ANA PAULA SOUZA ASSUNÇÃO

CRIMES VIRTUAIS

CURSO DE DIREITO – UniEVANGÉLICA
2018

ANA PAULA SOUZA ASSUNÇÃO

CRIMES VIRTUAIS

Monografia apresentada ao Núcleo de Trabalho de Curso da UniEvangélica, como exigência parcial para a obtenção do grau de bacharel em Direito, sob a orientação do Professor Juraci Cipriano.

ANÁPOLIS – 2018

ANA PAULA SOUZA ASSUNÇÃO

CRIMES VIRTUAIS

Anápolis, ____ de _____ de 2018.

Banca Examinadora

_____

_____

AGRADECIMENTOS

Agradeço a Deus por ter me sustentado até aqui e amparado meus estudos com sabedoria.
A minha família que é fonte de inspiração para meu sucesso profissional.
Ao meu professor orientador Juraci Cipriano, por seus ensinamentos, pela paciência e incentivo, sem ele não seria possível a conclusão deste trabalho.
Enfim, a todos que colaboraram de alguma forma para que eu chegasse até aqui. Obrigada.

DEDICATÓRIA

Dedico esse trabalho aos meus avós que torcem por mim de forma encantadora e não medem esforços para que meu sucesso seja conquistado.

RESUMO

O Trabalho de Conclusão de Curso apresenta uma explanação entre legislação vigente e projeto de lei acerca dos crimes virtuais. O trabalho tem por objetivo demonstrar a fragilidade do ordenamento jurídico quanto ao posicionamento tanto da jurisprudência quanto das leis para tipificarem condutas criminosas em relação a tais crimes. Após a analise de casos concretos e suas resoluções com relação a lei penal, decretos, jurisprudência e analogia foi evidenciado a vulnerabilidade para julgar casos que necessitam da aplicação da lei que trata dos crimes virtuais. A solução que tem sido aplicada para julgamento de conflitos relacionados a crimes cometidos em ambiente virtual tem sido feita por jurisprudência e leis existentes, porém ainda não se fazem totalmente eficazes. A pesquisa metodologicamente foi moldada por abordagem dedutiva e por procedimento bibliográfico, formatado por método positivista onde foram analisadas legislações e posicionamentos doutrinários. Após a construção de três capítulos pela análise é concluído que há carência de legislação para tratar de um conflito que cresce cada vez mais em nosso meio uma vez que nos tornamos cada vez mais dependentes do ambiente virtual.

Palavras chave: Crime Virtual. Projeto de lei. Jurisprudência. Legislação Vigente.

SUMÁRIO

INTRODUÇÃO

O presente trabalho monográfico tem a ideia central de analisar a legislação vigente e projetos de lei já existentes que abarcam a temática de crimes cometidos no meio virtual, uma vez que estes não possuem legislação específica.

Enfatizam-se pesquisas realizadas, por meio de compilação bibliográfica, bem como jurisprudências e normas do sistema jurídico brasileiro. Assim sendo, pondera-se que, este trabalho foi sistematizado de forma didática, em três partes.

O primeiro capítulo aborda o desenvolvimento histórico dos crimes virtuais e seu conceito, numa abordagem doutrinária que expõe todo o caminho percorrido de tal evolução sistematizando todos os conceitos entre si.

O segundo capítulo trata das espécies mais frequentes de crimes praticados no meio virtual, abordando com mais ênfase as modalidades de tais condutas criminosas, trazendo tipificações dos mesmos e exposição de como tais condutas são realizadas na pratica.

Por conseguinte, o terceiro capítulo elenca a leis que já tratam do assunto, seja por vertente específica ou por analogia assim como projetos de lei acerca do assunto que tramitam para que sejam analisados e aprovados.

CAPÍTULO I – CRIMES VIRTUAIS

O fenômeno da globalização transformou a forma como vemos o mundo atualmente. A globalização em si é algo difícil de se conceituar. O professor Boaventura de Souza Santos (1997) nos ensina que muitos doutrinadores acreditam que a globalização seja um fenômeno centrado na economia, melhor dizendo, em uma nova economia mundial que surgiu como um processo através do qual as empresas multinacionais ascenderam a um status, sem precedentes, de atores internacionais.

No entanto, para ele, é importante abordar uma definição de globalização "mais sensível às dimensões sociais, políticas e culturais", acreditando que:

> A globalização é o processo pelo qual determinada condição ou entidade local consegue estender sua influência a todo o globo e, ao fazê-lo, desenvolve a capacidade de designar como local outra condição social ou entidade rival (SANTOS, 1997, p.108).

Com o crescimento desse fenômeno chamado globalização, novas relações entre pessoas passaram a ser realizadas através de equipamentos eletrônicos, culturas diferentes se conheceram na rede mundial de computadores, novas relações tanto pessoais quanto profissionais passaram a surgir. Por essa razão o Direito percebeu a necessidade de se moldar a esta nova realidade para que a sociedade digital não se torne a margem do controle Estatal.

A tecnologia é um dos principais fatores de movimentação do direito, sendo o avanço tecnológico e sua adesão de suma importância no dia a dia das pessoas, se fazendo necessário à sua regulamentação para que as relações evoluam e passem a ser desenvolvidas em ambiente virtual. Uma das características fundamentais na definição das redes é a sua abertura e porosidade, possibilitando relacionamentos horizontais e não hierárquicos entre os participantes, referindo que

as redes não são, portanto, apenas uma outra forma de estrutura, mas quase uma não estrutura, no sentido de que parte de sua força está na habilidade de se fazer e desfazer rapidamente (DUARTE; FREI, 2008, *apud* TRENTIN; TRENTIN, 2012).

A internet é, sem dúvidas, a maior revolução tecnológica do último século. Com a sua expansão, as novas tecnologias de informação surgem trazendo mudanças ao contexto social contemporâneo. A comunicação virtual entre as pessoas se acentua de uma forma jamais vista, o que, de maneira positiva, contribui para o fenômeno da globalização na medida em que cria novas oportunidades às práticas comerciais, novos relacionamentos, velocidade e acesso irrestrito à informação entre outras vantagens. Por outro lado, cresce também a utilização desse importante meio tecnológico para a prática de atos ilícitos (TRENTIN; TRENTIN, 2012).

Na opinião do Professor Reginaldo César Pinheiro (2001, *apud* FIORILLO; CONTE, 2016, p. 183):

> Com a popularização da Internet em todo o mundo, milhares de pessoas começaram a se utilizar deste meio. Contemporaneamente se percebe que nem todos a utilizam de maneira sensata e, acreditando que a Internet é um espaço livre, acabam por exceder em suas condutas e criando novas modalidades de delito: os crimes virtuais.

Com o advento deste ambiente de relacionamentos digitais atemporais, os sistemas jurídicos de todo o mundo iniciaram uma cruzada para elaborar ou até atualizar suas leis de modo que abraçassem essa nova realidade (PINHEIRO, 2014).

É dever do Estado democrático de direitos garantir a seus cidadãos o desenvolvimento pacífico e a coexistência de semelhantes em igualdade de condições, agindo como mantenedor da ordem social. Nesse sentido, acaba por interferir na nova sociedade de informação, no chamado meio ambiente virtual, elaborando normativas que impõem limites à internet e à troca de informações por meio da tecnologia (SYDOW, 2014).

No mesmo diapasão, as legislações mundiais passaram a discutir novas regras para se enquadrar na atual realidade. Nessa “corrida”, o Brasil, de forma mais

lenta, promulgou leis para tratar da regulamentação da web, protegendo temas essenciais como liberdade de expressão, direitos do consumidor e crimes virtuais (PINHEIRO, 2014).

Como exemplos de evolução legislativa entrou em vigor no Brasil, no ano de 2012, a Lei de Crimes Informáticos (mais conhecida como Lei Carolina Dieckman), nº 12.737 que acresce ao Código Penal Brasileiro os artigos 154-A e 154-B.

Posteriormente, em 23 de abril de 2014, sanciona-se a Lei nº 12.965 (Marco Civil da Internet), que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil, com contribuição, em especial, na esfera cível.

Recentemente, no ano de 2016, foi apresentado o relatório final da Comissão Parlamentar de Inquérito (CPI) destinada a investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste país, que teve como presidente a Deputada Maria do Carvalho (PSDB) e relator deputado Esperidião Amim (PP).

O crime virtual deve ser analisado sob diferentes perspectivas por conta de suas peculiaridades. Comparando com o “crime real” que tem local precisado e mais fácil ação pelas autoridades coatoras, o crime virtual dispensa o contato físico entre vítima e agressor, ocorrendo em um ambiente sem povo, governo ou território, além de não gerar, a princípio, sensação de violência para um segmento social específico não havendo padrões para o seu acontecimento (SYDOW, 2009).

