CENTRO UNIVERSITÁRIO TABOSA DE ALMEIDA - ASCES/ UNITA

DIREITO

CRIMES CIBERNÉTICOS: a insuficiência das leis brasileiras

JULIO VINICIUS DE SALES SOARES

CARUARU

2020

JULIO VINICIUS DE SALES SOARES

CRIMES CIBERNÉTICOS: a insuficiência das leis brasileiras

Trabalho de Conclusão de Curso, apresentado ao Centro Universitário Tabosa de Almeida-ASCES/UNITA, como requisito parcial para obtenção do grau de Bacharel em Direito.

Orientador:Professor Msc. Rogério Cannizzaro Almeida

CARUARU

2020

BANCA EXAMINADORA

Aprovado em:____/___/_____

_____

Presidente: Prof. Msc. Rogério Cannizarro de Almeida

_____

Primeiro Avaliador: Prof.

_____

Segundo Avaliador: Prof.

RESUMO

O alvo central deste artigo científico foi mostrar a imensa dificuldade que o ordenamento jurídico brasileiro tem para enquadrar um crime cibernético diante das leis vigorantes no país. A partir das inovações tecnológicas cresceu de forma exorbitante número de ataques contra os computadores e redes vinculadas à internet. Esse progresso exige a modernização de aparelhos próprios para prevenir ou abater o avanço dos crimes virtuais para que se tenham uma maior segurança aos usuários quando estiverem navegando no espaço cibernético e usufruir de suas vantagens. No Brasil, existe uma grande insuficiência das leis para repreensão de transgressões virtuais. Logo, essa ausência de lei facilita a vida de criminosos que praticam crimes utilizados o âmbito virtual, contendo como exemplos, pedofilia, divulgação de conteúdo sem autorização e delitos contra a honra. Portanto, a invenção de leis adequadas é de vasta importância para combater tais crimes. Um ponto chave desse artigo é demonstrar a dificuldade para obter provas contra os criminosos que praticam esse tipo de delito, pois, em virtude da internet não possui fronteiras e graças às novas tecnologias que permitem o armazenamento dessas informações nos mais diferentes locais do mundo, desafiam os operadores de direitos punirem esses criminosos. À vista disso, a cooperação entre os operadores de direito é de vasta importância, pois muitas vezes as provas digitais somem rapidamente, logo a investigação dos crimes virtuais tem que ser rápida. Alguns casos possuem uma grande visibilidade, até mesmo em alcance pátrio, promove preocupação instantânea, mas que, passar do tempo, vira algo apático e esquecido pela sociedade, e, deste modo, seus motivadores não são responsabilizados na proporção de suas condutas. Destarte, com a análise de casos concretos e a sondagem das limitadas leis atualmente aplicáveis, o artigo exposto, busca uma perspectiva panorâmica de questões associadas aos ilícitos realizados por intermédio da Internet.

Palavras – Chave: Crimes; Internet; Pedofilia.

ABSTRACT

The central target of this scientific article was to show the immense difficulty that the Brazilian legal system has to frame a cybercrime in the face of the laws in force in the country. From technological innovations has grown exorbitantly the number of attacks against computers and networks linked to the internet. This progress requires the modernization of their own devices to prevent or trigger the advance of virtual crimes so that users are more secure when they are browsing the cyberspace and enjoy their advantages. In Brazil, there is a great failure of laws to rebuke virtual transgressions. Therefore, this absence of law facilitates the lives of criminals, who commit crimes used the virtual scope, containing as examples, pedophilia, dissemination of content without authorization and offenses against honor. Therefore, the invention of appropriate laws is of great importance to combat such crimes. A key point of this article is to demonstrate the difficulty in obtaining evidence against criminals who commit this type of crime, because, because of the internet has no borders and thanks to the new technologies that allow the storage of this information in the most different places around the world, challenge right-rate operators to punish these criminals. In view of this, cooperation between law operators is of great importance, as digital evidence often disappears quickly, so the investigation of virtual crimes has to be swift. Some cases have great visibility, even in a way, promotes instant concern, but that, passing time, becomes something apathetic and forgotten by society, and thus its motivators are not held accountable in proportion to their Conduct. It initiates, with the analysis of concrete cases and the probing of the limited laws currently applicable, the article exposed, seeks an overview of issues associated with illicit crimes carried out through the Internet.

Words - Key: Crimes; Internet; Pedophilia.

SUMÁRIO

INTRODUÇÃO 6

1. CRIMES CIBERNÉTICOS NO TERRITÓRIO BRASILEIRO 8

1.1 CRIMES CONTRA A HONRA NO MEIO VIRTUAL.....9

1.2 PEDOFILIA NA INTERNET 11

1.3 DIVULGAÇÃO DE CONTEÚDO SEM AUTORIZAÇÃO 14

2. JURISDIÇÃO NA INTERNET 15

3. CRIMES CIBERNETICOS PRÓPRIOS E IMPRÓPRIOS 18

4. A DIFICULDADE DE PUNIR OS CRIMES CIBERNÉTICOS NO ORDENAMENTO JURÍDICO BRASILEIRO.....21

CONSIDERAÇÕES FINAIS 23

REFERÊNCIAS 25

INTRODUÇÃO

O direito encontra-se sempre presente em cada ocasião da vida das pessoas, que convivem em um Estado governado pela democracia, como é exemplo o Brasil. Portanto, esse vem sendo designado por muitos anos por proporcionar respostas aos problemas entre pessoas e instituições que decorrem de uma coletividade atual, que prospera em ritmo veloz, por causa dos múltiplos descobrimentos e aperfeiçoamentos científicos e tecnológicos que tem como objetivo oferecer simplicidade e presteza à vida dos brasileiros.

No entanto, com o passar dos tempos, a sociedade brasileira desenvolveu-se de forma rápida, e ao lado desse acontecimento, surgiu a era da tecnologia, apresentando inúmeras mudanças e facilidades para melhorar a vida dos indivíduos. Excepcionalmente, alguns indivíduos mal-intencionados que viram na internet a possibilidade de realizar delitos, agindo de má fé, pondo várias pessoas em risco, de modo que se tornou comum, levando em consideração a facilidade que este é realizado, asseverando diversas vezes a impunidade daqueles que o concretizam.

