PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS

ESCOLA DE DIREITO E RELAÇÕES INTERNACIONAIS

NÚCLEO DE PRÁTICA JURÍDICA

COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO

ARTIGO CIENTÍFICO

A INEFICÁCIA DA PRESTAÇÃO JURISDICIONAL NO COMBATE AOS CRIMES VIRTUAIS:

A DIFICULDADE DA PERSECUÇÃO PENAL

ORIENTANDA: CLARA AUGUSTA SILVA BEZERRA

ORIENTADOR: PROF. GERMANO CAMPOS SILVA

GOIÂNIA

2020

CLARA AUGUSTA SILVA BEZERRA

A INEFICÁCIA DA PRESTAÇÃO JURISDICIONAL NO COMBATE AOS CRIMES VIRTUAIS:

A DIFICULDADE DA PERSECUÇÃO PENAL

Artigo Científico apresentado à disciplina Trabalho de Curso II, da Escola de Direito e Relações Internacionais, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUCGOIÁS).

Prof. Orientador: Germano Campos Silva

GOIÂNIA

2020

CLARA AUGUSTA SILVA BEZERRA

CLARA AUGUSTA SILVA BEZERRA

A INEFICÁCIA DA PRESTAÇÃO JURISDICIONAL NO COMBATE AOS CRIMES VIRTUAIS

A DIFICULDADE DA PERSECUÇÃO PENAL

Data da Defesa: ____ de _____ de _____

BANCA EXAMINADORA

_____
___

Orientador: Prof. Germano Campos Silva

Nota

_____
___

Examinador Convidado: Prof. Rogério Rodrigues de Paula Nota

SUMÁRIO

A INEFICÁCIA DA PRESTAÇÃO JURISDICIONAL NO COMBATE AOS CRIMES VIRTUAIS

A DIFICULDADE DA PERSECUÇÃO PENAL

Clara Augusta Silva Bezerra

AGRADECIMENTOS

Gostaria de agradecer primeiramente a Deus, por ter me concedido saúde e capacidade para chegar até aqui durante esta caminha de 5 anos de curso, a minha família como um todo, pelos momentos de apoio e incentivo dados nas horas boas e difíceis que tive durante todos os momentos, mas em especial ao meu pai , por nunca ter poupado esforços para me apoiar e ajudar a concretizar todos os meus sonhos. Aos amigos, que conheci nessa jornada e que tornaram essa caminhada mais leve e agradável. E não menos importante ao meu orientador Germano Campos Silva, que auxiliou o planejamento deste trabalho de curso tão importante acrescentando positivamente academicamente. Meus mais sinceros agradecimentos e gratidão a todos.

RESUMO

Este trabalho trata-se da “omissão” legislativa no combate aos crimes cibernéticos e como isso pode influenciar negativamente na vida dos afetados. Tendo assim uma enorme importância de discussão por tratar da dignidade da pessoa humana que esta sendo violada com os crimes cibernéticos, seja de qualquer forma, gerando danos morais ou materiais. Por isso a necessidade de discutir se as leis existentes bastam para inibir e punir o delito ou se deve ter uma melhora legislativa que acompanhe as necessidades atuais de delitos cometidos por meio da internet. Para isso, foram utilizados livros abordando o tema, pesquisas, artigos e reportagens sobre o delito, para que pudesse ter um maior domínio e conhecimento acerca do tema. O estudo deixa a análise de que a legislação possui falhas em relação a punição dos crimes cibernéticos, devendo assim criar leis e sansões de acordo com que a sociedade precisa e vai evoluindo.

Palavras-chave: Redes, impunidade, extorsão, intimidade e dano.

INTRODUÇÃO

Os crimes cibernéticos tiveram início com o advento das tecnologias e redes de conexão de internet. Este veio em crescente até os dias atuais e ocorre de diversas formas, afetando os próprios computadores que são uma forma de instrumento da prática do delito quanto pessoas que podem ser lesadas moralmente e financeiramente. Teve maior visibilidade com o ocorrido da Carolina Dieckmann, pois a mesma é atriz global e possui uma grande influencia. Dentre o tema a ser trabalhado é analisado a omissão legislativa acerca do crime cibernético praticado. Este deve ser punido com penas mais expressivas, que não permitem o benefício do SURSIS. Por muitas vezes os danos causados derivados do crime cibernético podem ser irreparáveis, como nos casos de divulgação de fotos íntimas, em que a pessoa sofre um grande constrangimento e abalos psicológicos. Desta forma, pode-se analisar que há uma leveza nas penas quando se trata de punir este crime a altura.