O criminoso informático pode cometer mais de uma conduta lesiva ao mesmo tempo, podendo estar em diversos lugares simultaneamente, contando ainda com o fato de ser, muitas vezes, discreto e silencioso. Além disso, culturalmente, a sociedade ainda conta com uma postura omissiva e, nem sempre, denuncia as condutas ofensivas (SYDOW, 2009).

Para o criminologista indiano Karuppannan Jaishankar (2007), as pessoas agem de forma diferente quando movem de um espaço para outro (por exemplo de

um espaço físico para o virtual). Pessoas que tem comportamentos criminosos reprimidos, no mundo físico, tem uma predisposição a cometer crimes virtuais, não cometendo os crimes no espaço físico devido, muitas vezes, ao seu status ou posição social (JAISHANKAR, 2007).

Os crimes virtuais impróprios mais recorrentes do mundo digital são velhos conhecidos dos ordenamentos jurídicos, tais como crimes contra a honra, discriminação, ameaça, fraude, falsidade ideológica entre outros, sendo que, agora, existem mais ocorrências dos mesmos. No caso da internet a possibilidade do anonimato estimula o descumprimento de regras, pois gera maior certeza de impunidade (PINHEIRO, 2014).

Já dentro dos crimes virtuais próprios, segundo o Centro de Estudos, Resposta e Tratamento de Segurança do Brasil (cert.br), que atende as redes brasileiras conectadas à internet, foram registradas, no Brasil, no ano de 2016, mais de 647.112 notificações de incidentes de segurança envolvendo redes conectadas à internet. Dessas notificações, as maiores ocorrências, de 59,33%, corresponderam ao chamado “scan”, classificados como notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles, permitindo associar possíveis vulnerabilidades aos serviços habilitados em um computador (CERT.COM, 2016).

A criminalidade informática traz como uma de suas principais características a informatização global, sendo a mais relevante delas a transnacionalidade uma vez que praticamente todos os países, hoje, tem acesso ou fazem uso da informática, de maneira que é possível praticar um ilícito penal a partir de qualquer lugar da denominada sociedade global (FIORILLO; CONTE, 2016).

Considerando esta característica da rede está fartamente disponível na internet uma gama de serviços para aqueles que pretendem se beneficiar indevidamente da atividade praticada pelos operadores do “cyber crime”. São ofertas de criação de documentos ou certificados de conclusão de cursos falsos, venda de dinheiro falso e prestação de serviço de modificação ilegal da velocidade de conexão à internet provida pelas prestadoras de telecomunicações (BRASIL, 2016).

1.1 Definições de crimes virtuais

A partir do momento que a criminologia percebeu que a internet se tornou um novo foco de criminalidade, foi necessária a criação de teorias para definir os crimes virtuais, bem como entender por qual razão eles ocorrem (JAISHANKAR, 2007).

No Brasil, infração penal é o gênero, podendo ser dividida, estruturalmente, em crime (ou delito) e contravenção penal (ou crime anão, delito liliputiano ou crime vagabundo). As condutas mais graves, por consequência, são etiquetadas pelo legislador como crimes, enquanto as menos lesivas, como contravenções penais (CUNHA, 2014).

Não cabe, no presente trabalho, trazer as distinções entre crime e contravenção penal, sendo apenas importante determinar que quando se utiliza a expressão “crimes virtuais” fala-se no mesmo sentido de infração penal (gênero).

O que realmente importa para a análise são as suas características. Guilherme de Souza Nucci (2011, p. 173), conceitua crime da seguinte maneira:

> Poucos institutos sobreviveram por tanto tempo e se desenvolveram sob formas tão diversas quanto o contrato, que se adaptou a sociedades com estruturas e escala de valores tão distintas quanto às que existiam na Antiguidade, na Idade Média, no mundo capitalista e no próprio regime comunista (2000, p. 43).

Já os crimes virtuais, além das características das infrações penais “reais” são identificados como cometidos através do uso de dispositivos tecnológicos. Alguns doutrinadores como o Professor Marcelo Xavier de Freitas Crespo (2011) se utilizam de outras nomenclaturas para tratar dos crimes virtuais.

Em que pese não existir consenso entre os doutrinadores que abordam o tema e a diversidade de nomenclaturas acerca do tema, todas abarcando as diversas condutas ilícitas realizadas por algum tipo de dispositivo tecnológico, a que será utilizada neste trabalho é a de “Crimes Virtuais” por entender-se que a realização das condutas são dadas em um ambiente virtual.

Corroboram com esse conceito os professores Damásio de Jesus e José Antônio Milagres (2016), quando arrematam que crimes virtuais são fatos típicos e antijurídicos cometidos por meio da ou contra a tecnologia da informação, ou seja, um ato típico e antijurídico, cometido através da informática em geral, ou contra um sistema, dispositivo informático ou redes de computadores.

O professor Paulo Marco Ferreira Lima define os crimes virtuais – chamados por ele de crimes de computador – como uma conduta humana, caracterizada no direito penal como fato típico, antijurídico e culpável, em que a máquina computadorizada tenha sido utilizada, facilitando de sobremodo a execução ou a consumação da figura delituosa, causando um prejuízo a outras pessoas, beneficiando ou não o autor do ilícito (apud PALAZZI, 2000, apud FIORILLO; CONTE, 2016).

A Organização para Cooperação Econômica e Desenvolvimento da Organização das Nações Unidas (OCDE), em 1983, definiu como crime informático “qualquer conduta ilegal, não ética, ou não autorizada que envolva processamento automático de dados e/ou a transmissão de dados” (PALAZZI, 2000, apud FIORILLO; CONTE, 2016, p. 186).

Pode-se dividir os crimes virtuais como próprios ou impróprios. Os primeiros, são aquelas condutas antijurídicas e culpáveis que visam atingir um sistema informático ou seus dados violando sua confiabilidade, sua integridade e/ou sua disponibilidade. Já os segundos, são condutas comuns – típicas, antijurídicas e culpáveis – que são perpetradas utilizando-se de mecanismos informáticos como ferramenta, mas que poderiam ter sido praticadas por outros meios (SYDOW, 2014).

Os crimes virtuais podem envolver uma multiplicidade de sujeitos. Pode-se tomar, como exemplo, a conduta de um hacker que é contratado por alguém para roubar segredos corporativos de um concorrente. Nesse caso, o hacker irá utilizar-se de seus conhecimentos em explorar falhas de segurança em um sistema. A princípio, os sujeitos envolvidos seriam o sujeito que contratou, o hacker e a vítima (concorrente). Entretanto, suponha que o hacker precise se dirigir à uma “lan house” para acessar o sistema, e, ao invés de se utilizar de uma falha na segurança da

empresa hackeada, prefira enviar um e-mail à algum funcionário solicitando algum tipo de informação. Esse funcionário irá passar para um responsável que confiará no funcionário anterior (e assim por diante) até que alguém instale um programa oculto que permita ao hacker invasão ao sistema informático. Nesse caso, teríamos uma multiplicidade de sujeitos ativos e vítimas (SYDOW, 2014).

Como falado, dentro dos crimes virtuais impróprios encontram-se crimes conhecidos cotidiano brasileiro. Um exemplo sério que se tem no país hoje é o da liberdade de expressão frente ao discurso de ódio. Embora a liberdade de expressão seja um princípio protegido constitucionalmente, não pode ser exercida de forma absoluta. É importante que se pondere o direito da livre expressão com a proteção aos direitos de terceiros, como à honra, imagem, privacidade, intimidade entre outros (COELHO; BRANCO, 2016).

1.2 Evolução histórica

A sociedade humana desenvolveu, há muito tempo, um modelo harmônico de convivência social baseado em um sistema de regras de condutas. Antes, as regras eram transmitidas de forma oral evoluindo, rapidamente, para um formato escrito e documentado. Essa mudança é importante, tendo em vista que quando as normas são claras, objetivas e organizadas, são de mais fácil aceitação e até mesmo imposição para uma coletividade (PINHEIRO, 2014).

Dessa forma, sempre passou por transformações e revoluções, e, dentre elas, algumas se destacam. É o caso, por exemplo, da Revolução Francesa, que trouxe o início da positivação de Direitos Fundamentais, sendo tida como fundadora dos direitos civis (ODALIA, 2013). A Revolução Industrial, trouxe a substituição das ferramentas pelas máquinas e consolidou o modelo capitalista de produção. Entretanto, os avanços trazidos pelas revoluções sempre acompanham problemas e sacrifícios. Nos casos citados, a Revolução Francesa trouxe morte e sangue, enquanto a Revolução Industrial desemprego e exploração da classe trabalhadora (SYDOW, 2014).

No período mais recente da nossa história, passamos por outra grande revolução, a Revolução Digital, entendida como “o movimento de inserção na

sociedade de novas tecnologias e serviços que utilizam desenvolvimentos recentes e que modificam a forma como o cotidiano cidadão progride" (SYDOW, 2014).

