas de conhecimento e também aumentou as formas como os criminosos agem para tirar proveito de suas vítimas. No meio cibernético, muitas pessoas acreditam que podem fazer o de tudo sem nunca serem encontrados e muito menos punidos. Porém, isso vem mudando nos últimos anos, e foram criadas leis, para que, dessa forma, fosse possível tipificar os crimes cibernéticos, com a identificação do autor e a sua consequente punição. Dessa forma, surge o seguinte questionamento: Com a omissão por parte da legislação, até quando isso contribui para o aumento dos crimes cibernéticos, e quais as medidas vêm sendo tomadas, por parte do poder legislativo para sanar essas omissões? Para responder tal problema tem-se o seguinte objetivo geral analisar como se da, a tipificação dos crimes cibernéticos e os objetivos específicos são conceituar crimes cibernéticos; localizar o responsável pela conduta criminosa, e a aplicabilidade da lei para essas ações tipificadas no código penal; apontar as dificuldades de identificar os criminosos da *internet*. A metodologia utilizada foi à pesquisa qualitativa, pois será feita uma análise das experiências dos indivíduos a respeito da tipificação dos crimes cibernéticos, por esse motivo também será feito uma pesquisa bibliográfica, doutrinária e jurisprudencial a respeito do tema.

PALAVRAS-CHAVE: Crimes Cibernéticos; Tecnologia; Direito Penal.

ABSTRACT: New technologies have changed the ways in which different areas of knowledge are managed and have also increased the ways in which criminals act to take advantage of their victims. In the cyber environment, many people believe they can do anything without ever being found, let alone punished. However, this has been changing in recent years, and laws were created, so that, in this way, it was possible to typify cybercrimes, with the identification of the author and his consequent punishment. Thus, the following question arises: With the omission on the part of the legislation, how long does this contribute to the increase in cybercrimes, and what measures have been taken by the legislature to remedy these omissions? To answer this problem, the following general objective is to analyze how cybercrimes are classified and the specific objectives are to conceptualize cybercrimes; locating the person responsible for the criminal conduct, and the applicability of the law to those crimes; point out the difficulties of identifying internet criminals. The methodology used was qualitative research, as an analysis of the experiences of individuals will be made regarding the typification of cybercrimes, for this reason a bibliographical, doctrinal and jurisprudential research will also be carried out on the subject.

KEYWORDS: Cyber-Crimes, Technology, Criminal Law.

1 INTRODUÇÃO

As novas tecnologias mudaram as formas de manejo de diversas áreas de conhecimento e também aumentou as formas como os criminosos agem para tirar proveito de suas vítimas. No meio cibernético, muitas pessoas acreditam que podem fazer o de tudo sem nunca serem encontrados e muito menos punidos. Porém, isso vem mudando nos últimos anos, e foram criadas leis, para que, dessa forma, fosse possível tipificar os crimes cibernéticos, com a identificação do autor e a sua consequente punição.

Justifica-se o presente trabalho devido da relevância do tema, pois ele se desenvolve a partir do argumento de que a compreensão sobre os crimes virtuais, ajuda na reflexão de maneiras de combater, minimizar e neutralizá-los de forma eficaz. Por esse motivo é muito importante que as pessoas conheçam suas classificações, para que elas possam identificar quais os crimes virtuais mais praticados e como a legislação trata tais delitos.

Assim, o problema do seguinte trabalho é com a omissão por parte da legislação, até quando isso contribui para o aumento dos crimes cibernéticos, e quais as medidas vêm sendo tomadas, por parte do poder legislativo para sanar essas omissões? Para responder tal questionamento o objetivo do presente trabalho será analisar como se da, a tipificação dos crimes cibernéticos. A princípio os objetivos específicos serão: conceituar crimes cibernéticos, localizar o responsável pela conduta criminosa, e a aplicabilidade da lei para esses crimes, bem como apontar as dificuldades de identificar os cibercriminosos.

2 O SURGIMENTO DA INTERNET

A *internet* é um canal de pesquisa, de interação e de relacionamento humano muito importante. Ela é uma criação humana que influencia a maior parte da população mundial e como toda criação humana, pode ser usada tanto para o bem, quanto para o mal. Por esse motivo, o Direito tem despertado crescente interesse por ela e pelas consequências jurídicas que ela pode produzir, e conhecer sua evolução é importante para se entender a evolução dos crimes virtuais.