I- CONCEITUANDO OS CRIMES VIRTUAIS

Com o surgimento da internet a humanidade se tornou globalizada, e com isso houve várias alterações na comunicação, na exposição de fatos e notícias entre outras situações. O Direito vem como forma de instrumento para regularizar os fatos jurídicos típicos relevantes que podem ocorrer com o mau uso da plataforma digital, como veremos a seguir. Com isso, foi necessária ao longo do tempo a regulamentação para resolver e tentar impedir certos tipos de crimes cibernéticos.

Primeiramente deve-se salientar do que vem a ser o crime cibernético, que é toda atividade criminosa vinda por meio de computadores ou aparelhos eletrônicos conectados à rede de internet com o intuito de causar algum dano a outrem. Outro conceito dado aos crimes virtuais pode ser o de Ivette Senise Ferreira (2005, p.) em seu livro “Direito & Internet: Aspectos Jurídicos Relevantes. 2 ed**.”:**

> Atos dirigidos contra um sistema de informática, tendo como subespécies atos contra o computador e atos contra os dados ou programas de computador. Atos cometidos por intermédio de um sistema de informática e dentro deles incluídos infrações contra o patrimônio; as infrações contra a liberdade individual e as infrações contra a propriedade imaterial.

Na década de 1990, com a explosão do uso dos meios, seguido pela globalização no setor da economia, surgiu uma nova categoria, de crimes chamados crimes virtuais informáticos ou crimes eletrônicos. Sabemos que são grandes e diversificadas as formas de se cometer crimes pelo instrumento da internet, por essa razão houve a necessidade de avançar em questão de ter um dispositivo legal, pois havia necessidade de garantir a segurança dos usuários.

1.1 LEI CAROLINA DIECKMANN

Antes de adentrar na análise da lei nº 12.737/2012, é importante destacar o art. 5º, X, da C.F: “São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente da sua violação”. A relação intrínseca deste artigo com o caso em questão é exatamente a intimidade violada, pois a atriz teve suas fotos roubadas por hackers sem ter poder de escolha ou não de divulgação das fotos íntimas. Na constituição está bem claro o que é assegurado e enquadra perfeitamente na lei Carolina Dieckmann. No crime virtual em estudo há violação da intimidade com o ato de pegar fotos íntimas que não são da pessoa; há violação na honra e moral também, pois espalha algo íntimo da vida privada do indivíduo que não deveria estar público, agravando mais os danos quando é pedido recompensa pelas suas próprias fotos. Desta forma, o texto constitucional presente no Art.5º da Constituição Federal está tipificando a conduta como ilícita e deixando claro que estas categorias são asseguradas, e caso violado devem ser punidas.

Um marco que impulsionou a edição desta lei foi o caso da atriz global Carolina Dieckmann, diante da reportagem do G1 (2021) que descreve como ocorreu todo o delito. Em março do ano de 2012, Carolina começou a ser chantageada por criminosos, a fazer um pagamento na quantia de dez mil reais (R$ 10.000,00), para que suas fotos, de teor íntimo, não fossem expostas na web. A atriz revela que foram feitas ligações para sua casa e até mesmo ameaças em seus sites pessoais na internet, tudo com o intuito dos criminosos obterem vantagens financeiras em troca da “privacidade” violada da atriz. Com isso, usavam desses artifícios de chantagem para chegar ao fim desejado.

Carolina Dieckmann não cedeu a essas chantagens, foi até uma delegacia e registrou queixa, então foi arquitetado um plano em conjunto com a polícia para conseguir pegar os criminosos em flagrante, plano esse posteriormente frustrado, por conseguinte trinta e seis fotos íntimas da atriz, em situações de nudez e em situações de intimidade que foram expostas na internet, juntamente com uma foto de seu filho menor, que na época tinha só 04 anos. Adiante a polícia conseguiu essas fotos, mediante uma invasão ao e-mail pessoal da atriz.