Na contemporaneidade em que o ser humano vive é evidente que as tecnologias avançaram muito nos últimos tempos. As pessoas estão cada dia mais interligadas umas com as outras ao redor do planeta através dos dispositivos tecnológicos. A internet nunca foi tão acessada quanto nos dias de hoje a partir desses aparelhos eletrônicos como: *smartphones*, computadores, *notebooks*, *tablets*, dentre muitos outros. Logo, tornou-se uma ferramenta de acesso constante por parte da população. Não obstante, obtiveram a atenção de bandidos que fazem uso dessa ferramenta de forma indevida.

Com o advento da internet e do computador, deu-se início ao acesso direto aos ambientes virtuais, nos quais, infelizmente, existem indivíduos que utilizam desse método para praticar atos ilícitos tanto por meio dessa esfera, quanto no mundo real.

O Direito existe para manter a prática do justo e do correto, mantendo um padrão de convivência entre os seres humanos, punindo, assim, aqueles que ousam cometer atos criminosos. O cenário atual não pode ser pior, uma vez que o ser humano tem visto atos criminosos sendo praticados virtualmente de forma espantosa e em larga escala, tamanha é a ousadia destes criminosos. Logo, é algo

extremamente preocupante, pois, mesmo sendo praticado em um ambiente virtual, esse tipo de crime tem impacto diretamente na vida real, tanto da vítima quanto de terceiros.

Nos tempos atuais, expandiu-se o quantitativo de ataques contra os usuários da internet e as redes de computadores. Tal comportamento exige que tenham uma melhoria e modernização de instrumentos adequados para evitar ou enfraquecer o progresso dos crimes cibernéticos para que se tenha uma máxima garantia ao se navegar no ambiente cibernético e desfrutar de seus benefícios. É diante tal assunto, que aparece a problemática que abrange este contexto, o ordenamento jurídico brasileiro possui leis suficientes para punir devidamente os delitos cibernéticos?

O presente estudo, irá mostrar o grande problema no ordenamento jurídico brasileiro para enquadrar os crimes cibernéticos diante da falta de regulamentação. E, como objetivos específicos, busca averiguar como são tipificados os crimes virtuais no Brasil, considerar quais os principais crimes realizados no âmbito virtual atualmente, contemplar o posicionamento dos tribunais quanto aos crimes cibernéticos e conceber qual a necessidade para a coletividade brasileira em se tipificar os crimes cibernéticos.

Logo, o presente estudo tem outro objetivo revelar a necessidade da evolução da legislação, no intuito de mostrar o quanto ainda são insuficientes as leis em relação a esse tipo de crime no Brasil, mostrando dessa forma o que a atual legislação nacional faz ou pretende fazer para reprimir os criminosos que vêm praticando estes delitos. Para tanto, o trabalho busca compreender as consequências causada por esse tipo de crime e ausência da atuação dos órgãos competentes em combate a este delito, pois mesmo com a legislação atual seguem altos os índices de crimes cibernéticos.

O alicerce metodológico do presente estudo fora predominantemente fundamentado em pesquisa bibliográfica, valendo-se de pesquisas desempenhadas por meio de documentos, artigos, resenhas, sites, resumos e teóricos relevantes sobre o assunto.

1. CRIMES CIBERNÉTICOS NO TERRITÓRIO BRASILEIRO

Hoje em dia, o Brasil ocupa o quarto lugar em número de usuários de internet, de acordo com dados da Conferência das Nações Unidas sobre Comércio e Desenvolvimento.

Com a ampliação dos sistemas de computadores e com o desenvolvimento da internet, tende a ficar mais comum as ocasiões em que as pessoas vão tirar proveito dos aparelhos para realizar atos que ocasionam danos ao patrimônio jurídicos de outros indivíduos. Segundo Rosa (2005, p.22) a perda da importância realizada através de tais instrumentos não possui limites, já que um computador que se encontra em certo país, pode entrar em um sistema e manusear suas informações, sendo que as consequências dessa atuação podem ser originadas em diferente computador muito longe daquele em que a ação foi iniciada, sendo possível, até mesmo, se encontrar situado em um país diferente.

Um aparelho eletrônico, em ação de segundos, pode averiguar milhões de informações. Neste mesmo tempo, ele pode também ser usado de forma indevida roubando milhões de reais. Todavia, pode ser realizado no conforto de sua residência tal delito, desde que tenham uma noção e um aparelhamento devido, sem os contratempos de como, por exemplo, roubar uma loja com arma de fogo ou um carro forte.

Conforme Stair (2008, p.54), os delitos realizados com a colaboração de um computador, normalmente, são complicados de se visualizar, isso porque costumem vinculas enormes valores e são delitos vistos como limpos.

No território nacional, existe um número elevado de episódios de publicações de fotos privadas sem a concordância da pessoa exposta. Recentemente, uma jovem de 15 anos enforcou-se no Estado de Mato Grosso do Sul por medo de ter suas fotografias íntimas expostas. Quando a adolescente tinha 14 anos ela teve relacionamento com um garoto de 17 anos, que a chantageou pelas fotos tiradas por ele, as quais a jovem não tinha ciência se eram verdadeiras. Deste modo, os crimes virtuais não alcançam apenas a rede social de uma pessoa, ou o computador, traz perturbações psicológicas que tem o poder de ocasionar danos irreversíveis a vida.

No cenário atual, se tem uma grande dependência de ferramentas eletrônicas para armazenamento de informações, sejam atinentes à vida profissional ou pessoal.

Como o caso citado acima, mostra que os dispositivos de assistência aos recursos computacionais não são adequados em sua integralidade. O caso da adolescente que se matou ratifica que o uso de dispositivos eletrônicos por indivíduos carentes de discernimento moral traz implicações além da esfera digital. Desse modo, é indispensável um meio que seja eficaz para garantir o amparo e segurança das pessoas, que necessitam gozar de sua vida privada e intimidade, como certifica a Constituição Federal de 1988 em seu artigo 5º, X:

> 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> X - 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 de sua violação;

Portanto, esse fato e apenas um simples exemplo do que os crimes cibernéticos podem causar a vida das pessoas. Logo, isso mostra o quanto e necessário a implementação de leis mais rígidas no ordenamento jurídico brasileiro, para os criminosos que praticam este tipo de crime, sofram punições severas, pois, se continuar da forma que se encontra, ao invés de baixar o número de crime no país, ele só vai acabar aumentando e prejudicando cada vez mais a vida das pessoas.