Desde a criação da internet, uma das maiores discussões é a respeito da necessidade ou não de regulamentação desse ambiente que surgiu, a princípio, sem nenhum controle impositivo (PINHEIRO, 2014).

O desenvolvimento tecnológico está diretamente ligado ao desenvolvimento econômico de um país. Após as décadas de 80 e 90 o Brasil vivenciou uma experiência positiva de abertura econômica e a influência do processo de globalização, demonstrando ser necessário a criação de uma estrutura adequada de desenvolvimento tecnológico no país (FIORILLO; CONTE, 2016).

As transformações em direção à sociedade da informação, que estão ligadas à expansão e reorganização do capitalismo a partir dos anos 80, podem ser consideradas como um fenômeno globalizado, observado até mesmo em economias menos industrializadas. Nesse cenário de mudanças e evolução uma das mais importantes formas de comunicação e difusão de dados e ideias na atualidade é a estabelecida por meio da rede mundial de computadores e suas interconexões. Assim, a sociedade não pode mais ser entendida ou representada sem a análise do impacto da Internet sobre a forma com que se estabelecem as relações interpessoais (PANNAIN; PEZZELLA, 2015).

Um novo padrão de comunicação e interação social é identificado a partir desse desenvolvimento tecnológico que, com o surgimento de aparelhos de telefonia como smartphones ou tablets, conectados entre si pela internet facilita as comunicações em tempo real e modifica, até mesmo, a forma como a sociedade civil responde à determinados assuntos políticos, sociais, econômicos, entre outros, que antes não despertavam tanto interesse (ALVES, 2014).

Os debates digitais, diferentemente dos debates "reais" em que o debatedor conta com sua perspicácia para derrotar seu adversário, permitindo a adesão dos demais à suas ideias, não contam com mediadores. Em um ambiente de livre expressão e instantânea tutelada pela Constituição da República, "a adoção de

posicionamentos por meio de técnicas argumentativas, com atingimento de grande público, resulta, muitas das vezes, na potencialização das discussões que tornam os debates verdadeiros embates" (COELHO; BRANCO, 2016).

Conforme a tecnologia vai fazendo parte do cotidiano humano torna-se fundamental que o indivíduo passe a ter certo conhecimento pressuposto para poder lidar com as modernidades. A informática passou a ser ramo independente de estudo tecnológico, exclusivo e imprescindível para o cidadão que, inclusive, dedica-se a cursos para aprender e melhorar as técnicas utilizadas na rede (SYDOW, 2014).

A internet se tornou, nos dias atuais, um verdadeiro fenômeno que modificou e remodelou sociedades em diversas áreas. Por exemplo, a internet melhora e fornece novas oportunidades para diferentes grupos minoritários adquirirem certos espaços de discussão na vida pública. Entretanto, com o crescimento do acesso, crescem também, conforme já assinalado anteriormente, as atividades baseadas nos discursos de ódio (WIGERFELT; WIGERFELT; DAHLSTRAND, 2015).

O Brasil é um país de diversidades sociais, raciais e culturais, um país que prioriza o respeito à diversas religiões e que pratica a chamada tolerância religiosa, um país que, segundo decisão do Supremo Tribunal Federal, não legitima a discriminação de pessoas em razão da orientação sexual. Em contrapartida, o Brasil figura em um patamar de desigualdades sociais extremas. Para todos os pontos positivos do país, infelizmente, tem-se exceções (BARROSO, 2014).

Crimes como o chamado "hate speech" - que nada mais é do que o discurso do ódio como manifestação do pensamento correspondente ao desprezo por determinados grupos por características que os identifiquem - cresceram muito com a evolução da internet. Nesse contexto, um Estado Democrático de Direitos como é o caso do Brasil, deve sobrepesar os princípios da liberdade de expressão e outros como a dignidade da pessoa humana para que possa viabilizar e preservar o acesso à internet enquanto espaço interativo, participativo e decisivo no contexto social atual (PANNAIN; PEZZELLA, 2015).

CAPÍTULO II – ESPÉCIES DE CRIMES VIRTUAIS

No presente capítulo será abordado, com mais ênfase, os crimes virtuais impróprios, tendo em vista a constatação de que, utilizando a internet como ferramenta, com a possibilidade de anonimato – o que estimula o descumprimento das regras – tem-se um aumento significativo na ocorrência dos mesmos.

Dentre esses, destacam-se os crimes mais comuns: crimes de ódio em geral (contra a honra, sentimento religioso, *bullyng*), crimes de invasão de privacidade e intimidade (que pode ou não incorrer em uma nova conduta lesiva contra a honra), crimes de estelionato, crimes de pedofilia, entre outros.

A internet possibilita um mundo utópico onde as pessoas encurtam as distâncias físicas, conectando as pessoas mais distantes como se estivessem próximas umas das outras. Para que aja participação efetiva e inserção da pessoa no chamado ciberespaço, é necessário que o Estado promova a proteção de seus direitos e garantias fundamentais, não podendo as novas tecnologias servirem de meios para violação desses direitos (PANNAIN; PEZZELLA, 2015).

2.1 Crimes contra honra

A honra é protegida constitucionalmente, tendo *status* de direito fundamental (artigo 5º, X, da Constituição Federal). Os crimes contra a honra são velhos conhecidos do cotidiano jurídico brasileira. A honra é um direito da personalidade previsto constitucionalmente, sendo necessária a proteção da dignidade pessoal do indivíduo e sua reputação (BARROSO, 2004).

A honra, para a doutrina brasileira, divide-se em honra objetiva e honra subjetiva. A primeira relaciona-se com a reputação e a boa fama que o indivíduo desfruta no meio social em que vive. A segunda está relacionada com a dignidade e o decoro pessoal da vítima, o juízo que cada indivíduo tem de si mesmo (CUNHA, 2014).

Para Guilherme de Souza Nucci (2017) a honra objetiva pode também ser chamada de objeto jurídico, que seria a reputação ou imagem que a pessoa tem perante terceiros, enquanto a honra subjetiva recebe o nome de objeto material.

Dentro do tópico dos crimes contra a honra encontramos, na legislação penal específica, três tipos de crimes distintos: calúnia, difamação e injúria. Distinguem-se, na legislação, o tipo penal e as penas, conforme observa-se:

> **Calúnia**
> Art. 138 Caluniar alguém, imputando-lhe falsamente fato definido como crime:
> Pena - detenção, de seis meses a dois anos, e multa.
> **Difamação**
> Art. 139 Difamar alguém, imputando-lhe fato ofensivo à sua reputação:
> Pena - detenção, de três meses a um ano, e multa.
> **Injúria**
> Art. 140 Injuriar alguém, ofendendo lhe a dignidade ou o decoro:
> Pena - detenção, de um a seis meses, ou multa (BRASIL, 1940, *online).*

Caluniar é, exatamente, imputar falsamente a alguém fato definido como crime. A difamação, por sua vez, se define como a imputação a alguém de fato não criminoso, porém ofensivo a sua reputação e, por fim, a injúria, diferente das outras condutas de “imputação”, é determinada pela atribuição de qualidades negativas ou defeitos (NORONHA, *apud* CUNHA, 2014).

Arrematando o tema, o professor Rogério Sanches Cunha (2014) explica que na calúnia e na difamação tem-se a presença de uma conduta específica de imputar a alguém um fato concreto e ofensivo, necessariamente falso e definido como crime no caso da calúnia – requisitos não exigidos na difamação. A injúria, por sua vez, trata-se de uma imputação genérica, uma má qualidade, um defeito ou algo que menospreze a vítima. Nas duas primeiras, exige-se que a frase desonrosa chegue ao conhecimento de terceiro, o que é desnecessário para a última.

A calúnia, com pena mais grave, poderá ocorrer nos casos em que o fato criminoso jamais tenha ocorrido ou, se ocorrido, não foi a pessoa apontada seu autor (CUNHA, 2014).

Caluniar é tirar a credibilidade da pessoa no meio social em que vive, havendo vontade específica de macular a imagem de alguém (*animus diffamandi*), pressupondo-se o dolo, se consumando no momento em que a imputação falsa chega ao conhecimento de terceiro (NUCCI, 2017).

O Código Penal Brasileiro permite, no § 3º, a chamada exceção da verdade, que se caracteriza pela prova da verdade da imputação, gerando atipicidade na conduta (a conduta expressa diz imputar *falsamente*):

> **Exceção da verdade**
> § 3º - Admite-se a prova da verdade, salvo:
> I - se, constituindo o fato imputado crime de ação privada, o ofendido não foi condenado por sentença irrecorrível;
> II - se o fato é imputado a qualquer das pessoas indicadas no nº I do art. 141;
> III - se do crime imputado, embora de ação pública, o ofendido foi absolvido por sentença irrecorrível (BRASIL, 1940, *online*). (Grifo nosso)

Tendo em vista a tipificação da exceção da verdade prevista no Código Penal Brasileiro, entende-se que a própria lei deixa a salvo hipóteses para tal exceção, ou seja, se o fato criminoso mencionado for verídico afasta-se o tipo penal.