De acordo com Zanellato, o ciberespaço é usado como uma forma de trocar correspondência, arquivo, ideias, além de permitir que as pessoas se comuniquem em tempo real, realizem pesquisas documentais ou então usar serviços e fazer a compra produtos (2012, P.173). Desse modo, ela é uma rede em escala mundial, onde os indivíduos armazenam dados e informações em todo o mundo.

Mesmo que hoje em dia a net possa ser usada em celulares, *tablets*, vídeo games entre outros dispositivos, sua invenção está associada ao desenvolvimento dos computadores, que tem sua origem no ano de 1847, com a máquina analítica do matemático inglês Charlie Babbage, e que foi se desenvolvendo ao longo dos anos e de acordo com a necessidade das pessoas (OLIVEIRA JÚNIOR, 2016).

A internet foi criada tendo objetivos militares no ano de 1969 pela ARPA, que é uma subdivisão do Departamento de Defesa dos Estados Unidos, sendo uma rede de dados e informações que estavam espalhadas em vários lugares estratégicos, para que não fosse possível destruí-las através dos bombardeios. Posteriormente, ela foi usada pelos estudantes de universidades, de modo a obterem resultados de estudos e pesquisas (OLIVEIRA JÚNIOR, 2016).

Na década de 1980 a rede começou a ser usada da mesma forma que se usa atualmente, sendo definida como o conjunto de redes que são interligadas e que são acessadas por todas as pessoas, fazendo com que, dessa forma, novos conceitos surgissem, como o de *hacker*, ciberespaço, entre outros. A partir desse momento começou a se discutir a respeito, da necessidade de regulamentação desse ambiente. (OLIVEIRA JÚNIOR, 2016).

3 A CRIMINALIDADE E OS AVANÇOS TECNOLOGICOS

Os cibercrimes começaram a ficar bem evidentes a partir da década de 1960, especialmente nos casos de manipulação e sabotagem de sistemas. Em 1970 já se conhecia o *hacker* devido invasão e furto de *software* que começaram a acontecer. Em 1980 esses crimes foram difundidos a partir das invasões de sistema, pirataria, pedofilia entre outras, sendo necessários maiores preocupações com a segurança virtual (CARNEIRO, 2012).

No ano de 1995 o Ministério das Comunicações criou o Comitê Gestor da *Internet* no Brasil, por meio da Portaria Interministerial n° 147, que tem como atribuições estabelecer diretrizes relacionadas ao uso da *web* no Brasil e também promover e recomendar procedimentos securitários. Além disso, inspirou a proposta legislativa do Marco Civil da *Interweb*, uma lei que regulamenta os direitos e deveres para o uso da net, que será tratado posteriormente. (CGI, s.d.)

Com o desenvolvimento dos computadores e a difusão do espaço virtual, tornam-se cada vez mais comuns situações em que pessoas prejudicam outras se utilizando dessas ferramentas, vez que elas possibilitaram a criação de um espaço público virtual que influencia diretamente na vida pessoal, pública, financeira e coletiva. Surgiram então, pessoas especializadas em

informática e tecnologia que praticam crimes por todo o mundo. São os denominados crimes virtuais ou cibernéticos.

Segundo Fernando Capez "O crime pode ser conceituado sob três enfoques, quais sejam, aspecto material, formal e analítico" (2020, p. 185). O aspecto material é aquele que está ligado aos bens jurídicos fundamentais e que são de alguma forma, lesados ou expostos a algum perigo, o aspecto formal resulta da legislação e da ligação da conduta ao tipo penal e por fim, o aspecto analítico em que crime é todo fato típico e ilícito.

Grande parte, dos atos ilegais também acontecem no mundo real, entretanto, no *cyberspace*, devido ao avanço tecnológico, diversas condutas se espalham mais rapidamente e são mais difíceis de encontrar o autor do delito, vez que ocorrem livremente, não encontram barreiras e possuem o anonimato. Existem diversas espécies de crimes cibernéticos, é possível citar os seguintes: pornografia infantil, crimes contra a honra, fraudes virtuais, crimes contra a propriedade intelectual e estelionato (GUIMARÃES, 2017).

A tecnologia da informação influência e modifica todas as esferas do cotidiano do homem, inclusiva a vida privada, que se torna cada vez mais exposta aos holofotes da internet. Nessa perspectiva encontra–se o cidadão comum, que desperta em um universo, onde não se tem mais domínio dos dados pessoais, nem das informações ao seu respeito, o próprio titular não tem controle sobre sua vida privada.