1.1 CRIMES CONTRA A HONRA NO MEIO VIRTUAL

A internet é usada por indivíduos de todas as idades ou classes sócias, esse meio facilitou a interação dos usuários, que a partir desse evento as pessoas utilizam esse ambiente para expor seus pensamentos, opiniões e ideias. Contudo, muitos usuários pensam que podem falar o que quiser e ofender outras pessoas, como traz o artigo 11 da Declaração dos Direitos do Homem e do Cidadão:

> A livre comunicação dos pensamentos e opiniões é um dos direitos mais preciosos do homem: todo cidadão pode, portanto, falar, escrever, imprimir livremente, embora deva responder pelo abuso dessa liberdade nos casos determinados pela lei.

Portanto, este artigo mostra que todas as pessoas são livres para fazerem suas escolhas, até o ponto que este ato, não ofenda a honra da outra pessoa ou que denigra ela moralmente. Deste modo, existe uma grande dúvida: até onde as pessoas podem expressar sua opinião na internet, sem que cometam crimes?

A internet deve ser vista como uma fonte ampla e liberal para todas as formas de pensamento, respeitando sempre o limite de não ofender a honra dos indivíduos, um local no qual seja debatido dos os tipos de ponto de vista. Todas as pessoas têm direito à liberdade de expressão e opinião como está tipificada na Declaração Universal dos Direitos Humanos, no artigo XIX:

> Toda pessoa tem direito à liberdade de opinião e expressão; este direito inclui a liberdade de, sem interferência, ter opiniões e de procurar, receber e transmitir informações e ideias por quaisquer meios e independentemente de fronteiras.

Logo, isso mostra o quanto o ser humano tem o total direito a expor seu pensamento. Contudo, se faz necessário prevenir qualquer prática de delito pelo meio virtual, pois existe limites na liberdade de expressão, que muitas vezes são ultrapassados pelos os usuários, fazendo isto virar crime. Um dos crimes que mais ocorre no âmbito virtual é a prática do racismo que está prevista na Lei 7.716 de 1989, que no artigo 20 diz que “praticar induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional, configura crime.”

Neste evento, a pena é de reclusão e 2 (dois) a 3 (três) anos e multa, porém quando o racismo é praticado no meio virtual, pode ter sua pena majorada, por ter usado meios de comunicação social, ou publicação de qualquer natureza, aumentando a pena para reclusão de 2 (dois) a 5 (cinco) anos e multa.

Atualmente, os tribunais encontrar-se adotando decisões diversas sobre os fatos de ofensas que são praticados no meio virtual. Contudo, ainda há mais três tipos de crimes contra a honra que são corriqueiros na internet, todos tipificados no Código Penal Brasileiro. O primeiro deles, é a calúnia que é avaliada como um comportamento no qual se atribui a alguém um crime sem que este o verdadeiramente tenha o feito, como assegura o artigo 138 do Código Penal: “Caluniar alguém, imputando-lhe falsamente fato definido como crime.”

Um exemplo de calúnia virtual que virou até reportagem da rede globo, é o da dona de casa Fabiane Maria de Jesus, morta aos 33 anos de idade, em 5 de maio de 2014. Espancada até a morte por habitantes do Guarujá-SP, onde residia, a dona de casa foi apontada de estar fazendo magia negra com crianças. A seguir, foi espalhada uma notícia falsa pelas redes sociais. Junto com a história propagada pela internet, foi postado um retrato falado de Fabiane que rapidamente se espalhou pela rede, juntamente com histórias falsas e relatos de mentirosos que afirmavam ter

testemunhado os sequestros. Os outros dois de crimes são a difamação, artigo 139: “Difamar alguém, imputando-lhe fato ofensivo à sua reputação”, e a injúria, artigo 140: “Injuriar alguém, ofendendo-lhe a dignidade ou o decoro.”

Portanto, no primeiro caso não é necessário que a atribuição se mencione um crime, tal como na calúnia, basta apenas a simples acusação, um exemplo desse tipo de crime no meio virtual é aquele do sujeito que divulga foto do outro, em grupos de vendas, aludindo que ele entregou material distinto do contratado ou até mesmo não o entregou, de tal modo, existindo a difamação da imagem do vendedor.

Já no segundo caso, tem-se a injúria quando há insulto à dignidade de um indivíduo que afete sua honra subjetiva, pouco implicando sua visão diante da comunidade, um exemplo básico seria o de comentar na foto de alguém “ladra”, “estupido” e outros modos de insultos que atinjam a honra da vítima.

No entanto, por mais que estes comportamentos se encontrem tipificados no Código Penal, o dispositivo estar desatualizado para combater os crimes virtuais, pois foi criado em 1940, e a tecnologia veio a crescer recentemente, a partir disso as punições são fracas quando acontecem no ambiente virtual. Além disso, é imprescindível majorar as penas em uma lei especial, e detalhar condutas quando se aborda de crimes contra a dignidade cometida no meio virtual. Ainda, é de vasta importância, que o Estado proporcione uma grande capacitação dos agentes encarregados pela persecução penal, além disso, um melhoramento na estrutura organizacional dos meios utilizados pela polícia investigativa. Além disso, o Estado deve conceder um equipamento mais adequado para que exista um desempenho melhor nas investigações. Desse modo, prestando uma melhor proteção a população, no combate aos infratores dos crimes cibernéticos.

1.2 PEDOFILIA NA INTERNET

A pedofilia é definida como uma perversão que leva um indivíduo adulto a se sentir sexualmente atraído por crianças. A psiquiatria e psicologia definem o assunto como uma conduta, e não uma ação, consistindo, dessa forma como uma atração desviada.

A Organização Mundial de Saúde (OMS) tem como entendimento quer a pedofilia é um distúrbio mental, dominante e constante, no sujeito que tem vontade de ter relações sexuais com crianças.

Na sua obra Martinelli, julga pedofilia como:

> A pedofilia talvez seja o crime que mais provoque a repulsa da sociedade. Não há qualquer forma de se aceitar as situações constrangedores a que crianças são subordinadas, para saciar as fantasias de pessoas desequilibradas. A pedofilia é um fenômeno fora dos padrões comuns toleráveis pela sociedade, encontrando na Internet um veículo para satisfazer virtualmente os seguidores dessa prática. Esta modalidade aparece na Internet de duas maneiras: pelas "home pages" e por correio eletrônico. Na primeira opção, os gerenciadores das páginas recebem uma quantia dos usuários (através de depósito ou cartão de crédito), que dispõem de um acervo de fotos e vídeos. Na segunda opção, o material é distribuído de um usuário a outro, diretamente (MARTINELLI, 2000, p. 33).