Para Guilherme de Souza Nucci:

> Trata-se de um incidente processual, que é uma questão secundária refletida sobre o processo principal, merecendo solução antes da decisão da causa ser proferida, prevista no § 3.º. É uma forma de defesa indireta, através da qual o acusado de ter praticado calúnia pretende provar a veracidade do que alegou, demonstrando ser a pretensa vítima realmente autora de fato definido como crime. Afinal, se falou a verdade, não está preenchido o tipo penal (‘imputar *falsamente* fato definido como crime’) (2017, p. 658).

O próprio artigo do Código Penal apresente as vedações da aplicação da exceção da verdade, que devem ser observadas. A exemplo da calúnia, na difamação, protege-se a honra objetiva da vítima, caracterizada na imputação de

fato que, embora não seja criminoso, é ofensivo à reputação da vítima perante terceiros (CUNHA, 2014).

Difamar seria desacreditar publicamente uma pessoa, imputando-lhe algo desonroso a sua reputação por vontade específica (*animus diffamandi*), também ocorrendo no momento em que a acusação chega ao conhecimento de terceiros (NUCCI, 2017).

Admite-se, como no estudo do crime anterior, a chamada exceção da verdade, entretanto apenas em casos em que o ofendido é funcionário público e a ofensa é relativa ao exercício de suas funções, cabendo ao ofensor comprovar a verdade da imputação, excluindo-se a ilicitude da sua conduta (CUNHA, 2014).

> **Exceção da verdade**
> Parágrafo único - A exceção da verdade somente se admite se o ofendido é funcionário público e a ofensa é relativa ao exercício de suas funções (BRASIL, 1940, *online*).

Na injúria, ao contrário dos delitos anteriores, o direito tutelado é o da honra subjetiva do ofendido, sendo tipificada como ofender, por ação ou omissão, pessoa determinada, ofendendo lhe sua dignidade, não havendo, em regra, imputação de fatos específicos, mas a conceituação negativa da vítima (CUNHA, 2014).

É um insulto que macula a honra subjetiva de alguém, capaz de atingir a sua dignidade, ferindo a sua autoimagem, por vontade específica (*animus diffamandi)*, ocorrendo no momento em que o insulto chega ao conhecimento do ofendido, independente da ciência de terceiros, não se admitindo a exceção da verdade (NUCCI, 2017).

As múltiplas possibilidades do uso dos computadores e das ferramentas *online* levaram o Estado a constatar que não estava necessariamente preparado para julgar e punir usuários potencialmente criminosos, cujas ações atingem a honra, o decoro e a dignidade de terceiros (SILVA; BEZERRA; SANTOS, 2016).

Não há como se falar nessas condutas sem adentrar no tema da liberdade de expressão. A liberdade de expressão se funda no respeito à autonomia

e dignidade humana, sendo necessário um respeito dos direitos fundamentais de outrem. As tecnologias digitais colocam a liberdade de expressão em uma nova luz devendo-se destacar, positivamente, o aumento das oportunidades de participação social, de interação cultural, aumentando o acesso à uma verdadeira democracia (PANNAIN; PEZZELLA, 2015).

A ideia da liberdade de expressão é a de um meio para obtenção de respostas adequadas para os problemas da humanidade, por meio do debate livre de ideias contrárias em que as melhores prevalecerão (SARMENTO, 2018).

O conflito que ocorre entre a liberdade de expressão do indivíduo, protegido constitucionalmente e as condutas que atingem a honra (objetiva ou subjetiva) das vítimas é latente. Sabe-se que a liberdade de expressão não pode ser exercida livremente e que é necessário ponderar o direito de se expressar com o direito de outros, devendo os agressores responder por seus excessos. Entretanto, nem sempre as condutas realizadas pela internet são punidas penalmente, quer seja por conta da dificuldade de se comprovar o real infrator (anonimato) quer seja pela falta de preparo do Estado para lidar com tal situação (COELHO; BRANCO, 2016).

As condutas são, por vezes, motivadas por ódio puro e simples, sem qualquer tipo de filtro social. Um caso que chamou a atenção dos noticiários foi o da jornalista Maria Júlia Coutinho, em 2015, que recebeu uma chuva de comentários racistas pelo simples fato de ter postado uma foto de si mesma em uma rede social (GLOBO.COM, 2015, *online*).

Outro crime que acaba, por consequência, surgindo relacionado com os crimes anteriores é o crime de ameaça, crime contra a liberdade individual previsto no artigo 147 do Código Penal Brasileiro.

Ao analisar o crime de ameaça deve-se levar em conta a individualidade da vítima. Portanto, idade, sexo, raça, cor, opção sexual, entre outras características, são fatores que devem ser analisados no caso concreto para se analisar se houve ou não a conduta, tipificada como a promessa de se causar a alguém um dano injusto (CUNHA, 2014).

Em caso recente, ocorrido no dia 08 de março de 2018, um torcedor do Palmeiras levantou a bandeira contra a homofobia em sua conta nas redes sociais. Conta a reportagem que a vítima recebeu diversas ameaças dos próprios torcedores do Palmeiras que veem a atitude como uma forma de “manchar” a imagem do clube (GLOBO.COM, 2018, *online*).

Infelizmente, casos como esse ocorrem todos os dias, muito por conta do machismo, homofobia e preconceito inseridos na cultura da sociedade. Esses crimes de ódio em geral, contra raça, religião, cor, gênero vem crescendo muito no meio social, em especial após o advento e consolidação das redes sociais. Cresceu, também, o número de casos de *cyberbullying,* crime que ganhou destaque nos últimos anos e tem relação direta com os crimes estudados nesse tópico.

2.2 Crimes de invasão de privacidade e intimidade

Existe proteção constitucional à privacidade e intimidade, ambos previstos no artigo 5º, X, da Constituição Federal, sendo inseridos no *roll* de direitos fundamentais.

Inserido pela Lei nº 12.737 de 2012 (conhecida comumente como Lei Carolina Dieckmann), tem-se a disposição legal do artigo 154-A do Código Penal a respeito da invasão de dispositivo informático, *in verbis*:

> 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:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. (BRASIL, 1940, *online*).

Os objetos jurídicos tutelados são a intimidade, a vida privada e o direito ao sigilo em dados constantes em dispositivo informático, sendo o núcleo essencial da primeira parte do tipo penal o verbo “invadir”, ou seja, ingressar virtualmente sem autorização expressa ou tácita do titular do dispositivo, não sendo necessária a ocorrência de adulteração, obtenção ou destruição de dados ou informações. A segunda figura do tipo é caracterizada pelo verbo “instalar” e configura-se com a

mera instalação de vulnerabilidade, não sendo necessária a obtenção efetiva da vantagem ilícita, tratando-se, portanto, de crime formal (CAPEZ, 2016).

A atriz Carolina Dieckmann foi vítima de invasão de seu computador e consequente distribuição de arquivos pessoais, vendo expostas suas fotos íntimas na rede mundial de computadores. O objeto jurídico do crime tipificado no artigo 154-A é a privacidade individual e/ou profissional armazenada em dispositivo informático, punindo-se a conduta de invasão de dispositivo informático alheio, mediante violação de seus mecanismos de segurança ou instalação de dispositivo de vulnerabilidade (CUNHA, 2014).

O legislador previu, no § 3º, uma qualificadora importante para o crime, que se liga, diretamente, com a invasão de intimidade da vítima. Nessa situação, a invasão resulta em obtenção de conteúdo de comunicações eletrônicas privadas, informações sigilosas (entre outras coisas), aumentando a pena para seis meses a dois anos, com a ressalva de sua não incidência em caso de crime mais grave praticado (CAPEZ, 2016).

Na mesma esteira, o § 4º aponta uma fundamental majorante do crime, ligada à qualificadora anterior, estabelecendo-se que a pena aumenta-se “de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos” (BRASIL, 1940, *online*).

2.3 Crimes contra a inviolabilidade do patrimônio - Estelionato

Outro crime que teve sua incidência aumentada com o advento e popularização dos meios de comunicação *online* foi o crime de estelionato. Crime mais corriqueiro quando tratado o assunto de inviolabilidade de patrimônio, ganhou mais notoriedade com os chamados golpes virtuais.

Prevê o artigo 171 do Código Penal: Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento.

O crime dá-se com a obtenção da vantagem ilícita indevida, em prejuízo alheio, ao induzir ou manter a vítima em erro. É crime doloso apresentado pela vontade livre e consciente de induzir ou manter alguém em erro (CAPEZ, 2016).

A doutrina discute a respeito da diferença entre fraude penal e fraude civil, sinalizando negativamente. Fraude é fraude, considerada como ato ardiloso, de má-fé, que visa a obtenção de vantagem indevida, acarretando prejuízo a outrem. O Código Penal visou punir a “astúcia”, a “esperteza” daquele que visa despojar a vítima de seu patrimônio fazendo com que o entregue, espontaneamente (CUNHA, 2014).