De acordo com a Jornalista Patrícia Poeta:

> Depois do ocorrido em momentos mais de calma, relata em uma entrevista para o Jornal Nacional diante da apresentadora Patrícia Poeta, neste momento Carolina Dickemann discorre “que foram momentos de desespero

> e euforia“ acho que agora vou poder voltar a viver, porque minha vida estava em suspenso “(POETA, 2010, p.1)”.

Foi um alvoroço, um escândalo, um caso de grande repercussão, tendo em vista que a atriz nunca tinha sido exposta de tal forma na mídia, então começou a ter uma pressão pelo Congresso Nacional, por conta de não ter sequer alguma tipificação legal e sim só um projeto de Lei – PL n° 2793/2011 que não tinha ainda sido analisado.

Para muitas especialistas não ter Lei própria ou algum meio de inibir os crimes informáticos no ano de 2012, era um atraso muito grande para legislação brasileira. E quando se deparou com esse caso que teve uma repercussão nacional, a ação promovida pela atriz, fez com que os criminosos respondessem por legislação já tipificada, no Código Penal sendo por extorsão, furto e difamação.

Esse acontecimento em 2012 foi um propulsor para que mudanças fossem feitas e medidas emergenciais fossem realizadas, porem o debate sobre ter uma legislação específica já vinha sido discutida há tempo anterior, por exemplo, no ano de 2011 houve ataques de hackers a sites de serviços do governo brasileiro, por conta desse crime e outros que vinham tomando tão habitual no Brasil, já havia sendo tramitado um pedido de regulamentação de uma lei especifica.

Somente com os vazamentos das imagens intimas da atriz global e o fato de terem sido divulgadas nas mídias sócias e tomado uma proporção nacional, que o Congresso sentiu se pressionado, dando à atenção necessária, para o tema dos crimes virtuais. Então foram aprovados os Projetos de Lei n° 35/2012 na Câmara dos Deputados, que foi originado pelo Projeto de Lei n° 2.793/201, no qual foi apresentado como uma proposta alternativa ao Projeto de Lei n° 84/99. Foi sancionada e promulgada pela Presidência da República em 30 de novembro de 2012, através da Lei n° 12.737, apelidada de Lei Carolina Dieckmann.

A Lei 12.737, veio para estabelecer a tipificação criminal de delitos informáticos, e alterar o Código Penal Brasileiro acrescentado os artigos 154- A e 154-B, criando um novo tipo penal “invasão de dispositivo informático”. E fazendo também pequenas modificações realizadas nos artigos 266 e 298, ambos do Código Penal, para tipificar a “interrupção ou perturbação de serviço informático, telemático ou de informação de utilidade público” e a falsificação de cartões de débito e crédito, respectivamente.

1.2 Objetividade Jurídica e Sujeito Ativo e Passivo

A objetividade jurídica a ser tutelada pelo novo tipo penal corresponde à liberdade individual, mais especialmente ao sigilo de dados ou informações armazenadas nos dispositivos informáticos em geral. Configura-se como sujeito passivo qualquer pessoa que possa sofrer algum dano pela invasão, em especial o proprietário ou possuidor do dispositivo informático, e inclusive terceiros prejudicados, em ocasiões em que a conduta típica atingir direitos e interesses de outras pessoas.

Podemos classificar um delito comum quando figure como sujeito ativo qualquer pessoa, vez que a descrição típica da conduta não exige nenhuma qualidade especial do autor do crime. Classificado como crime formal, a consumação da figura típica ocorrerá com a efetiva violação indevida de mecanismo de segurança, e a consequente entrada sem autorização em dispositivo informático alheio, independente da ocorrência de qualquer outro resultado naturalístico. Em ocorrendo o resultado visado pelo agente, o crime já estará consumado, se tratando de mero exaurimento de crime.

II- CRIMES CIBERNÉTICOS NO COTIDIANO E AS MODALIDADES DOS CRIMES VIRTUAIS

O estudo sobre os crimes cibernéticos se deu com a evolução da tecnologia e das ameaças virtuais, trazendo a necessidade de conhecimento acerca dos crimes cibernéticos, tanto a nível conceitual, quando em relação a suas classificações. Por isso é necessário à intervenção do Direito na informática, e a aplicabilidade de uma regulamentação do ciberespaço, que ainda não é um desafio superado. Dentre os crimes possíveis de ocorrer, pode-se citar: Fraude por e-mail pela internet; Fraude de identidades, quando as informações pessoais são usadas por pessoas diversas; Roubo de dados financeiros ou relacionados a pagamento de cartão bancário; Roubo e venda de dados corporativos; Extorsão cibernética, que é quando há uma exigência em dinheiro para impedir que o ataque ou exposição de dados e fotos ocorra;

Espionagem cibernética, quando, por exemplo, hackers acessam dados sigilosos de empresas ou do governo.