Logo, ela gera uma inquietação psicológica que leva o indivíduo desenvolver vontades sexuais por meninas ou meninos. Com a internet, esses sujeitos avistaram um novo meio de se satisfazerem seus desejos sexuais, pois usam o meio virtual para praticar este tipo de crime.

Na maior parte dos casos, o perfil de um pedófilo são indivíduos divorciados ou solteiros, que já tem certa idade avançada e grande parte deles tem um isolamento em seu cotidiano e não se satisfazem com uma pornografia adulta e usa outras formas de para se contentar sexualmente, utilizando muitas vezes o meio virtual, se aproveitando de crianças que não tem total discernimento do que vão passar nas mãos desse tipo de criminosos.

Em uma das suas obras, o autor Guedes fazer referência aos acontecimentos analisados em suas pesquisas:

> Em 2007 a Policia Federal entrou em uma grande operação chamada Carrossel com objetivo de acabar com a pedofilia na internet, e foram localizadas um grande grupo de pessoas com um programa específico de compartilhamento pornográfico infantil vídeos imagens que é uma grande forma que os pedófilos encontra para a divulgação de falsas agências de modelos infantis. (GUEDES, 2009, p.143)

A partir da internet, estes criminosos acessam a rede inventando perfis falsos, para conversar com as crianças com objetivo de conseguir informações com os menores, com a intenção de obter telefones, localização de onde eles moram.

Portanto, a partir do momento que conseguem ganhar a confiança começam a pedir vídeos pornográficos ou fotos nuas, aos menores.

O meio virtual, que deveria ser uma ferramenta utilizada para o bem, se mostrou para os criminosos, como um mercado para praticar esse tipo de crime, que em alguns casos traz um alto percentual de lucros. Os pedófilos alcançam mais um objetivo o de criar uma de organização com outros sujeitos que praticam esse tipo de crime, utilizando a internet como um meio para se conectar com indivíduos de do o planeta, com o objetivo central de difundir a pedofilia, seja por imagens seja por filmagens, até mesmo, a sujeitaram-se a expor seus próprios corpos durante a relação sexual, como Liborio mostra em sua obra:

> Os chamados “Clubes” servem para “associar” pedófilos pelo mundo; onde estes podem adquirir fotos ou vídeos contendo pornografia infantil ou, pior, “contratar” serviços de Exploradores Sexuais, fazer Turismo sexual ou mesmo efetivar o Tráfico de menores ou aliciá-los para práticas e abusos sexuais. (LIBORIO, 2004, p. 358).

De tal modo, as práticas de pedófilas são desde os tempos antigos, porém, nos dias atuais conseguiram se estender graças à internet, pois se adaptaram ao mundo virtual e devido a isso obtiveram o alcancem de mais vítimas, causando um dano bem maior do que antes.

Logo, estão tipificados nos artigos 240 e 241 do Estatuto da Criança e do Adolescente que foi alterado no ano de 2008 pela lei 11.829. A pornografia infantil está tipificada no artigo 241-E, que trata sobre sexo explícito, como mostra o texto:

> Art. 241-E. Para efeito dos crimes previstos nesta Lei, a expressão “cena de sexo explícito ou pornográfica” compreende qualquer situação que envolva criança ou adolescente em atividades sexuais explícitas, reais ou simuladas, ou exibição dos órgãos genitais de uma criança ou adolescente para fins primordialmente sexuais. (Incluído pela Lei nº 11.829, de 2008)

Assim, este tipo de delito quando ocorrido traz um grande impacto e revolta a sociedade. Todavia, depois de algumas mudanças que ocorreram no ECA, deu aos operados de direito uma forma de punir corretamente os criminosos que praticam este crime. O maior obstáculo para as autoridades é conseguir identificar o sujeito, que está gerando o conteúdo pornográfico ou a conversa abusiva com o menor. As punições para esse crime não são pequenas, como é nos acontecimentos de delitos contra a honra, entretanto, a pornografia e pedofilia ainda são os delitos mais corriqueiros feitos

no meio cibernético. De acordo com a Polícia Federal, existe uma grande demora no processo e, mesmo recebendo cerca de 50 mil relatórios em um ano, correlacionar os dados cadastrais de IPs dos acusados por meio de tabela eletrônica é um processo lento e que acaba por acarretar a impunidade.

Portanto, apesar de que as leis consigam avanços para condenar esses delinquentes, ainda não é fácil identifica-los, dessa forma deve haver a criação de meios mais rápidos e de equipamentos de primeira linha para quer as autoridades consigam punir os infratores, pois grande parte dos criminosos tem um grande conhecimento e equipamentos para cometer o crime da forma correta no meio virtual, muitas vezes saindo impune do delito. Deste modo, deve existir um desenvolvimento no equipamento tecnológico das autoridades responsáveis por combater este crime, para que eles consigam lutar em igualdade de armas como os pedófilos, uma vez que estes tem uma grande intelectualidade bem apurada em relação a tecnologia.

1.3 DIVULGAÇÃO DE CONTEÚDO SEM AUTORIZAÇÃO

Um evento que trouxe vasta repercussão no Brasil foi o da atriz Carolina Dieckman, que lidou com uma invasão de um aparelho eletrônico que tinha uso particular, e partir desse fato os criminosos invadiram este aparelho tirando dele arquivos e fotos que logo após foram publicadas em redes sócias. Assim, devido a este fato a atriz, teve seu nome utilizado como título da lei 12.737/12, que acarretou mudanças no Código Penal Brasileiro, classificando acerca da tipificação criminal de crimes cibernéticos. Há pouco tempo, aconteceu um fato com o ator Stênio Garcia, que foi mais uma vítima de *crackers,* que roubaram e publicaram imagens do ator juntamente com as da esposa na internet.

No Brasil, são numerosos os episódios de divulgação de conteúdo sem autorização, e que acontecem meio da invasão dos aparelhos eletrônicos da população. Pesquisas mostram que as mulheres são vítimas periódicas de tal crime, conforme a Safernet Brasil, no ano de 2016, 300 indivíduos tiveram suas fotos íntimas vazadas, desse número 202 eram mulheres.