Conforme dito, a fraude se popularizou e se disseminou, ainda mais, por meio do uso de ferramentas virtuais, dispositivos tecnológicos e da internet, podendo se passar por uma mensagem não identificada, por uma comunicação falsa de uma instituição verdadeira e conhecida, como um banco, procurando induzir o destinatário-vítima a compartilhar informações como senhas, dados pessoais e financeiros (CUNHA, 2014).

O estelionato praticado por meio de meio eletrônico encaixa-se, perfeitamente, no tipo penal estabelecido pelo artigo 171 do Código Penal, sendo possível sua aplicação sem maiores ressalvas (CAPEZ, 2016).

2.4 Crimes contra a liberdade sexual envolvendo menores

De suma importância abordar o tema da liberdade sexual, em especial envolvendo menores de idade. O Estatuto da Criança e do Adolescente apresenta a principal tipificação dos crimes contra crianças e adolescentes tentando prever diversas condutas que podem ser praticadas (CAPEZ, 2016).

Diferentemente das condutas anteriormente descritas, estas acontecem em sigilo, na maioria das vezes. Alguns aplicativos de telefone celular facilitam a troca de informações e mensagens, de forma instantânea, o que leva diversos usuários a compartilhar informações sem perceber que estão incorrendo, necessariamente, em crime (CUNHA, 2014).

Além disso, um tópico que não será abraçado no trabalho - mas que merece um destaque – é a *deep web (rede profunda)*. Praticamente desconhecida pela maioria dos usuários, a plataforma permite a prática de condutas ilícitas por meio de sites considerados “invisíveis”, pois não aparecem nos mecanismos de busca tradicionais como o *Google*. Nessa plataforma são encontradas as mais diversas situações ilícitas como o tráfico livre de drogas, pedofilia, tráfico de pessoas, tráfico de órgãos entre outras condutas (GLOBO.COM, 2016, *online*).

O artigo 241 do Estatuto da Criança e do Adolescente e seus artigos subsequentes descrevem as condutas ilícitas envolvendo criança e adolescente, *in verbis*:

> Art. 241. Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
> Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa (BRASIL, 1990, *online*).

As condutas que mais se destacam no ambiente virtual são as do artigo 241-A e 241-B do Estatuto da Criança e do Adolescente. O artigo 241-A prevê reprimenda às condutas ilícitas de intercâmbio de qualquer processo de difusão de figuras de sexo aberto ou pornografia de que participem crianças e adolescentes. Já o 241-B pune quem adquire, por qualquer meio, possui ou guarda qualquer imagem / fotografia de qualquer natureza contendo sexo aberto ou manifestação de pornografia envolvendo criança e/ou adolescente (TAVARES, 2012).

Com relação ao crime ser praticado no meio virtual, a jurisprudência é dura na aplicação da pena, considerando, até mesmo, que os crimes cometidos pela rede mundial de computadores têm caráter transnacional / internacional. Em destaque, decisão do Superior Tribunal de Justiça sobre o tema:

> 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 Cuida-se de habeas corpus substitutivo de recurso próprio, com pedido de liminar, impetrado em benefício de MICHAEL LEME DE QUEIROZ, contra acórdão do Tribunal Regional Federal da 3ª Região (APC n. 2016.61.14.002516-6). Consta dos autos que o paciente foi condenado em primeiro grau pela prática dos crimes do

> arts. 241-A e 241-B, do Estatuto da Criança e do Adolescente c.c. art. 69 do Código Penal, à pena de 4 (quatro) anos de reclusão, em regime aberto, consistentes em prestação de serviços à comunidade e prestação pecuniária. O Tribunal Regional Federal da 3ª Região, por sua vez, negou provimento ao recurso defensivo e deu parcial provimento ao recurso ministerial, conforme ementa a seguir transcrita: 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. 1. **Réu flagrado em posse de acervo de fotografias e vídeos de pornografia infanto-juvenil, acervo este armazenado digitalmente em discos rígidos de sua propriedade. Teria, ainda, compartilhado arquivo do mesmo teor anteriormente**. [...] Em outros termos: ao disponibilizar arquivos de conteúdo pornográfico infanto-juvenil em servidor mundialmente acessível, **o que há é a disponibilização/divulgação de pornografia infanto-juvenil além das fronteiras nacionais, o que torna claro seu caráter transnacional**. [...] 3. Por sua vez, **a constatação da internacionalidade do delito demandaria apenas que a publicação do material pornográfico tivesse sido feita em "ambiência virtual de sítios de amplo e fácil acesso a qualquer sujeito, em qualquer parte do planeta, que esteja conectado à internet" e que "o material pornográfico, envolvendo crianças ou adolescentes tenha estado acessível por alguém no estrangeiro, ainda que não haja evidências de que esse acesso realmente ocorreu"** [...] 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) (grifos nossos)

As condutas previstas como crime nos artigos destacados têm o condão de proteger a dignidade e a liberdade sexual de crianças e adolescentes. São crimes dolosos, exigindo-se o dano potencial, não necessitando de dano material efetivo para serem consumados (NUCCI, 2016).

Com a popularização de aplicativos como *whatsapp* a conduta do artigo 241-B se tornou mais frequente. Com a inclusão dos tipos penais estabelecidos nesse artigo, torna-se mais fácil a punição do agente que mantêm, em seu poder, imagens de menores de 18 anos envolvidos em pornografia. O objeto material é a foto, o vídeo ou a imagem contendo pornografia ou sexo explícito envolvendo criança ou adolescente, enquanto o objeto jurídico é a proteção à formação moral da criança ou adolescente (NUCCI, 2016).

Nas palavras de Guilherme de Souza Nucci (2016, p. 785):

> A maneira pela qual o autor do crime adquire, possui ou armazena o material é livre, valendo-se o tipo da expressão “por qualquer meio”. Comumente, com o avanço da tecnologia e da difusão dos computadores pessoais, dá-se a obtenção de extenso número de fotos e vídeos pela Internet, guardando-se o material no disco rígido do computador, em disquetes, DVDs, CDs, *pen drives*, entre outros.

CAPÍTULO III – CRIMES VIRTUAIS NA LEGISLAÇÃO

Serão analisados neste capítulo a legislação existente acerca dos crimes virtuais bem como os projetos de lei em tramitação na Câmara e no Senado bem como medidas legislativas em fase de concepção e anteprojeto.

Observa-se que destarte tenha ocorrido no passado recente significativos avanços acerca da temática, ainda há muito a se fazer no sentido do aperfeiçoamento normativo em razão da temática se tratar de novidade tanto aos olhos da sociedade quanto ao legislativo, bem como à constante mutação das práticas delitivas nos ambientes virtuais além de a legislação recente estar em fase de teste prático.

O dinâmico ambiente virtual e a constante ampliação do acesso aos ambientes virtuais impõe à legislação e aos legisladores o considerável desafio de contemplar as práticas delitivas cometidas no ambiente virtual, notadamente heterogêneas e mutáveis, em tipos penais rígidos com alcance razoável e de assertividade prática.

3.1 Legislação vigente

Em breve retrospectiva histórica cumpre registrar que o desenvolvimento e a ampliação do acesso à tecnologia, e em sentido estrito às redes sociais onde os indivíduos passaram a ser sujeitos ativos na produção de conteúdo e de atuação nas redes é questão recente. (BARBOSA et al, 2014)

Tendo em vista a atualidade de grande parte das atuações e interações sociais nas redes é compreensível que a legislação ainda esteja em processo de atualização, neste sentido num passado recente os crimes cometidos no ambiente virtual eram tipificados por analogia em tipos penais comuns, cuja conduta perpetrada no ambiente virtual ocorresse de modo análogo à conduta enquadrada no tipo comum. (TAVARES, 2012)

Desafia a legislação atual as dificuldades que têm os órgãos judiciais e investigativos em identificar os sujeitos ativos dos crimes, o que se deve às nuances tecnológicas que facilitam a fuga e a ocultação da autoria, isso ocorre sobretudo em razão do “grande número de usuários dessa nova tecnologia e a possibilidade de colocar informações inverídicas sobre seu endereço de IP”. (SIQUEIRA, 2017, pág. 122)

Quanto a identificação e responsabilização pelos delitos, Siqueira (2017) aponta:

> Seria possível a identificação do criminoso obtendo o seu endereço de IP, login e senha do aparelho utilizado para a prática do crime, porém, os criminosos utilizam endereços falsos, dificultando o trabalho investigativo dos policiais. (SIQUEIRA, 2017, pág.122)

No Brasil a Lei 9.609 de 19 de fevereiro de 1998, que substituiu a Lei 7.646 de 18 de Dezembro de 1987, trouxe à legislação as considerações inovadoras acerca da tecnologia virtual ao dispor sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País e outras providências.