A Constituição Federal resguarda a vida privada e assegura a sua inviolabilidade. De acordo com Liliana Minardi Paesani 'O direito à privacidade ou direito ao resguardo tem como fundamento a defesa da personalidade humana contra injunções ou intromissões alheias' (2019, p. 34). Sendo assim, é compreensível que exista um limite entre a esfera da privacidade e o direito à informação. Apesar de a privacidade ser colocada como uma aspiração individual trata-se de um valor social, um elemento fundamental para a organização da sociedade, com relevância em toda a sociedade e está entrelaçada com a dignidade da pessoa humana. Portanto, ao protegê-la o Estado busca a manutenção de uma vida digna, onde há liberdade e autonomia.

A tecnologia tem sido usada como uma forma de ameaça à privacidade, pelo fato de que muitas pessoas utilizam do anonimato que a *web* proporciona para cometer delitos e invadir a intimidade dos outros. O espaço virtual transfere as informações, além de acumular dados em quantidade ilimitada, sejam elas físicas, mentais, econômicas, opiniões religiosas ou políticas, também possibilita o confronto das informações obtidas.

As redes sociais, que ganharam grande força ao longo dos anos, possibilitam a exposição da privacidade, vez que as pessoas publicam fotos, sentimentos, opiniões e se desnudam ao

expor características e experiências íntimas, além disso, por meio delas, criam-se comunidades entre usuários com interesses comuns. Vale ressaltar que essas informações podem ser utilizadas livremente por qualquer um.

A violação da vida privada se dá devido à falta de regulamentação através de leis e também porque existe uma dificuldade muito grande de limitar e acompanhar os acessos. Existe também uma inconsciência de diversos usuários não sabem a respeito do limite existente entre a liberdade de expressão e o respeito que deve existir entre as pessoas que enviam dados de um ambiente virtual privado para um ambiente público.

Simultaneamente tem-se a consciência que nem toda divulgação de informações acerca da vida privada é ilícito, pois às vezes as próprias pessoas expõem dados pessoais com algum intuito. Com isso acontece que tais dados não podem ser repassados com o propósito de humilhar ou depreciar a honra do cidadão. Com a invasão da intranet à vida privada estão em risco às contas correntes, números de cartões de crédito, nomes e endereços, contatos comerciais e pessoais, disponíveis em qualquer lugar do mundo. Atualmente o mais grave é que esses dados podem ser alterados, será um crime, porém de difícil apuração e punição. Essa ameaça vem de um lado negro do avanço tecnológico.

Por esse motivo é tão importante que as pessoas tenham consciência a respeito dos riscos que a rede mundial de computadores pode causar à privacidade, para que, dessa forma, o usuário consiga se proteger de programas muitas vezes bem duvidosos e, dessa forma, use o computador e a *internet* de uma maneira mais segura, sem exagerar na alta exposição para se sentirem digitalmente incluídos.

Quanto a legislação nacional a respeito dos crimes cibernético, é possível citar algumas, como a Lei n. 12.737/2012, também conhecida como Lei Carolina Dieckmann, foi sancionada em novembro de 2012. Essa lei surgiu, após um inesperado episódio envolvendo a atriz Carolina Dieckmann, em que várias fotos íntimas da atriz foram divulgadas e expostas ao público, em razão da invasão de sua privacidade seguida de extorsão. Tal episódio além de ser amplamente debatido em caráter de urgência desencadeou na referida lei que alterou textos do Código Penal Brasileiro.

Existe também a Lei n. 12.735/2012, conhecida como Lei Azeredo que teve origem no projeto de lei n. 1999 (PL 84/99). Essa lei visa à tipificação de condutas realizadas através do uso sistema eletrônico, digital ou similar e que seja práticas contra sistemas informatizados. Assim, como a Lei n.12.737/2012, esta surgiu em um momento em que os crimes virtuais ocorreram com mais frequência (BRASIL, 2012).

Diante da importância da tipificação penal acerca de crimes cibernéticos, existem também os projetos de lei que tramitam no nosso cenário legislativo, representando uma possibilidade de serem aprovados um dia e trazerem outras modificações no Código Penal. O crescente desenvolvimento tecnológico e o uso massificado da rede impulsionam as casas legislativas a se debruçarem cada vez mais sobre esse assunto.