Existem casos em que casais compartilham imagens entre si, imagens esta que na linguagem popular são conhecidas como “nude”, que dizer fotos sem roupa, por conhecer seu parceiro e ter seguranças nele, diversas pessoas acabam fazendo este

tipo de compartilhamento, contudo com o término da união, como forma de vingança ou de não consentimento do termino da relação, uma das partes acaba por divulgando o conteúdo sem a autorização, que pode ocasionar estragos irreparáveis ao indivíduo sujeitado a esta situação.

Embora de ter tipificação para tal comportamento, como vai ser falado no último capítulo desse estudo, as penalidades não são satisfatórias para conter os delinquentes. Uma pessoa que propaga as imagens comete um delito, entretanto o indivíduo que sofre a maior consequência e aquele que foi exposto de forma indevida.

2. JURISDIÇÃO NA INTERNET

Na internet não existem fronteiras, de tal modo, foi idealizada para que a utilização ou acesso fosse feita de qualquer parte do mundo. Logo, este processo denota a criação de uma realidade virtual onde não existem as barreiras físicas das limitações territoriais dos Estados.

Graças a essa ferramenta as interações humanas multiplicaram-se. Um meio que era para ajudar e facilitar a vida das pessoas, hoje me dia está à mercê dos criminosos, gerando um grande problema para os operadores do direito que são as diferenças culturais englobadas nas distintas legislações existentes. Prontamente, tal assunto pode ser tratado como legal em um país e ilegal em outro, dependendo assim da legislação que é em vigente no devido país. Quando o delito se trata de um crime virtual sua investigação se torna mais complexa, devido ao fato de não saber ao certo onde se encontrar as provas a serem coletadas.

A internet para funcionar, estar sujeita a uma infraestrutura bem real, assim sendo, para conectar-se a esta rede virtual, são indispensáveis provedores de conexão à rede, que designa ao usuário um número IP (Internet Protocol) que a partir desde número passa a navegar no ciberespaço. O assunto a ser acessado ou as plataformas que permitem a fabricação de conteúdo pelo próprio usuário, junto as mensagens de e-mail ou outros meios de comunicação via internet, todos eles dependem de estrutura atribuída pelos provedores de aplicações de internet.

O desempenho correto dessa ferramenta respeita critérios de estruturas matemáticas, que consentem a fluidez dessa estrutura. Portanto, isto significa dizer que as empresas de provedores de internet possuem todas as informações referentes

a cada passo que as pessoas fazem na rede, tais como: postagens, acessos e comunicações.

Deste modo, são estas informações específicas que muitas vezes são o local onde se encontra a prova, de forma precisa, para conseguir descobrir se ocorreu ou não o delito cibernético ou conseguir uma prova digital para esclarecer o crime. O que tem mais difícil no mundo jurídico é a obtenção dessas informações que no futuro vão se tornar a prova digital tão almejada pelas autoridades. As empresas desse ramo de mercado passaram a ter vários de pedidos que buscam informações sobre os dados, recebendo ordens e solicitações de toda parte do planeta, e algumas vezes criminosos tentam falsificar estes pedidos buscando obter dados para dessas pessoas, que no futuro vão sofrer com este tipo de crime.

As empresas podem ter sede em um país, contundo o armazenamento de suas informações pode estar em servidores em qualquer parte do mundo, diante desse fato os operadores do Direito deparar-se com uma questão muito difícil de saber qual local possuiria jurisdição para decidir a respeito do provimento de tais dados. Ademais, cada território tem um entendimento sobre a proteção dessas informações, portanto devido a isso existem as diferenças legislativas sobre como proceder para fornecer conteúdo e dados acerca de qualquer questão virtual, adicionado a difícil missão de obter a prova digital, pois graças a grande circulação de informações no planeta faz com que as provas sumam facilmente, dificultando mais ainda achar o criminoso que cometeu tal delito virtual, deve-se adicionar também o armazenamento de dados que gera um alto custo as empresas.

Logo, este evento levantou uma necessidade, pois as firmas precisam armazenar grande quantidade de dados por assuntos internos gerenciais, ou por decisão das legislações às quais são cobradas ou submetidas, resultando-se que o armazenamento de informações fosse feito em servidores pelo os mais diversos lugares do mundo, buscando o diminuir o custo, adotando as leis daquela região na qual se encontra armazenadas os dados. Ainda, por motivos de segurança, existem servidores replicados em lugares diferentes do mundo e documentos que são guardados de forma fracionada.

Conforme, La Chapelle e Fehlinger (2016), os critérios admissíveis para decidir qual a lei aplicável na obtenção de dados digitais são:

A. a lei do local em que está o usuário, do qual se pretende obter os dados;
B. a lei do local onde estão os servidores que armazenam os dados;
C. a lei do local de incorporação da empresa que presta o serviço;
D. a lei do local dos registradores de onde o domínio foi registrado.

As soluções apresentadas têm dificuldades e entram em conflito com os códigos de aplicação da lei penal de cada território. A primeira alternativa, que submeteria os provedores de internet a disponibilizar informações acercado local onde está situado o usuário, pode encontra-se na circunstância em que o usuário está localizado em um determinado lugar, cometendo um ato criminoso pelo os meios virtuais e causando resultado criminoso no país que carece dos seus elementos para investigação e processo, valendo-se deum provedor de internet que tem localização em terceiro lugar do mundo.

A alternativa que almeja se utilizar das leis do país que estão localizados os servidores que guardam os dados, e que tem protegido as grandes empresas provedoras de internet, sob o contexto que necessitam obedecer às leis de proteção de dados e privacidade, atribui um papel difícil ao profissional do Direito que precisa da prova virtual. Pois, como revelado acima, as informações podem ter cópia em diversos servidores espalhados ao mesmo tempo pelo planeta, ou até fragmentados, arquivados em distintos lugares. Portanto, não existiria nem mesmo confiança integral a respeito do lugar correto em que determinada informação indispensável à investigação ficaria guardada.

A seleção que fala a respeito de emprego da lei do local em que a empresa foi incorporada também soa estranha, quando a região onde o serviço está sendo feito não corresponde com o da incorporação, visto como encontrar-se adotadas leis estrangeiras no território nacional. A alternativa sobre a aplicabilidade da legislação do Estado de procedência do registrador também provoca a aplicação de leis estrangeiras a acontecimentos que têm conflito com a jurisdição nacional.