A Lei 9.609/1998 apresenta conceituação de programa de computador nos seguintes termos:

> Art. 1º Programa de computador é a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento da informação, dispositivos, instrumentos ou equipamentos periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de modo e para fins determinados. (BRASIL, 1998, *online*)

A mencionada legislação dispôs ainda acerca de proteção aos direitos de autoria e do registro de programas virtuais, de garantias aos usuários de programas

de computador, de contratos de licença de uso, comercialização e transferência de tecnologia, e ainda, dispôs sobre “infrações e penalidades”, em seu quinto capítulo, naquilo que pode ser considerado como primeira tipificação notadamente voltada à crimes virtuais.

O tipo penal previsto pela Lei 9.609/1998 apresenta a seguinte redação:

> Art. 12. Violar direitos de autor de programa de computador:
> Pena - Detenção de seis meses a dois anos ou multa.
> § 1º Se a violação consistir na reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente:
> Pena - Reclusão de um a quatro anos e multa.
> § 2º Na mesma pena do parágrafo anterior incorre quem vende, expõe à venda, introduz no País, adquire, oculta ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral.

Complementarmente, ainda no capítulo voltado às infrações e penalidades a Lei apresentou nuances aplicáveis à investigação do delito, diligências e outras questões processuais, possibilidade de propositura de demandas cíveis e confidencialidade das questões.

Ainda, a Lei 9.610/1998 é complementar à Lei 9.609/1998 ao dedicar-se extensamente à questão dos direitos autorais, portanto, a primeira aplica-se à tudo que for omisso na segunda, ainda que se trate se questão envolta à tecnologia. (SIQUEIRA, 2017).

Mais adiante, em razão a necessidade eminente do aperfeiçoamento da legislação envolta aos crimes cibernéticos ou virtuais, o Congresso Nacional aprovou no ano de 2012, a Lei 12.737 de 30 de novembro de 2012, que dispôs acerca da tipificação criminal de delitos informáticos e alterou o Código Penal. (BARBOSA et al, 2014).

A inovação legislativa trazida pela Lei 12.737/2012, introduziu no Código Penal o tipo nominado “Invasão de dispositivo informático”, art. 154-A do Código Penal Brasileiro, caracterizado pela conduta assim descrita:

> 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;
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.” (BRASIL, 2012, online)

Ao tipo penal retro mencionado foi atribuída pena de detenção de três meses a um ano mais multa, há ainda causa de aumento de pena em um sexto “se da invasão resultar prejuízo econômico” (BRASIL, 2012).

Ainda, o parágrafo 3º do retro mencionado tipo penal estabelece agravante quando da invasão se consubstancia “obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas” (BRASIL, 2012, *online*), hipótese em que o indivíduo poderá ser submetido à pena de reclusão de seis meses à dois anos, e, no caso de prática contra Presidente, Governador, Prefeito, Presidente do Supremo Tribunal Federal, Câmara dos Deputados, Senado Federal, Assembleias Legislativas e Câmaras Municipais, ou dirigente máximo da administração direta ou indireta da União, Estados e Municípios fica a pena aumentada em um terço.

Houve ainda a atualização dos artigos 266 e 298 do Código Penal, pela Lei 12.737/2012, que versão respectivamente sobre “Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública” e “Falsificação de documento particular”, para que em relação ao primeiro passasse a constar a conduta equiparada ao tipo penal assim descrita: “Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento” e em relação ao segundo fosse equiparado o cartão de crédito e de débito ao “documento particular” mencionado no artigo. (BRASIL, 2012, online)

Cumpre registrar que a polêmica envolta à tramitação da matéria da Lei 12.737/2012 fez com que projetos de lei que versavam acerca da mesma temática

tramitassem por mais de 10 anos sem produção legislativa final o que se dava em razão da dificuldade de compreensão e finalização da legislação. (SIQUEIRA, 2017).

Em termos sociológicos e históricos foi fator determinante à aprovação da Lei 12.737/2012 a ocorrência de escândalos reiterados de vazamento de fotos íntimas que passaram a afetar um número cada vez maior de pessoas, fazendo com que houvesse uma pressão social cada vez maior sobre o legislativo para que houvesse o endurecimento das penas envoltas à este tipo de delito. (BARBOSA et al, 2014).

Mais notadamente, antecedeu a aprovação da Lei 12.737/2012 o vazamento de fotos íntimas da atriz Carolina Dieckmann, o que impulsionou a visibilidade sobre o tema, fez aumentar a já crescente pressão popular e fez com que a norma ficasse conhecida popularmente como “Lei Carolina Dieckmann” (SIQUEIRA, 2017).

> A lei 12.737/12 ficou popularmente conhecida como lei Carolina Dieckmann em virtude do episódio com a atriz, que em maio de 2012, teve seu computador invadido por criminosos que divulgaram 36 fotos íntimas da mesma, causando um grande transtorno e constrangimento à vítima. (SIQUEIRA, 2017, p.126)

Todavia, ainda que a Lei 12.737 tenha representado uma significativa inovação normativa relacionada à prática criminosa virtual, a mesma se mostrou insuficiente o que forçou aprovação de novas normas como o Marco Civil da Internet, Lei 12.965/014. (TOMASEVICIUS FILHO, 2016)

Siqueira (2017) aponta a intenção da aprovação do Marco Civil da Internet nos seguintes termos:

> A lei do Marco Civil foi criada para suprir as lacunas no sistema jurídico em relação aos crimes virtuais, num primeiro momento tratando dos fundamentos, conceitos para sua interpretação e objetivos que o norteiam, além de enumerar os direitos dos usuários, tratar de assunto polêmicos como por exemplo a solicitação de histórico de registros, a atuação do poder público perante os crimes virtuais e por último garante o exercício do direito do cidadão de usufruir da internet de modo individual e coletivo estando devidamente protegido. (SIQUEIRA, 2017, p. 126)

Embora as considerações acerca da pressão popular pela aprovação de Lei que enrijecesse as penas para criminosos virtuais que expusessem a vida de terceiros indivíduos e a necessidade aprovação de uma espécie de Código que norteasse todas as relações na rede como premissas de aprovação do Marco Civil da internet sejam verdadeiras, é sintomático que a aprovação da norma tenha se dado com bastante pressão do Executivo sobre o Legislativo, sobretudo após a publicação de vários casos de espionagem de chefes de estado e líderes globais, inclusive do Brasil. (SILVA; BEZERRA; SANTOS; 2013).

Neste diapasão surge o Marco Civil da Internet, Lei 12.965 de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil bem como diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios nesta matéria. (BRASIL, 2014*, online*)

Em seus artigos iniciais a Lei 12.965/2014 aponta os fundamentos, princípios, objetivos bem como conceitos básicos aplicáveis à matéria.

Cumpre destacar os princípios que são mencionados em seu art. 3º:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
> II - proteção da privacidade;
> III - proteção dos dados pessoais, na forma da lei;
> IV - preservação e garantia da neutralidade de rede;
> V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
> VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
> VII - preservação da natureza participativa da rede;
> VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei. (BRASIL, 2014, *online*)

Dentre os conceitos apontados no art. 5º e respectivos incisos estão os de internet, terminal, endereço de protocolo de internet (endereço IP), conexão à internet, administrador de sistema autônomo, registro de conexão, aplicações de internet e registros de acesso a aplicações de internet. (BRASIL, 2014, *online*)

Na sequência dos princípios elencados no art.5º o Marco Civil da Internet apontam os direitos e garantias dos usuários (Capítulo II), provisão de conexão e de aplicações de internet (Capítulo III) que compreende Neutralidade de Rede (Seção I), Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas (Seção II), Guarda de Registros de Conexão (Subseção I), Guarda de Registros de Acesso a Aplicações de Internet na Provisão de Conexão (Subseção II) e Guarda de Registros de Acesso a Aplicações de Internet na Provisão de Aplicações (Subseção III), Responsabilidade por Danos Decorrentes de Conteúdo Gerado por Terceiros (Seção III) e Requisição Judicial de Registros (Seção IV) e, por fim, estabelece as diretrizes para a Atuação do Poder Público.

Aspecto marcante da Lei 12.965/2014 é o contraste entre seu objetivo normatizador e de ofertar maior segurança e respaldo legal à internet bem como as relações desenvolvidas em seu âmbito e a clara e perceptível intenção do legislador de manter afastada qualquer impressão de censura e intervenção Estatal às relações daquele ambiente, neste sentido o legislador fez questão de mencionar direitos constitucionalmente garantidos como garantia da liberdade de expressão, comunicação e manifestação do pensamento. (TOMASEVICIUS FILHO, 2016)

Destarte tenha havido o esforço legislativo para normatização das relações sociais desenvolvidas no âmbito da internet há críticas à legislação em razão de suas lacunas sobretudo em razão de que as normas ali contidas “não abrangem todo o campo de atuação dos criminosos da internet, ficando ainda algumas lacunas supridas por outras legislações, como por exemplo, a regulamentação usada para as compras feitas pela internet” (SIQUEIRA, 2017, p.126) entre outras circunstâncias eventualmente utilizadas por criminosos para perpetração de suas práticas delitivas.