Em um mundo caracterizado pela acelerada adaptação social e inovação tecnológica, onde quase que diariamente surgem novas formas de convivência, convívio e interação coletiva, inclusive na ceara jurídica e judicial, que atualmente, principalmente em razão do (Covid-19) está desenvolvendo vastas transformações na forma dos atos processuais em que o remoto se torna cada vez mais frequente, a normatização específica de crimes virtuais e de um aparato policial especializado seria, realmente, um avanço gigantesco.

Outra inovação é trazida pelo Projeto de lei n. 4.161/2020 que também altera o Código Penal que determina o agravamento da pena no crime de estelionato e fraude, quando forem praticados no ambiente virtual. Esse projeto foi apresentado pelo Senador Marcos do Val (Podemos-ES) e reflete o recente cenário do isolamento social, causado pelo (Covid-19), vez que, em razão disso houve acréscimos das fraudes efetuadas dentro *cyberspace*.

Por fim, o Projeto de Lei n. 154/19, que também altera o Código Penal e agrava a pena aplicada a quem comete crimes cibernéticos, conforme o texto a agravante será aplicada quando o crime for praticado através de computador ou outro dispositivo compatível. A proposta foi aprovada pelo CNJ e segue para análise do Plenário da Câmara dos Deputados. (CÂMARA DOS DEPUTADOS, 2019).

4 FRAUDES VIRTUAIS

Os crimes ou fraudes virtuais são fatos típicos e antijurídicos cometidos no ambiente digital, ou seja, ato típico e antijurídico, praticados por meio da informática em geral, ou então contra um sistema, dispositivo informático ou redes de computadores (Jesus e Milagre, 2016). Dessa forma, são práticas realizadas através de alguma categoria de dispositivo tecnológico, isto é, condutas ilícitas praticadas em um ambiente virtual (ROCHA, 2017).

Não existe um consenso doutrinário em relação aos crimes praticados através de meios eletrônicos, bem como não há um consenso quanto a sua classificação, pois existem os que conceituam como “crimes digitais”, outros como “crimes virtuais” e ainda “crimes cibernéticos”. Tal classificação, como visto, não é fácil de fazer, pelo fato de que a tecnologia está sempre em evolução, mudando rapidamente e constantemente (FRAGOSO, 1983).

Os primeiros crimes ou fraudes virtuais eram voltados para sabotar os sistemas e tecnologias. Porém, devido à expansão da *internet*, mais pessoas passaram a utilizá-lá, aumentando, assim, a oportunidade para a prática de diferentes crimes (ROCHA, 2017). Assim, tal conduta teve uma evolução muito rápida, saindo das práticas de sabotagens e passando a englobar outras práticas transgressoras, como, por exemplo, o estelionato virtual, roubo e exposição de informações e de imagens íntimas (FERREIRA, SANTOS E COSTA, 2019).

Dessa forma, o estelionato, que já é um crime conhecido pela sociedade, está sendo cometido tanto na esfera virtual, quanto fora dela, e está disposto no artigo 171, do Código Penal. Hoje em dia, ainda mais com a pandemia do novo Coronavírus, houve um aumento muito grande dessa conduta criminosa por meio da rede, o que acarretou a criação da PL 4.554/2020, a qual prevê a modalidade qualificada dos crimes de furto e estelionato através da *web*, com o consequente aumento de pena para referidos delitos.

É bastante comum a utilização de *links*, encaminhados por *e-mail*, mensagens de texto ou por redes sociais como o WhatsApp, Instagram, com algum conteúdo falso, que serve de "isca" aos usuários. Dessa forma, o usuário é induzido a clicar no referido endereço eletrônico, que o direciona a um site falso onde acaba indicando seus dados pessoais e/ou até bancários, permitindo que o criminoso se aproprie de tais dados para, posteriormente, transferir valores disponíveis em contas bancárias para o seu domínio ou realizar compras em nome do usuário, vítima desse golpe.

Outra forma de estelionato é a utilização de sites falsos com a mesma aparência e registro semelhante dos originais, para a captação de dados do usuário. Essa prática é conhecida como Typosquatting (BARRETO, 2021). Com essa modalidade, os agentes estruturam uma página web que registra o domínio idêntico ao de alguma grande empresa conhecida, resultando, por exemplo, em: site original – www.walmart.com; site falso – www.wallmart.com (BARRETO, 2021).