Todas as alternativas, mostram o quanto é necessário a troca de informações virtuais, já as empresas provedoras de internet precisam corresponder aos princípios legais de jurisdições distintas do lugar aonde os eventos aconteceram ou o serviço foi oferecido, com isso mostra-se a grande necessidade de cooperação internacional, para que estes criminosos sejam punindo da forma devida.

Porém, a cooperação está muito longe de ser algo fácil, pois estas solicitações passam por um processo muito demorado, até conseguirem ser compartilhadas, são conhecidas como *Mutual Legal Agreement Treaties* (MLATs) – Acordos de Assistência Mútua em Matéria Penal, como tradição apresentam um processo extremamente demorado, porque estar sujeito aos os pedidos serem perpetrados de forma adequada, de que sejam feitos e expedidos pelas autoridades adequadas, para que uma autoridade na região requerida dê entrada a cumprimento da solicitação, ocasionando uma grande facilidades aos criminosos conseguirem se livrar dos crimes praticados.

Esse processo formal mostra o quanto é demorado por demais, pois as provas digitais somem rapidamente, e devido a este procedimento acabam sendo perdidas, não se encontrando apropriado às inovações tecnológicas, deixando brechas na lei para que os criminosos continuem praticados estes delitos.

3.CRIMES CIBERNETICOS PRÓPRIOS E IMPRÓPRIOS

Nos dias atuais, os progressos tecnológicos de comunicação e computação ocasionam modificações e transformações a cada dia, tornando o mundo mais globalizado e com informações instantâneas. Fica claro que às melhorias tecnológicas traz um crescimento no ramo mercantil, político e pessoal em todo o mundo, permitindo máximo acesso a dados, documentos, conhecimento e a notícia, a agilidade nas transações bancárias, união dos mercados de diferentes países, da quebra de fronteiras entre esses mercados e cada vez mais aproximando pessoais de diferentes locais da esfera global. De tal modo, progressos como esses devem ser reconhecidos como apropriados, adequados para o desenvolvimento mundial, contudo, junto a todo esse desenvolvimento, apareceu uma nova modalidade de como praticar crimes, conduta esta conhecida como crimes virtuais.

Desse modo, as classificações para este tipo de crime se tornam difíceis. Porém, existem na doutrina duas formas de classificação: crimes cibernéticos puros, mistos e comuns e crimes cibernéticos próprios e impróprios.

Os delitos virtuais puros são definidos como aquela conduta que visa apenas o sistema do computador, atacando ele de forma física ou os seus componentes, até mesmo os dados nele inseridos ou o sistema. O indivíduo tem como objetivo central

invadir o computador, o sistema de informática ou os dados e as informações que estão armazenadas no aparelho. Estes indivíduos que praticam esse tipo delito são os famosos *hackers*, que são sujeito que tem uma grande noção e conhecimento sobre informática. Contudo, utilizam todo este conhecimento para invadir ou prejudicar servidores e sistemas.

Um caso muito emblemático e conhecido em todo o mundo é o do vírus Melissa, que em 1999 causou um prejuízo de mais de US$ 80.000.000,00 (oitenta milhões de dólares americanos). Outro exemplo que pode ser usado para explicar mais detalhadamente ocorreu em 2011, que acordo com a Sony existiu um furto de dados, nomes, endereços e possivelmente detalhes de cartões de crédito de 77 milhões de usuários da *Playstation Network*.

Prontamente, os crimes cibernéticos mistos podem ser classificados da seguinte forma, quando um sujeito utiliza o meio virtual para realizar uma conduta ilícita. Um exemplo desse tipo de delito é as transações ilegais de valores em uma *home-banking*. Nessa modalidade o sujeito, não pretende invadir o sistema de informática e seus componentes, mas utilizar a informática como instrumento, que se torna imprescindível para realização do crime.

Os crimes cibernéticos comuns, assim, são aqueles que utilizam a rede, exclusivamente como instrumento para realização de um crime que já se encontra tipificado no Código Penal, um exemplo disto, é a distribuição de conteúdo pornográfico infantil pelo meio de vídeos e fotografias ou algum outro meio de compartilhamento de dados.

O criminoso que comete este tipo de delito é denominado *cracker,* desse modo pode ser classificado em dois tipos: o interno que é aquele em quer os sujeitos acessam de forma incorreta dados sigilosos de um nível superior, habitualmente esses criminosos são os servidores públicos ou trabalhadores da empresa. Já no caso do externo, classificar-se ele como aquele que não tem acesso e usa um computador ou uma rede externa, lembrando que este sujeito não tem ligação com à organização criminosa que praticou o ataque.

São próprios os delitos que são cometidos por meio de um aparelho eletrônico e tem o intuito invadir redes e programas, acarretando contra tempos aos usuários, por exemplo, deixando o sistema lento, alterando documentos de seu lugar de origem, atrapalhando o funcionamento do aparelho.

Em analogia a estes comportamentos, a jurisdição brasileira depara-se com problemas em punir os transgressores, tanto pela ausência de tipificação penal exclusiva para os comportamentos lesivos próprios virtuais, seja na carência de órgãos e legislação que auxiliem a captação de evidências. Nessa situação, há um retrocesso na base de uns 10 (dez) anos, em semelhança com a legislação aplicada na Europa, pois, tal tema é de feitio muito específico.

A única previsão judicial nesse sentido em nossa jurisdição é o tipo penal do art. 154-A do Código Penal, que assim o especifica:

> 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:

Portanto, é necessário notar que tanto no delito do caput do art. 154-A do Código Penal, assim como no delito do seu § 3º, os comportamentos delituosos são abordados como delitos de menor potencial ofensivo, admitindo, no delito do caput, a suspensão condicional do processo nos termos do art. 89 da Lei 9.099/95, e, em ambas as condutas caput e § 3º, admitem a transação penal, nos termos dos artigos 61, 72 e 76 da Lei 9.099/95.

Prontamente, os delitos digitais impróprios, são os comportamentos cometidos por indivíduos que exclusivamente usam o aparelhamento de informática como aparelho para a prática do delito. Exemplo disso são os crimes citados anteriormente no trabalho como: injúria, calunia, difamação e furto que já se localizam tipificados na legislação penal brasileira e mais adiante de existir a probabilidade de serem cometidos com o amparo dos aparelhos digitais.

Neste contexto, Castela (2005, p.110), esclarece que os crimes de informática impróprios são: "(impuros), onde a máquina é tão-somente um meio, um instrumento para se alcançar o fim desejado. Nesta categoria, estão os delitos constantes no Código Penal e legislação especial."