Todavia, no que diz respeito ao compêndio normativo voltado ao combate das ilicitudes cíveis e criminais houve por parte da Lei 12.965/2014 preocupação, portanto, atenção e regulamentação.

> Outro aspecto que recebeu grande atenção do legislador foi o combate às ilicitudes civil e criminal praticadas sob o manto da privacidade na internet. Se, do ponto de vista social, a internet proporciona contatos interpessoais anônimos, do ponto de vista

> técnico, toda ação realizada pela internet é passível de registro pelos provedores de acesso e de conteúdo, o que torna possível a identificação dos usuários. (TOMASEVICIUS FILHO, 2016, p. 274)

Neste sentido o art. 22 do Marco Civil da Internet busca ofertar ao indivíduo subsídio normativo hábil a pedido de guarda de informações que possam servir de prova em processo judicial. (BRASIL, 2014, *online*)

Além do Marco Civil da Internet, Lei 12.965/2014, da Lei Carolina Dieckmann, Lei 12.737/2012 e das Leis 9.609 de 19 de fevereiro de 1998 e 9.610 de 19 de fevereiro de 1998, houve ainda inovação normativa no Estatuto da Criança e do Adolescente ao introduzir o Art. 241-A que dispôs sobre a oferta, troca, disponibilização, transmissão, distribuição e publicação, ainda que por meios virtuais, de fotografia, vídeo ou outro registro que contenha conteúdo de sexo explícito ou pornográfica envolvendo criança ou adolescente. (SIQUEIRA, 2017)

3.2 Projetos de lei

As sociedades contemporâneas são caracterizadas pela sua acelerada dinâmica de inovação e adaptação social, os fluxos tecnológicos e o desenvolvimento de novos mecanismos de convivência trazem à tona todos os dias novas formas de convívio e interação entre os indivíduos, a consequência prática desta realidade é a permanente necessidade de avaliação e aprimoramento legislativo.

Assim como em todos os vetores da sociedade, em sentido estrito, o convívio humano na rede mundial de computadores sofre diuturnamente alterações, sobretudo em razão da criação de novos aplicativos, novos dispositivos e novas funções já existentes, daí o enquadramento das condutas perpetradas nestes meios perante a legislação já existente é desafio cotidiano das forças investigativas e do poder judiciário, por sua vez estes elementos constantemente se reportam ao legislativo para aprimoramento do conjunto normativo. (TOMASEVICIUS FILHO, 2016)

> O crescente desenvolvimento de tecnologias de informação e o uso massificado da Internet têm facilitado o acesso das pessoas a mais conhecimentos e a processos mais rápidos de tomada de decisões. De outro lado, a informatização tem sido utilizada para fins

> delituosos, geralmente denominados de “crimes virtuais” ou “cibernéticos”. (SENADO FEDERAL, 2012)

Esta perspectiva tem impulsionado as casas legislativas pátrias à desenvolverem e se debruçarem cada vez mais sobre projetos de lei afins.

> Seria um grande avanço se fosse elaborado um novo código especificando crimes virtuais, adentrando em todos seus aspectos e criando uma área policial especializada no assunto, com nível de conhecimento em computadores avançado para que possa se resolver o conflito de forma mais habilidosa, facilitando o encontro do criminoso virtual. Nota-se que o sistema jurídico não está totalmente preparado para coibir tais condutas, portanto se as normas que tratam de determinado assunto fossem, talvez, aperfeiçoadas, poderíamos ter a esperança de que os índices de criminalidade virtual reduziriam devido a eficácia de suas respectivas leis. (SIQUEIRA, 2017, p. 128)

Atentas à este fenômeno social as casas legislativas federais brasileiras, Senado e Câmara, e nesta perspectiva grande parte de seus legisladores têm dedicado esforços e trabalhos à produção legislativa com a temática dos crimes virtuais.

No Senado Federal a Revista “Em Pauta - O processo legislativo do Senado à Serviço da Cidadania” Ano V - nº 235 - Brasília, 10 de setembro de 2012, aponta a tramitação de vários projetos de lei com matérias correlatas, em destaque o Projeto de Lei do Senado (PLS) nº 427, de 2011, apresentado pelo Senador Jorge Viana (PT-AC), o Projeto de Lei da Câmara (PLC) nº 35, de 2012, de autoria do Deputado Federal Paulo Teixeira (PT-SP), atualmente pronto para votação em Plenário no Senado Federal após ter sido aprovado nas comissões temáticas desta casa e ainda o PL do SENADO nº 236, de 2012, de autoria do Senador José Sarney (PMDB-AP).

O Projeto de Lei do Senado (PLS) nº 427, de 2011, encontra-se aguardando relatório para que possa ser apreciado pela Comissão de Constituição e Justiça desta casa, e busca alteração no Código Penal para inserir o tipo penal de “crime de atentado contra a segurança de meio ou serviço de comunicação informatizado”. (SENADO FEDERAL, 2012)

Já o Projeto de Lei da Câmara (PLC) nº 35, de 2012 já aprovado naquela casa, versa acerca de tipificação criminal de vários delitos informáticos à serem

incluídos no Código Penal, este projeto aguarda deliberação do plenário do Senado Federal já tendo sido aprovado nas comissões temáticas. (SENADO FEDERAL, 2012)

Na Câmara dos Deputados as iniciativas dos legisladores se deram em clima extremamente construtivo após acalorados debates que ocorreram no âmbito da CPI dos Crimes cibernéticos instituída no ano de 2016. (CÂMARA DOS DEPUTADOS, 2016)

Dentre as propostas de Lei decorrentes da mencionada CPI estão, Projeto de Lei da Câmara que estabelece “a perda dos instrumentos do crime doloso destinados à prática reiterada de crimes”, notadamente computadores, celulares e dispositivos eletrônicos utilizados nos crimes virtuais. Outra propositura têm o intuito de ampliar a abrangência do crime de invasão de dispositivo informático. (CÂMARA DOS DEPUTADOS, 2016)

Ainda, outra proposta pretende incluir os crimes praticados contra ou mediante computador, conectado ou não a rede, dispositivo de comunicação ou sistema informatizado ou de telecomunicação no rol das infrações de repercussão interestadual ou internacional que exigem repressão uniforme. (CÂMARA DOS DEPUTADOS, 2016)

Ainda, entre as propostas já apontadas o Relatório da CPI dos Crimes Cibernéticos propôs alteração do Marco Civil da Internet, Lei no 12.965, de 23 de abril de 2014, determinando a indisponibilidade de cópia idêntica de conteúdo reconhecido como infringente, sem a necessidade de nova ordem judicial e nova norma que possibilite o bloqueio a aplicações de internet por ordem judicial, nos casos em que especifica. (CÂMARA DOS DEPUTADOS, 2016)

Todas as propostas legislativas encontram-se em tramitação nas comissões temáticas junto à outras inúmeras propostas de Projetos de Lei. É notável o esforço recente da produção legislativas nas duas casas do legislativo federal, todavia as várias iniciativas encontram dificuldades de aprovação devido à questões normais do trâmite legislativo entre as quais a sobrecarga de projetos em tramitação e as questões políticas naturais da tramitação.

CONCLUSÃO

Entendendo que o tema abordado é de extrema relevância para a legislação brasileira, uma vez que a globalização e a inserção da tecnologia estão totalmente presentes no meio profissional e pessoal das pessoas.

Compreendendo que já existem leis previstas tratando e amparando crimes cometidos pelo meio virtual, porém a fragilidade dessas mesmas leis não podem se manter tendo em vista a grande demanda de processos que clamam um posicionamento eficaz para suas tipificações.

Como acadêmica do Curso de Direito do Centro Universitário de Anápolis – UniEVANGÉLICA, após entender e compreender por meio de diversas leituras e reflexões críticas e analíticas, afirmo que a temática precisa ser evidenciada e tratada de forma emergente considerando os projetos de lei, tendo em vista que este é o caminho para que tais projetos se tornem definitivamente leis promulgadas e publicadas para amparar a sociedade como todo.

REFERÊNCIAS BIBLIOGRÁFICAS

ALVES, Fernando Antonio. O Ativismo Popular nas Redes Sociais Pela Internet e o Marco Constitucional da Multidão, no Estado Democrático de Direito: uma discussão prévia sobre participação popular e liberdade de expressão no Brasil, pós-manifestações de junho de 2013. **Revista Direitos Emergentes da Sociedade Global**, Santa Maria, v. 3, n. 1, p. 16-49, jan.jun/2014.