Assim, a plataforma criada não tem nenhuma relação com a verdadeira empresa, e ao inserir os dados, como usuário e senha ou numeração do cartão de crédito, os estelionatários adquirem tais informações para si, e as utilizam, posteriormente. Outra categoria de delito praticado na internet são os delitos contra a honra, os quais estão previstos nos artigos 138 (calúnia), 139 (difamação) e 140 (injuria), do Código Penal, contando com uma dimensão muito maior quando praticados na esfera virtual. Salienta-se que, a "honra" nesse diploma, abrange os aspectos objetivos e subjetivos.

Essa forma de delito é muito comum no ambiente virtual, pois as pessoas acreditam que o ciberespaço é uma terra sem lei e, por esse motivo, a maior exposição em que os indivíduos ficam sujeitos, além do fato de muitos usuários usarem do anonimato ou pensarem que podem se esconder através de uma conta nas redes sociais, fica cada dia mais frequente a prática de crimes contra a honra no âmbito virtual.

Existe também a pornografia infantil, que é um modelo de violência sexual cometida contra vulneráveis (crianças e adolescentes), que acabou ganhando força devido a facilidade de acesso à *interweb* que se tem no presente. A prática desse crime está tipificada no Estatuto da Criança e do Adolescente (ECA), e no Código Penal, assim como também na Convenção dos Direitos da Criança da ONU, de 1989.

Os artigos 240 a 241-E, do ECA, descrevem as condutas que tipificam a pornografia infantil, tendo como objetivo criminalizar a aquisição e a posse de tal material, bem como, combater à produção, venda e distribuição de pornografia infantil. Além disso, esse padrão de delito não é praticado somente por aqueles que querem prazer próprio, é praticado também por aqueles que visam lucro com a criação e comercialização de material pornográfico.

Esse crime aumentou de forma assustadora devido à expansão da rede mundial de computadores e com a criação da *deep web*, a qual não será abordada amplamente no presente trabalho, mas, de forma resumida, trata-se de uma plataforma pouco conhecida pela população em geral, de difícil acesso e que permite a prática de condutas ilícitas mediante sites considerados “invisíveis”, uma vez que, não aparecem nos mecanismos de busca tradicionais como o Google.

Por ser uma conduta típica que causa muita repulsa na população, a jurisprudência é dura na aplicação das penas envolvendo tais condutas, podendo ser destacado a decisão do Superior Tribunal de Justiça, a qual estabelece que quando praticado na rede tem caráter transnacional. Veja-se:

> HABEAS CORPUS No 413.069 - SP (2017/0208680-6) RELATOR: MINISTRO JOEL ILAN PACIORNIK IMPETRANTE: DEFENSORIA PÚBLICA DA UNIÃO ADVOGADO: DEFENSORIA PÚBLICA DA UNIÃO IMPETRADO: TRIBUNAL REGIONAL FEDERAL DA 3A REGIÃO PACIENTE: MICHAEL LEME DE QUEIROZ DECISÃO. (...) DIREITO PENAL. PROCESSO PENAL APELAÇÕES CRIMINAIS. PORNOGRAFIA INFANTO-JUVENIL. LEI 8.069/90. ARTIGOS 241-A E 241-B. PROGRAMA DE COMPARTILHAMENTO DE DADOS. USO. COMPETÊNCIA. JUSTIÇA FEDERAL. DOLO CARACTERIZADO NO COMPARTILHAMENTO DOS ARQUIVOS ILÍCITOS. AUTORIA E MATERIALIDADE INCONTROVERSAS. ABSORÇÃO. INOCORRÊNCIA NO CASO CONCRETO. CONDENAÇÃO MANTIDA. DOSIMETRIA. ALTERAÇÕES. [...] Publique-se. Intime-se. Brasília (DF), 23 de fevereiro de 2018.

(STJ - HC: 413069 SP 2017/0208680-6, Relator: Ministro Joel Ilan Paciornik, Data de Publicação: DJ 28/02/2018).

O Superior Tribunal Federal, ainda estabelece que a mera divulgação do conteúdo sexual envolvendo os vulneráveis já se consuma o crime de pornografia infantil. No julgado diz que a publicação de conteúdo que contêm cena de sexo infanto-juvenil, é preciso somente a publicação de tal conteúdo para a tipificação do crime contido no artigo 241 do Estatuto da Criança e do Adolescente. Dessa forma, a divulgação dessa classe de conteúdo viola gravemente a integridade da criança e do adolescente, sendo um crime cometido em ambiente virtual, passível de condenação para quem praticou tal delito.