Deste modo, o crime de informática próprio tem como intenção o próprio aparelhamento, o próprio sistema, seu exercício, desde modo não podendo ser feito de diferente maneira que não seja pelo meio do aparelho, do equipamento. Logo, o crime de informática impróprio é aquele cometido por meio do aparelho, usando esta

exclusivamente como forma para alcançar o intuito, de tal modo, nesse evento o delito pode ser cometido por outras formas, em outras modalidades e meios que não seja por meio do aparelhamento de informática. Em todos esses casos, é complicada a coleta de evidências, porque o mundo cibernético é ágil, permitindo a veloz ação do indivíduo.

4. A DIFICULDADE DE PUNIR OS CRIMES CIBERNÉTICOS NO ORDENAMENTO JURÍDICO BRASILEIRO

A lei nº 12.737, de 30 de novembro de 2012, que tem como título Carolina Dieckman, causou mudanças no Código Penal vigente no país, adicionando os artigos 154-A e 154-B, portanto, criou o tipo penal “Invasão de dispositivo informático”.

De tal modo, o bem jurídico defendido por estes artigos é a inviolabilidade dos dados informáticos. Deste modo, busca defendera privacidade e intimidade, tipificadas no artigo 5º da Constituição Federal de 1988. O sujeito ativo é qualquer pessoa que não está habilitado ao acesso as informações. Prontamente, o sujeito passivo é qualquer, sendo ele pessoa física ou jurídica, proprietário dos documentos computacionais.

Entretanto, uma das maiores desaprovação a respeito da lei localiza-se no sujeito ativo, porque é atípico o comportamento da pessoa que invade aparelho computacional próprio para conseguir dados de outrem que lá se encontre, tendo como exemplo, em um *Cyber*, o dono não irá cometer crime se ele acessaras informações do usuário do computador. Dessa maneira, existe erro no regulamento, porque quem cometeu o delito necessitaria ser sentenciado, não carecendo importar quem que o cometeu. Mais uma falha, ou melhor, uma brecha, oferecida por esta lei, localizar-se nos “mecanismos de segurança”, uma vez que um usuário sem experiência que não faz uso de aparelhos de segurança, exemplo, antivírus ou *firewall*, não será protegido pela lei, sendo o crime atípico.

Ademais, a pena é somente a de detenção de três meses a um ano, deste modo, avaliada como uma conduta de médio potencial ofensivo. Além disso, esta penalidade tolera o cumprimento no regime semiaberto ou prontamente no regime aberto, e ainda existe o direito dessa pena ser substituída por uma pena pecuniária com fulcro no artigo 44, §2º do Código Penal. Possui, ainda, oportunidade de ser

trocada por pena alternativa ou restritiva de direitos. Desse modo, um comportamento que pode gerar um dano irreparável a suas vítimas, tem uma penalidade serena e insuficiente.

No ano de 2014, foi aprovada a Lei nº 12.965, intitulada “Marco Civil da Internet”. Essa foi feita com a finalidade de preencher os buracos de nossa norma jurídica no tocante aos delitos cibernéticos. Primeiramente, abordamos fundamentos e conceitos, especificado os direitos dos usuários. Elenca princípios, dentre eles livre-arbítrio, justiça e privacidade, igualmente, produzir garantias de direitos e obrigações no espaço virtual. Uma evidência nesse “marco” se dá ao direito e garantia a inviolabilidade da intimidade e da vida privada.

Apesar disso, compreende-se que na ocasião da penalidade ao desrespeito destes princípios as punições são fracas e não alcançando um efeito aceitável. Ademais, para exigências de dados privados é imprescindível ordem judicial, não podendo o provedor fornecer informações como IP de senha e *login* dos delituosos, consentindo para que a investigação se torne demorada. Logo, por mais adequada que seja a determinação de garantias e direitos, estes artigos não abrangem por todo este campo onde os delituosos praticam atividades criminosas no âmbito virtual, permanecendo com brechas que ficam à mercê de suprimento advindo de outros ramos do direito, um grande exemplo, são aqueles eventos de compras na internet, que são regidas pelo CDC (Código de Defesa do Consumidor).

Além disso, como já visto no atual estudo, alguns delitos cometidos com a ajuda da internet estão fundamentados no Código Penal, entre eles os delitos contra a honra. Entretanto, o Código vigente é do ano de 1940. Assim, em alguns episódios, acaba se tornando ultrapassado tratar de delitos modernos, nascidos no transcorrer dos anos, consistindo empenas moles em semelhança os efeitos sofridos pelas os indivíduos.

Desse modo, a ausência de uma legislação específica aos crimes virtuais no Brasil acarreta, em muitos eventos, a falta de punição aos criminosos, porque determinados comportamentos não são penalizados da forma correta, e a lei nº 12.737/12, tem várias brechas e interpretações ambíguas. Nos dias atuais, no qual o mundo se tornou mais globalizado e as tecnologias não param de avançar, o número de usuários no âmbito virtual só cresce, tornando-se de extrema importância a invenção de uma legislação que resolva as condutas criminosas cometidas no meio cibernético, com penas mais fortes e adequadas para resolver os efeitos danosos que

estes produzem, para que os indivíduos pensem duas vezes antes de cometer algum crime cibernético.

CONSIDERAÇÕES FINAIS

Com o fim da pesquisa nota-se a relevância do tema visto, pois a evolução tecnológica tem se expandido a cada dia, surgindo diversos tipos de delitos cibernéticos, mostrou o quanto é necessária a evolução do ordenamento jurídico brasileiro acerca dos crimes virtuais, pois mesmo com leis que enquadrem os crimes cibernéticos as penas são muito brandas.

A fim de aprofundar mais o assunto na primeira parte do trabalho mostrou como são os crimes cibernéticos em território brasileiro quais os crimes mais praticados no âmbito virtual. Em segundo momento mostrou que a internet não possui barreiras e que o crime virtual pode ser praticado de qualquer lugar do mundo, trazendo mais uma problemática para a solução desse tipo de delito, pois muitas vezes se faz necessário a cooperação dos operadores de direito de diferentes lugares do planeta, algo que que muitas vezes não ocorre ou demora a acontecer, ocasionando a perca das provas digitais. Portanto, os Acordos de Assistência Mútua em Matéria Penal devem ser revistos e adaptados ao cenário atual para que o processo seja efetuado de forma mais rápido para punir e prender estes criminosos.