Esses tipos de crimes podem se enquadrar em duas categorias diversas que são as atividades criminosas que visam computadores, que ocorrem diretamente atacando outro computador/ sistema para que perca dados ou que fique com vírus para obter a finalidade querida. Já a outra categoria é a chamada atividade criminosa que usa computadores para cometer outros crimes, que é a mais comum que ocorre no cotidiano. Nesta o ataque é direcionado a alguém, visando vingança, extorsão, humilhação, exposição entre outros.

A tecnologia trouxe um nível de vida, que jamais fora imaginado por pessoas de tempos mais antigos. Um dos avanços mais impressionantes vivenciados pela humanidade foi à criação da internet. Por isso podemos dizer que vivemos em uma era digital que influencia os setores da sociedade, comércio, política, serviços, entretenimento, informação e relacionamentos. Com a rede mundial de computadores fronteiras foram vencidas, e podemos realizar negociações para obter informações como, por exemplo, ter uma comunicação ativa com diversas pessoas do mundo.

Mas infelizmente, o poder que a tecnologia nos trouxe veio acompanhado de riscos para as pessoas. A facilidade de ocultar a sua identidade através da internet atrai diversos tipos de criminosos, tanto tradicionais como ocasionais.

De acordo com Ferreira, dispõe sobre a impunidade:

> Por isso temos a sensação de impunidade, sendo um atrativo muito forte para o crescimento desse tipo de delito. As ameaças podem ser tanto por meio de monitoramentos não autorizados do sistema como a (DEP WEB), como através de ataques mais sofisticados por hackers. (FERREIRA, 2015, p.32).

Já se tratando da investigação na esfera penal, com o avanço é necessário haver uma assistência para o combate para este tipo de crime. Já existem algumas Delegacias Especializadas (onze), mas ainda falta muito para que a população tenha acesso ao aparato investigativo e judicial do Estado. A maioria dos crimes nem sequer são denunciados até mesmo pelo descredito que a população tem em relação á justiça do país.

Os crimes cibernéticos não reconhecem fronteiras, e se faz necessária uma maior integração internacional entre os Estados para lidar com esses crimes que afetam ou apresentam riscos para todos os países, e esse risco fica ainda maior quando considerarmos o crescimento das organizações criminosas.

2.1 CRIMES VIRTUAIS IMPUROS OU IMPRÓPRIOS

Os crimes virtuais impróprios são aquelas nos quais o instrumento é o computador, ou seja, por meio da máquina é usado na execução de condutas ilícitas.

O computador é apenas instrumento para efetivar o crime, não sendo essencial para o cometimento do crime, pois pode se realizar o crime sem o próprio, como exemplo se há extorsão, então está já é tipificada no Código Penal e consta no art.158.

> **158** - Constranger alguém, mediante violência ou grave ameaça, e com o intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixar de fazer alguma coisa: Pena - reclusão, de quatro a dez anos, e multa.

Há uma grande dificuldade em se identificar crimes virtuais impuros por não se reconhecer a informação como um bem material, mas sim um bem imaterial sendo assim impossível a apreensão.

A informação neste caso, por se tratar de patrimônio, refere-se ao bem material, apenas grafado por meio de bits, suscetível, portanto, de subtração. Assim, ações como alteração de dados referentes ao patrimônio, como a supressão de quantia em uma conta bancaria, pertencem á esfera dos crimes contra o patrimônio.

2.2 CRIMES VIRTUAIS PRÓPRIOS OU PUROS

Apesar de toda conduta ilícita ter como objetivo atingir o sistema do computador do sujeito passivo é necessário que atinja o hardware ou o software, nesse momento o computador é usado como meio e objeto para execução dos crimes,

e nessa categoria está incluída não só a invasão de dados não autorizados, mas qualquer interferência em dados informatizados que atinjam diretamente os sistemas eletrônicos, tornado assim puro ou próprio, que não precisam ser praticados necessariamente por computador e se realizarem em meio eletrônico.