BARBOSA, Adriana Silva et al. **Relações Humanas e Privacidade na Internet: implicações Bioéticas.** Rev. Bioética y Derecho, Barcelona, n. 30, p. 109-124, 2014 . Disponível em <http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1886-58872014000100008&lng=es&nrm=iso>. Acesso em: 01 mar. 2018

BARROSO, LUÍS ROBERTO. **Estado, Sociedade e Direito: Diagnósticos E Propostas para o Brasil**. In: XXII Conferência Nacional dos Advogados. Rio de Janeiro, 2014.

_____. Colisão entre Liberdade de Expressão e Direitos da Personalidade. Critérios de Ponderação. Interpretação Constitucionalmente Adequada do Código Civil e da Lei de Imprensa. **Revista de Direito Administrativo**, Rio de Janeiro, n. 235, p. 1-36, jan.mar/2004.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012.** Dispõe sobre a Tipificação Criminal de Delitos Informáticos; Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm> Acesso em: 20 Nov. 2017.

_____. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece Princípios, Garantias, Direitos e Deveres para o Uso da Internet no Brasil. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em: 20 Nov. 2017.

_____. **Câmara dos Deputados – CPI dos Crimes Cibernéticos, de 04 de maio de 2016.** Disponível em: < http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra;jsessionid=214D61B364D3F74027CAB7F56C3E0C39.proposicoesWeb2?codteor=1455189&filename=REL+4/2016+CPICIBER+%3D%3E+RCP+10/2015> Acesso em 21 Nov. 2017.

_____. **Decreto-Lei nº 2.848 de 7 de dezembro de 1940.** Código Penal Brasileiro**.** Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm> Acesso em: 24 nov. 2017.

_____. **Lei nº 8.069 de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente. Disponível em: <http://www.planalto.gov.br/Ccivil_03/leis/L8069.htm>. Acesso em: 07 mar. 2018.

_____. **Lei 9.609 de 19 de fevereiro de 1998.** Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/l9609.htm> Acesso em: 07 mar. 2018.

_____. Senado Federal. **"O Senado e os Crimes cibernéticos"**. Rev. Em Pauta. Ano V - nº 235 - Brasília, 10 de setembro de 2012.

_____. Tribunal Regional Federal da 3ª Região. Escola de Magistrados **Investigação e prova nos crimes cibernéticos**. São Paulo: EMAG, 2017. 352p. (Cadernos de estudos ; 1)

CÂMARA DOS DEPUTADOS. Deputada Mariana Carvalho; Deputado Esperidião Amin; Deputado Sandro Alex; Deputado Rafael Motta; Deputado Daniel Coelho; e Deputado Rodrigo Martins. **Câmara dos Deputados CPI – Crimes Cibernéticos – Relatório Final.** Brasília; 04 de maio de 2016.

CAPEZ, Fernando Prado. **Código Penal Comentado.** São Paulo: Saraiva, 2016.

CERT.COM. **Incidentes Reportados ao CERT.br Janeiro a Dezembro de 2016.** Disponível em: <https://www.cert.br/stats/incidentes/2016-jan-dec/tipos-ataque.html>. Acesso em: 23 Nov. 2017.

COELHO, Ivana Pereira; BRANCO, Sérgio. Humor e Ódio na Internet. **Cadernos Adenauer XV,** Rio de Janeiro, s/n, out/2016. Disponível em: < http://www.kas.de/wf/doc/20595-1442-5-30.pdf> Acesso em 23 nov. 2017.

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

CUNHA, Rogério Sanches. **Manual de Direito Penal: Parte Geral.** Salvador: Juspodivm, 2014.

_____. **Manual de Direito Penal: Parte Especial.** Salvador: Juspodivm, 2014.

FIORILLO, Celso Antonio Pacheco; CONTE, Christiany Pegorari. **Crimes no Meio Ambiente Digital.** 2. ed. São Paulo: Saraiva, 2016.

GLOBO.COM. **Maria Júlia Coutinho, a Maju, é vítima de comentários racistas no Facebook.** Disponível em: < http://g1.globo.com/pop-arte/noticia/2015/07/maria-julia-coutinho-maju-e-vitima-de-racismo-no-facebook.html> Acesso em 01 mar. 2018.

_____. **Deep Web – O que é e Como Funciona.** 2016. Disponível em: <http://g1.globo.com/tecnologia/blog/seguranca-digital/post/deep-web-o-que-e-e-como-funciona-g1-explica.html>. Acesso em 09 mar. 2018.

_____. **Torcedor do Palmeiras reclama de homofobia nos estádios e é ofendido em redes sociais.** Disponível em: <https://globoesporte.globo.com/futebol/times/palmeiras/noticia/torcedor-do-palmeiras-reclama-de-homofobia-nos-estadios-e-e-ofendido-em-redes-sociais.ghtml>. Acesso em 09 mar. 2018.

JAISHANKAR, Karuppannan. Establishing a Theory of Cyber Crimes. **International Journal of Cyber Criminology,** v. 1, p. 7-9, 2007. Disponível em: <http://www.cybercrimejournal.com/Editoriaijccjuly.pdf>. Acesso em: 21 Nov. 2017.

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

NUCCI, Guilherme de Souza. **Manual do Direito Penal.** 7. ed. São Paulo: Revista dos Tribunais, 2011.

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

ODALIA, Nilo. **A Liberdade Como Meta Coletiva**. In: PINSKY, Jaime; PINSKY, Carla Bassanezi. História da Cidadania. São Paulo: Contexto, 2013.

PANNAIN, Camila Nunes; PEZZELLA, Maria Cristina. Liberdade de Expressão e Hate Speech na Sociedade da Informação. **Revista Direitos Emergentes da Sociedade Global**, Santa Maria, v. 4, n.1, p. 72-87, 2015.

PINHEIRO, Patrícia Peck. Regulamentação da Web. **Cadernos Adenauer XV,** Rio de Janeiro, n. 4, p. 33-44, out/2014. Disponível em: < http://www.kas.de/wf/doc/16471-1442-5-30.pdf> Acesso em: 21 Nov. 2017.

SARMENTO, Daniel. **A Liberdade de Expressão e o Problema do *Hate Speech***. S/D. Disponível em: <http://www.dsarmento.adv.br/content/3-publicacoes/19-a-liberdade-de-expressao-e-o-problema-do-hate-speech/a-liberdade-de-expressao-e-o-problema-do-hate-speech-daniel-sarmento.pdf> Acesso em: 01 mar. 2018.

SIQUEIRA, Marcela Scheuer et al. **Crimes virtuais e a legislação brasileira. (Re)Pensando o Direito** – Rev. do Curso de Graduação em Direito da Faculdade CNEC Santo Ângelo. v. 7, n. 13 (2017). Disponível em http://local.cnecsan.edu.br/revista/index.php/direito/article/view/468. Acesso em: 01 mar. 2018.

SILVA, Aurélia Carla Queiroga; BEZERRA, Margaret Darling; SANTOS, Wallaz Tomaz**. Relações Jurídicas Virtuais: Análise de Crimes Cometidos com o Uso da Internet.** Revista Cesumar Ciências Humanas e Sociais Aplicadas, v.21, n.1, p. 7-28, jan./jun. 2016.

SYDOW, Spencer Toth. **Delitos informáticos próprios: uma abordagem sob a perspectiva vitimodogmática.** 2009. Dissertação (Mestrado em Direito Penal) - Faculdade de Direito - Universidade de São Paulo, São Paulo, 2009. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/delitos_informaticos_proprios_uma_abordagem_sob_a_perspectiva_vitimodogmatica.pdf>. Acesso em: 20 Nov. 2017.

_____. **Delitos informáticos e suas vítimas**. 2. ed. São Paulo: Saraiva, 2014.

TAVARES, José de Farias. **Comentários ao Estatuto da Criança e do Adolescente.** Rio de Janeiro: Forense, 2012.

TOMASEVICIUS FILHO, Eduardo. **Marco Civil da Internet: uma lei sem conteúdo normativo.** Estud. av., São Paulo , v. 30, n. 86, p. 269-285, Abr. 2016. Disponível em <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-40142016000100269&lng=en&nrm=iso>. Acesso em: 01 mar. 2018

TRENTIN, Taise Rabelo Dutra; TRENTIN, Sandro Seixas. Internet: Publicações Ofensivas em Redes Sociais e o Direito à Indenização por Danos Morais. **Revista Direitos Emergentes da Sociedade Global**, Santa Maria, n. 1, p. 79-93, jan.jun/2012.

WIGERFELT, Anders S.; WIGERFELT, Berit. DAHLSTRAND, Karl Johan. Online Hate Crime – Social Norms And The Legal System. **Revista Quaestio Iuris.** v. 8, n. 3, Rio de Janeiro, p. 1859-1878, 2015. Disponível em: <http://www.e-publicacoes.uerj.br/index.php/quaestioiuris/article/view/19383/14175> Acesso em 20 Nov. 2017.