Logo, foram abordados dos tipos de crimes os próprios que são aqueles cometidos por meio de um aparelho eletrônico e tem como o intuito invadir redes e programas. Logo, os impróprios são comportamentos cometidos por indivíduos que exclusivamente utilizam os aparelhos para praticar crimes como, por exemplo: injuria, calunia e difamação.

Por conseguinte, aborda-se a insuficiência das leis brasileiras acerca dos crimes virtuais, pois os danos sofridos pelas as vítimas desse tipo de crime são geralmente irreparáveis, a falta de uma legislação especifica mais rígida aos crimes virtuais no Brasil deixa muitas vezes a população à mercê dos criminosos que quando são presos sofrem penas brandas e voltam a praticar esse tipo de crime. É de extrema importância a criação de leis específicas que englobem de maneira mais eficaz os atos cometidos no mundo virtual, porque por mais que o legislador tenha criado leis para tanto, observa-se deficiências quanto a efetividade da lei.

Logo, existe um progresso muito grande na criminalidade realizada por meios cibernéticos, contudo o Brasil encontra-se atrasado no aspecto jurídico, fazendo necessário equiparar-se aos países que já têm legislação específica para crimes cibernéticos, para que o país não se torne um paraíso aos criminosos que praticam esse tipo de delito.

O Brasil ocupa o quarto lugar em número de usuários de internet, em um meio que cresce a cada dia que se passa, com isso muitos desses usuários acabam sendo vítimas de crimes virtuais, com uma legislação que atualmente não pune corretamente esse tipo de delito. Desse modo, mostrar-se a necessidade de leis que amparem os usuários desse serviço.

Portanto, é de vasta importância a Cooperação Internacional que é essencial para combater os crimes cibernéticos, do mesmo modo que as convenções entre países que visam habituar-se com esse tipo de crime, para dessa maneira melhorar e tornar mais rígido o seu ordenamento jurídico.

Concluir-se, que a sociedade vem sofrendo uma grande evolução das ciências tecnológicas e o Direito Penal não está conseguindo alcançar essas mudanças, deixando várias brechas na legislação que são aproveitadas pelos os criminosos, por fim é de ampla importância torná-lo concomitante com a realidade fática social.

REFERÊNCIAS

A obtenção das provas digitais na investigação dos delitos de violência e exploração sexual online. In: SILVA, Ângelo Roberto Ilha da (Org.). Crimes Cibernéticos. Porto Alegre: Livraria do Advogado Editora, 2017.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília. 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 07 nov. 2019.

_____. **CÓDIGO PENAL BRASILEIRO.** Decreto Lei 2848/40. Disponível em:

https://www.jusbrasil.com.br/topicos/28004011/artigo-154a-do-decreto-lei-n-2848-de07-de-dezembro-de-1940. Acesso em 11 Set. 2019.

_____. **Estatuto da Criança e do Adolescente** -. Artigo 241-E – Incluído pela Lei n° 11.829/2008. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm . Acesso: 11 set. 2019.

_____. **Lei nº 7.716, de 5 de janeiro de 1989**. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l7716.htm. Acesso em 10 out. 2019.

_____. **Lei nº 12.737, de 30 de novembro de 2012**. Brasília.

2012.Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 08 out. 2019.

_____.**Lei nº 12.965, de 23 de abril de 2014.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 17 out. 2019

DOMINGOS, Fernanda Teixeira Souza Domingos. **As provas digitais nos delitos de pornografia infantil na internet.** In: SALGADO, Daniel de Resende; QUEIROZ, Ronaldo Pinheiro (Org.). A prova no enfrentamento à macrocriminalidade. Salvador: Editora JusPodivim, 2015.

FERREIRA, Nunes Andreza; JUNIOR, Anchieta de José. Pedofilia no mundo virtual. **In: Revista Jus.** Disponível em: https://jus.com.br/artigos/74996/pedofilia-nomundo-virtual. Acesso em 17 Out. 2019.

FRANÇA. **Declaração dos Direitos do Homem e do Cidadão**. 1789. Disponível em: http://www.direitoshumanos.usp.br/declaracao-de-direitos-dohomem-e-do-cidadao-1789.html. Acesso em 07 out 2019.

_____. **Declaração Universal dos Direitos Humanos.** 1948. Artigo XIX. Disponível em: https://www.mdh.gov.br/todasasnoticias/2018/novembro/artigo19deg-todo-ser-humano-tem-direito-a-liberdade-de-expressao-e-opiniao-1. Acesso em 22 out. 2019.

GOMES, Helton Simões. **Cai o nº de vítimas de 'nudes' vazadas na internet do Brasil em 2016, diz ONG**. Disponível em: https://g1.globo.com/tecnologia/noticia/cai-o-n-de-vitimas-de-nudes-vazadas-nainternet-do-brasil-em-2016-diz-ong.ghtml. Acesso em: 08 set. 2019.

LA CHAPELLE, Bertrand; FEHLINGER, Paul. Jurisdição na internet: da corrida armamentista legal à cooperação transnacional. Documento sobre Internet e Jurisdição. **In: Internet & jurisdiction policy network.**, 2016. Disponível em: <www.internetjurisdiction.net>. Acesso em: 08 set. 2019

MARTINELLI, João Paulo Orsini. Aspectos relevantes da criminalidade na Internet**. In: Jus.** Disponível em < http://jus2.uol.com.br/doutrina/texto.asp?id=1829 > Acesso em 17 out. 2019.

ROSANNE, D' Agostino. **Três anos depois, linchamento de Fabiane após boato na web pode ajudar a endurecer lei**. Disponível em: https://g1.globo.com/eou-nao-e/noticia/tres-anos-depois-linchamento-de-fabiane-apos-boato-na-web-podeajudar-a-endurecer-lei.ghtml. Acesso em: 08 set. 2019.

ROSA, Fabrizio. **Crimes de Informática.** Campinas: Bookseller, 2005. P. 22.

STAIR, Ralph M. **Princípios de sistemas de informação: uma abordagem gerencial**. 2ª ed. Rio de Janeiro: LTC, 2008.

SANCHES, Gasques Ademir; ANGELO, De Elisa Ana. Insuficiência das leis em relação aos crimes cibernéticos no Brasil. **In: Jus.** Disponível em: https://jus.com.br/artigos/66527/insuficiencia-das-leis-em-relacao-aos-crimesciberneticos-no-brasil/2. Acesso em 17 out. 2019.