Assim, a pornografia infantil é um crime doloso, o qual exige-se apenas o dano potencial, não necessitando de dano material efetivo para ser consumado, tendo como objeto material a foto, o vídeo ou a imagem contendo pornografia ou sexo explícito envolvendo criança ou adolescente e, ainda, tendo como objeto jurídico a proteção à formação moral da criança ou adolescente, que, por ser pessoa incapaz, causa a elevação da pena da pessoa que praticou tais crimes virtuais (NUCCI, 2016).

5 LEGISLAÇÃO NACIONAL DE USO DOS MEIOS ELETRÔNICOS E O MARCO CIVIL DA INTERNET

O marco civil da *internet* foi criado com o objetivo de regulamentar as questões referentes ao ambiente virtual, estabelecendo direitos, deveres, princípios e garantias para que fosse possível consolidar os avanços significativos que o ambiente virtual teve nos últimos anos. Assim, ele é considerado uma construção democrática e social, pois no decorrer de seu processo de criação a sociedade participou de forma ativa, tornando-se um verdadeiro marco civil e social.

A elaboração do projeto de lei que resultaria no marco que foi dividida em duas partes, onde a primeira foi um debate a respeito dos princípios que norteariam todo o projeto e a partir desses princípios fundamentais e a segunda fase concretizou tais princípios, sendo efetivamente a construção do texto legal. De acordo com Ronaldo Lemos "O Marco Civil deveria promover a liberdade de expressão, a privacidade, a neutralidade da rede, o direito de acesso à net, os limites à responsabilidade dos intermediários e a defesa da abertura (*openness*) da rede, crucial para a inovação." (LEMOS, *et al*, 2014, P. 5)

Importante destacar também que o Marco civil da *internet* possui três pilares fundamentais que são: a garantia da neutralidade da rede; a garantia da liberdade de expressão e comunicação; e a privacidade dos usuários e proteção de seus dados. Esses princípios são muito importantes diante de um poderoso ambiente em que se preocupa com os dados pessoais que são disponibilizados, com os provedores que irão receber tais dados e ainda existe uma preocupação de não suprimir um direito constitucional diante de regras de prevenção e proteção (AKCHAR, 2017).

Além disso, o interesse despertado pela *cyberspace* vem devido a possibilidade de acesso por qualquer pessoa, proporcionando a sua valoração no vasto banco de informações que ela disponibiliza e as pessoas podem acessar bem como a possibilidade poder se comunicar com qualquer lugar do planeta. Por esse motivo não é razoável que alguém possa se apropriar dessa rede colocando em detrimento interesse alheio.

Dessa forma, ao estabelecer o tratamento isonômico aos pacotes de dados, a *web* se transforma em um canal universal de comunicação, que preserva a livre concorrência, a liberdade dos usuários e impede o abuso de poder. Caso não aconteça a neutralidade da rede, os provedores podem tratar com certa discriminação de determinados conteúdos ou até mesmo bloqueá-los, impedindo que eles chegassem até o usuário.

O Artigo 3° da lei garante a proteção da privacidade e a proteção dos dados pessoais dos usuários, o Art. 7° dispõe a respeito dos direitos dos usuários e o Art. 8° contém normas voltadas à nulidade das cláusulas contratuais que impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas no espaço virtual, esses são alguns exemplos de normas contidas num importante momento histórico para o direito civil com o fito de proteger os usuários e sua privacidade (BRASIL, 2014).

A promulgação do Marco Civil da *Internet*, mesmo que não trate de forma específica a respeito das questões criminais, é considerado um passo importante para a evolução do tratamento legal a respeito de temas referentes ao ambiente virtual, inclusive na ceara criminal, pois com essa lei, o ambiente virtual ficou regulamentado, e os atos praticados por eles ficaram passiveis de punição para quem cometeu algum delito.

Mas, além do Marco Civil da *Internet*, é possível citar algumas leis criadas para combater crimes praticados no ambiente virtual. Um exemplo disso é a Lei n.º 12.737/2012, também conhecida como Lei Carolina Dieckmann, a qual foi criada depois que fotos intimas da atriz Carolina Dieckmann foram expostas ao público, devido a uma invasão de sua

privacidade seguida de extorsão. Esse episódio além de ser amplamente debatido em caráter de urgência encadeou na referida lei que alterou textos do Código Penal Brasileiro.