Neles a informática, segurança dos sistemas, a titularidade das informações e a integridade das máquinas e periféricos, torna-se o objeto jurídico tutelado.

2.3 CLASSIFICAÇÕES DOS CRIMES CIBERNÉTICOS

Há uma divisão que classificam os tipos de crime informáticos em tipos caracterizados pelo uso de instrumentos informáticos, crimes caracterizados pela agressão ao meio informático, e pelo conteúdo da mensagem disponível em redes.

O autor Ascensão sobre a classificação dessas modalidades:

> Essa classificação ajuda a entender a motivação do criminoso, se o mesmo desejar atingir diretamente um determinado sistema informático, ou se o infrator visa um bem diverso do computacional, utilizando o elemento digital como instrumento para a prática de outro delito. (ASCENSÃO, 2010, p.256).

Por isso iremos tratar desta classificação que é muito utilizada pela doutrina, onde o mesmo se divide em crimes cibernéticos:

Crimes centrados no computador, que são os tipos de crime que apresentam como objetivo primordial o ataque em sistemas ocupacionais, dispositivos de armazenamento e outros dispositivos.

Crimes auxiliados por computador, este é utilizado como uma ferramenta para auxiliar na pratica de um crime onde o uso do computador é estritamente necessário.

Crimes incidentais por computador, este é uma atividade criminosa, onde a utilização do computador seja incidental ou eventual que podem ser caracterizados como crimes próprios ou impróprios.

Tais classificações tem a vantagem de categorizar bem os crimes, dando uma ideia ampla acerca das possibilidades de utilização dos meios informativos para o ataque a diferentes bens jurídicos a serem protegidos pela legislação penal.

Á prática criminosa dos crimes cibernéticos se dá através da utilização de algum computador atrelado com a internet e a web, portanto é fundamental conhecer os tipos de crimes informáticos protegidos em nosso ordenamento jurídico, pois na pratica o autor não terá o benefício do princípio da inocência.

Depois da publicação da Lei, doutrinadores de renome do nosso ordenamento jurídico como Fernando e Guilherme de Souza Nucci e tantos outros juristas vieram com suas conclusões na intenção de elucidar e facilitar as interpretações no que tange os temas, como por exemplo, o bem jurídico tutelado que a luz da lei protege a liberdade individual da pessoa como forma direta, já indiretamente abrange tanto a intimidade quanto a privacidade, e a inviolabilidade de se comunicar e de se corresponder.

A ação central da conduta, a tipificação do crime, e o ato de invadir sem permissão a segurança de algum dispositivo eletrônico pessoal de alguém, sendo esse o crime. Constitui-se no ato ilegal de invadir o dispositivo informático de alguém, sendo uma violação indevida do mecanismo se segurança, segundo ele consiste também na finalidade de obter, adulterar ou destruir as informações do dispositivo.

O dispositivo ativo do ato é qualquer pessoa que invade sem autorização os equipamentos eletrônicos e o sujeito passivo é qualquer pessoa que sofra a consequência do sujeito ativo.

O disposto no dispositivo da lei varia com outras interpretações como a consumação e tentativa, causas especiais de aumento de pena e modalidades equiparada e qualificada, e omissiva ação penal, suspensão condicional do processo e tantas outras.

III- PENAS QUE DIFICULTAM A PUNIBILIDADE DO AGENTE

Ficou evidenciado diante o fato ocorrido com a atriz que o texto legal foi publicado em um curto espaço de tempo e consequentemente de uma forma célere, porem com essa rapidez na tramitação da lei incorreu má elaboração, trazendo uma

ineficácia ao ver de muitos juristas as penas foram ínfimas demais pela gravidade dos crimes virtuais e no seu artigo 154 – A, do Código Penal.

> 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: (Incluído pela Lei nº 12.737, de 2012) Vigência Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. (Incluído pela Lei nº 12.737, de 2012) Vigência.

Preconiza que para quem pratica o ato é culminada na pena que vai de 03 meses a 1 (um) ano e multa, artigo que é bastante criticado por muitos doutrinadores e operadores do direito penal e do digital, em que favorece o criminoso, que induz a defesa para que algum possível processo a aplicar o pedido de suspensão condicional do processo (SURSI), tirando a gravidade e os danos causados ás vítimas, onde a pena poderia ser maior para que o réu não se beneficiasse dos juizados comuns cíveis que converte a prisão em serviços á comunidade, ou pena pecuniária como elucida França.