De acordo com Uchôa, "para ser legitima a tutela penal é necessário que o bem seja 'digno' dessa proteção, e que sua lesão ou ameaça efetivamente mereça uma sanção penal" (2009, *online*). Porém, a problemática que envolvia às novas condutas virtuais eram ilegítimas diante do Direito Penal, e, em razão dessa lacuna na legislação surgiu a Lei n.º 12.737/2012 (BRASIL, 2012).

Antes da referida lei, haviam outros projetos de lei que tenha por objetivo combater tais condutas, dentre eles o Projeto de Lei n.º 89/2003, o qual tramitou por mais de 10 anos no Congresso Nacional desencadeando vários embates jurídicos e criticas, houve também o Projeto de Lei n.º 2793/2011 que tinha o intuito de combater o Projeto de Lei n.º 89/2003, pois se acreditava que seria mais proveitoso para a sociedade (ROCHA, 2013).

Com a lei Carolina Dieckamnn foram acrescidos ao Código Penal os artigos 154-A e 154-B, os quais tipificam o crime de invasão de dispositivo de informática, onde o agente comete a conduta de invadir dispositivo informático alheio, através de uma violação indevida de mecanismo de segurança com o fim de obter, adulterar ou destruir dados, ou informações sem autorização do titular do dispositivo (BRASIL, 2012).

Por fim, a citada lei também modificou os artigos 266 e 298 do Código Penal, para que eles ficassem adequados à realidade cibernética. O artigo 266 teve seu título alterado passando a inserir a interrupção quanto aos serviços informáticos, passando a se titular "Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública*"* e no parágrafo único do artigo 298 o legislador equiparou o cartão de crédito ou débito ao documento particular no crime de Falsificação de documento particular (BRASIL, 2012).

Outra lei importante para combater fraudes pela *internet* foi promulgada no ano de 2012, a Lei n.º 12.735, conhecida como Lei Azeredo que teve origem no projeto de lei n.º 1999 (PL 84/99). Tal legislação tem o objetivo de tipificar as condutas realizadas por meio do uso de sistema eletrônico, digital ou similar praticadas contra sistemas informatizados. Por conseguinte, da mesma forma que a Lei n.º 12.737/2012, esta surgiu em um momento em que os crimes virtuais ocorreram com mais frequência. (BRASIL, 20q12)

Devido à importância da tipificação dos crimes cibernéticos, existem também os projetos de lei que tramitam no legislativo, e, se forem aprovados, podem trazer outras

modificações no Código Penal. O crescente desenvolvimento tecnológico e o uso massificado da rede impulsionam as casas legislativas a se debruçarem cada vez mais sobre esse assunto.

Entre tais projetos de lei em trâmite, consta o projeto de Lei n° 4287 de 2019 o qual altera os artigos 141 e 154-A do Código Penal e acrescenta hipóteses de agravamento da pena nos crimes contra a honra praticados usando a net e tipifica a conduta de invadir dispositivo informático, como a conduta de obter, adulterar ou destruir dados sem autorização do usuário do dispositivo (SENADO FEDERAL, s.d.).

Por fim, o Projeto de Lei n. 154/19, que também altera o Código Penal e agrava a pena aplicada ao agente que comete crimes cibernéticos, e, de acordo com o texto, a agravante será aplicada sempre que o crime for cometido por intermédio de computador ou outro dispositivo compatível. A proposta foi aprovada pelo CNJ e segue para análise do Plenário da Câmara dos Deputados (CÂMARA DOS DEPUTADOS, 2019).

6 CONSIDERAÇÕES FINAIS

A presente pesquisa buscou fazer uma análise desde o surgimento da *internet* chegando até as características e conceitos do cibercrime e do cibercriminoso, para que fosse possível chegar às tipicidades das principais condutas ilícitas que são praticadas no ambiente virtual. Além disso, foram analisadas as medidas no combate aos crimes virtuais até as legislações atuais.

Diante das análises feitas ao longo de todo o trabalho, foi possível perceber o quanto esse tema é relevante, pelo fato de que cada vez mais pessoas tem acesso à rede na atualidade. Por esse motivo, os crimes e fraudes virtuais vêm aumentando de forma drástica, e os danos causados por essa modalidade delitiva são imensuráveis, provocando diversos impactos psicológicos, econômicos e financeiros nas vítimas. O combate dessas condutas exige um aperfeiçoamento tecnológico na esfera policial e judicial, o qual ainda se demonstra um desafio.

Foi possível notar também que a legislação brasileira não conseguiu acompanhar a rápida e intensa evolução dos crimes virtuais, sendo preciso uma legislação mais ampla, específica e eficaz para esse tema, precisando, também, de uma cooperação mais efetiva entre os Estados e entidades Internacionais para sua elaboração, como também para restarem frutíferas as ações preventivas e repressivas, no âmbito judicial e policial.

REFÊRENCIAS BILIOGRÁFICAS

ALMEIDA, Daniel Freire e. **Um tribunal internacional para a internet**. São Paulo. Almedina. 2015.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília. 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 12 de mai.2022.

BRASIL**. Decreto-Lei n° 3.689, de 03 de outubro de 1941. Institui o Código Penal.** Brasília. 1941. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 12 de mai.2022.

BRASIL. **Lei n° 12735, 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. Brasília. 2012 Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 12 de mai.2022.

BRASIL**. Lei n° 12965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília. 2015. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 12 de mai.2022.

BRASIL. **Lei n° 13. 709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasilia. 2018. Disponivel em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 12 de mai.2022.

BRASIL. **Lei n° 8.069, de 13 de julho de 1990.** Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Brasília. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 12 de mai.2022.
BRASIL. **Projeto de Lei n° 4287/2019 - Senado Federal**.

BRASIL. Superior Tribunal de Justiça. Conflito de Competência n° 133.534/SP, Rel. Ministro REYNALDO SOARES DA FONSECA, TERCEIRA SEÇÃO, julgado em 28/10/2015, DJe 06/11/2015. **Diário de Justiça Eletrônico**. Disponível em: https://scon.stj.jus.br/SCON/pesquisar.jsp. Acesso em: 04 out. 2022.

CAPEZ, Fernando. **Curso de processo penal**. 27. ed. – São Paulo: Saraiva Educação, 2020.

CAPEZ, Fernando. **Curso de processo penal**. 28. ed. – São Paulo: Saraiva Educação, 2021.

CALDERON, Bárbara. **Deep & Dark Web**. Rio de Janeiro. Alta Books, 2017.

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

CASTELLS, M. **A galáxia da Internet**: reflexões sobre a Internet, os negócios e a sociedade. Rio de Janeiro: Jorge Zahar, 2003.

CASTRO, Ana Lara; SYDOW, Spencer. **Stalking e Cyberstalking**: obsessão, internet, amedrontamento. Belo Horizonte: D' Plácido, 2017.

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011. p.48.

DELMANTO, Celsom et al. **Código Penal comentado**. 9. ed. rev., atual. e ampl. — São Paulo: Saraiva, 2016.

DOTTI, René Ariel. **Curso de Direito Penal**: parte geral. Rio de janeiro: Forense, 2020.

GOMES, Luiz Flávio; GARCÍA-PABLOS DE MOLINA, Antônio. **Direito Penal**: parte geral, v. 2. São Paulo: Revista dos Tribunais, 2017.

LOPES JÚNIOR, Aury. **Direito processual penal**. 16. ed. – São Paulo : Saraiva Educação, 2019.

MARCACINI, Augusto Tavares Rosa. **Aspectos Fundamentais do Marco Civil da Internet: Lei no 12.965/2014**. São Paulo: Edição do autor, 2016.

MEDINA. José Miguel Garcia. **Constituição Federal comentada.** 3. ed. rev., atual. e ampl. – São Paulo: Editora Revista dos Tribunais, 2014.

MENDES, Gilmar; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. 7 ed. São Paulo: Saraiva, 2011.

NUCCI, Guilherme de Souza. **Manual de direito penal**. Rio de Janeiro: Forense, 2014.

NUCCI. Estatuto da Criança e do Adolescente Comentado. 3 ed. São Paulo: Revista dos Tribunais, 2016.

PRADO, Luiz R. **Curso de Direito Penal brasileiro**: parte especial, 5 ed. São Paulo, Revista dos Tribunais, 2006, p.273.

PRADO, Luiz Regis; CARVALHO, Érika Mendes de; CARVALHO, Gisele Mendes de. **Curso de direito penal brasileiro**. 13.ed., rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2014