A pena mínima, abaixo de 01 ano favorece a suspensão condicional do processo, se não houve condenação ou se não existe processo por outro crime. Nesse caso a reprimenda, associada ao comportamento delitivo, tem de ser idônea, isto é, deve fazer jus á gravidade da sua efetivação em face da liberdade do indivíduo, sob pena de, desnaturando as suas próprias funções, dá azo a inevitável autofagia. Em outras palavras, penas insignificantes não atendem aos princípios clássicos de Direito Penal, sobretudo o da lesividade.

3.1 A FALTA DE TIPIFICAÇÃO DOS CRIMES PELA DEEP WEB

É outra questão polêmica por se tratar da Internet Oculta, onde só quem entende desse universo dos computadores e internet consegue acessar esse paralelo.

Sendo uma internet paralela que quase nunca deixa rastros, por exemplo, um hacker consegue acessar e adquirir dados sigilosos, sem deixar rastros ou IP, sem que seja identificado. São tão ocultos esses ambientes que até mesmo um hacker não consegue localizar o outro.

Não há hoje nenhuma lei capaz de combater um hacker que usa a Deep Web para invadir computadores no mundo inteiro, não existe uma base legal em que as autoridades competentes possam se apoiar para fazer uma investigação com uma punição, e tentar impedir essa ação de hackers tornando a web ainda mais vulnerável como descreve Cordeiro, 2015: “infelizmente não há regramento jurídico existente para tal ferramenta, concluindo-se que o direito é especifico não alcança este mundo virtual, ao menos agora, quem sabe em futuro mais próximo”.

Vale destacar que as Leis são confusas e rasas, e podem dar abertura para várias interpretações maliciosas de quem gosta de se aproveitar de brechas, para quando cometer crimes sair impune, para o indivíduo que cometer este tipo de delito, seja punido pela Lei Carolina Dieckmann, no entanto não podemos esquecer que a decisão dependerá de jurisprudências e atos normativos, também precisará de investimento e leis complementares para funcionar e pessoas qualificadas e especializadas plenamente no assunto para que a Lei possa se tornar eficaz.

3.2 A OMISSÃO LEGISLATIVA NOS CRIMES CIBERNÉTICOS

Todas as condutas ilícitas praticadas em ambiente informático podem prejudicar a manutenção dos níveis adequados de segurança, que visam à credibilidade dentro de qualquer jurídico. Mas o que realmente preocupa são as situações que exigem, uma segurança maior como, por exemplo, uma transferência bancaria.

Diante dessa situação os crimes virtuais interferem no cotidiano, de modo que esse novo ambiente se torna inapto, para a manutenção de relações sociais. É necessário que haja confiança, de tal forma que se deve buscar a redução dos riscos de fraude, erro, roubo e uso indevido de informações.

Esse tipo de conduta, ainda encontra-se sem a devida regulamentação, de tal forma que o mundo virtual acaba por se transformar em um “mundo sem leis”. Por isso é necessário que as leis convencionais existentes sejam realmente válidas e

colocadas em prática, para este tipo de situação não fique impune e para que haja um tratamento especializado.

Com o avanço tecnológico, é perceptível o atraso existente entre as normas do Código Penal e o momento histórico no qual estamos vivendo, restando aos operadores do direito a árdua missão de conciliar os institutos penais com as constantes mudanças na tecnologia.

De acordo com Ferreira aduz sobre a normatização:

> A ineficácia na normatização nos crimes virtuais, ainda não foi suprida para um combate efetivo contra estes delitos, por isso diante dessa dificuldade encontrada, ou até mesmo pela natureza taxativa do Código Penal, á uma grande impossibilidade da aplicação da analogia nos crimes virtuais. (FERREIRA, 2015, 44).

A duas possibilidades de tratamentos legislativos, o primeiro trata-se no Código Civil e o outro no Código de Defesa do Consumidor, estes podem ser utilizados em parte para sanar alguns conflitos, mesmo com a falta de normas específicas do tema.

Já em relação ao Direito Penal, deve-se criar uma legislação específica para tipificação dos delitos, caso contrário, na aplicação da analogia, haveria uma afronta a um direito fundamental.

Devido à falta de legislação especifica para os crimes virtuais, ainda se utilizam das seguintes normas tipificadas na legislação penal sendo estas: Pedofilia (ART. 241-a da Lei n° 8.069/90 Estatuto da Criança e do Adolescente); Interceptação de comunicações de informática art. 10 da Lei n° 9.296/96); Crimes contra software Pirataria (art. 12 da Lei n° 9.609/98), Calúnia (art. 138 do CP); Difamação (art. 139 do CP); Injúria (art. 140 do CP); Ameaça (art. 147 do Código Penal), dentre outras.

Importante destacar que além das condutas descritas como crimes, ainda existem alguns ilícitos que não são considerados crimes, e que também não apresentam legislação especifica, a exemplo dos praticados contra as informações, a propagação de ameaças virtuais, isso dificulta ainda mais punições que deveriam ser consideradas ilícitas pelo potencial danoso que apresentam, e não são tipificadas pelo atraso penal.

Por isso e necessário haver uma legislação que defina os termos para determinar até onde podemos chegar, com a utilização das redes, mas infelizmente esta não é a realidade em que vivemos, sendo necessária uma decisão em relação à omissão estatal.

CONCLUSÃO

Com o presente artigo reforço a tese de que apesar de existirem leis específicas no Brasil que visam o combate aos crimes virtuais, estas são ineficientes e incompletas, necessitando de grandes alterações e complementos, para que sua finalidade seja cumprida. Pois o que se nota atualmente é um

sentimento de injustiça, tendo em vista que a grande maioria dos crimes virtuais seguem sem solução ou punição. No momento em que vivemos onde a internet torna o mundo extremamente globalizado, é urgente que essas alterações sejam feitas, para que assim todos os seus usuários sejam protegidos, e tenham respaldo na lei. Para que as vítimas não fiquem injustiçadas, ou sem vontade de denunciar, pois sabem que nada será feito para solucionar o problema. O delito é grave, pois pode mexer tanto financeiramente quanto emocionalmente com as pessoas, levando algumas a se isolarem, mudarem de cidade, entrarem em depressão, terem ansiedade e diversos outros problemas que se colocados em pauta em relação a pena proposta não seriam supridos e muito menos dar a sensação de punibilidade e justiça feita, pois nenhum dano causado desta gravidade pode ser reparado com 3 meses a 1 ano e multa. A vida de alguém vai além.

REFERÊNCIAS

BLUM, Renato M. S. Opice; ABRUSIO, Juliana Canha. Os hackers e os tribunais. **IBDI –** Instituto Brasileiro de Direito da Informática, 9 mar. 2004. Disponível em:

<http://www.ibdi.org.br/index.php?secao=&id_noticia=287&acao=lendo>. Acesso em: 12 mar. 2012.

http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm

http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm

MEDEIROS, Claudia Lucio de. DEFICIÊNCIAS DA LEGISLAÇÃO PENAL BRASILEIRA
FRENTE AOS CRIMES CIBERNÉTICOS. Universidade Estadual do Ceará, 2010.

MIRANDA, Marcelo Baeta Neves. Abordagem dinâmica aos crimes via Internet. **Jus Navigandi**, Teresina, a. 4, n. 37, dez. 1999. Disponível em: <http://www1.jus.com.br/ doutrina/texto.asp?id=1828>. Acesso em: 12 mar. 2012.

NIGRI, Deborah Fisch. Crimes e segurança na Internet. **In Verbis**, Rio de Janeiro: Instituto dos Magistrados do Brasil, Ano 4, n. 20, p. 34-41, 2000. p. 38
RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. **Crimes virtuais**. 2005. Disponível em: <http://www.advogadocriminalista.com.br>. Acesso em: 27 jun. 2005

RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. O problema na tipificação penal dos crimes virtuais. **Jus Navigandi**, Teresina, a. 6, n. 58, ago. 2002. Disponível em:
<http://jus2.uol.com.br/doutrina/texto.asp?id=3186>. Acesso em: 20 abr. 2006.

ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004. p. 24-25.

SANTOS, Coriolano Aurélio Almeida Camargo. ATUAL CENÁRIO DOS CRIMES CIBERNÉTICOS NO BRASIL. 2008.

VIANNA, Túlio Lima. **Fundamentos de Direito Penal Informático**. Rio de Janeiro: Forense, 2003. https://ambitojuridico.com.br/edicoes/revista-191/crimes-ciberneticos-phishing/